

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ
ИНСТИТУТ КИБЕРНЕТИКИ им. В.М. ГЛУШКОВА

Г.А. ДОНЕЦ, И.В. СЕРГИЕНКО

**ЧИСЛОВЫЕ
ГРАФЫ И ПОСТРОЕНИЕ
ДИСКРЕТНЫХ
ОБРАЗОВ**

*ПРОЕКТ
«НАУКОВА КНИГА»*

КИЕВ • НАУКОВА ДУМКА • 2014

Монография состоит из двух частей. В первой части излагается новый подход к представлению графов в виде пары множеств действительных чисел и порождающей функции. Преимущество такого подхода по сравнению с традиционным представлением графов выражается в значительной экономии памяти при размещении данных в компьютере. Это является основанием для создания усовершенствованных алгоритмов решения многих практических задач на графах. Во второй части приведены методы построения дискретных образов из элементов, которые называются шаблонами. Это наборы чисел, адекватные набору красок, которыми окрашены данные шаблоны. Проблема сводится к решению системы линейных уравнений в классе вычетов по конечному модулю, равному числу заданных красок.

Для специалистов в области теории графов и комбинаторики, а также для студентов, аспирантов, которые интересуются проблемами дискретной математики и ее приложениями.

Монографія складається з двох частин. У першій частині викладено новий підхід до представлення графів, а саме у вигляді двох множин дійсних чисел та породжувальної функції. Перевага такого підходу порівняно з традиційним представленням графів полягає в значній економії пам'яті при розміщенні даних у комп'ютері. Це є базою для створення удосконалених алгоритмів розв'язування багатьох практичних задач на графах. У другій частині викладено методи побудови дискретних образів з елементів, що називаються шаблонами. Це набори чисел, адекватні набору фарб, якими зафарбовані дані шаблони. Проблема зводиться до розв'язування системи лінійних рівнянь у класі лишків за скінченним модулем, рівним кількості заданих фарб.

Для спеціалістів у галузі теорії графів та комбінаторики, а також для студентів, аспірантів, які цікавляться проблемами дискретної математики та її застосуваннями.

Р е ц е н з е н т ы:

доктор физико-математических наук, профессор *Ф.А.Шарифов*,
доктор физико-математических наук, профессор *А.И.Проватарь*

*Рекомендовано к печати ученым советом
Института кибернетики НАН Украины (протокол № 18 от 12.11.2013 г.)*

***Видання здійснено за державним замовленням
на випуск видавничої продукції***

Научно-издательский отдел
физико-математической и технической литературы

Редактор *В.В. Вероцкая*

© Г.А. Донец, И.В. Сергиенко, 2014
© НВП «Видавництво “Наукова думка”
НАН України», дизайн, 2014

ISBN 978-966-00-1435-0

ЧИСЛОВЫЕ ГРАФЫ

ВВЕДЕНИЕ

Идея написания монографии возникла из серии статей, опубликованных в последние 35 лет сначала армянскими авторами (Ю.Г. Григорян, Л.М. Адонц), а затем сотрудниками Института кибернетики им. В.М. Глушкова НАН Украины (Г.А. Донец, И.Э. Шулинок, Г.А. Шулинок, И.М. Асельдерова). Название «Числовые графы» устоялось, и оно естественным образом подчиняется более общему понятию теории графов.

Начало теории графов как математической дисциплины было заложено Л.Эйлером в его знаменитой статье о Кенигсбергских мостах (1876). Однако статья оказалась единственной по данной тематике на протяжении почти ста лет.

Интерес к проблемам теории графов возродился около середины XIX столетия главным образом в Англии, где в то время проводились исследования по электрическим сетям, моделям кристаллов и химическим структурам молекул. Однако возникновение теории графов как отдельной, полностью сформировавшейся математической дисциплины принято датировать 1936 годом, когда вышла в свет монография Д. Кенига «Теория конечных и бесконечных графов». В книге Д. Кенига была изложена общая и полная для своего времени систематизация фактов, приведено превосходное введение в предмет. Она содержала новые результаты, а также идеи, получившие дальнейшее развитие в работах многих математиков. Вызывает удивление тот факт, что книги, касающиеся данной теории, на английском языке до тех пор не было издано, несмотря на то, что многие важнейшие результаты были получены английскими и американскими учеными.

После выхода упомянутой книги быстро увеличивается количество исследований по теории графов, появляются некоторые общие методы решения задач с помощью этой теории.

Постепенно было доказано, что некоторые постановки задач алгебры, теории чисел, геометрии, теории множеств, топологии и даже традиционных задач классических наук можно переформулировать на языке чистой теории графов, причем в отдельных случаях это позволяет быстрее (или впервые) получить их решение.

В связи с бурным развитием математической логики, теории игр, вычислительной математики, автоматизации, информатики, математической экономики, исследования операций, математической лингвистики и других областей, где в отличие от классического анализа непрерывных величин на первый план выдвигаются рассуждения и построения дискретного характера, теория графов становилась все более востребованной наукой. Многие практические задачи, которые формулировались при помощи теории графов, имеют такое простое свойство, что их можно принципиально решать без всякой теории полным перебором всех имеющихся вариантов. Однако очень скоро пришлось расстаться с этой иллюзией и согласиться с необходимостью построения для графов общей теории и общих методов.

Эти тенденции отчасти нашли свое выражение в монографиях К. Берга «Теория графов и ее применение» (1958, русский перевод 1962) и О.Оре «Теория графов» (1962, русский перевод 1968). С их выходом наступил период бурного развития дискретной математики, период ее дальнейшего проникновения в самые разнообразные отрасли знания, характеризуемый мощным, все возрастающим потоком информации, различные стороны которого особенно ярко проявились в теории графов — одном из разделов дискретной математики. Однако многообразие направлений и обилие новых работ привели к трудностям, мешающим математикам и специалистам в смежных областях знания постоянно следить за развитием этой теории. Даже специалисту, занимающемуся другим разделом дискретной математики, но проявляющему интерес к теории графов, бывает необычайно сложно систематически следить за литературой в этой области в основном из-за трудностей технического характера: статьи по теории графов и ее приложениям можно было найти в разных изданиях, которые, однако, не всегда были доступными. Кроме того, отсутствовала четкая рубрикация теории графов, в ее определениях и обозначениях был такой разнобой, что авторы большинства работ вынуждены начинать изложение с разъяснений, под какими именно названиями и символами в данной работе указываются давно известные понятия.

В 1968 г. А.А. Зыков подготовил к изданию двухтомную монографию «Теория конечных графов», в которой сделал попытку изложить все интересные на то время результаты, методы и проблемы теории графов на основе единой терминологии и символики. К концу 1969 г. первый том увидел свет. В книге «Основы теории графов» (1987 г.) А.А. Зыков писал: «... Дальнейший ход событий привел к выводу о нецелесообразности издания второго тома и переиздании первого в прежнем объеме ввиду их перегруженности второстепенными материалами и отягощенности излишним стремлением к детализации даже в заведомо очевидных случаях». Последняя книга включала в переработанном виде важнейший материал обоих томов и ряд дальнейших результатов, однако и ей были присущи некоторые недостатки, в частности, излишняя перегруженность обозначений и символов. Поэтому книга осталась почти незамеченной широкими кругами читателей, да пожалуй, и многими специалистами.

Теория графов, хотя и не является основным содержанием, но в той или иной мере излагается в таких книгах: П.С. Солтан, Д.К. Замбицкий, К.Ф. Присакару. Экстремальные задачи на графах и алгоритмы их решения. — Кишинев: Штиинца, 1973; Р.Дж. Басакер, Т.Д. Саати. Конечные графы и сети. — М.: Мир, 1974; П. Кристофидес. Теория графов. Алгоритмический подход. — М.: Мир, 1978; М. Свами, К. Тхуласираман. Графы, сети и алгоритмы. — М.: Мир, 1984.

Следует отметить переводную монографию «Теория графов» (М.: Мир, 1973). Ее автор Ф. Харари — американский математик, известный по дискретной математике. Он написал огромное число статей топологического, алгебраического и теоретико-графового характера, несколько монографий по комбинаторной математике и ее применениям в физике, социологии и экономике. Ф. Харари активно участвует во многих конференциях по теории графов и смежным с ней наукам и неизменно является редактором трудов этих конференций. Одна из целей (и притом весьма нелегкая), поставленная в этой книге автором, такая же, как и у А.А. Зыкова, — унифицировать обозначения и упорядочить терминологию теории графов. В значительной мере это ему удалось, что подтверждается огромной популярностью книги среди зарубежных (особенно американских) специалистов, связанных по работе с дискретной математикой, а также тем, что большинство ссылок в статьях и кратких сообщениях по теории графов приходится на долю этого издания. Такой же популярностью книга пользуется и на территории бывшего СССР.

Числовые графы возникли как альтернатива обычным графам, которые представляются традиционным способом в виде списков смежностей. Основная операция при работе с числовыми графами — поиск необходимой информации среди таких списков. Возникла идея: можно ли заменить операции поиска более быстрыми операциями, какими являются обычные арифметические операции? Это привело к тому, что вопрос о смежности двух вершин, представленных числами, был сведен к определенным вычислениям над этими числами. В зависимости от результатов вычислений решается вопрос о смежности указанных вершин. Здесь добавляется еще одна быстрая операция — сравнение. Для сравнения надо хранить некоторое множество специальных величин, причем это множество во много раз меньше списка смежностей. Данное множество и множество вершин определяют структуру графа. В целом получается двойная выгода — за счет увеличения быстродействия вычислений и экономии памяти. В зависимости от вида арифметических операций получают различные типы числовых графов.

ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ЧИСЛОВЫХ ГРАФОВ

1.1. НУМЕРАЦИЯ ГРАФОВ

Одно из первых определений графа приведено в работе К. Берга [11]. В соответствии с ним *граф*, обозначаемый символом

$$G = (X, \Gamma), \quad (1.1)$$

есть пара, которая состоит из множества X и отображения Γ множества X на себя. Элементы множества X , изображаемые на плоскости точками, называются *вершинами* графа G , а пара элементов (x, y) , где $y \in \Gamma x$, и соединенная линией со стрелкой в направлении от x к y — *дугой* графа.

Это определение имело тот недостаток, что молчаливо предполагало все графы *ориентированными*, т. е. такими, у которых линии, соединяющие произвольные пары вершин, имели ориентацию или направление. Кроме того, если положить $x = y$, то в вершине возникала *петля*, что также вызывало неудобства. Но на практике для тех объектов, которые изображались в виде графов, важнейшей информацией был факт, в первую очередь, о существовании связи между двумя элементами и, во вторую очередь, их упорядоченность. Этому требованию в большей степени соответствует определение графа О. Оре [68].

Рассматривается множество V , состоящее из соединенных некоторым образом точек, которые называются *вершинами*. Граф $G = G(V)$ с множеством вершин V есть некоторое семейство сочетаний или пар вида $E = (a, b)$, $a, b \in V$, указывающее, какие вершины считаются соединенными. В соответствии с геометрическими представлениями графа каждая пара E называется *ребром* графа, а вершины a и b — *концами ребра* E . Можно также уточнить понятие графа G как некоторое подмножество декартового произведения $V \times V$. В это определение необходимо внести дополнение в одном важном отношении. В определении ребра можно принимать или не принимать во внимание порядок рас-

положения двух его концов. Если порядок не имеет значения, т. е. пара $E = (a, b) = (b, a)$, то E есть *неориентированное* ребро, если же порядок учитывается, то E называют *ориентированным* ребром или *дугой*.

Если в определении К. Бержа граф всегда ориентирован, то у О. Оре граф может иметь ориентированные ребра (дуги), т. е. получается *смешанный* граф. Предполагается, что двигаться по дуге можно только в одном направлении (куда показывает стрелка), а по неориентированному ребру — в оба направления. Чтобы позволить себе это в графе К. Бержа, стали соединять вершины двумя дугами противоположных направлений. Получались параллельные ребра, кроме того, если $a = b$, то появляются новые объекты, называемые *петлей*. Все это приводило к новым неудобствам, особенно при использовании вычислительной техники. Ф. Харари ввел понятие *обыкновенного* графа, который соответствовал определению О. Оре, но был неориентированным, без параллельных ребер и петель. Хотя при желании можно было переходить к ориентированному графу. Как упоминалось ранее, А.А. Зыков пытался унифицировать всю терминологию о графах. В своей первой книге [59] он предложил следующее всеобъемлющее определение графа.

Точное определение графа состоит в том, что задаются два множества (первое из них обязательно непустое) и предикат, указывающий, какую пару элементов первого множества соединяет тот или иной элемент второго множества. Именно, дан граф $L = (X, U, P)$, если заданы два множества $X \neq \emptyset$, $U (X \cap U \neq \emptyset)$ и трехместный предикат P , удовлетворяющий двум условиям:

А) P определен на всех таких упорядоченных тройках элементов x, u, y , для которых $x, y \in X, u \in U$;

Б) для всякого u существуют x, y такие, что $P(x, u, y)$, а если существуют такие x^*, y^* , что $P(x^*, u, y^*)$, то $(x = x^* \& y = y^*)$ или $(x = y^* \& y = x^*)$.

Элементы множества X называются *вершинами*, элементы U — *ребрами*, а предикат P — *инцидентором* графа L ; выражение $P(x, u, y)$ имеет такой смысл: ребро u соединяет вершину x с вершиной y или u соединяет пару \overline{xy} (*упорядоченную*) вершин. Условие Б показывает, что каждое ребро графа соединяет какую-то пару \overline{xy} его вершин, но кроме этой пары может (хотя и не обязательно) соединять еще только обратную пару \overline{yx} .

Теория графов — сравнительно молодая наука, но за годы почти семидесятилетнего существования она проникла в различные области теории и практики, где в отличие от классического анализа непрерывных величин на первый план выдвигаются рассуждения и построения дискретно-комбинаторного характера.

В настоящее время количество важных практических и теоретических задач самого разнообразного конкретного содержания и самой различной степени сложности, сводящихся к задачам и проблемам чистой теории графов, увеличивается так быстро, что для их решения уже не хватает старых традиционных методов. Единственный выход — научиться решать эти задачи, используя, с одной стороны, новейшие достижения и идеи теоретической математики, а с другой стороны — мощную современную вычислительную технику.

Попытки целиком отнести теорию графов к какому-либо разделу уже сложившихся математических дисциплин (алгебре, комбинаторной топологии, математической логике) оказались несостоятельными. Правда, аппарат алгебры нередко удается использовать в теории графов не только как вычислительное средство, но и как орудие исследования, однако в изучении графов слишком большую роль играет чисто комбинаторное искусство, недостаточно охваченное алгебраической наукой.

Самой близкой по природе к теории графов оказалась теория чисел. Однако сначала применение теории чисел для исследования графов носило чисто случайный характер. Известна одна классическая теорема, связывающая теорию графов и теорию чисел, в которой доказывается матричное равенство в классах вычетов по модулю 2.

Теорема 1.1. [6] Если граф G имеет матрицу инцидентий B и матрицу циклов C , то

$$CB = 0 \pmod{2}.$$

Это соотношение имеет многочисленные применения в теории релейных схем. В свое время, решая проблему 4-х красок, Хивуд доказал следующую теорему.

Теорема 1.2. [60] Для того чтобы вершины плоской триангуляции L допускали раскраску четырьмя цветами, необходимо и достаточно, чтобы к каждой грани можно было отнести одно из чисел 1, 2 с соблюдением условия: для каждой вершины L сумма чисел, отнесенных к примыкающим к ней граням, равна 0 по модулю 3.

Чаще всего теория чисел применяется в теории графов для различного рода кодирования (нумерации) графов.

Решение широкого круга прикладных задач связано с размещением объектов той или иной природы в элементах определенной структуры. Необходимость в подобных действиях возникает, например, при расстановке оборудования в цехах, размещении элементов радиоэлектронной аппаратуры, расположении программ и исходных данных в памяти компьютеров и т.п.

Многие из этих практических задач моделируются задачами оптимизации на перестановках. В таких задачах необходимо отыскать перестановку, доставляющую экстремум заданной функции, определенный на некотором множестве перестановок элементов конечного множества.

Задачи оптимизации на перестановках относятся к дискретным задачам оптимизации. Для их решения используются такие универсальные методы, как метод последовательного анализа вариантов, метод ветвей и границ, метод динамического программирования, которые по оценке теории сложности вычислений не являются эффективными.

Во многих задачах оптимизации на перестановках размещаемые объекты обладают определенной совокупностью взаимосвязей, которую часто можно задать с помощью графа или гиперграфа. В этом случае задача состоит в поиске такой нумерации вершин графа или гиперграфа, которая доставила бы экстремальное значение некоторому функционалу, определенному на множестве нумераций. Эта задача имеет и матричную эквивалентную формулировку. Тогда необходимо найти либо симметричную перестановку строк и столбцов, либо независимые перестановки строк и столбцов, дающие экстремум функционалу.

За последние три десятилетия появилось немало работ, посвященных решению задач нумерации графов, гиперграфов и упорядочению матриц. В них в зависимости от конкретной области исследований рассматривались различные классы графов и разнообразные критерии оптимальности.

В общем случае большинство задач оптимальной нумерации для графов и матриц является *NP*-полными и поэтому для них не существует эффективных алгоритмов точного решения. В этой ситуации представляется актуальным исследование частных случаев задач нумерации, поставленных на ограниченных классах графов. Причем важно как нахождение полиномиально разрешимых случаев задачи, так и выяснение пределов тех упрощений или ограничений, при которых она остается *NP*-полной.

Нумерацией (упорядочением) n -вершинного графа $G(X, Y)$ называется взаимно однозначное отображение $f: X \Rightarrow I$, где $I = \{i_1, i_2, \dots, i_n\}$ — множество целых чисел, а f в общем случае принадлежит какому-то классу функций K .

Общая задача о нумерации ставится так: для заданного графа G найти такую нумерацию $f \in K$, чтобы функционал $B(G, f)$ принимал наименьшее значение.

Среди задач нумерации можно выделить наиболее известные.

1. Задача о ширине графа

Шириной графа G при нумерации f называется число

$$B(G, f) = \max \left\{ |f(x_i) - f(x_j)| : (x_i, x_j) \in Y \right\},$$

а шириной графа G — число $B(G) = \min_{f \in K} B(G, f)$.

Задача о построении минимальной по ширине нумерации называется задачей о ширине графа.

Впервые задача о ширине графа была сформулирована в 1954 г. в работе [72]. В ней поставлена задача о ширине n -куба, которая была решена позже. В 1976 г. установлена NP -полнота задачи о ширине графа, а в 1978 г. доказано, что задача остается NP -полной для деревьев с максимальной вершинной степенью три [76]. И, наконец, в 1986 г. было показано, что задача остается NP -полной даже для следующих классов деревьев: 3-гусениц и n -гусениц с максимальной вершинной степенью три [75].

2. Задача о профиле графа

Профилем графа G при нумерации f называется число

$$P(G, f) = \sum |f(x_i) - \min_{x_j \cong x_i} f(x_j)|,$$

а профилем графа G — число $P(G) = \min_{f \in K} P(G, f)$.

Здесь знак \cong означает смежность или совпадение. Задача о профиле возникает в вычислительной математике при обработке разреженных матриц. Она также является NP -полной [76].

3. Задача о длине гиперграфа

По определению гиперграф $H = (X, \varepsilon)$ — некоторый математический объект с множеством вершин $X = \{x_1, x_2, \dots, x_n\}$ и множеством ребер $\varepsilon = \{e_1, e_2, \dots, e_m\}$, где e_i ($1 \leq i \leq m$) — непустые подмножества X (но не обязательно из двух элементов, как в обычных графах).

Нумерацией (упорядочиванием) n -вершинного гиперграфа $H = (X, \varepsilon)$ называется взаимно однозначное отображение $f: X \Rightarrow I$, где $I = \{i_1, i_2, \dots, i_m\}$ — нумерующая последовательность. Длиной гиперграфа $H = (X, \varepsilon)$ при нумерации f называется число

$$d(H, f) = \sum_{f \in K} \left[\max_{x_i \in e} f(x_i) - \min_{x_j \in e} f(x_j) \right],$$

а длиной гиперграфа $H = (X, \varepsilon)$ — число $d(H) = \min_{f \in K} d(H, f)$.

Задача о длине гиперграфа возникает в ряде практических задач при автоматизации проектирования интегральных схем и компонент компьютеров, в биологии при решении задач о наследственности, а также в различных областях теории информации. Если использовать матрицу инцидентий гиперграфа $A(H)$ размером $n \times n$, которая является $(0,1)$ -матрицей, то задача сводится к построению путем перестановок столбцов исходной матрицы такой матрицы $A'(H)$, у которой в каждой строке единицы будут размещены подряд, за исключением некоторых пробелов из нулей, число которых необходимо минимизировать. Если таких пробелов нет, то считают, что матрица обладает свойством связности. В общем случае задача является NP -полной. Соответствующая задача приведена в [36] и называется «Дополнение до матрицы со свойством связности».

Описанные здесь задачи нумерации графов сводились к определению экстремума функционала, который был независимым от структуры графа, т.е. способ задания графа мог быть произвольным.

Существует отдельное направление в теории нумерации графов, в котором сама нумерация используется для оптимизации представления графов.

В обычных представлениях графов обязательно перечисляются множества его вершин и ребер. Существует ряд задач, когда

такое представление при увеличении размеров графа вызывает серьезные трудности и требует более компактного (или более удобного) специфического представления.

Для некоторых дискретных объектов важными являются задачи построения полной совокупности симметрий объекта или задачи реализуемости в естественных евклидовых пространствах. Такие задачи возникают, если в качестве исследуемых объектов рассматриваются графы химических соединений, формулы или схемы, реализующие булевские функции, цифровые автоматы, многогранники и др.

Проблема установления симметрий, в свою очередь, является основой решения задач количественной оценки информативности дискретных объектов, используемых в научных исследованиях, связанных с разработкой различных систем автоматизации проектирования. В частности, оценка сложности объектов имеет много применений в области автоматизации вычислительных систем, при минимизации описания исходных объектов, выделения информативных признаков в области распознавания образов.

При обычном кодировании графов решение перечисленных выше задач затруднено, поэтому актуальной является проблема построения специального кодирования графов, обладающего такими свойствами: а) переход к специальному кодированию от естественного является достаточно нетрудоемким; б) трудоемкость алгоритмов на графах при таком кодировании должна быть меньшей, чем при стандартном кодировании.

С учетом этих требований **закодированный** граф должен представлять собой тройку $G = (X, U, F)$, где $X = \{x_1, x_2, \dots, x_n\}$ — множество действительных чисел, каждое из которых соответствует одной вершине; $U = \{u_1, u_2, \dots, u_m\}$ — множество действительных чисел, называемых образующими, а F — функция двух переменных такая, что $F(x_i, x_j) \in U$ тогда и только тогда, когда пара вершин (x_i, x_j) образует ребро исходного графа.

Накладывая различные ограничения на множества X , U и на функцию F , можно получать кодирование графа, которое отражает те или иные свойства этого графа. При этом, в отличие от обычного представления графов, где почти все операции сводятся к поиску элемента из множества данных, здесь основные операции сводятся к вычислению функции F .

Практика показала, что в связи с увеличением размерности задач, решаемых на компьютерах, все больше внимания необхо-

димому уделять вопросам эффективности алгоритмов. Для оценки сложности алгоритмов есть много критериев, основной из которых — продолжительность времени решения задачи, выраженная как функция от объема необходимой машинной памяти для исходных данных.

Существует несколько способов представления графов в машинной памяти. Если обыкновенный граф состоит из n вершин и m ребер, то представление его в виде матрицы смежности требует объем памяти порядка n^2 , а в виде списка смежностей — $(n+m)$. Списком смежностей часто пользуются, когда $m \leq n^2$, поэтому на практике матрицы смежности используются редко.

1.2. ГРАФЫ, ЗАДАВАЕМЫЕ АНАЛИТИЧЕСКИМ СПОСОБОМ

При решении многих задач на графах часто важно определить только смежность двух любых вершин данного графа. Возникает вопрос, можно ли получить всю полезную информацию о графе с помощью определенных вычислений, не загромождая память машины исходными данными о структуре графа? Рассмотрим некоторые способы представления графа, которые имеют важное значение при кодировании графов, а также при поиске способа размещения в машинной памяти данных о графах и их обработке.

Относительно функции F в закодированном графе $G = (X, U, F)$ будем предполагать, что она в какой-то мере «легко вычисляема», т.е. имеет аналитическое выражение. Отсюда название для таких графов, которые задаются аналитическим способом, — A -графы. Граф будет конечным, если X — конечное множество.

Будем считать, что в графе G из вершины x_i в вершину x_j заходит дуга, если $F(x_i, x_j) \in U$. Если $F(x_j, x_j) \in U$, то в вершине x_j существует петля.

Определение 1.1. Назовем *степенью полуисхода* вершины x_i

$$\rho^+(x_i) = \left| \{x_j / F(x_i, x_j) \in U\} \right|, \quad (1.2)$$

а *степенью полузахода* —

$$\rho^-(x_i) = \left| \{x_j / F(x_j, x_i) \in U\} \right|. \quad (1.3)$$

Эти числа определены для *ориентированных* графов. A -граф, у которого $F(x_i, x_j) = F(x_j, x_i)$, называется *неориентированным*.

Определение 1.2. Граф $G = (X, U, F)$ называется *изоморфным* графу $G' = (X', U', F')$, если существует взаимно однозначное соответствие φ между множествами X и X' , сохраняющее смежность, т.е. $G \cong G'$, если

$$\forall x_i, x_j \in X [F(x_i, x_j) \in U \Leftrightarrow F'(\varphi x_i, \varphi x_j) \in U']. \quad (1.4)$$

Определение 1.3. Представление графа $G = (X, U, F)$ называется *минимальным* относительно отображения F , если для любого $G' = (X', U', F) \cong G = (X, U, F)$ справедливо

$$|U| \leq |U'|. \quad (1.5)$$

Следует заметить, что мощность множества U в общем случае не равна количеству ребер графа.

Элементами множества X могут быть произвольные объекты: числа, векторы, матрицы и т.д. Однако наибольший интерес представляет случай, когда элементы множества X — числа (целые, рациональные, действительные, комплексные), а в качестве F задана функция на множестве действительных чисел. В дальнейшем будем рассматривать только такие графы, которые назовем *числовыми*.

Нетрудно убедиться, что классическое определение графа по Зыкову и определение числового графа эквивалентны, если предикат P заменить порождающей функцией, хотя для числовых графов не всегда можно найти подходящую порождающую функцию.

Определение 1.4. Представление графа $G = (X, U, F)$ называется *совершенным* относительно отображения F , если оно минимально и для любого минимального $G' = (X', U', F) \cong G = (X, U, F)$ справедливо

$$\max_{x_i, x_j \in X} |x_i - x_j| \leq \max_{x'_k, x'_l \in X'} |x'_k - x'_l|. \quad (1.6)$$

Особый интерес представляют A -графы, у которых множество X содержит только целые числа.

Определение 1.5. Числовой граф G называется *натуральным*, если у него $X = \{1, 2, \dots, n\}$.

Рассмотрим некоторые частные виды порождающих функций. Наиболее простой является линейная порождающая функция, которая имеет вид

$$F(x_i, x_j) = ax_i + bx_j + c. \quad (1.7)$$

Обозначим αX ($\alpha \neq 0$) множество $\{\alpha x_1, \alpha x_2, \dots, \alpha x_n\}$, а $\bar{\alpha} + x$ — множество $\{\alpha + x_1, \alpha + x_2, \dots, \alpha + x_n\}$.

Докажем ряд утверждений для линейной функции F графа $G' = (\alpha X, \alpha U, f)$.

Лемма 1.1. A -графы $G = (X, U, F)$ и $G' = (\alpha X, \alpha U, f)$ изоморфны, если положить $f(x_i, x_j) = F(x_i, x_j) + (\alpha - 1)c$.

Действительно, пусть $F(x_i, x_j) = ax_i + bx_j + c = u_1 \in U$. Тогда $f(\alpha x_i, \alpha x_j) = F(\alpha x_i, \alpha x_j) + (\alpha - 1)c = \alpha(ax_i + bx_j) + c + (\alpha - 1)c = \alpha(ax_i + bx_j + c) = \alpha u_1$.

Очевидно, что $\alpha u_1 \in \alpha U$.

Лемма 1.2. A -графы $G = (X, U, F)$ и $G' = (\bar{\alpha} + X, \overline{\alpha(a+b)} + U, F)$ изоморфны.

Проверяется непосредственно:

$$F(\alpha + x_i, \alpha + x_j) = a(x_i + \alpha) + b(x_j + \alpha) + c = ax_i + bx_j + \alpha(a + b) + c.$$

Очевидно, что если $ax_i + bx_j + c = u_1 \in U$, то $F(\alpha + x_i, \alpha + x_j) \in \overline{\alpha(a+b)} + u_1$.

Лемма 1.3. A -графы $G = (X, U, F)$ и $G' = (X, U + \bar{\alpha}, f)$ изоморфны, если положить $f(x_i, x_j) = F(x_i, x_j) + \alpha$.

Проверяется так же, как и следующая

Лемма 1.4. A -графы $G = (X, U, F)$ и $G' = (X, \alpha U, \alpha F)$ изоморфны.

A -граф с линейной порождающей функцией будет неориентированным, если $a = b$, т.е.

$$F = a(x_i + x_j) + c. \quad (1.8)$$

В частности, если $a = 1$ и $c = 0$, то получаем числовой граф, который называется *арифметическим* [25].

Лемма 1.5. Всякий неориентированный A -граф с линейной порождающей функцией изоморфен арифметическому графу.

Возьмем $X' = X$, $U' = \frac{U - c}{a}$, а $F'(x_i, x_j) = \frac{F(x_i, x_j)}{a} - c = x_i + x_j$. Проверим, что если $F(x_i, x_j) \in U$, то $x_i + x_j \in U'$.

Таким образом, изучение неориентированных A -графов с линейной порождающей функцией можно сводить к изучению арифметических графов, которые оказываются очень простыми. Однако и для них существуют задачи, которые еще не решены.

Нетрудно показать, что если в графе $G = (X, U, F)$ X и U принадлежат множеству рациональных чисел, то можно построить числовой граф $G'(X', U', F')$, который изоморфен графу G и у которого X' и U' принадлежат множеству натуральных чисел. Для этого необходимо умножить X и U на наименьшее общее кратное знаменателей их элементов. Неочевидно, однако справедливо следующее утверждение.

Утверждение 1.1. Для каждого конечного числового графа $G = (X, U, F)$ можно построить граф $G' = (X', U', F') \cong G = (X, U, F)$, у которого X' и U' принадлежат множеству натуральных чисел.

В действительности, можно построить даже арифметический граф, который изоморфен исходному графу. Для этого каждой вершине исходного графа $G = (X, U, F)$ присвоим код $x_i = 2^i$ ($1 \leq i \leq n$), где n — число вершин графа, а функцию выберем $F = x_i + x_j$, как для арифметического графа. При этом максимальное значение $|U| = C_n^2$ и все образующие — разные. В самом деле, допустим, что найдется четверка вершин k, l, r, s , отличных друг от друга и таких, что $2^k + 2^l = 2^r + 2^s$. Не нарушая общности, пусть $k = \min(k, l, r, s)$. Тогда после сокращения обеих частей на 2^k получим $1 + 2^{l-k} = 2^{r-k} + 2^{s-k}$. Но в левой части стоит нечетное число, а в правой — четное, что невозможно. Это и доказывает, что одинаковых образующих U не содержит. Оставим в U только те образующие, которые в исходном графе соответствуют ребрам. Это и завершает доказательство утверждения 1.1.

Пусть F — квадратичная порождающая функция. Эту функцию в общем виде запишем так:

$$F(x_i, x_j) = ax_i^2 + 2bx_i x_j + cx_j^2 + 2dx_i + 2ex_j + f. \quad (1.9)$$

В качестве иллюстрации рассмотрим функцию $F(x_i, x_j) = 2x_i^2 - 3x_i x_j + x_j^2 - x_i + 1$ на множестве $X = \{1, 2, 3, 4, 5\}$. При этом порождающее множество состоит из одного элемента $U = \{2\}$, что легко проверить:

$$F(2,1) = 2 \cdot 2^2 - 3 \cdot 2 \cdot 1 + 1^2 - 2 + 1 = 2,$$

$$F(1,3) = 2 \cdot 1^2 - 3 \cdot 1 \cdot 3 + 3^2 - 1 + 1 = 2,$$

$$F(3,2) = 2 \cdot 3^2 - 3 \cdot 3 \cdot 2 + 2^2 - 3 + 1 = 2,$$

$$F(2,5) = 2 \cdot 2^2 - 3 \cdot 2 \cdot 5 + 5^2 - 2 + 1 = 2,$$

$$F(4,3) = 2 \cdot 4^2 - 3 \cdot 4 \cdot 3 + 3^2 - 4 + 1 = 2,$$

$$F(5,4) = 2 \cdot 5^2 - 3 \cdot 5 \cdot 4 + 4^2 - 5 + 1 = 2.$$

Этому A -графу соответствует граф на рис.1.1. Здесь граф имеет вид двух склеенных контуров и для его представления оказалось достаточно одной образующей. Если граф на рис. 1.1 представить в качестве арифметического графа, то нетрудно убедиться, что для этого понадобятся 3 образующих (рис. 1.2). Здесь $X = \{1, 2, 3, 4, 5\}$ и $U = \{5, 6, 7\}$.

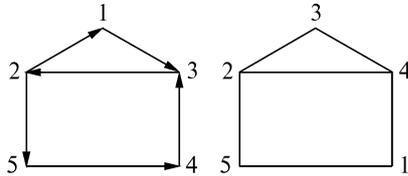


Рис. 1.1

Рис. 1.2

Если сравнить «легко вычисляемые функции» арифметического графа и квадратичную функцию, то очевидно, что вторая намного сложнее. В первой число операций сложения равно 1, зато поиск на множестве U , т. е. число сравнений больше, чем для второй функции. И наоборот, во второй функции число умножений равно 3, число сложений — 4, зато сравниваем всегда только один раз. Очевидно, что если множество образующих A -графа состоит из одного элемента u , то его можно

приравнять нулю, если изменить порождающую функцию, т. е. заменить

$$F(x_i, x_j) - u_1 \Rightarrow F'(x_i, x_j). \quad (1.9a)$$

Тогда вопрос о смежности вершин x_i и x_j сводится к решению уравнения от двух переменных $F'(x_i, x_j) = 0$.

Здесь возникает одна интересная задача об аналитическом расширении порождающей функции: можно ли генерировать граф большей размерности, для которого порождающая функция остается прежней, так же, как и множество образующих, состоящее из одного элемента? Легко вычислить, что квадратичное уравнение, представляющее граф на рис. 1.1, справедливо для пар чисел (3,7), (7,6) и (6,5):

$$2 \cdot 3^2 - 3 \cdot 3 \cdot 7 + 7^2 - 3 + 1 = 2; \quad 2 \cdot 7^2 - 3 \cdot 6 \cdot 7 + 6^2 - 7 + 1 = 2;$$

$$2 \cdot 6^2 - 3 \cdot 6 \cdot 5 + 5^2 - 6 + 1 = 2.$$

Чтобы объяснить это свойство, представим $x_j = x_i + \Delta$ и подставим это в уравнение (1.9a). Получим уравнение

$$F(x_i) = 2x_i^2 - 3x_i^2 - 3\Delta x + x_i^2 + 2\Delta x + \Delta^2 - x_i - 1 = 0$$

или

$$-\Delta x_i + x_i^2 + \Delta^2 - x_i - 1 = 0.$$

Решая его относительно Δ , находим решение $\Delta = \frac{x_i \pm \sqrt{x_i^2 + 4x_i + 4}}{2}$, откуда окончательно имеем: $\Delta_1 = -1$ и $\Delta_2 = x + 1$.

По этой формуле, увеличивая число вершин графа до 7, с помощью Δ_1 получаем дуги (7,6) и (6,5), а с помощью Δ_2 — дугу (3,7). Если число вершин увеличить до 9, то можно найти дуги (9,8), (8,7) и (4,9) и т.д. до произвольного значения n . Это позволяет строить числовые графы, не проводя лишних вычислений. Соответствующий граф показан на рис. 1.3.

Некоторые А-графы допускают графический способ представления.

Рассмотрим линейную функцию (1.7). Для проверки смежности вершин решим уравне-

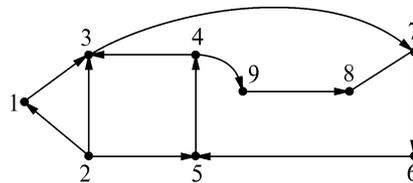


Рис. 1.3

ния

$$a x_i + b x_j + c = u_k \quad (k = 1, 2, \dots, m). \quad (1.10)$$

Изобразим на координатной плоскости параллельные прямые:

$$a x + b y + c = u_k. \quad (1.11)$$

Из вершины x_i в x_j будет выходить дуга в том и только в том случае, если точка с координатами $x = x_i, y = x_j$ принадлежит одной из прямых (1.11).

Для арифметических графов уравнения (1.11) преобразуются в следующие:

$$x + y = u_k. \quad (1.12)$$

Рассмотрим, как представить цепь в виде совершенного натурального A -графа. Пусть необходимо для цепи из n вершин найти минимальное число образующих. Очевидно, что их число $m \geq 2$. Покажем, что $m = 2$. Проведем на координатной плоскости две прямые (рис. 1.4):

$$x + y = n + 1 \quad x + y = n + 2. \quad (1.13)$$

Из графика на рис. 1.4 следует, что первая прямая связывает вершины $(1, n), (2, n-1), (3, n-2)$ и т.д., что соответствует паросочетанию для цепи. Вторая прямая связывает вершины $(2, n), (3, n-1), (4, n-2)$ и т.д., что соответствует паросочетанию, сопряженному с первым паросочетанием. С помощью этого мы получаем способ нумерации вершин цепи при двух образующих.

Следует заметить, что если n — нечетное, то в вершине $\frac{n+1}{2}$ образуется петля.

Рассмотрим приведенный выше пример квадратичной функции и запишем для нее уравнение:

$$2x^2 - 3xy + y^2 - x - 1 = 0. \quad (1.14)$$

Из аналитической геометрии известно, что это уравнение

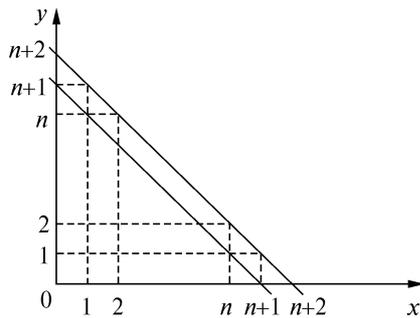


Рис. 1.4

кривой второго порядка. Важное значение для таких уравнений имеют инварианты, которые в соответствии с обозначениями (1.9) записываем в виде

$$I = a + c; \quad D = \begin{vmatrix} a & b \\ b & c \end{vmatrix}; \quad A = \begin{vmatrix} a & b & d \\ b & c & e \\ d & e & f - u_k \end{vmatrix} \quad (1.15)$$

($k = 1, 2, \dots, m$).

Определяем значения инвариантов (1.15):

$$I = 3; \quad A = \begin{vmatrix} 2 & -\frac{3}{2} & -\frac{1}{2} \\ -\frac{3}{2} & 1 & 0 \\ -\frac{1}{2} & 0 & -1 \end{vmatrix} = 0; \quad D = \begin{vmatrix} 2 & -\frac{3}{2} \\ -\frac{3}{2} & 1 \end{vmatrix} = -\frac{1}{4} < 0. \quad (1.16)$$

Это означает, что выражение (1.14) является вырожденным уравнением гиперболического типа, т.е. представляет собой пару пересекающихся прямых. Запишем его в виде

$$(y - x + 1)(y - 2x - 1) = 0. \quad (1.17)$$

На графике ему соответствуют две прямые (рис. 1.5):

$$y_1 = x - 1, \quad y_2 = 2x + 1. \quad (1.18)$$

Как видно из графика на рис. 1.5, для множества вершин $X = \{1, 2, 3, 4, 5\}$ осуществляется смежность, которая соответствует ориентированному графу на рис. 1.1. Если множество образующих имеет больше одного элемента, то для каждого k в формулах (1.15) значение инварианта A будет разным. Это означает, что тип порождающей функции будет всегда постоянным (эллиптический, гиперболический, параболический), но для некоторых u_k уравнение может быть выро-

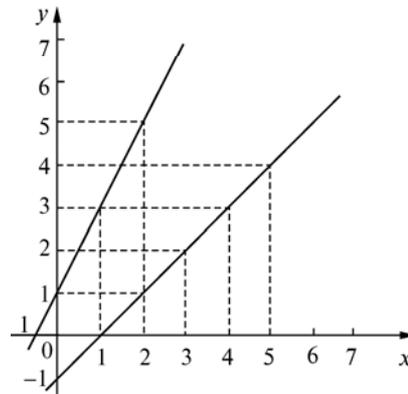


Рис. 1.5

денным и представлять собой либо одну точку, либо пару прямых (пересекающихся, параллельных или совпадающих).

Мы рассмотрели только два частных случая порождающей функции. В связи с обнаруженными свойствами числовых графов можно поставить две задачи.

Задача 1. Для заданного числового графа G и порождающей функции F построить минимальный (совершенный) граф.

Задача 2. Для заданного графа G построить на множестве вершин $X \in N$ минимальный (совершенный) граф.

Эти задачи отличаются друг от друга тем, что в первой фиксирована образующая функция, а во второй определен тип множества вершин. Другие задачи, которые возникают в представлении числовых графов, являются производными от указанных двух. В зависимости от вида F эти задачи могут быть решены либо для всех графов, либо для некоторых классов.

Рассмотрим еще примеры порождающих функций, при этом воспользуемся некоторыми новыми соображениями. Решая задачу 2, необходимо подобрать некоторую функцию F и попробовать с ее помощью построить заданный граф. Для этого можно применить графический способ, суть которого состоит в следующем. Обозначим $x_i = x$, а $x_j = y$. Рассмотрим на координатной плоскости функцию $F(x, y) - u = 0$, где u пока не определено. Это пока несущественно, так как график функции можно перемещать вдоль оси OY на величину u . Если $F(x, y)$ — линейная функция, то ее графиком будет прямая линия:

$$ax + by + c = u_k \quad (k = 1, 2, 3, \dots, m). \quad (1.19)$$

Если множество $X = \{1, 2, 3, \dots, n\}$, то вершина с номером $i \in X$ будет смежна с вершиной $j \in X$, если точка (i, j) или (j, i) является решением уравнения (1.19). Подбирая необходимые коэффициенты a, b, c и значение u_k , можно построить заданный граф.

Если $F(x, y)$ — квадратичная функция, то ее графиком будет кривая второго порядка:

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f - u = 0. \quad (1.20)$$

Из этого уравнения можно получить соотношение

$$y = \frac{-(bx + e) \pm \sqrt{x^2(b^2 - ac) + 2(be - cd)x + e^2 + c(u - f)}}{c}.$$

Если $b^2 - ac \neq 0$, то кривая представляет собой либо эллипсоид, либо гиперболу. Рассмотрим условие, при котором выражение под корнем будет полным квадратом, а именно:

$$(be - cd)^2 = (b^2 - ac)[e^2 + c(u - f)]. \quad (1.21)$$

Условие (1.21) равносильно следующему:

$$\begin{vmatrix} a & b & d \\ b & c & e \\ d & e & f - u \end{vmatrix} = 0. \quad (1.22)$$

Это условие того, что кривая второго порядка распадается на пару пересекающихся прямых. Явный вид этих прямых получим, если раскроем полный квадрат под знаком корня. В этом случае, исследуя каждую прямую в отдельности, поступаем так же, как и в случае, когда $F(x, y)$ — линейная функция. Из (1.21) для u можно получить явное значение, когда кривая второго порядка вырождается в пару прямых:

$$u = f + \frac{ae^2 - 2bde + cd^2}{b^2 - ac}. \quad (1.23)$$

Насколько сложно бывает подобрать подходящую функцию $F(x, y)$, покажем на примере. Пусть заданы изоморфный граф (рис.1.6) и квадратичная функция:

$$F(x, y) = 2x^2 - 3xy + y^2 - x + 3. \quad (1.24)$$

Здесь $a = 2$, $b = -\frac{3}{2}$, $c = 1$, $d = -\frac{1}{2}$, $e = 0$ и $f = 3$. По формуле (1.23) находим необходимое $u = 4$. При этом значении кривая (1.20) распадается на две пересекающиеся прямые:

$$y_1 = 2x + 1 \text{ и } y_2 = x - 1.$$

Поскольку $F(x, y) \neq F(y, x)$, то заданный граф — ориентированный. Построим графики полученных прямых (рис. 1.7, а) на множестве значений $1 \leq x \leq 7$ и $1 \leq y \leq 7$, что соответствует мно-

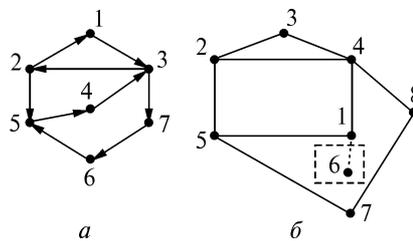


Рис. 1.6

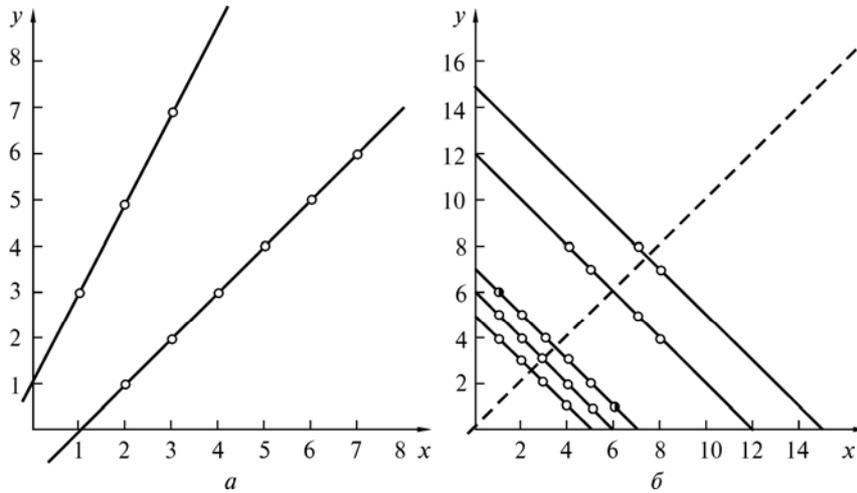


Рис. 1.7

жеству вершин $X = \{1, 2, 3, 4, 5, 6, 7\}$. Все точки на графике 1.7, *а* (график квадратичной функции), обведенные кружками, удовлетворяют уравнению (1.20). Координаты их (x, y) указывают, что из вершины графа $x_i = x$ идет дуга в вершину $x_j = y$. Таким образом, граф $G = (X, U, F)$ задается множеством $X = N_7, U = \{4\}$ и порождающей функцией (1.24).

Поставим теперь задачу 2 для того же графа. Для $X \in N$ найти порождающую функцию в виде $F(x_i, x_j) = x_i + x_j$. Поскольку $F(x_i, x_j) = F(x_j, x_i)$, то граф будет неориентированным. Строим графики прямых на множестве $X \in N$:

$$x + y = u_k \quad (k = 1, 2, \dots, m).$$

Путем подбора u_k находим соответствующие прямые. На рис. 1.6, *б* (график линейной порождающей функции) показано, что множество образующих $U = \{5, 6, 7, 12, 15\}$ на множестве вершин $X = N_8$ определяет исходный граф, за исключением дополнительного висячего ребра (1,6) (обведено квадратом). Поэтому если вершину 6 исключить из множества X , то получим искомый граф, изображенный на рис. 1.6, *б*.

1.3. ЧИСЛОВЫЕ ГРАФЫ

Итак, в результате обобщений определения графа, взятого по А.А. Зыкову, мы пришли к новому понятию графа, определение которого после различных упрощений имеет такой вид.

Определение 1.6. *Числовым графом* G называется тройка $G = (X, U, F)$, где $X = \{x_1, x_2, \dots, x_n\} \in N$ — множество вершин, $U = \{u_1, u_2, \dots, u_m\} \in N$ — множество образующих, а F — некоторая порождающая однозначная функция двух аргументов, обладающая свойством

$$\forall u \in U \exists (x_i, x_j) \in X [F(x_i, x_j) = u]. \quad (1.25)$$

Кроме функции сложения, большой интерес представляют также функция $F(x_i, x_j) = |x_i - x_j|$, которая по естественным причинам определяет *модульные* графы, алгебраические функции выше второго порядка, $F(x_i, x_j) = \sin \pi(x_i + x_j)$ и др.

На наш взгляд, А.А. Зыков имел представление о числовых графах, хотя такое название в его работах отсутствует. В [60, с. 6] он приводит 3 примера графов, которые полностью можно назвать числовыми (в более раннем определении — и бесконечными).

1. Вершинами графа служат натуральные числа, причем вершины x_i и x_j соединены ребром в том и только в том случае, если оба числа простые и $F(x_i, x_j) = |x_i - x_j| = 2$. Множество вершин этого графа счетно, а является ли множество ребер счетным или только конечным — неизвестно до сих пор (проблема близнецов в теории чисел). По определению 1.6 это — *бесконечный натуральный модульный граф*.

2. Вершинами являются числа $1, 2, \dots, n$, а каждое действительное число x , удовлетворяющее условию $i < x < i + 1$, служит дугой из вершины i в вершину $i + 1$. Граф содержит конечное множество вершин и континуум ребер (дуг).

3. Вершинами служат все действительные числа, и при фиксированном $\delta > 0$ разные вершины x_i и x_j соединены ребром тогда и только тогда, когда $F(x_i, x_j) = |x_i - x_j| < \delta$. Каждому значению δ соответствует свой граф, у которого множества вершин и ребер континуальны.

В своем развитии теория графов соприкасается с различными задачами теоретического и прикладного характера. Некоторые

такие задачи решаются непосредственно с помощью методов теории графов, а другие задачи для своего решения требуют определенной модификации обычных представлений графов. Это приводит к выделению из обширного класса графов некоторых подклассов, которые имеют свою специфику и могут быть намного проще обычных графов по своей структуре и способу представления.

Понятие числового графа возникло в математической литературе не сразу. В 60-х годах прошлого века академик В.М. Глушков и его ученики разрабатывали теорию проектирования дискретных систем [19], которая основывалась на такой фундаментальной проблеме, как минимизация дизъюнктивных нормальных форм. Из теории дизъюнктивных нормальных форм известно [62, 63], что всякую булеву функцию $f(x_1, x_2, \dots, x_n)$ однозначно можно представить в виде сокращенной дизъюнктивной нормальной формы:

$$f(x_1, x_2, \dots, x_n) = u_1 \vee u_2 \vee \dots \vee u_t,$$

где u_i ($i = 1, 2, \dots, t$) — простые импликанты функции f , т. е. выражение, состоящее из произведения переменных x_j ($j = 1, 2, \dots, n$), взятых непосредственно либо с отрицанием. Каждой импликанте можно поставить в соответствие значение истинности на вершинах единичного n -мерного куба. Если число переменных импликанты u_i равно r (ранг импликанты), то значения истинности образуют $(n - r)$ -мерный подкуб единичного куба. Для простоты понимания использовали граф, который адекватным образом изображал часть единичного куба, на которой заданная функция $f(x_1, x_2, \dots, x_n)$ принимала истинные значения. Однако для больших значений n такое изображение было неэффективным.

В 1964 г. [23] Ю.Г. Григорьян предложил способ изображения булевых функций в виде другого графа, который назвал булевым, и который давал некоторую экономию для изображения. Он обратил внимание на то, что если выразить координаты вершины единичного куба десятичными числами, то каждая главная диагональ $(n - r)$ -мерного подкуба соединяет вершины, сумма которых для этого подкуба постоянна. Это послужило основанием для введения понятия графа, у которого сумма кодов смежных вершин принадлежит заданному множеству чисел. Представленные таким образом графы стали называть *арифметическими*. Первоначально арифметические графы применялись только для иссле-

дования булевых графов, однако впоследствии оказалось, что последние не всегда можно представить в виде арифметических графов. И хотя это обстоятельство не привело к заметным результатам в проблеме минимизации дизъюнктивных нормальных форм, само понятие арифметического графа устоялось и получило дальнейшее развитие.

За последующие 25 лет Ю.Г. Григорьян (в соавторстве с Г.К. Манояном и А.М. Адонцем) опубликовал еще около десяти работ об арифметических графах. С математической точки зрения эти работы не носили фундаментальный характер и были посвящены второстепенным особенностям арифметических графов.

В связи с тем, что булевы графы допускают несколько представлений, возникла необходимость введения понятия булевого автоморфизма, при котором множество представлений одного и того же булевого графа отображается на себя [23, 27]. Установлено, что множество булевых автоморфизмов образует группу, которая принципиально отличается от известных групп автоморфизмов обычных графов. Тем самым было доказано, что булевой граф может отражать некоторую новую концепцию кодирования графов, и что он порождает новые группы со свойствами только ему алгебраическими особенностями. Из арифметических графов можно выделить натуральные арифметические графы, у которых множество вершин X совпадает с начальным отрезком натурального ряда, т. е. $X = N_n$.

Ю.Г. Григорьян изучал натуральные арифметические графы и доказал ряд утверждений об их структуре.

В частности, было показано, что существуют натуральные арифметические графы с любым количеством ребер. Приведены примеры некоторых однородных арифметических графов и найдены условия, при которых они преобразуются в фактороиды. Была применена определенная теоретико-числовая интерпретация графов, которая создала предпосылки для построения и изучения новых типов конечных групп, характеризующих наиболее общие свойства определенных классов арифметических графов. Известно [64, 72], что основной целью теории групп является описание всех групповых композиций. Построение групповых композиций в теории конечных групп, в свою очередь, основывается на обнаружении различных систем автоморфизмов над определенными объектами. Ю.Г. Григорьян изучал различные системы автоморфизмов, порождаемых арифметическими графа-

ми. По аналогии с булевым автоморфизмом было введено понятие арифметического автоморфизма, при котором множество арифметических представлений одного и того же графа отражается само на себя. Построенные конечные группы оказываются в некотором смысле «мощнее», чем обычные группы автоморфизмов графов, и описывают симметрию не одного графа, что характерно для обычных графов [58], а семейства графов [26, 27].

Указанным способом с помощью компьютерных программ была построена некоммутативная группа порядка $4n^2$ (n — простое число) с четырехзначной операцией, порождаемая арифметическими автоморфизмами простых циклов. Также было показано, что эта группа сверхразрешима, имеет восемь собственных нормальных делителей и восемь композиционных рядов длиной пять. Новая операция является новой композицией в теории групп и обобщает ранее известные операции. Поскольку неприводимые представления групп играют фундаментальную роль в различных квантово-механических задачах [59], была полностью решена задача представления указанной выше группы. Показано, что эта группа гомоморфно отображается в линейное пространство размерности $\left(\frac{n+3}{2}\right)^2$. Получены таблицы характеров

неприводимых представителей группы и исследованы другие вопросы теории представлений группы. Таким образом, было показано, что арифметические графы, отражающие определенный порядок в природе чисел, являются новым источником формирования различных групп с качественно новыми характеристиками.

Была сделана попытка обоснования концепции кодирования графов геометрическими методами, так как геометрия любой пространственной структуры представляет собой, в итоге, граф, параметры которого, такие как длины ребер, координаты вершин, оси симметрии и другие элементы, взаимосвязаны и удовлетворяют некоторым стандартным условиям, диктуемым этой структурой. В связи с установлением универсальности кодирования арифметических графов была поставлена и решена задача для некоторых геометрических пространственных фигур о взаимном соответствии координат вершин (а также других параметров) и определенной кодировки подходящих арифметических графов.

Указанная задача является частной задачей построения структур, которая используется при физических, биологических и

других методах синтеза кристаллов. По аналогии с этой задачей можно поставить задачу **математического синтеза геометрических тел**, которая звучит так: в трехмерном пространстве найти координаты вершин заданного многогранника (графа), чтобы он соответствовал необходимым ограничениям на свои параметры.

Из определения арифметического графа вытекает два его важных свойства:

1) всякий конечный граф может быть представлен в виде арифметического графа;

2) кодирование графа обеспечивает его параметризуемость на теоретико-числовом уровне (благодаря подбору функции образующих). Введем понятие арифметического многогранника.

Многогранник называется арифметическим, если:

(1) соответствующий ему граф представлен в виде арифметического графа $G = (V, U)$;

(2) длина ребра (v_i, v_j) удовлетворяет условию

$$|(v_i, v_j)| = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2},$$

где $v_i = (x_i, y_i, z_i)$ и $v_j = (x_j, y_j, z_j)$ — координаты вершин v_i и v_j , а $v_i + v_j = u_k \in U$.

Задача синтеза арифметического многогранника сводится к нахождению неизвестных координат вершин данного графа, являющихся решением системы уравнений $|(v_i, v_j)| = \sqrt{u_k}$, или доказательству несуществования такого решения (несуществования арифметического многогранника). В качестве дополнительных условий можно использовать уравнение грани для четырех точек:

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \end{vmatrix} = 0.$$

Ю.Г. Григорьян доказал, что существует ровно 8 арифметических многогранников, которые можно представить в виде натуральных арифметических графов. С помощью вышеуказанных уравнений можно синтезировать различные арифметические многогранники и получать из них произвольное геометрическое тело в трехмерном пространстве. Это дает возможность форма-

лизовать некоторые задачи построения структур в кристаллографии и минералогии.

Описанные результаты исследований были применены к задачам по автоматизации проектирования вычислительных систем. При этом используется понятие количественной сложности различных дискретных объектов, таких как дизъюнктивная нормальная форма, двоичная матрица, булевы графы. Устанавливаются критерии, позволяющие отличать «более сложные» объекты от «менее сложных», что приводит к положительным результатам в различных областях исследований, связанных с математическим моделированием сложных систем.

Согласно определению информации, приведенному В.М. Глушковым [11], как меры неравномерности в распределении материи или энергии в пространстве и времени, оценка сложности дискретных объектов основана на получении эффективных критериев, характеризующих степень неравномерности, содержащейся в структуре дискретного объекта.

Первые алгоритмы вычисления оценок [37], построенных на понятии теста [56], появились в 60-х годах прошлого века и были связаны с расшифровкой признаков в задачах распознавания образов. В последующем с помощью методов распознавания образов, разработанных Ю.И. Журавлевым и другими учеными бывшего СССР, было показано, что решение этого класса задач необходимо искать на алгебраической основе [57]. В настоящее время во многих публикациях по различным областям естествознания для решения задач оценки сложности химических и физических структур использованы методы теории информации и теории графов. При этом под структурой подразумевается любое конечное множество, элементы которого распределены по подмножествам (классам эквивалентности) в соответствии с заданным отношением эквивалентности. Однако построение классов эквивалентности, как известно, осуществляется на теоретико-числовой и алгебраической основе.

На основе интерпретации дизъюнктивной нормальной формы, булевого графа и арифметического графа как структур Ю.Г. Григорьян получил новые критерии оценок сложности дискретных объектов. Эти критерии установлены с помощью введения новых понятий «прямая» и «обратная» информационная сложность дискретного объекта. Полученный результат позволил построить эффективный эвристический алгоритм решения одной из трудных задач комбинаторной математики — задачи минимального покрытия. Алгоритм основан на последовательном удалении из

исходного семейства множеств, обладающих наименьшей информативностью. Эти алгоритмы прошли адаптацию при определении минимального покрытия и оценки сложности схем, используемых в системах по автоматизации проектирования вычислительных машин, разработанных Ереванским НИИ математических машин.

Ю.Г. Григорьян и его соавторы ввели новое понятие такого математического объекта, как арифметический граф. Однако дальнейшее использование этого понятия имело чисто практический характер, в основном обусловленный задачами представления геометрических объектов в виде арифметических графов. Другие, чисто теоретические вопросы не интересовали Ю.Г. Григорьяна и его соавторов, которые были заинтересованы лишь в решении конкретных практических, но важных в то время задач. В результате многие теоретические вопросы, выпавшие из поля зрения первооткрывателей числовых графов, так и остались неразрешенными. Их увлечение чисто практической стороной привело к полнейшему забвению этого направления в математике. За последние 40 лет эта группа армянских ученых не опубликовала ни одной работы по данному направлению. Любой математик на их месте обязательно поставил бы следующие вопросы: (1) какое соотношение между натуральными арифметическими графами и просто арифметическими графами? (2) какие графы можно представить в виде натуральных арифметических графов? (3) как найти оптимальное представление заданного графа в виде арифметического графа? (4) как найти необходимые признаки для определения характеристических чисел арифметических графов, таких как цикломатическое число, связность, хроматическое число и другие?

Итак, можно констатировать, что самые простые числовые графы — арифметические (в дальнейшем A -графы), для которых $F = x_i + x_j$, $X \in N$, и модульные (в дальнейшем M -графы), для которых $F(x_i, x_j) = |x_i - x_j|$, $X \in N$.

Изучению указанных графов и посвящены две последующие главы.

АРИФМЕТИЧЕСКИЕ ГРАФЫ (A-ГРАФЫ) И ИХ СВОЙСТВА

2.1. ОБ ОПТИМАЛЬНОМ КОДИРОВАНИИ ЦЕПЕЙ В КЛАССЕ NA-ГРАФОВ

Как было показано, если вопрос о смежности вершин определяется путем вычисления некоторой функции двух переменных [38], то граф можно задать аналитическим образом. Если эта функция имеет простой вид $F = x_i + x_j$, то получается арифметический граф [25, 26] (в дальнейшем A -граф). Согласно этим работам введем следующие определения.

Определение 2.1. Под конечным арифметическим графом $G(X, U)$ подразумевается два множества действительных чисел: множество вершин $X = \{x_1, x_2, \dots, x_n\}$ и множество образующих $U = \{u_1, u_2, \dots, u_m\}$, причем вершины x_i и x_j смежны тогда и только тогда, когда $x_i + x_j \in U$.

Особый интерес представляет случай, когда множество X является подмножеством натуральных чисел.

Определение 2.2. A -графы $G_1(X_1, U_1)$ и $G_2(X_2, U_2)$ изоморфны, если существует взаимно однозначное соответствие φ между X_1 и X_2 , U_1 и U_2 , сохраняющее смежность в этих графах, или $G_1(X_1, U_1) \cong G_2(X_2, U_2)$, если $\forall x_i, x_j \in X_1 [(x_i + x_j) \in U_1 \Leftrightarrow (\varphi(x_i) + \varphi(x_j)) \in U_2]$.

В дальнейшем будем рассматривать только такие арифметические графы, у которых элементами X являются натуральные числа.

Рассмотрим случай, когда $X = \{1, 2, \dots, n\}$. Назовем такой граф натуральным или NA -графом. Возникает вопрос: существует ли для заданного топологического графа его представление в виде NA -графа? Для некоторых классов графов, простых по структуре, в работах [27, 28] дан положительный ответ. Это такие графы, как односвязная цепь, один цикл, полный граф. Следует заметить, что не всякий граф, как бы мы ни задавали U , может быть натуральным.

Определение 2.3. Два способа задания графа $G(X, U)$ и $G'(X', U')$ с одним и тем же числом образующих называется эквивалентными, если для них выполняется условие $x_i = \pm x'_i + c$ ($i = 1, 2, \dots, m$).

Очевидно, что при этом все образующие эквивалентных заданий графа различаются на постоянную величину. Будем называть разные способы задания графа *кодировками*.

Теорема 2.1. Для того чтобы односвязная цепь была закодирована с помощью двух образующих в классе *NA*-графов, необходимо и достаточно, чтобы коды ее четных вершин представляли арифметическую возрастающую прогрессию, а коды нечетных вершин — арифметическую убывающую прогрессию, причем обе прогрессии с одной и той же разностью.

Предполагается, что нумерация вершин цепи соответствует порядку их следования.

Необходимость. Пусть цепь закодирована множеством чисел $\{x_i\}$ ($i = 1, 2, \dots, n$), а ее образующие равны d_1 и d_2 . Не нарушая общности, будем считать, что $d_1 \leq d_2$.

Составляем отношения для чисел x_i :

$$x_1 + x_2 = d_1,$$

$$x_2 + x_3 = d_2,$$

$$x_3 + x_4 = d_1.$$

Получаем

$$d_1 - d_2 = x_3 - x_1,$$

$$d_2 - d_1 = x_2 - x_4.$$

Для вершины с нечетными номерами находим зависимость:

$$x_3 - x_1 = x_5 - x_3,$$

$$2x_3 = x_1 + x_5,$$

$$x_3 = (x_1 + x_5)/2$$

или в общем случае

$$x_{2k-1} = (x_{2k-3} + x_{2k+1})/2.$$

Для вершин с четными номерами получаем $x_4 = (x_2 + x_6)/2$ или в общем случае

$$x_{2k} = (x_{2k-2} + x_{2k+2})/2.$$

Эти зависимости характеризуют арифметическую прогрессию с разностью $d_2 - d_1$. Учитывая, что $x_{2k+1} > x_{2k-1}$, $x_{2k+2} < x_{2k}$, приходим к необходимому утверждению.

Достаточность. Пусть $\{x_i\}$ удовлетворяет следующим соотношениям:

$$x_{2k+1} = x_{2k-1} + d_1, x_{2k+2} = x_{2k} - d$$

или

$$x_{2k+1} = x_1 + kd \ (k > 1), x_{2k+2} = x_2 - kd.$$

Эти соотношения задают кодировку вершин цепи с помощью двух образующих. Зафиксируем сумму кодов первой и второй вершин:

$$x_1 + x_2 = d_1.$$

Отсюда $x_2 + x_3 = x_2 + (x_1 + d) = d_1 + d_2$.

В общем случае

$$x_{2k+1} + x_{2k+2} = x_1 + kd + x_2 - kd = x_1 + x_2 = d_1,$$

$$x_{2k+2} + x_{2k+3} = x_2 + kd + x_1 - kd + d = d_1 + d_2.$$

Таким образом, образующие цепи равны d_1 и $d_1 + d_2$, что и требовалось доказать.

Покажем теперь, что для кодировки с помощью двух образующих существует эквивалентная кодировка, представляющая цепь в виде NA -графа. Присвоим первой вершине цепи число (код) 1. Поскольку количество четных и нечетных вершин цепи различается не больше чем на единицу, то и соответствующие им арифметические прогрессии должны быть по длине равновеликими. Множество чисел от 1 до n можно разбить на две равновеликие арифметические прогрессии только двумя способами:

- 1) 1, 2, 3, ..., $[n/2]$ и $[n/2] + 1, [n/2] + 2, \dots, n$;
- 2) 1, 3, 5, ... и 2, 4, 6,

Получаем две арифметические прогрессии с разностью $d = 1$ и $d = 2$. Им соответствуют два способа кодирования цепи (рис.2.1 ($d = 1$, $u_1 = n + 1, u_2 = n + 2$), рис. 2.2 ($d = 2, u_1 = n + 1, u_2 = n + 3$) для $n=10$).

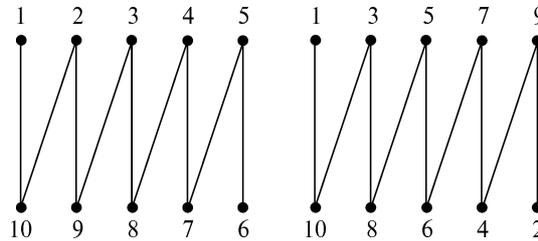


Рис. 2.1

Рис. 2.2

Лемма 2.1. Преобразование множества вершин $x'_i = n + 1 - x_i$ и множества образующих $u'_k = 2n + 2 - u_k$ является эквивалентным для любого NA -графа.

Действительно, пусть $x_i + x_j = u$. Тогда в преобразованных множествах $(n + 1 - x_i) + (n + 1 - x_j) = 2n + 2 - (x_i + x_j) = 2n + 2 - u$. Это подтверждает вышеизложенное, при этом преобразование не нарушает натуральности графа.

Применив приведенное преобразование к цепи, получим еще две эквивалентные кодировки (рис.2.3 ($d = 1, u_1 = n, u_2 = n + 1$), рис. 2.4 ($d = 2, u_1 = n + 1, u_2 = n + 1$)).

Остальные кодировки находим с помощью перестановок начала и конца цепи. Эти четыре разные кодировки получены для четного n . В случае нечетного n имеем только три разные кодировки. В первых двух случаях, как и для четного n , получаем ($d = 1, u_1 = n + 1, u_2 = n + 2$) и ($d = 2, u_1 = n, u_2 = n + 2$); затем с помощью эквивалентного преобразования имеем ($d = 1, u_1 = n + 1, u_2 = n$), а второй вариант переходит в себя ($d = 2, u'_1 = 2n + 2 - u_1 = n + 2, u'_2 = 2n + 2 - u_2 - 2 = n$).

Рассмотрим случай нескольких цепей. При кодировании вершин цепей можно использовать тот же способ, что и при кодировании односвязной цепи. Для этого достаточно добавить к m цепям ($m > 1$, в каждой цепи n_i вершин) $m - 1$ фиктивные вершины, которые склеят все цепи в одну, и применить вышеизложенный метод, как показано на рис. 2.5 ($u_1 = n + 1, u_2 = n + 2$). Здесь имеются четыре цепи ($m = 4, n_1 = 8, n_2 = 7, n_3 = 4, n_4 = 4$). При решении добавлены 3 фиктивные вершины, закодированные числами 5, 9 и 16.

Описанная кодировка задает минимальный граф (2 образующие), но несовершенный. Очевидно, что если будет получен NA -граф, то он и будет совершенным. В данном случае этого удастся

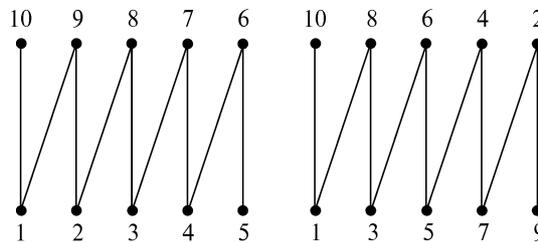


Рис. 2.3

Рис. 2.4

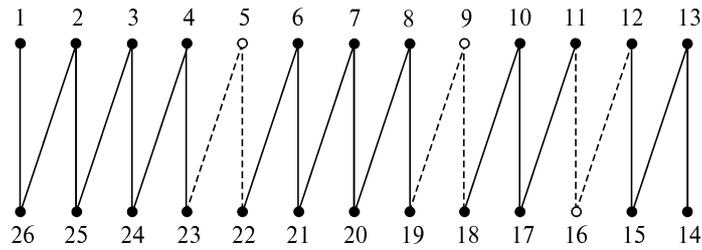


Рис. 2.5

достигнуть, как видно из рис. 2.6 ($u_1 = 20, u_2 = 26$). Вертикальные ребра соответствуют образующей $u_1 = 20$, а наклонные — образующей $u_2 = 26$. Цепи получают кодировки (3, 5, 9, 11, 15, 17, 21, 23), (2, 6, 8, 12, 14, 18, 20), (1, 7, 13, 19) и (4, 10, 16, 22).

Нетрудно заметить, что для каждой отдельно взятой цепи выполняются необходимые условия теоремы 2.1, т.е. коды, соответствующие четным (или нечетным) номерам вершин, составляют возрастающую или убывающую арифметическую прогрессию. Общая разность этих прогрессий $d = 6$. Возникает вопрос, при каких значениях можно закодировать цепи с помощью двух образующих? Для одной цепи, как указано в теореме 2.1, $d = 1, 2$.

Лемма 2.2. Для $d = 1$ не существует NA -графа с двумя образующими, представляющего несколько цепей.

Прежде всего заметим, что для двух образующих справедливо условие

$$u_1 \leq n + 1 \leq u_2. \quad (2.1)$$

Выполнение левого неравенства достаточно для того, чтобы вершина с кодом 1 не была изолированной, а правого — чтобы не была изолированной вершина с кодом n .

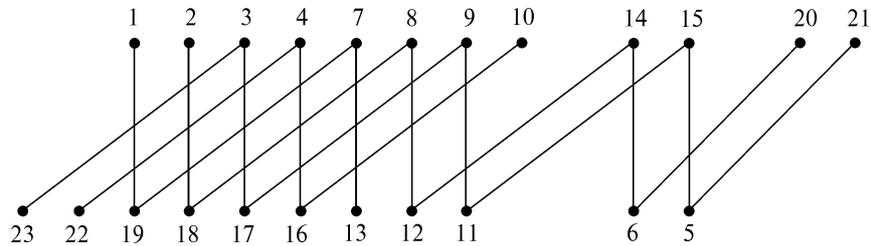


Рис. 2.6

Допустим противное, что нам удалось закодировать больше одной цепи для $d = 1$. Возьмем три последовательные вершины x_k, x_{k+1} и x_{k+2} . Для них справедливы равенства

$$x_k + x_{k+1} = u_1, \quad x_{k+1} + x_{k+2} = u_2.$$

Так как $|x_{k+2} - x_k| = d$, то $(u_2 - u_1) = 1$. При условии (2.1) это возможно только в двух случаях:

А. $u_1 = n + 1; u_2 = n + 2;$

Б. $u_1 = n; u_2 = n + 1.$

Случай Б получается из А при эквивалентном преобразовании $u' = 2n + 2 - u$ и его можно не рассматривать. Вычислим, скольким ребрам соответствуют образующие в случае А. Находим: u_1 соответствует ребрам $(1, n), (2, n - 1), (3, n - 2)$ и т.д. При n четном число таких ребер равно $n/2$, при n нечетном — $(n - 1)/2$. Аналогично для u_2 получаем при n четном число соответствующих ребер равно $n/2 - 1$, для n нечетных — $(n - 1)/2$. В каждом случае образующие задают в графе $n - 1$ ребро. Но для m цепей ($m > 1$) число ребер должно быть равным $n - m$. Это подтверждает справедливость леммы.

Для заданного d множество чисел от 1 до n однозначно разбивается на d классов с представителем $i \pmod{d}$, $i = 0, 1, \dots, d - 1$. Чтобы закодировать одну цепь с помощью двух образующих, необходимо четным вершинам присвоить числа $i \pmod{d}$ в возрастающем порядке, а нечетным — $j \pmod{d}$ (j/i) в убывающем порядке. Отсюда можно сделать вывод, что $d \leq 2m$. Рассмотрим вопрос, когда можно закодировать m цепей с помощью двух образующих при $d = 2m$. Ответ на него дает следующая теорема.

Теорема 2.2. Набор m цепей, состоящий из a_1 цепей длины l_1 , a_2 цепей длины l_2 и a_3 цепей длины l_3 ($a_i \geq 0$) допускает представление в виде NA -графа с помощью двух образующих при $d = 2m$ в том и только в том случае, если

$$l_1 = 2\lambda + 2, \quad l_2 = 2\lambda + 1, \quad l_3 = 2\lambda, \quad \text{где } \lambda = [n/2m].$$

При этом в качестве образующих можно взять

$$u_1 = 2m\lambda + 2a_1 + 1, \quad u_2 = 2m(\lambda + 1) + 2a_1 + 1.$$

Доказательство. Так как цепь составляется из чисел, принадлежащих двум разным классам вычетов по модулю d , то задача сводится к разбиению $2m$ классов на m пар, сумма которых одинакова по модулю d . Расположим числа от 1 до n в таблице, где

в первой строке находятся числа от 1 до $2m$, во второй строке — числа от $2m + 1$ до $4m$ и т.д. В результате каждый столбец с номером i будет содержать в возрастающем порядке числа класса вычетов $i(\bmod d)$. Как правило, все столбцы содержат по λ чисел, где $\lambda = \lfloor n/2m \rfloor$, только β первых столбцов, где $\beta = n(\bmod 2m)$, содержат по $\lambda + 1$ числу. Цепи длиной $2\lambda + 2$ кодируются с помощью двух таких столбцов, цепи длиной $2\lambda + 1$ — с помощью одного такого столбца и одного столбца с номером больше β , а цепи длиной 2λ — с помощью столбцов, номера которых больше β .

Возьмем первые два столбца и поставим их числа в соответствие одной цепи длиной $2\lambda + 2$. Кодировку будем осуществлять так: первой вершине присвоим число 1; второй вершине — наибольшее число второго столбца, т. е. $2m\lambda + 2$; третьей вершине — второе число первого столбца, т. е. $2m + 1$; четвертой вершине — предпоследнее число второго столбца, т. е. $2m(\lambda - 1) + 2$ и т. д. В результате получаем кодировку цепи с образующими $u_1 = 2m\lambda + 3$, $u_2 = 2m(\lambda + 1) + 3$. Так как сумма чисел первого и второго столбцов всегда будет равна $3(\bmod 2m)$, то остальные столбцы необходимо разбить по парам так, чтобы их номера удовлетворяли соотношению

$$i + j \equiv 3(\bmod 2m).$$

Номера столбцов составят пары $(3, 2m)$, $(4, 2m - 1)$, $(5, 2m - 2)$, ..., $(m + 1, m + 2)$. Применяя описанный способ кодировки и учитывая, что последние столбцы имеют длину λ , получаем, например, для пары $(3, 2m)$ образующие $u_1 = 3 + 2m\lambda$, $u_2 = 3 + 2m + 2m\lambda = 2m(\lambda + 1) + 3$, которые совпадают с образующими для первого и второго столбцов. Пара $(3, 2m)$, очевидно, представляет цепь длиной $2\lambda + 1$. И таких пар, как легко определить, будет $\beta - 2a_1$. Отсюда нетрудно построить кодировку для цепей с произвольными параметрами a_i . Для этого $2a_1$ первых столбцов используем для кодировки цепей длиной $2\lambda + 2$, затем $\beta - 2a_1$ следующих столбцов и $\beta - 2a_1$ последних столбцов — для кодировки цепей длиной $2\lambda + 1$, а оставшиеся $n - 2\beta + 2a_1$ столбца для кодировки цепей длиной 2λ . При этом номера столбцов, использующихся для каждой цепи, должны удовлетворять соотношению

$$i + j \equiv (2a_1 + 1) (\bmod 2m). \quad (2.2)$$

Из соотношения (2.2) вытекает, что

$$u_1 = 2m\lambda + 2a_1 + 1; \quad u_2 = 2m(\lambda + 1) + 2a_1 + 1.$$

2.2. О ПЕРЕЧИСЛЕНИИ СПОСОБОВ КОДИРОВАНИЯ НАБОРА ЦЕПЕЙ

Теорема о возможности кодирования m цепей с помощью двух образующих доказана в работе [41]. Показано, что такая кодировка основана на арифметической прогрессии с разностью $d = 2m$. Рассмотрим общую ситуацию, когда возможны и другие разности. Будем излагать теорию кодирования с помощью примеров. Пусть $n = 23$, $m = 4$.

А. $d = 2m$ ($d = 8$).

Разобьем все числа от 1 до 23 на классы вычетов по mod 8:

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 17 & 18 & 19 & 20 & 21 & 22 & 23 & \end{array} \quad (2.3)$$

Здесь в i -м столбце находятся числа $i(\text{mod } 8)$. Для кодирования одной цепи возьмем два столбца таких чисел (i, j) , для которых справедливо выражение

$$i + j = 1(\text{mod } 8). \quad (2.4)$$

Уравнение (2.4) имеет четыре решения, а именно: (1,8), (2,7), (3,6) и (4,5).

Выпишем два столбца чисел, например для (2,7):

$$\begin{array}{cc} 2 & 7 \\ 10 & 15 \\ 18 & 23 \end{array}$$

Теперь, поочередно выбирая числа из этих столбцов, получаем кодировку цепи из 6 вершин:

$$2 - 23 - 10 - 15 - 18 - 7.$$

Назовем такую кодировку верхней, так как первое число 2 здесь берется сверху из левого столбца. Нижнюю кодировку получаем, выбирая первым число снизу из левого столбца:

$$18 - 7 - 10 - 15 - 2 - 23.$$

Очевидно, что верхняя и нижняя кодировки возможны, если оба столбца имеют одинаковую высоту. Если один столбец содержит на один элемент больше, чем другой, то получается единственная кодировка, которая является одновременно и верхней, и нижней.

Верхняя и нижняя кодировки различаются своими образующими: для верхней — $u_1 = 25, u_2 = 33$, для нижней — $u_1 = 17, u_2 = 25$, т. е. происходит уменьшение на число $d = 8$.

Обозначим n -вершинный набор из m цепей с длинами l_i , ($i = 1, 2, \dots, m$) через $L = (l_1, l_2, \dots, l_m)$. Если он закодирован с помощью двух образующих, то обозначим $\pi = (L; U)$, где $U = \{u_1, u_2\}$, и назовем представлением (n, m) -набора цепей. Два множества $\pi_i \neq \pi_j$, если $L_i \neq L_j$ или $U_i \neq U_j$. Очевидно, что если $L_i = L_j$, то мы имеем дело с изоморфными графами. Множество всех отличных друг от друга представлений обозначим $\Pi(n, m)$. Если в уравнение (2.4) вместо 1 подставить 3, то получим уравнение для новой кодировки. В общем случае уравнение (2.4) имеет вид

$$i + j \equiv (2q + 1) \pmod{d} \quad (q = 0, 1, 2, \dots, m - 1). \quad (2.5)$$

Используя указанный метод построения, записываем все кодировки:

1) $q = 0$ ($u_1 = 17, u_2 = 25$)

$$\begin{aligned} &1 - 16 - 9 - 8 - 17 \\ &23 - 2 - 15 - 10 - 7 - 18 \\ &22 - 3 - 14 - 11 - 6 - 19 \\ &21 - 4 - 13 - 12 - 5 - 20 \end{aligned}$$

2) $q = 1$ ($u_1 = 19, u_2 = 27$)

$$\begin{aligned} &1 - 18 - 9 - 10 - 17 - 2 \\ &3 - 16 - 11 - 8 - 19 \\ &23 - 4 - 15 - 12 - 7 - 20 \\ &22 - 5 - 14 - 13 - 6 - 21 \end{aligned}$$

3) $q = 2$ ($u_1 = 21, u_2 = 29$)

$$\begin{aligned} &1 - 20 - 9 - 12 - 17 - 4 \\ &2 - 19 - 10 - 11 - 18 - 3 \\ &5 - 16 - 13 - 8 - 21 \\ &23 - 6 - 15 - 14 - 7 - 22 \end{aligned}$$

4) $q = 3$ ($u_1 = 23, u_2 = 31$)

$$\begin{aligned} &1 - 22 - 9 - 14 - 17 - 6 \\ &2 - 21 - 10 - 13 - 18 - 5 \\ &3 - 20 - 11 - 12 - 19 - 4 \\ &7 - 16 - 15 - 8 - 23 \end{aligned}$$

Здесь разбиение вершин графа по цепям всюду одинаковое, $L = (6, 6, 6, 5)$, т. е. все представленные графы изоморфны. Ввиду того, что всегда присутствует цепь длиной 5, то нигде не используется нижняя кодировка.

Б. $d = 2m - 1$ ($d = 7$).

Разобьем все числа от 1 до 23 на семь столбцов соответственно классам вычетов по mod 7:

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \\ 8 & 9 & 10 & 11 & 12 & 13 & 14 & \\ 15 & 16 & 17 & 18 & 19 & 20 & 21 & \\ 22 & 23 & & & & & & \end{array} \quad (2.6)$$

Так как число цепей по-прежнему должно быть равным 4, а в таблице теперь 7 столбцов, то в этом случае на каждую цепь по два столбца не хватит. Это означает, что для какой-то цепи придется использовать один столбец. Так как номера столбцов мы находим из уравнения типа (2.5), то для этого столбца будет справедливо $i + i \equiv \alpha \pmod{d}$, т. е. в правой части может стоять и четное число.

Объединяя эти случаи, приходим к выводу, что необходимо решать уравнение

$$i + j \equiv q \pmod{d} \quad (q = 1, 2, \dots, d). \quad (2.7)$$

Для каждого заданного q всегда найдется номер столбца $q/2$ (если q — четное), либо $(d + q)/2$ (если q — нечетное), который удовлетворяет уравнению (2.7), если сложить этот номер сам с собой.

Учитывая изложенное выше, записываем все решения:

1) $q = 1$ ($u_1 = 22, u_2 = 29$)

$$\begin{array}{l} 1 - 21 - 8 - 14 - 15 - 7 - 22 \\ 2 - 20 - 9 - 13 - 16 - 6 - 23 \\ 3 - 19 - 10 - 12 - 17 - 5 \\ 4 - 18 - 11 \end{array}$$

Разбиение вершин проведено по цепям $L = (7, 7, 6, 3)$. Столбец 4 использован для кодирования одной цепи;

2) $q = 2$ ($u_1 = 23, u_2 = 30$). Здесь одинокий столбец 1.

$$\begin{array}{l} 1 - 22 - 8 - 15 \\ 2 - 21 - 9 - 14 - 16 - 7 - 23 \\ 3 - 20 - 10 - 13 - 17 - 6 \\ 4 - 19 - 11 - 12 - 18 - 5 \end{array}$$

Разбиение проведено по цепям $L = (7, 6, 6, 4)$;

3) $q = 3$ ($u_1 = 24, u_2 = 31$)

1 – 23 – 8 – 16 – 15 – 9 – 22 – 2
 3 – 21 – 10 – 14 – 17 – 7
 4 – 20 – 11 – 13 – 18 – 6
 5 – 19 – 12

Здесь длинные цепи имеют четную длину, а нечетную длину — цепь, которая использует только один столбец 5. Это позволяет использовать и нижнюю кодировку, так как для одного столбца это всегда возможно.

Нижняя кодировка имеет вид ($u_1 = 17, u_2 = 24$)

22 – 2 – 9 – 8 – 16 – 1 – 23
 17 – 7 – 10 – 14 – 3 – 21
 18 – 6 – 11 – 13 – 4 – 20
 19 – 5 – 12

В обоих случаях разбиение вершин проведено по цепям $L = (8, 6, 6, 3)$;

4) $q = 4$ ($u_1 = 18, u_2 = 25$)

1 – 17 – 8 – 10 – 15 – 3 – 22
 23 – 2 – 16 – 9
 18 – 7 – 11 – 14 – 4 – 21
 19 – 6 – 12 – 13 – 5 – 20

Здесь следует обратить внимание на то, что первая цепь длиной 7 имеет единственную кодировку, что и определяет значения образующих. Остальные цепи при заданных образующих тоже кодируются однозначно, но только с помощью нижней кодировки.

Разбиение вершин проведено по цепям $L = (7, 6, 6, 4)$;

5) $q = 5$ ($u_1 = 19, u_2 = 26$)

1 – 18 – 8 – 11 – 15 – 4 – 22
 2 – 17 – 9 – 10 – 16 – 3 – 23
 21 – 5 – 14 – 12 – 7 – 19
 20 – 6 – 13

Здесь также первые две цепи, имеющие нечетную длину, определяют значения образующих, что обуславливает использование для двух других цепей лишь нижней кодировки. При этом разбиение вершин проведено по цепям $L = (7, 7, 6, 3)$;

6) $q = 6$ ($u_1 = 20, u_2 = 27$)

1 – 19 – 8 – 12 – 15 – 5 – 22

2 – 18 – 9 – 11 – 16 – 4 – 23

3 – 17 – 10

20 – 7 – 13 – 14 – 6 – 21

Здесь только для одной цепи используется нижняя кодировка, которая также определяется однозначно кодировками для предыдущих цепей. Так как разбиение вершин проведено по цепям $L = (7, 7, 6, 3)$, то получаем граф, изоморфный графу при $q = 5$;

7) $q = 7$ ($u_1 = 21, u_2 = 28$)

1 – 20 – 8 – 13 – 15 – 6 – 22

2 – 19 – 9 – 12 – 16 – 5 – 23

3 – 18 – 10 – 11 – 17 – 4

21 – 7 – 14

Здесь нижняя кодировка используется для самой короткой цепи. Разбиение вершин по цепям такое же, как и в двух предыдущих случаях: $L = (7, 7, 6, 3)$, т. е. в последних трех случаях получены изоморфные графы.

В. $d = 2m - 2$ ($d = 6$).

Для этого значения еще можно закодировать m цепей, но при этом ровно две цепи необходимо кодировать только с помощью одного столбца. Составляем таблицу, располагая в каждом столбце числа, соответствующие вычетам по модулю 6:

1	2	3	4	5	6	
7	8	9	10	11	12	
13	14	15	16	17	18	(2.8)
19	20	21	22	23		

Заметим, что уравнение (2.5) имеет решения, которые кодируют ровно $m - 1$ цепь. Поэтому будем искать решение следующего уравнения:

$$i + j \equiv 2q \pmod{d} \quad (q = 1, 2, \dots, m - 1). \quad (2.9)$$

Наряду с различными решениями этого уравнения, которые используют $2m - 4$ столбца, соответствующие $m - 2$ цепям, существуют еще два решения, использующие только один столбец. Это столбцы с номерами q и $q + d/2$;

1) $q = 1$ ($u_1 = 20$, $u_2 = 26$). Здесь одинокие столбцы 1 и 4.

1 – 19 – 7 – 13
 2 – 18 – 8 – 12 – 14 – 6 – 20
 23 – 3 – 17 – 9 – 11 – 15 – 5 – 21
 22 – 4 – 16 – 10

Для двух последних цепей взято нижнюю кодировку и разбиение вершин проведено по цепям $L = (8, 7, 4, 4)$;

2) $q = 2$ ($u_1 = 22$, $u_2 = 28$). Здесь одинокие столбцы 2 и 5.

1 – 21 – 7 – 15 – 13 – 9 – 19 – 3
 2 – 20 – 8 – 14
 4 – 18 – 10 – 12 – 16 – 6 – 22
 23 – 5 – 17 – 11

Для последней цепи использована нижняя кодировка и разбиение вершин проведено по цепям $L = (8, 7, 4, 4)$, т. е. получен граф, изоморфный предыдущему;

3) $q = 3$ ($u_1 = 21$, $u_2 = 30$). Здесь одинокие столбцы 3 и 6.

1 – 23 – 7 – 17 – 13 – 11 – 19 – 5
 2 – 22 – 8 – 16 – 14 – 10 – 20 – 4
 3 – 21 – 9 – 15
 6 – 18 – 12

В данном случае разбиение вершин проведено по цепям $L = (8, 8, 4, 3)$, при этом нечетную длину имеет цепь, для кодировки которой используется только один столбец. Так как вышеприведенная кодировка — верхняя, то появляется возможность для использования нижней кодировки ($u_1 = 18$, $u_2 = 24$):

19 – 5 – 13 – 11 – 7 – 17 – 1 – 23
 20 – 4 – 14 – 10 – 8 – 16 – 2 – 22
 21 – 3 – 15 – 9
 18 – 6 – 12

Этим и исчерпываются все кодировки четырех цепей с общим числом вершин 23. Две кодировки из такого набора приведены на рис. 2.7 ($n = 23$, $l = 4$, $u_1 = 23$, $u_2 = 31$, $d = 8$) и рис. 2.8 ($n = 23$, $u_1 = 24$, $u_2 = 30$, $l = 4$, $d = 6$).

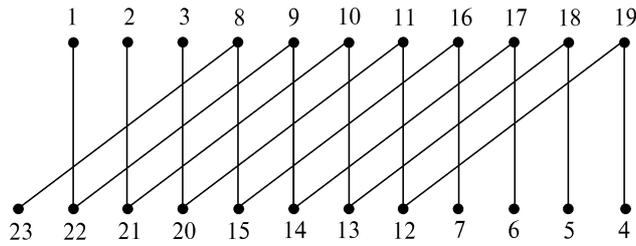


Рис. 2.7

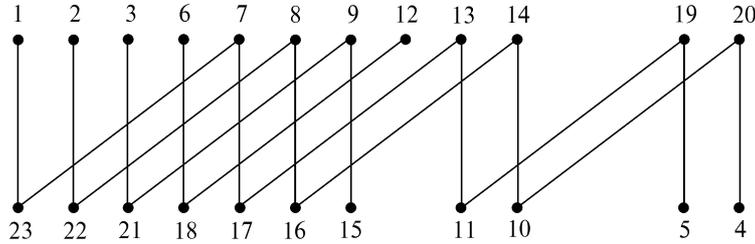


Рис. 2.8

Число всех представлений легко вычислить: для $d = 8$ оно равно 4, для $d = 7 - 8$ и для $d = 6 -$ всего 4. В сумме получаем $|\Pi(23,4)| = 4 + 8 + 4 = 16$. Зная все эти способы представления, можно поставить обратную задачу: пусть заданы m цепей с набором вершин $L = (l_1, l_2, \dots, l_m)$. Найти для них минимальную кодировку.

2.3. МАТРИЦА ОБРАЗУЮЩИХ A-ГРАФОВ И ЦИКЛЫ

Рассмотрим матрицу $A = (a_{ij})$, где

$$a_{ij} = i + j; a_{ij} = 0 \quad (1 < i, j < n). \quad (2.10)$$

Эта матрица соответствует произвольному полному натуральному арифметическому графу:

$$\begin{pmatrix} 0 & 3 & 4 & 5 & \dots & n & n+1 \\ 3 & 0 & 5 & 6 & \dots & n+1 & n+2 \\ 4 & 5 & 0 & 7 & \dots & n+2 & n+3 \\ 5 & 6 & 7 & 0 & \dots & n+3 & n+4 \\ \cdot & \cdot & \cdot & \cdot & \dots & & \\ & & & & \cdot & \dots & 0 & 2n-1 \\ & & & & \cdot & \dots & 2n-1 & 0 \end{pmatrix}. \quad (2.11)$$

Очевидно, что матрица представляет этот граф однозначно, так как у него множество образующих состоит из отрезка натурального ряда $U = \{3, 4, 5, \dots, 2n - 1\}$. Любое собственное подмножество этого множества определяет некоторый NA -граф $G = (X, U)$.

Определение 2.4. Матрицей образующих для произвольного NA -графа $G = (X, U)$ называется матрица $A(G) = (a_{ij})$, у которой $a_{ij} = 1$, если существует такое $u_k \in U$, что $u_k = i + j$; $a_{ij} = 0$ для остальных значений i и j .

Такое задание NA -графа не избыточно, т. е. для любого $u \in U$ обязательно найдется пара вершин x_i и x_j ($x_i \neq x_j$) таких, что $x_i + x_j = u$. Кроме того, будем считать, что множество U упорядочено естественным образом.

В этой матрице число ненулевых элементов равно удвоенному числу ребер заданного NA -графа, так как каждое ребро (x_i, x_j) задается двумя элементами матрицы a_{ij} и a_{ji} .

Одной из главных задач в теории арифметических графов является нахождение для заданного графа множества U с минимальной мощностью. Наряду с поиском таких множеств отдельный интерес представляет и перечисление всех таких множеств. Для каждого $u \in U$ можно вычислить число $r_n(u)$ соответствующих элементов матрицы $A(G)$. Наибольшее значение $r_n(u)$ принимает для $u = n + 1$, и эти элементы образуют боковую диагональ матрицы.

Нетрудно заметить, что $r_n(u)$ симметрична относительно значения $u = n + 1$, т. е. имеет место равенство

$$r_n(n + 1 - \Delta) = r_n(n + 1 + \Delta) \quad (0 < \Delta < n - 2). \quad (2.12)$$

Если обозначить аргументы функции через u , то из равенства (2.12) получим

$$\Delta = |n + 1 - u|,$$

$$r_n(u) = r_n(n + 1 - |n + 1 - u|). \quad (2.13)$$

Для вычисления функции теперь можно ограничиться значениями $u \leq n$. Легко видеть, что

$$r_n(u) = \begin{cases} u - 2 & \text{для } u \text{ четного,} \\ u - 1 & \text{для } u \text{ нечетного,} \end{cases} \quad (2.14)$$

или

$$r_n(u) = 2 \left\lfloor \frac{u - 1}{2} \right\rfloor, \quad (2.15)$$

Подставляя это значение в (2.13), окончательно получаем

$$r_n(u) = 2 \left\lfloor \frac{n - |n + 1 - u|}{2} \right\rfloor. \quad (2.16)$$

Подбирая различные значения u для множества образующих U , можно определить число ребер полученного графа и степени его вершин. Для того чтобы две образующие u_1 и u_2 соответствовали двум смежным ребрам, необходимо выполнение условия $|u_1 - u_2| < n$. Оптимальное представление цепей и перечисление всех множеств образующих полностью описано в работе [40], там же приведены некоторые результаты о циклах. Прежде всего заметим, что для множества образующих, состоящего из двух элементов $U = \{u_1, u_2\}$, справедливо условие

$$u_1 \leq n + 1 \leq u_2. \quad (2.17)$$

Выполнение левого неравенства достаточно для того, чтобы вершина с кодом 1 не была изолированной, а правого — чтобы не была изолированной вершина с кодом n .

В натуральных графах любая образующая u задает столько ребер, сколько решений имеет уравнение

$$x_1 + x_2 = u \quad (2.18)$$

на множестве чисел $\{1, 2, \dots, n\}$.

Используя функцию $r_n(u)$, для произвольного натурального графа с m ребрами и n вершинами можно подбирать некоторые образующие, чтобы выполнялось условие

$$\sum_{i=1}^k r_n(u_i) = 2m. \quad (2.19)$$

В этом смысле можно проверить правильность формул в (2.19) для образующих в теореме 2.2. Так как $n = 2m\lambda + n(\bmod 2m)$, а $2\alpha_1 \leq n(\bmod 2m)$, то $u_1 = 2m\lambda + 2\alpha_1 + 1 \leq n + 1$. Для u_1 по (2.15) имеем

$$r_n(u_1) = r_n(2m\lambda + 2\alpha_1 + 1) = 2(m\lambda + \alpha_1).$$

Для $u_2 \geq n + 1$ по (2.16) получаем

$$\begin{aligned} r_n(u_2) &= r_n(2m\lambda + 2m + 2\alpha_1 + 1) = \\ &= 2 \lfloor (2n + 1 - u_2)/2 \rfloor = 2n - 2m\lambda - 2m - 2\alpha_1. \end{aligned}$$

Удвоенное число ребер в m цепях составляет

$$r_n(u_1) + r_n(u_2) = 2n - 2m = 2(n - m).$$

Это выражение показывает, что m цепей содержат $n - m$ ребер.

Определение 2.5. Множество образующих $U' = \{u'_1, u'_2, \dots, u'_m\}$ называется двойственным относительно множества $U = \{u_1, u_2, \dots, u_m\}$, если его элементы в матрице A симметричны относительно боковой диагонали элементам, соответствующим множеству U .

Между множествами U и U' легко установить зависимость. Очевидно, что $(U')' = U$.

Лемма 2.3. Между элементами двойственных множеств U и U' существует взаимно-однозначное соответствие $u' = 2n - u + 2$.

Покажем, что $r_n(u) = r_n(u')$ и тем самым установим справедливость леммы 2.3:

$$\begin{aligned} r_n(u') &= r_n(2n + 2 - u) = 2 \left\lfloor \frac{n - |n + 1 - (2n + 2 - u)|}{2} \right\rfloor = \\ &= 2 \left\lfloor \frac{n - |u - 1 - n|}{2} \right\rfloor = 2 \left\lfloor \frac{n - |n + 1 - u|}{2} \right\rfloor = r_n(u). \end{aligned}$$

В дальнейшем при перечислении множеств образующих двойственные множества будут учитываться автоматически.

Лемма 2.4. Для всякого цикла C_n необходимо существование двух образующих $u_i \leq n + 1$ и двух образующих $u_j \geq n + 1$.

Так как степень каждой вершины равна 2, то образующие, связывающие вершину 1 с двумя другими, должны быть не больше $n + 1$. Аналогично вершина n , будучи связанной с двумя вершинами, требует двух образующих не меньше $n + 1$.

2.4. ПРЕДСТАВЛЕНИЕ ФАКТОРОИДОВ

Очевидно, что те же необходимые условия леммы 2.4, которые выполняются для цикла C_n , справедливы и для произвольного факториода, т. е. набора циклов. Для достаточных условий требуется более сложная зависимость между образующими NA -графа. Рассмотрим NA -графы с тремя образующими.

Теорема 2.3. Для того чтобы NA -граф с тремя образующими представлял собой факториод, необходимо и достаточно, чтобы

- а) для $n \equiv 3 \pmod{4}$ $U = \left\{ \frac{n+3}{2}, n+1, \frac{3n+1}{2} \right\}$;
- б) для четного n $U = \{u, n+1, n+u\}$, где u — нечетное и $3 < u < n-1$.

Из леммы 2.4 вытекает, что в случае трех образующих обязательно выполнено $u_2 = n + 1$, $u_1 < n + 1$, $u_3 > n + 1$. Так как степень

каждой вершины цикла равна 2, то образующим обязательно соответствует ровно два ненулевых элемента матрицы A в каждой строке и в каждом столбце. Для первых $u_1 - 1$ строк по два элемента в строке гарантируют образующие u_1 и $u_2 = n + 1$, в остальных строках это должны гарантировать образующие $u_2 = n + 1$ и u_3 . Пусть n будет нечетным. В этом случае $u_2 = n + 1$ является четным числом, поэтому элемент $a_{ii} = 0$, где $i = (n + 1)/2$. С другой стороны, в этой строке должно быть два ненулевых элемента, что возможно только при условии $a_{i1} = u_1$, $a_{in} = u_3$. Из этого вытекают два соотношения:

$$\begin{aligned}(n+1)/2 + 1 &= u_1, \\ (n+1)/2 + n &= u_3.\end{aligned}$$

Отсюда получаем $u_1 = (n + 3)/2$, $u_3 = (3n + 1)/2$. Чтобы в остальных строках было ровно два ненулевых элемента, необходимо чтобы u_1 и u_3 были нечетными, поэтому

$$(n + 3)/2 = u_1 = 2k + 1 \quad (k > 1).$$

Отсюда получаем $n = 4k - 1 \equiv 3 \pmod{4}$, а $u_3 = 6k - 1$ и тоже нечетное.

Пусть теперь n — четное, тогда $u_2 = n + 1$ — нечетное число, что дает ровно по одному ненулевому элементу в каждой строке матрицы образующих. Если вычеркнуть первые $u_1 - 1$ строк и $u_1 - 1$ столбец из матрицы A , то в оставшейся матрице боковую диагональ должны занимать элементы, соответствующие образующей u_3 , что равносильно $u_3 = n + u_1$. Число ребер в цикле равно n , поэтому необходимо выполнение условия

$$r_n(u_1) + r_n(n + 1) + r_n(n + u_1) = 2n. \quad (2.20)$$

Для проверки в уравнение (2.20) подставляем выражения (2.15) и (2.16):

$$2 \left\lfloor \frac{u_1 - 1}{2} \right\rfloor + n + 2 \left\lfloor \frac{n - |n + 1 - n - u_1|}{2} \right\rfloor = 2 \left\lfloor \frac{u_1 - 1}{2} \right\rfloor + n + n + 2 \left\lfloor \frac{-|u_1 - 1|}{2} \right\rfloor.$$

Это выражение будет равным $2n$ только при равенстве

$$\left\lfloor \frac{-|u_1 - 1|}{2} \right\rfloor = - \left\lfloor \frac{u_1 - 1}{2} \right\rfloor,$$

что возможно только при u_1 нечетном.

Двойственное множество имеет вид

$$U' = \{n + 2 - u, n + 1, 2n + 2 - u\}.$$

Существование представлений C_n для n четных с помощью трех образующих показано в работах [25—27].

Для $n < 4$ кодирование фактороидов с помощью трех образующих почти единственно. Для $n = 3$ это $U = \{3, 4, 5\}$, для $n = 4$ это $U_1 = \{3, 5, 7\}$ и $U_2 = \{4, 5, 6\}$. Рассмотрим теперь NA -графы с четырьмя образующими.

Теорема 2.4. Для того чтобы NA -граф с нечетным количеством вершин ($n > 3$) представлял собой фактороид с помощью четырех образующих, необходимо и достаточно, чтобы они составляли два типа однопараметрических множеств:

$$U_1 = \{u, 2(u - 1), n + u - 1, n + 2(u - 1)\},$$

где u — нечетное и $3 < u < (n + 1)/2$,

$$U_2 = \{u, (n + u)/2 + 1, n + u, (3n + u)/2\},$$

где $u \equiv -n \pmod{4}$ и $3 \leq u \leq n - 2$.

Покажем, что u_1 не может быть четным. Если u_1 — четное, то $a_{ii} = 0$, где $i = u_1/2$. В этой строке должны быть два ненулевых элемента, принадлежащие множеству U . Пусть это $u_2 = i + k_1$ и $u_3 = i + k_2$. Но тогда в $(i + 1)$ -й строке вершина $(u_1/2 + 1)$ смежна с тремя вершинами $(u_1/2 - 1)$, $(k_1 - 1)$ и $(k_2 - 1)$ (эти вершины существуют, так как $u_1 < u_2 < u_3$), что невозможно. Относительно u_2 можно заметить, что оно может быть произвольным. Пусть u_2 будет четным. На пересечении $(u/2, u/2)$ в матрице A стоит 0. В этой же строке отличные от нуля элементы равны u_j и u_i , что означает, что вершина $(u_2/2 + 1)$ смежна с вершинами $(u_2/2 - 1)$, $(u_i - u_2/2 - 1)$, $(u_j - u_2/2 - 1)$, а это невозможно. Отсюда можно сделать вывод, что одна из указанных вершин должна превращаться в 0, т. е. $u_i - u_2/2 - 1 = 0$. Но это возможно только при $i = 1$, откуда

$$u_2 = 2(u_1 - 1).$$

С другой стороны, в $(u_2/2 - 1)$ -й строке два необходимых элемента уже равны u_1 и u_2 , поэтому первый элемент, равный u_3 , появляется только в $(u_2/2)$ -й строке и n -м столбце, т. е. $u_3 = u_2/2 + n = n + u_1 - 1$. Теперь и u_4 определяются однозначно: $u_4 = n + 2(u_1 - 1)$. Для контроля проверим равенство (2.20). Подставим в него выражения (2.15) и (2.16):

$$2 \left\lfloor \frac{u_1 - 1}{2} \right\rfloor + 2 \left\lfloor \frac{2(u_1 - 1) - 1}{2} \right\rfloor + 2 \left\lfloor \frac{n - |n + 1 - n - u_1 + 1|}{2} \right\rfloor +$$

$$+2 \left\lfloor \frac{n - |n + 1 - n - 2(u_1 - 1)|}{2} \right\rfloor = u - 1 + 2(u - 2) + 2 \left\lfloor \frac{n + 1 - (u_1 - 1)}{2} \right\rfloor +$$

$$+ 2 \left\lfloor \frac{n + 1}{2} - (u_1 - 1) \right\rfloor = 3(u_1 - 1) - 2 + n + 1 - (u_1 - 1) + n + 1 - 2(u_1 - 1) = 2n.$$

Получаем множество образующих, зависящее от одного параметра. Так как $u_4 \leq 2n - 1$, то имеем $n + 2(u_1 - 1) \leq 2n - 1$ и $u_1 \leq (n + 1)/2$. Далее, так как $u_1 = 2k + 1$ ($k \geq 1$), то получаем $u_1 \leq 2\lfloor (n - 1)/4 \rfloor + 1$.

Таким образом, при четном u_2 фактороид можно представить однопараметрическим множеством $U_1 = \{u, 2(u - 1), n + u - 1, n + 2(u - 1)\}$, где u — нечетное и $3 \leq u \leq 2\lfloor (n - 1)/4 \rfloor + 1$. При этом двойственное множество имеет вид $U'_1 = \{n + 4 - 2u, n + 3 - u, 2(n + 2 - u), 2n + 2 - u\}$.

Пусть u_2 — нечетное. Тогда в первых $(u_1 - 1)$ строках есть ровно по два ненулевых элемента, что и требуется. Чтобы в u_1 -й строке было два ненулевых элемента, необходимо, чтобы $u_3 = n + u_1$, а это есть четное число. Тогда для $i = u_3/2$ в матрице $a_{ii} = 0$. В i -й строке два ненулевых элемента могут быть только в первом и последнем столбце, что дает две зависимости: $u_2 = u_3/2 + 1$ и $u_4 + 1 = u_3/2 + n$. В результате получаем новое однопараметрическое множество образующих: $U_2 = \{u_1, n + u_1/2 + 1, n + u_1, (3n + u_1)/2\}$. Так как $u_4 \leq 2n - 1$, то $(3n + u_1)/2 \leq 2n - 1$ и $u_1 \leq n - 2$.

С другой стороны, u_2 — нечетное, поэтому $(n + 1)/2 + 1 = 2k + 1$, или $n + u = 4k$, откуда $u_1 = -n \pmod{4}$. Это означает, что минимальное $u_1 = 3$ для $n \equiv 1 \pmod{4}$ и $u_1 = 5$, иначе $u_1 = n \pmod{4} + 2$ для $n \equiv 3 \pmod{4}$. Остается проверить формулу (2.16) для u_2 :

$$2 \left\lfloor \frac{u_1 - 1}{2} \right\rfloor + 2 \left\lfloor \frac{n + u_1}{2} \right\rfloor + 2 \left\lfloor \frac{n - |n + 1 - n - u_1|}{2} \right\rfloor +$$

$$+ 2 \left\lfloor \frac{n - |n + 1 - (3n + u_1)/2|}{2} \right\rfloor = u_1 - 1 + (n + u_1)/2 + 2 \left\lfloor \frac{n - u_1 + 1}{2} \right\rfloor +$$

$$+ 2 \left\lfloor \frac{n - u_1 + 2}{2} \right\rfloor = u_1 - 1 + (n + u_1)/2 + n - u_1 + (n - u_1)/2 + 1 = 2n.$$

Двойственное множество для U_2 имеет вид

$$U'_2 = \{(n - u)/2 + 2, n - u + 2, (3n + u)/2 - 1, 2n + 2 - u\}.$$

Существование представлений для C_n при нечетных n с помощью четырех образующих показано в работах [12, 13, 16].

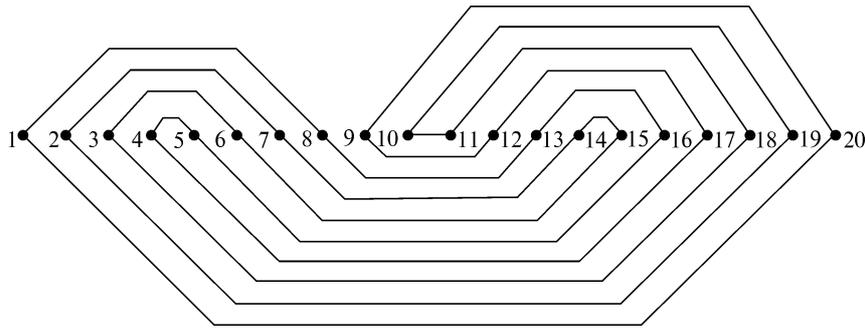


Рис. 2.9

На рис.2.9 изображен граф из 20 вершин с множеством образующих $U = \{9, 21, 29\}$. Граф представляет собой два равновеликих цикла длиной десять: $C_{10}^{(1)} = (1, 8, 13, 16, 5, 4, 17, 12, 9, 20)$ и $C_{10}^{(2)} = (2, 7, 14, 15, 6, 3, 18, 11, 10, 19)$.

Полный ответ о структуре графа с четным числом вершин для произвольного параметра множества образующих дает следующая теорема.

Теорема 2.5. Для того чтобы NA -граф с четным количеством вершин представлял факториод с помощью четырех образующих, необходимо и достаточно, чтобы они составляли или единственное множество $U_1 = \{(n + 5)/3, (2n + 4)/3, (4n + 2)/3, (5n + 1)/3\}$ для $n \equiv 4 \pmod{6}$, или множество, зависящее от двух параметров $U_2 = \{u, v, n + u, n + v\}$, где u, v — нечетные числа и $3 \leq u < v \leq n - 1$.

Так же, как и в теореме 2.4, доказывается, что u является нечетным числом. Относительно v нельзя утверждать того же. Если предположить, что v — четное, то на месте элемента a_{iv} , где $i = v/2$, будет нуль. Для компенсации этого нулевого элемента необходимо, чтобы $v = 2(u - 1)$ и $u_3 = n + u - 1$. Но тогда u_3 — четное число и элемент $a_{ij} = 0$, где $j = (n + u - 1)/2$. Чтобы граф был однородным степени 2, что соответствует факториоду, необходимо выполнение условия

$$(n + u - 1)/2 = 2(u - 1) - 1.$$

Отсюда находим $u = (n + 5)/3 = 2k + 1$ ($k \geq 1$), так как u — нечетное. Это возможно только при $n = 6k - 2$ или $n \equiv 4 \pmod{6}$. В результате получаем единственное множество образующих:

$$U = \{(n + 5)/3, (2n + 4)/3, (4n + 2)/3, (5n + 1)/3\}.$$

Пусть v — нечетное. Тогда для u и для v остаются единственные образующие $n+u$ и $n+v$, которые дополняют их до однородности графа. Кроме того, они являются нечетными числами, что не приводит к появлению нулевых элементов на диагонали. Этим и завершается доказательство теоремы.

Лемма 2.5. Множества из трех образующих NA -графов, представляющих фактороиды, являются двойственными самим себе.

Для нечетного n это проверяется непосредственно, так как U здесь единственное:

$$2n + 2 - u_1 = 2n + 2 - (n + 3)/2 = (3n + 1)/2 = u_3 = u'_1.$$

Далее $u_2 = u'_2$, а $u_1 = u'_3$ по аналогии.

Пусть теперь n — четное. Если $u_1 = 3$, то $u'_1 = n - 1$. При возрастании u_1 от 3 до $n - 1$ u'_1 соответственно убывает от $n - 1$ до 3. Поскольку $u_2 = u'_2$, то аналогично ведут себя u_3 и u'_3 . Это позволяет рассматривать только те фактороиды, у которых $u_1 \leq u'_1$, т. е. $u \leq n + 2 - u$, что дает $u \leq n/2 + 1$.

Таким образом, при перечислении всех фактороидов NA -графов с тремя образующими можно указывать только половину множества U (т. е. $3 \leq u \leq n/2 + 1$).

Лемма 2.6. Два однопараметрических множества из четырех образующих для нечетного числа вершин находятся в соотношении $U_1 = U'_2$; $U_2 = U'_1$. Для четного числа вершин двухпараметрическое множество из четырех образующих с параметрами (u, v) двойственно множеству с параметрами $(n + 2 - v, n + 2 - u)$.

Предположим сначала, что n — нечетное. Тогда, если $u_1 = 3$, то $U'_1 = \{n - 2, n, 2n - 2, 2n - 1\}$, что соответствует U_2 для $u_1 = n - 2$. Если u_1 увеличивается в U_1 , то u_1 в U_2 убывает. Проверим соответствие для максимального u_1 . Пусть $n = 4l + 1$. Тогда $u_1 = 2l + 1$, $U'_1 = \{3, 2l + 3, 4l + 4, 6l + 3\}$, что соответствует U_2 , если подставить $u_1 = 3$. Аналогично для $n = 4l + 3$ получаем $u_1 = 2l + 1$, и тогда $U'_1 = \{5, 2l + 5, 4l + 8, 6l + 7\}$, что соответствует U_2 , если подставить $u_1 = 5$.

Пусть теперь n — четное. Двойственное множество образующих $U' = \{2n + 2 - u, 2n + 2 - v, n + 2 - u, n + 2 - v\}$. Если его упорядочить, полагая $v > u$, то получим $U' = \{n + 2 - v, n + 2 - u, 2n + 2 - v, n + 2 - v\}$. Если теперь подставить в исходное множество $u = n + 2 - v$, $v = n + 2 - u$, то получим U' .

Все множества, у которых $u + v = n + 2$, являются самодвойственными.

Таким образом, при перечислении фактороидов, представленных четырьмя образующими, для нечетного n необходимо перечислять только U_1 для всего интервала изменения параметра u , а для четного n — только параметры (u, v) , для которых $u + v \leq n + 2$.

Легко показать, что единственное множество образующих для $n \equiv 4 \pmod{6}$ является самодвойственным.

Поскольку u_1 во всех множествах образующих — нечетное, будем его представлять в виде $u_1 = 2s + 1$ ($s \geq 1$).

Для трех образующих число фактороидов определяет следующая теорема

Теорема 2.6. Множество образующих $U = \{2s + 1, n + 1, n + 2s + 1\}$ ($1 \leq s \leq n/2 - 1$) для четного n представляет набор из k циклов длиной n/k , где $k = \text{НОД}^*[s, n/2]$.

Доказательство. Предположим, что выполняются условия теоремы и $s = kl$, $n = 2km$, где l и m — взаимно простые числа и пусть $l < m$. Рассмотрим цепь, которая начинается в вершине α , где $1 \leq \alpha \leq k$. С помощью образующей $u = 2s + 1$ эта вершина соединяется с вершиной $u - \alpha = 2kl - \alpha + 1$. Далее с помощью образующей $n + 1 = 2km + 1$ вершина $u - \alpha$ соединяется с вершиной $2k(m - l) + \alpha$. Затем эта вершина с помощью образующей $n + u = 2k(m + l) + 1$ соединяется с вершиной $4kl - \alpha + 1$. Обозначим $f_1(p) = 2klp - \alpha + 1$ и $f_2(p) = 2k(m - lp) - \alpha$. Тогда в результате последовательного продвижения с помощью образующих $n + u$ и $n + 1$ получаем чередующуюся последовательность $f_2(0), f_1(1), f_2(1), f_1(2), f_2(2), \dots$. Все аргументы типа $pl > m$ записываем по наименьшему абсолютному вычету по модулю m . В этом смысле иногда применяется образующая $u \equiv (n + u) \pmod{2m}$. Так как l и m — взаимно простые, то после конечного числа шагов мы получаем замыкание последовательности $f_2(m) = f_2(0)$, что равносильно замыканию цикла длиной $2m$. То же самое получаем для других значений α . Поскольку всюду присутствует множитель $2k$, то все числа α и $-\alpha + 1$ будут разными, и таких пар будет ровно k , что обуславливает разбиение всех вершин NA -графа на k циклов длиной $2m$ или n/k .

При доказательстве теоремы использовались все значения параметра u в диапазоне от 3 до $n - 1$. Как было показано ранее, можно использовать только образующие, равные $\min\{u, n + 2 - u\}$. Непосредственно видно, что $(u - 1)/2 = s$ и $(n + 2 - u - 1)/2 = n/2 - s$ имеют одинаковый наибольший общий делитель с числом $n/2$.

* НОД — наибольший общий делитель.

Нетрудно показать, что для нечетного n три образующие представляют один цикл длиной 3 по вершинам $\{1, n, (n+1)/2\}$ и $(n-3)/4$ циклов длиной 4. Для четырех образующих структура фактороидов будет описана в следующих теоремах.

Теорема 2.7. Множество $U = \{2p+1, 2r+1, n+2p+1, n+2r+1\}$ ($1 \leq p < r < n/2 - 1$) для четного n представляет набор k циклов длиной n/k , где $k = \text{НОД}(r-p, n/2)$.

Доказательство. Обозначим $\delta = 2(r-p)$ и $\lambda = n/k$. Построим таблицу (b_{ij}) размером $k \times \lambda$. В первой строке расположим элементы $p, p+1, p+\delta, p+1-\delta, p+2\delta, \dots, p + [\lambda/2 - 1]\delta, p+1 - [\lambda/2 - 1]\delta$. При этом сложение и вычитание проводится по модулю n с положительными вычетами. В i -й ($i > 1$) строке поместим элементы $b_{ij} = b_{1j} - i + 1$ для $j \equiv 1 \pmod{2}$ и $b_{ij} = b_{1j} + i - 1$ для $i \equiv 0 \pmod{2}$. В результате получаем таблицу, в которой все элементы разные и они принимают все значения от 1 до n . Действительно, первые два столбца — разные, а остальные столбцы отличаются друг от друга на величину $\delta \geq 2k$, а каждый столбец имеет диапазон значений, не превышающий k .

Сумма произвольных соседних элементов любой строки равна либо $2p+1$, либо $2p+1+\delta = 2r+1$. Сумма крайних значений равна $p+p+1-\lambda\delta/2+\delta = 2p+1-n(\delta/2k)+2(r-p) = 2r+1-\alpha n \equiv (2r+1) \pmod{n}$. Это означает, что каждая строка представляет собой цикл, а множество образующих — набор циклов длиной $2n/k$.

Для $n \equiv 4 \pmod{6}$ можно представить еще один фактороид $U = \{(n+5)/3, (2n+4)/3, (4n+2)/3, (5n+1)/3\}$. Структура такого графа проста: он состоит из одного цикла длиной 4 по вершинам $\{1, (2n+1)/3, n, (n+2)/3\}$ и $(n-4)/6$ циклов длиной 6.

Для нечетных n возникает такая же проблема, когда при определенных соотношениях параметров граф с данным множеством образующих будет представлять несколько циклов. Решение этой проблемы дает следующая теорема.

Теорема 2.8. Множество образующих $U = \{2s+1, 4s, n+2s, n+4s\}$ ($1 \leq s \leq \lfloor (n-1)/4 \rfloor$) для нечетного n представляет набор $k-1$ циклов длиной $(n+1)/k$ и один цикл длиной $(n+1)/k-1$, где $k = \text{НОД}[s, (n+1)/2]$.

Доказательство. Рассмотрим вершину графа (рис. 2.10, а) с номером $2s$. Она смежна с вершинами 1 и n . Возьмем и расцепим ее на две вершины с номерами $2s$ и $2s+1$, а все остальные с большим номером увеличим на 1. Общее число вершин в графе составит $n' = n+1$ (рис. 2.10, б). Этот граф останется NA -графом, если взять в качестве образующих $U' = \{2s+1, 4s+1, n'+2s+1,$

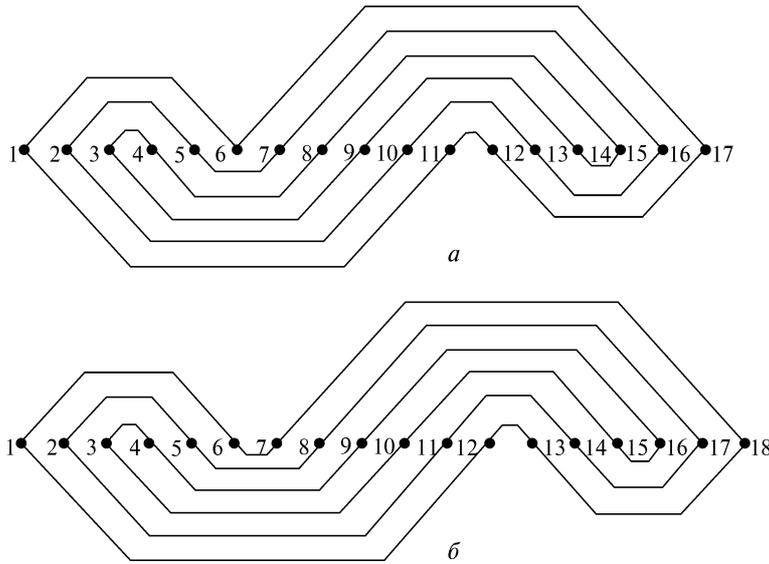


Рис. 2.10

$n' + 4s + 1$ }, в чем нетрудно убедиться непосредственно. В результате получаем NA -граф с четным числом вершин n . К нему можно применить теорему 2.7, для чего приравняем $p = s$, $r = 2s$. Тогда $k = \text{НОД}(2s - s, n'/2) = \text{НОД}[s, (n + 1)/2]$ и справедливость теоремы 2.8 вытекает из теоремы 2.7. Если теперь вернуться к исходному графу, отождествив вершины $2s$ и $2s + 1$, то получим один цикл длиной $(n + 1)/k - 1$, что и требовалось доказать.

Эта теорема сформулирована только для одного семейства образующих. Учитывая, что второе семейство является сопряженным к первому, из теоремы 2.8 можно вывести следствие.

Следствие. Множество образующих произвольного NA -графа $U = \{u, (n + u)/2 + 1, n + u, (3n + u)/2\}$, где $u \equiv -n \pmod{4}$, а $n \pmod{4} + 2 \leq u \leq n - 2$ для нечетного n , представляет набор $k - 1$ циклов длиной $(n + 1)/k$ и один цикл длиной $(n + 1)/k - 1$, где $k = \text{НОД}\{(n + 2 - u)/4, (n + 1)/2\}$.

Действительно, двойственное множество к U из теоремы 2.7 $U' = \{n + 2 - 4s, n + 2 - 2s, 2n + 2 - 4s, 2n + 1 - 2s\}$, откуда $u = n + 2 - 4s$ и $s = (n + 2 - u)/4$.

Особый интерес вызывает вопрос о существовании гамильтонова цикла. Для NA -графов с четным n ответ на этот вопрос дает следующая лемма.

Лемма 2.7. Множество образующих $U = \{2s + 1, n + 1, n + 2s + 1\}$ для четного n при изменении s от 1 до $n/2 - 1$ представляет $\varphi(n/2)$ гамильтоновых циклов, где $\varphi(Z)$ — функция Эйлера, равная количеству чисел, взаимно простых с Z и не превышающих его.

Действительно, образующие представляют гамильтонов цикл, если $\varphi = \text{НОД}[s, n/2] = 1$. Так как s пробегает все значения от 1 до $n/2 - 1$, то s будет принимать значение 1 ровно $\varphi(n/2)$ раз.

Для четырех образующих с нечетным числом вершин такой вывод сделать нельзя, так как там параметр s пробегает значения от 1 до $\lfloor (n - 1)/4 \rfloor$. Гамильтонов цикл будет представлен тогда, когда s и $(n + 1)/2$ взаимно простые числа.

По теореме 2.8 два NA -графа с четным числом вершин, у которых образующие имеют вид $U_1 = \{2p_1 + 1, 2r_1 + 1, n + 2p_1 + 1, n + 2r_1 + 1\}$ и $U_2 = \{2p_2 + 1, 2r_2 + 1, n + 2p_2 + 1, n + 2r_2 + 1\}$, изоморфны, если $\text{НОД}(r_1 - p_1, r_2 - p_2) = \text{НОД}(r_1 - p_1, n/2)$.

Таким образом, граф будет гамильтоновым, если $r_1 - p_1$ и $n/2$ — взаимно простые числа.

2.5. ПРЕДСТАВЛЕНИЕ НАБОРА ЦЕПЕЙ

При оптимальном представлении цепей коды вершин образуют две чередующиеся арифметические прогрессии с общей разностью, при этом достаточно двух образующих [38]. Этим же свойством обладает и оптимальное представление (кодирование) набора цепей.

Определение 2.6. Спецификацией n -вершинного набора k цепей называется множество $L = [l_1^{\alpha_1}, l_2^{\alpha_2}, \dots, l_k^{\alpha_k}]$, где α_i — число цепей, имеющих l_i вершин ($i = 1, 2, \dots, k$), удовлетворяющее системе уравнений

$$\sum_{i=1}^k \alpha_i = m, \quad \sum_{i=1}^k \alpha_i l_i = n. \quad (2.21)$$

В работе [38] доказано, что при определенных условиях такой набор цепей можно представить в виде натурального арифметического графа, используя лишь две образующих. Коды вершин образуют чередующиеся арифметические прогрессии — возрастающую и убывающую с общей разностью d , которая может быть равна $2m, 2m - 1, 2m - 2$.

Обозначим $\lambda = \left\lfloor \frac{n}{d} \right\rfloor$.

Теорема 2.9. Набор из m цепей может быть представлен в классе n -вершинных NA -графов с помощью двух образующих в том и только в том случае, если он имеет спецификацию

$$L = [(2\lambda + 2)^{\alpha_1}, (2\lambda + 1)^{\alpha_2}, (2\lambda)^{\alpha_3}, (\lambda + 1)^{\alpha_4}, (\lambda)^{\alpha_5}],$$

где $\alpha_1, \alpha_2, \alpha_3$ — произвольные, а для α_4 и α_5 выполняется одно из условий:

- 1) $\alpha_4 = \alpha_5 = 0$,
- 2) $\alpha_4 + \alpha_5 = 1$,
- 3) $\alpha_4 + \alpha_5 = 2$, при этом $\alpha_4(\alpha_5)$ может быть равным 2, если $n \pmod{(2m - 2)} \geq m (\leq m)$.

Рассмотрим все значения, которые могут принимать d, α_1, α_2 и α_3 . Определим условия, когда набор цепей с заданной спецификацией может быть представлен с помощью двух образующих. Эти образующие либо обе нечетные, либо разной четности, либо обе четные.

А. Пусть $u_1 = 2k + 1, u_2 = 2l + 1 (l > k > 1)$.

Чтобы эти образующие представляли набор из m цепей, необходимо, чтобы в матрице образующих данного графа ровно $2m$ строк содержали один ненулевой элемент, а остальные $n - 2m$ строк — ровно по два ненулевых элемента. Это возможно только при условии

$$u_2 - u_1 = 2m = 2(l - k). \quad (2.22)$$

Возьмем цепь, у которой наименьший номер есть γ . С помощью двух образующих эта цепь нумеруется далее следующим образом:

$$\gamma, u_1 - \gamma, (u_2 - u_1) + \gamma, u_1 - \gamma - (u_2 - u_1), 2(u_2 - u_1) + \gamma, \dots$$

Вершины с нечетными местами в этой последовательности образуют возрастающую арифметическую прогрессию с начальным элементом γ и разностью $u_2 - u_1 = 2m$, а вершины на четных местах — убывающую арифметическую прогрессию с начальным элементом $u_1 - \gamma$ и с такой же разностью.

Разобьем множество чисел от 1 до n на d классов $\{S_i\}_1^d$, где $S_i = \{p/p \equiv i \pmod{d}, 1 \leq p \leq n\}$. Расположим все эти числа в виде таблицы в порядке возрастания классов от S_1 до S_d . В первой строке будут находиться числа от 1 до $2m$, во второй — от $2m + 1$ до $4m$ и т. д. Пусть $\beta = n \pmod{2m}$, тогда λ строк будут содержать по $2m$ элементов, а в $(\lambda + 1)$ -й строке будут находиться β чисел от $2m\lambda + 1$ до n . Таким образом, составленная таблица содержит

β столбцов из $\lambda + 1$ чисел и $2m - \beta$ столбцов из λ чисел. Цепям длиной $2\lambda + 2$ поставим в соответствие $2\alpha_1$ первых столбцов таблицы, цепям длиной $2\lambda + 1 - \alpha_2$ столбцов высотой $\lambda + 1$ и α_2 столбцов высотой λ , а цепям длиной $2\lambda - 2\alpha_3$ столбцов высотой λ . Из этого вытекает, что имеет место система уравнений

$$\begin{aligned} 2\alpha_1 + \alpha_2 &= n(\bmod 2m) = \beta, \\ 2\alpha_3 + \alpha_2 &= 2m - \beta. \end{aligned} \quad (2.23)$$

Очевидно, что $\max\alpha_2 = \min\{\beta, 2m - \beta\}$, а $\min\alpha_2 = n(\bmod 2)$.

Из (2.22) следует, что $u_1 \equiv u_2(\bmod 2m)$, а из (2.23) — что сумма двух соседних кодов любой цепи равна $u_1(\bmod 2m)$. Так как u_1 — нечетное число, то все представления набора цепей сводятся к решению уравнения

$$i + j \equiv (2q + 1)(\bmod 2m) \quad (q = 1, 2, \dots, m), \quad (2.24)$$

где i и j — номера соответствующих классов S_i и S_j .

Решением уравнения (2.24) являются m пар, часть из которых в сумме дает $2q + 1$, а часть — $2m + 2q + 1$. Если $\alpha_2 \neq 0$, то кодировка определяется однозначно по нечетной цепи. В зависимости от образующих этой цепи получаем однозначную кодировку и для других цепей, которая может быть как верхней, так и нижней.

Подставляя значения q в (2.24) в порядке возрастания, можно получить все решения уравнения, и тем самым провести полный перебор всех представлений графа. Однако качественная картина при этом не очень проясняется. Рассмотрим решения в порядке возрастания меньшей образующей u_1 . Пусть $\alpha_2 \neq 0$, что равносильно $n(\bmod 2) \equiv \beta(\bmod 2) \equiv 1$. В уравнении (2.24) первый столбец всегда используется в паре со столбцом $2q$. Наименьшее значение u_1 будет принимать тогда, когда q имеет наименьшее значение для $2q > \beta$. Это означает, что должен использоваться самый левый столбец длиной λ , а именно $2q = \beta + 1$. Тогда получаем

$$u_1 = \beta + 2 + 2m(\lambda - 1); \quad u_2 = \beta + 2 + 2m\lambda. \quad (2.25)$$

Так как $n = 2m\lambda + n(\bmod 2m)$ или $n = 2m\lambda + \beta$, то

$$u_1 = n + 2 - 2m; \quad u_2 = n + 2. \quad (2.26)$$

Если теперь в таблице выбирать числа, следующие за $n + 1 - 2m$ через одно, пока не дойдем до $n - 1$, то получим все значения u_1 без 1 в порядке возрастания. В уравнении (2.24) им будут соответствовать значения q , начиная с $(\beta + 1)/2$ и больше, а заканчивая

$(\beta - 1)/2 \pmod{2m}$. Как уже отмечалось, все уравнения, кроме одного для $q = t$, делят все столбцы таблицы на две группы. В левой группе левая часть уравнения (2.24) не превышает $2m$, а в правой группе — превышает это значение. Рассмотрим динамику изменения значений u_1 . Здесь существует различие.

1) $n \pmod{2m} = \beta \leq t$.

Для начального значения $q = (\beta + 1)/2$ получаем решение системы (2.23): $\alpha_2 = 1$; $\alpha_1 = (\beta - 1)/2$; $\alpha_3 = t - (\beta - 1)/2$. В этом случае для кодировок цепей и в левой, и в правой группах применяется нижняя кодировка. Действительно, при верхней кодировке в левой группе для столбцов 2 и β получаем

$$u_1 = 2 + \beta + 2m\lambda; u_2 = 2 + \beta + 2m(\lambda - 1).$$

Это на $2m$ больше, чем в (2.26), поэтому нужно использовать нижнюю кодировку. Также и в правой группе при верхней кодировке для столбцов $\beta + 2$ и $2m$ имеем

$$u_1 = \beta + 2 + 2m\lambda; u_2 = \beta + 2 + 2m\lambda + 2m.$$

Следовательно, в обеих группах необходимо использовать нижнюю кодировку. При увеличении u_1 значение α_1 будет убывать и при $q = \beta$ получаем $\alpha_1 = 0$, $\alpha_2 = \beta$, $\alpha_3 = t - \beta$. Дальнейшее увеличение q обуславливает всегда одно и то же решение, но левая группа таблицы будет увеличиваться за счет появления в ней столбцов, дающих решение для α_3 . Их номера будут превышать β .

Покажем, что для этих столбцов нужно уже применять верхнюю кодировку, в отличие от таких же столбцов в правой группе таблицы.

Возьмем столбцы q и $q + 1$ ($q > \beta$):

$$u_1 = q + q + 1 + 2m(\lambda - 1); u_2 = 2q + 1 + 2m\lambda.$$

В правой группе верхней кодировкой для столбцов $2q + 1$ и $2m$ получаем

$$u_1 = 2q + 1 + 2m\lambda; u_2 = 2q + 1 + 2m(\lambda + 1).$$

Значит, надо выбрать нижнюю кодировку. При $q = t$ правая группа исчезает, таблица состоит из одной группы. Далее следует $q = 1$, и появляется левая группа. Теперь в обеих группах применяется верхняя кодировка. Покажем это на примере столбцов q и $q + 1$, где $q < (\beta + 1)/2$:

$$u_1 = q + q + 1 + 2m\lambda; u_2 = 2q + 1 + 2m(\lambda + 1).$$

В правой группе для столбцов $2q + 1$ и $2m$ верхней кодировкой получаем $u_1 = 2q + 1 + 2m\lambda$. Это соответствует верхней кодировке в обеих группах. И так будет выполняться для оставшихся значений q .

$$2) n(\bmod 2m) = \beta \geq m.$$

Здесь картина несколько отличается от случая 1, но можно проследить и аналогию. Убеждаемся, что и здесь при возрастании q от $(\beta + 1)/2$ до m в левой и правой группах таблицы нужно использовать нижнюю кодировку. Затем правая группа исчезает и при значениях q от 1 до $\beta - m$ параметры уравнения (2.23) становятся постоянными: $\alpha_2 = 2m - \beta$, $\alpha_3 = 0$, $\alpha_1 = \beta - m$. При этом появляется левая группа, столбцы которой дают значения для α_1 , как и столбцы правой группы. Нетрудно показать, что в левой группе нужно применять верхнюю кодировку, а в правой должна оставаться нижняя кодировка. После $q > \beta - m$ в правой группе столбцы, дающие значения для α_1 , исчезают и появляются столбцы, дающие значения параметру α_3 . При этом в обеих группах применяется верхняя кодировка.

Число решений уравнения (2.24) получилось равным m . Осталось рассмотреть случай, когда α_2 может быть равным 0, т. е. $n \equiv 0(\bmod 2)$.

Здесь минимальное значение u_1 принимает при $\alpha_2 = 0$. Тогда все цепи имеют четную длину и возможны обе кодировки — нижняя и верхняя. Минимальное значение u_1 принимает при $q = \beta/2$ и нижней кодировке, т. е. $u_1 = 2m\lambda + 1 + \beta - 2m$ или $u_1 = n + 1 - 2m$. Затем u_1 , увеличиваясь на 2, возрастает и максимальное значение принимает при том же $q = \beta/2$, но уже для верхней кодировки, т. е. $\max u_1 = n + 1$. Тогда число представлений будет равным $m + 1$.

Среди множеств образующих, представляющих набор цепей, обязательно есть двойственные им. Нетрудно установить справедливость следующей леммы.

Лемма 2.8. Решения уравнения

$$i + j \equiv \{n + 1 \pm [2q + n(\bmod 2)]\}(\bmod 2m) \quad (2.27)$$

являются двойственными при различных знаках в правой части для $q = 0, 1, \dots, [m/2] - n(\bmod 2)$.

То, что образующие являются двойственными для разных знаков, видно непосредственно, так как их сумма равна $2n + 2$. Если $n \equiv 1(\bmod 2)$, то правая часть дает ровно m решений, как и должно быть. Если $n \equiv 0(\bmod 2)$, то при $q = 0$ получают два решения, что соответствует нижней и верхней кодировкам, которые, к тому же, оказываются двойственными для соответствующих об-

разующих. Если $q = [m/2]$, то для нечетных m получаются две пары образующих, а для четного m , поскольку $m \equiv -m \pmod{2m}$ — только одна пара образующих. Тогда она будет самодвойственной.

Таким образом, для произвольных n при $d = 2m$ получается $m + 1 + n \pmod{2}$ представлений.

Б. Пусть образующие равны $2k$ и $2l + 1$ ($l > 1, k > 2$). Тогда в матрице образующих $\alpha_{kk} = 0$ и в k -й строке имеется только один ненулевой элемент. Так как таких строк должно быть ровно $2m$, то

$$|u_2 - u_1| = 2m - 1. \quad (2.28)$$

Здесь также можно закодировать цепь с помощью последовательности типа (2.26). Она также состоит из двух арифметических прогрессий с одной и той же разностью $d = 2m - 1$.

Разобьем все числа от 1 до n на d классов $\{S_i\}_1^d$, где $S_i = \{p/p = i \pmod{d}\}$, $1 \leq p \leq n$. Составим соответствующую таблицу, в которой первая строка содержит числа от 1 до $2m - 1$, вторая — от $2m$ до $4m - 2$ и т. д. Ровно λ строк будут состоять из $2m - 1$ элементов, а $(\lambda + 1)$ -я строка — из β элементов, где $\beta = n \pmod{2m - 1}$, а именно: $2m\lambda - \lambda + 1, 2m\lambda - \lambda + 2, \dots, n$. Вся таблица будет состоять из β столбцов по $\lambda + 1$ элементов и $2m - \beta - 1$ столбцов по λ элементов. Как и в случае А, цепям длиной $2\lambda + 2$ поставим в соответствие $2\alpha_1$ столбцов высотой $\lambda + 1$, цепям длиной $2\lambda + 1$ — α_2 столбцов высотой $\lambda + 1$ и α_2 столбцов высотой λ , цепям длиной $2\lambda - 2\alpha_3$ столбцов высотой λ . Кроме того, одна цепь будет иметь длину $\lambda + 1$ или λ . Это значит, что имеет место система уравнений

$$\begin{aligned} 2\alpha_1 + \alpha_2 + \alpha_4 &= n \pmod{d} = \beta; \\ 2\alpha_3 + \alpha_2 + \alpha_5 &= 2m - \beta - 1; \\ \alpha_4 + \alpha_5 &= 1. \end{aligned} \quad (2.29)$$

Из (2.29) следует, что $u_2 \equiv u_1 \pmod{d}$, а из (2.23) — что сумма двух соседних кодов любой цепи равна $u_1 \pmod{d}$. Так как u_1 может быть и четным, и нечетным, то все представления набора цепей сводятся к решению уравнения

$$i + j \equiv q \pmod{2m - 1} \quad (q = 1, 2, \dots, 2m - 1), \quad (2.30)$$

где i и j — номера соответствующих классов S_i и S_j .

Любое значение q (кроме 1) разбивает столбцы таблицы на две группы: в левой группе столбцы соответствуют решению $i + j = q$, а в правой группе — решению $i + j = q + 2m - 1$. Если q — чет-

ное, то в левой группе существует столбец под номером $q/2$, который дает решение уравнению. Если q — нечетное, то такой столбец появляется в правой группе под номером $(q - 1)/2 + m$.

Рассмотрим динамику изменения образующей u_1 , когда во всех решениях зафиксирован первый столбец. Наименьшее значение u_1 будет принимать при $q = \beta + 1$, когда используется нижняя кодировка. В этом случае независимо от четности β всегда $\alpha_2 = 0$, так как все столбцы длиной $\lambda + 1$ дают решение для α_1 и α_4 . На пересечении строки λ и столбца β находится элемент $(2m - 1)(\lambda + 1) + \beta$, который с единицей первого столбца составляет u_1 :

$$u_1 = 2m\lambda - 2m - \lambda + \beta + 2.$$

Увеличивая значение q до $q = m + 1$, выбирая следующие элементы в строке λ и суммируя их с 1 из первого столбца, получаем соответствующие значения для u_1 . Очевидно, что все это время в обеих группах нужно применять нижнюю кодировку. При $q = 2$ начинаем выбирать элементы $(\lambda + 1)$ -й строки, что соответствует верхней кодировке в левой группе. Поскольку в левой группе на одну строку больше, то в правой группе также необходимо применять верхнюю кодировку. В дальнейшем, если в обеих группах появляются столбцы, дающие одновременно решения для параметра α_1 (или α_3), то в левой группе необходимо использовать верхнюю кодировку, а в правой — нижнюю. Впрочем, за этим специально следить не надо, так как образующие для цепей длиной $2\lambda + 1$, а такие цепи всегда присутствуют при $q \neq \beta + 1$, однозначно определяют тип кодировки для каждой из групп.

Лемма 2.9. Решения уравнения (2.30) являются двойственными для пар

$$q_1 + q_2 \equiv (2\beta + 2) \pmod{2m - 1}. \quad (2.31)$$

Действительно, для $q = \beta + 1$ получается кратное решение, что соответствует верхней и нижней кодировкам для таких образующих: $U = \{n + 1, n + 2m\}$ и $U' = \{n - 2m, n + 1\}$. Для других значений образующих это следует из предыдущих рассуждений.

Таким образом, для произвольных n при $d = 2m - 1$ получается $m + 1$ представление.

В. Пусть обе образующие четные: $u_1 = 2k$, $u_2 = 2l$ ($l > k$). Тогда в матрице образующих $a_{kk} = a_{ll} = 0$ и в k -й и l -й строках имеется только один ненулевой элемент. Так как всех таких элементов должно быть $2m$, то

$$u_2 - u_1 = 2m - 2 = 2(l - k). \quad (2.32)$$

Так же, как и в случаях А и Б, кодировка цепей представляет комбинацию двух арифметических прогрессий с одной и той же разностью $d = 2m - 2$. Разобьем числа от 1 до n на d классов, как и в предыдущих случаях. Так как на все цепи для кодирования не хватает по два столбца, то две цепи должны использовать только по одному столбцу. Длина этих цепей может быть одинаковой, поэтому весь набор параметров должен удовлетворять системе уравнений

$$\begin{aligned} 2\alpha_1 + \alpha_2 + \alpha_4 &= n(\bmod d) = \beta; \\ 2\alpha_3 + \alpha_2 + \alpha_5 &= 2m - \beta - 2; \\ \alpha_4 + \alpha_5 &= 2. \end{aligned} \quad (2.33)$$

Из (2.32) следует, что $u_1 \equiv u_2 \pmod{d}$, а сумма двух соседних кодов цепи равна u_1 либо u_2 . Так как u_1 и u_2 — четные числа, то все представления набора цепей сводятся к решению уравнения

$$i + j \equiv 2q \pmod{(2m-2)} \quad (q = 1, 2, \dots, m-1). \quad (2.34)$$

Любое значение q разбивает таблицу на две группы: в левой группе $i + j = 2q$, а в правой группе $i + j = 2q + 2m - 2$. В каждой из групп есть один столбец, который сам дает решение уравнения. В левой группе — столбец q , а в правой — столбец $q + m - 1$.

Зафиксируем первый столбец во всех решениях (элемент 1) и рассмотрим динамику изменения значений u_1 . Пусть $a_2 \neq 0$, что равносильно $n \equiv 0 \pmod{2}$. Минимальное значение u_1 принимает при $q = \beta/2 + 1$. Тогда элемент в строке λ и столбце $\beta + 1$ вместе с 1 дает

$$u_1 = (2m - 2)(\lambda - 1) + \beta + 2 = 2m\lambda - 2m - \lambda + \beta + 2.$$

Увеличивая значение q , будем перебирать элементы строки λ через один, пока не дойдем до столбца $2m - 3$ при $q = m - 1$. Затем переходим на $(\lambda + 1)$ -ю строку, начиная с первого столбца. Последний элемент этой строки $n - 1$ дает $u_1 = n$ при $q = \beta/2$.

Вопрос о применении нижней или верхней кодировок в этом случае также решается сам собой, так как $\alpha_2 \neq 0$ и кодировка цепей длиной $2\lambda + 1$ определяет это однозначно. Как и в предыдущих случаях, здесь наблюдается такая же картина. Пока выбираются элементы в строке λ , в левой и правой группах применяется нижняя кодировка. Если при этом в левой группе появляются столбцы, дающие решения параметру α_3 , то в левой группе применяется верхняя кодировка. Когда перебираются элементы $(\lambda + 1)$ -й строки, то в обеих группах применяется верхняя кодировка. Если же

при этом в правой группе присутствуют столбцы, которые дают решение параметру α_1 , то для них применяется нижняя кодировка.

Остается выяснить вопрос, когда может появиться решение $\alpha_4 = 0, \alpha_5 = 2$ (или $\alpha_4 = 2, \alpha_5 = 0$)? Так как разница в номерах между столбцами, дающими решение для α_4 и α_5 , равна $m - 1$, то отсюда легко сделать вывод: α_4 (α_5) может принимать значение 2, если $n(\bmod 2) = \beta \geq m(\leq m)$.

Лемма 2.10. Решения уравнения (1.52) являются двойственными для следующих пар:

$$q_1 + q_2 \equiv (\beta+1)[\bmod(m - 1)]. \quad (2.35)$$

Здесь для нечетных n получается решение $q_1 = q_2 = (\beta + 1)/2$, которое соответствует случаю при $\alpha_2 = 0$ и возможности применить нижнюю и верхнюю кодировки, которые являются двойственными. При этом $U = \{n - 2m + 3, n + 1\}$ и $U' = \{n + 1, n + 2m - 1\}$.

Для $d = 2m - 2$ число представлений равно $m + n(\bmod 2)$. В итоге, суммируя числа представлений, найденные при условиях А—В, получаем следующее следствие.

Следствие. Число представлений для (n, m) -набора цепей равно $3m + 1$.

2.6. ОДНОРОДНЫЕ НАТУРАЛЬНЫЕ АРИФМЕТИЧЕСКИЕ ГРАФЫ

Рассмотрим условия, при которых натуральный граф будет однородным (регулярным), когда степени всех его вершин равны числу $\rho \geq 1$. Частичные результаты, когда натуральные графы являются набором циклов, получены в работе [32].

По определению матрицы образующих (1.6) степень любой вершины x_i равна числу ненулевых элементов матрицы в i -м столбце или строке с тем же номером. Рассмотрим однородные степени ρ *NA*-графы, т. е. графы, у которых каждая строка или столбец матрицы образующих содержит ровно ρ ненулевых элементов.

В отличие от главной диагонали матрицы, состоящей из элементов $a_{ii} = 0$, *боковой диагональю* назовем совокупность элементов a_{ij} , где $i + j = n + 1$. Множества элементов матрицы, параллельных диагоналям, будем называть соответственно *главными* или *боковыми линиями*. По определению каждая боковая линия, содержащая хотя бы один ненулевой элемент, соответствует од-

ной образующей из множества $(2, 4, 5, \dots, 2n-1)$. Если эта образующая — нечетная, то ее линия не пересекается с главной диагональю, и все ее элементы равны, если же она четная, то один элемент ее линии принадлежит диагонали и равен 0.

Определим условия, которым должно соответствовать множество образующих, чтобы MA -граф был регулярным степени $\rho = 1$.

Так как каждая боковая линия лежит либо выше боковой диагонали для $u < n+1$, либо ниже для $u > n+1$, то одной образующей не достаточно для регулярности графа. Выберем две образующие. Если $u_1 < n+1$, то первые $u_1 - 1$ столбцов содержат ровно по одному ненулевому элементу. Остальные столбцы должна покрывать образующая u_2 , поэтому ее значение определяется однозначно: $u_2 = n + u_1$. Если хотя бы одна из образующих u_1 или $n + u_1$ — четная, то в соответствующей линии матрицы существует нулевой элемент, который нарушает регулярность графа. Поэтому необходимо, чтобы u_1 и $n + u_1$ были нечетными. Тогда n — всегда четное, поэтому справедлива следующая лемма.

Лемма 2.11. Не существует регулярных степени 1 MA -графов с нечетным числом вершин.

Этот результат для обычных графов легко получить, так как регулярный степени 1 граф является совершенным паросочетанием, а для нечетного n его не существует.

На основании данного утверждения можно сделать вывод, что для регулярности графа к каждой образующей $u < n+1$ должна добавляться образующая $n + u$, и наоборот, к каждой образующей $v > n+1$ должна добавляться образующая $v - n$.

Кроме того, любой четной образующей u_i в матрице на месте $\left(\frac{u_i}{2}, \frac{u_i}{2}\right)$ соответствует нулевой элемент, что тоже может нарушать регулярность графа.

А также любой четной образующей u_i в матрице на месте $\left(\frac{u_i}{2}, \frac{u_i}{2}\right)$ соответствует нулевой элемент, что тоже может нарушать регулярность графа. Поэтому для соблюдения регулярности графа необходимо ввести еще две образующих: левую $u_{i-1} = \frac{u_i}{2} + 1$ и

правую $u_{i+1} = \frac{u_i}{2} + n$, которые компенсируют указанный нулевой элемент, но в сумме увеличивают степень регулярности графа на 1. Если какая-то из добавленных образующих окажется четной, то процесс добавления двух новых образующих продлится до тех пор, пока либо он заикнется, либо все новые образующие окажутся нечетными. Для количества левых образующих существенную роль играет степень двойки в разложении образующей u на множители, а для правых образующих — те же свойства числа n .

Для того чтобы изучить детальнее зависимости между образующими в регулярном графе, введем в рассмотрение граф разложения образующих $R(n)$, вершинами которого являются все образующие n -вершинного NA -графа, число которых равно $N = 2n - 3$. Все четные образующие u связаны ребрами с образующими $\frac{u}{2} + 1$ и $n + \frac{u}{2}$. Всем нечетным образующим соответствуют висячие вершины, так как на них процесс разложения образующих заканчивается. По понятным причинам обозначим $R_1(n)$ [$R_0(n)$] — граф для нечетных (четных) n .

Пусть $n \equiv 1 \pmod{2}$. Если выбрать нечетную образующую, то ее дополнение будет четной величиной, и необходимо добавить две образующие в процессе ее разложения. Рассмотрим обратный процесс построения всех четных образующих, начиная со всех нечетных. Рассмотрим для определенности пример при $n = 29$.

Число возможных образующих равно $2n - 3 = 55$. Расположим на самом нижнем (нулевом) уровне все нечетные образующие от 3 до $2n - 1$. Их можно разбить на следующие пары: $(x_0, y_0) = (2k + 1, n + 2k)$, где $k = 1, 2, \dots, \frac{n-1}{2}$ и разница между ними равна $n - 1$. Очевидно, на эти пары разлагаются четные образующие вида $u = 4k$. Будем считать, что эти образующие составляют первый уровень. Соединим их дугами, направленными сверху вниз, с соответствующими вершинами нулевого уровня. Вершины первого уровня зависят от левых вершин нулевого уровня по формуле $x_1 = 2(x_0 - 1) = 4k$. Аналогично они зависят от правых вершин нулевого уровня по формуле $x_1 = 2(y_0 - n)$. В нашем примере это вершины $(4, 8, 12, \dots, 52, 56)$. Если среди вершин первого уровня существуют пары вершин (x_1, y_1) , разница кодов которых $y_1 - x_1$

равна $n - 1$, то их можно соединить ребрами с вершиной второго уровня. Присваиваем ей код по тому же правилу: $x_2 = 2(x_1 - 1)$, где x_1 — код левой вершины первого уровня, или $x_2 = 2(y_1 - n)$. Очевидно, все остальные вершины первого уровня объединятся в такие пары и будут вершинами второго уровня. В данном примере это вершины (6, 14, 22, 30, 38, 46, 54). На каждом уровне вершин в два раза меньше, чем на нижнем. Подобные построения закончатся тогда, когда на самом верхнем уровне коды любых вершин x_i, x_j будут удовлетворять условию $|x_i - x_j| \neq n - 1$. Если взять какую-либо вершину k -го уровня и спуститься по левым ребрам в самую нижнюю вершину x_0 , то нетрудно установить зависимость $x_k = 2^k x_0 - 2^{k+1} + 2$. По этой причине коды k -го уровня ($k \geq 1$) составляют арифметическую прогрессию с начальным элементом $a = 3 \cdot 2^k - 2^{k+1} + 2$ и разностью $d = 2^{k+1}$, т. е. коды $(2l - 1)2^k + 2$, где $l = 1, 2, \dots$.

Лемма 2.12. Число уровней графа разложения $R_1(n)$ равно β , которое определяется из условия $n = 2^\beta(2m + 1) + 1$.

Очевидно, что $\beta \geq 1$, поэтому первый уровень всегда существует для любого NA -графа. На нулевом уровне число вершин равно $2(n - 1)/2 = n - 1 = 2^\beta(2m + 1)$. Затем оно уменьшается ровно в два раза на каждом уровне и на самом верхнем уровне становится равным $2m + 1$. В сумме число вершин на всех уровнях равно $(2m + 1)(1 + 2 + 4 + \dots + 2^\beta) = (2m + 1)(2^{\beta+1} - 1)$. Так как все нечетные образующие учтены на нулевом уровне, а всего образующих $2n - 3 = 2^{\beta+1}(2m + 1) - 1$, то остаются еще четные образующие, не принадлежащие ни одному уровню, и их количество равно $2m$. Назовем эти образующие *остаточным множеством*. Эти значения составляют арифметическую прогрессию с начальным членом $a = 2^{\beta+1} + 2$ и разностью $d = 2^{\beta+1}$, т.е. $u_i = i \cdot 2^{\beta+1} + 2$ ($i = 1, 2, \dots, 2m$). В нашем примере это (10, 18, 26, 34, 42, 50). Каждая такая образующая разлагается на $v_1 = \frac{u_i}{2} + 1 = i \cdot 2^\beta + 2$ и $v_2 = \frac{u_i}{2} + n = i \cdot 2^\beta + n + 1 = 2^\beta(2m + i + 1) + 2$. Если $i = 2l$ — четное, то $v_2 = (2m + 2l + 1)2^\beta + 2$ принадлежит наименьшему уровню, а $v_2 = l \cdot 2^{\beta+1} + 2$ — остаточному множеству. Если $i = 2l - 1$ — нечетное число, то об-

разующая $v_1 = (2l - 1)2^\beta + 2$ принадлежит наивысшему уровню, а $v_2 = 2^\beta(2m + 2l) + 2 = 2^{\beta+1}(m + l) + 2$ — остаточному множеству. Это означает, что образующая из верхнего уровня является корнем бинарного дерева, висячие вершины которого принадлежат нулевому уровню. Другим ребром образующие верхнего уровня соединены с образующими из остаточного множества. Так как вершины остаточного множества — четные образующие, то от них идет одно ребро в вершины верхнего уровня, а одно ребро — в вершину этого же множества. Поэтому подграф графа $R_1(n)$ на этом множестве образует циклы.

Образующая $u = n + 1$ принадлежит наивысшему уровню β , так как $n + 1 = 2^\beta(2m + 1) + 2$. С другой стороны, она не связана с остаточным множеством, так как иначе существовала бы образующая из этого множества χ , которая по формулам должна быть равной либо $2(n + 1 - 1) = 2n$, либо $2(n + 1 - n) = 2$. Но таких образующих в NA -графе не существует, так как $3 \leq u_i \leq 2n - 1$.

Таким образом, конструкция графа $R_1(n)$ становится понятной. Он состоит из набора циклов одинаковой длины с общим числом вершин $2m$, и каждая из этих вершин соединена с бинарным деревом с наибольшим уровнем β . Кроме того, существует отдельная компонента, которая является таким же деревом с верхней вершиной (корнем) $u = n + 1$. На рис. 2.11 показан граф $R_1(29)$ ($n = 2^2(2 \cdot 3 + 1) + 1$; $m = 3$; $\beta = 2$), состоящий из трех компонент: бинарное дерево с корнем $n + 1 = 30$, и два цикла длиной 3, вершинам которого инцидентны такие же бинарные деревья.

Прежде чем рассматривать регулярные NA -графы с четным числом вершин, рассмотрим некоторые операции на графе разложения $R_1(n)$. Как известно, *элементарным гомоморфизмом* в графах называется отождествление (стягивание) двух смежных вершин. Назовем *радиальным гомоморфизмом* графа $R_1(n)$, у которого $\beta \geq 1$, последовательность операций:

- а) удаление всех висячих вершин;
- б) перекодировка оставшихся вершин по правилу $y_i = \frac{x_i}{2} + 1$.

Граф, полученный в результате такой последовательности операций, обозначим $Gr(R_1(n))$. Так как после удаления висячих

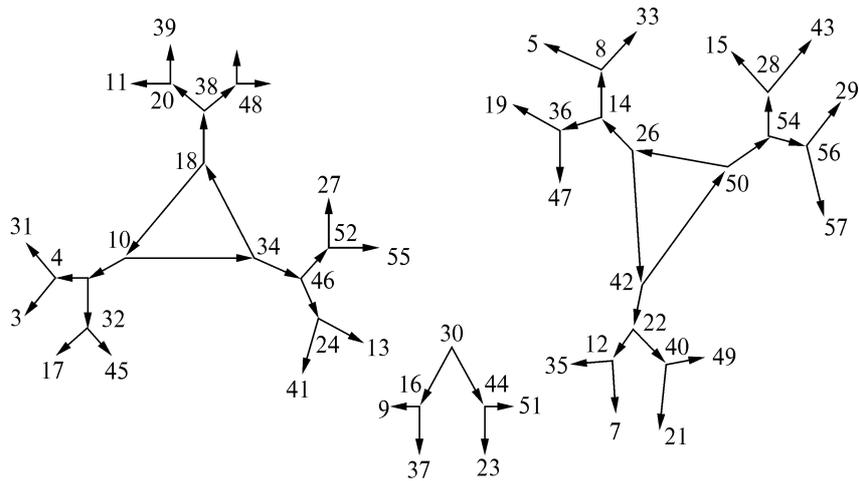


Рис. 2.11

вершин останутся только четные вершины, то вторая операция корректна. После выполнения первой операции коды висячих вершин в графе имеют вид $4i$, где $i = 1, 2, \dots, \frac{n-1}{2}$. Применяя операцию б) к этим вершинам, получаем все нечетные коды от 3 до n . Число удаленных вершин равно $n - 1 = 2^\beta(2m + 1)$, а число оставшихся вершин равно $2n - 3 - (n - 1) = n - 2 = 2^\beta(2m + 1) - 1$.

Структура оставшегося графа совпадает со структурой $R_1(n')$, где $n' = 2^{\beta-1}(2m + 1) + 1$. Операция б) преобразует коды графа $R_1(n)$ в коды графа $R_1(n')$, у которого $N' = 2n' - 3 = 2[2^{\beta-1}(2m + 1) + 1] - 3 = 2^\beta(2m + 1) - 1$. Если обозначить зависимость графа $R(n)$ от параметров β и m как $R(m, \beta)$, то в результате радиального гомоморфизма получим зависимость

$$Gr(R(m, \beta)) = R(m, \beta - 1).$$

Это означает, что в результате радиального гомоморфизма в графе $R_1(n)$ удаляются все висячие вершины, образующие вилки. После $\beta - 1$ операций радиального гомоморфизма в графе останется $2(2m + 1) + 1$ вершин.

Лемма 2.13. Граф разложений $R_1(2^\beta + 1)$ представляет собой бинарное дерево с корневой вершиной $u = n + 1$.

Действительно, $n = 2^\beta + 1$ только при $m = 0$. После $\beta - 1$ последовательных радиальных гомоморфизмов получаем $n' = 3$ с $U = \{3, 4, 5\}$. Это вилка с вершиной $u = 4$, т. е. $u = n' + 1$. Путем добавления β раз вилок к висячим вершинам можно восстановить исходный граф, который будет бинарным деревом. Вершина самого верхнего уровня имеет код $2^\beta + 2$, т. е. $u = n + 1$, что и требовалось доказать.

Таким образом, все графы $R_1(n)$ можно свести к $R_1(4m + 3) = R(m, 1)$, где $m > 0$. Число m будем называть *кардинальным числом* графа разложений $R_1(n)$.

Обозначим $\mu_2(b)$ — наибольшее нечетное число, на которое делится b .

Если $n = 4m + 3$, то все графы $R_1(n)$ имеют только один уровень, где будут все числа вида $4k$ ($k = 1, 2, \dots, 2m + 1$). От этих вершин идут ребра в остаточное множество, которое можно разделить на две равные части V и W в зависимости от формул, по которым они образуются:

$$V = \{v_l = 2(4l - 1) = 8l - 2, \quad l = 1, 2, \dots, m\};$$

$$W = \{w_k = 2(4k - n) = 8(k - m - 1) + 2, \quad k = m + 2, m + 3, \dots, 2m + 1\}.$$

Рассмотрим множество перестановок S_m из m элементов:

$$S_m = \begin{pmatrix} 1 & 2 & \dots & m \\ i_1 & i_2 & \dots & i_m \end{pmatrix}.$$

Определение 2.7. Характеристической перестановкой для графа разложений образующих $R_1(4m + 3)$ назовем такую

$$f_m = \{i \Rightarrow \frac{\mu_2(m + i) + 1}{2}\},$$

где $i = 1, 2, \dots, m$.

Прежде всего, покажем, что это отображение будет перестановкой, т. е. что при этом получаются все числа от 1 до m . Предположим обратное, что в результате получаем два одинаковых числа: $i_1 = \frac{\mu_2(m + i) + 1}{2} = i_2 = \frac{\mu_2(m + j)}{2}$, где $1 \leq i, j \leq m$. Если

$i > j$, то $i = (2^p - 1)m + 2^p \cdot j$ ($p \geq 1$). Отсюда вытекает, что $i > m$, но этого не может быть по виду самого определения функции $\mu_2(b)$. Поэтому все числа получаются разные и не больше m .

Определение 2.8. Весом элемента i на перестановке S_m называется величина

$$\lambda(i) = \left\lfloor \log_2 \left(\frac{m}{2i-1} \right) \right\rfloor + 2.$$

Теорема 2.10. Граф разложений образующих $R_1(4m+3)$ состоит из $p+1$ компонент связности, из которых одна является цепью длиной 3, а остальные компоненты содержат ровно один цикл из вершин остаточного множества. Число p равно числу циклов в характеристической перестановке $f_m \in S_m$, а длина каждого цикла равна сумме весов элементов цикла в той же f_m .

Покажем, что множества V и W не пересекаются. Действительно, если это так, то найдутся k и l такие, что $8k - 2n = 8l - 2$ или $8k - 8m - 6 = 8l - 2$. Отсюда $2l = 2(k - m) - 1$, что невозможно.

Рассмотрим последовательность $x_s = 2x_{s-1} - 2$, где $x_1 \in V$. Для любого $s \geq 2$ всегда $x_s = 2^{s-1}x_1 - 2^s + 2$. Если подставить значение $x_1 = 8l - 2 \in V$, то получим $x_s = 2^{s+1} \cdot (2l - 1) + 2$, т. е. для $s \geq 2$ все члены последовательности принадлежат W . При этом для разных l_1 и l_2 эти последовательности не имеют общих членов. В противном случае, если какие-то $x_s = x_r$ или $2^{s+1}(2l_1 + 1) = 2^{r+1}(2l_2 + 1)$, то это возможно только при $s = r$ и $l_1 = l_2$, что противоречит предположению. Итак, каждый элемент множества V служит начальным членом последовательности, в которой последующие члены принадлежат W . Так как V и W равномощны, то эти последовательности исчерпывают множество W . Наибольший член этого множества w_k получим при $k = 2m + 1$, т. е. $w_{\max} = 8m + 2$. Так как $x_s \leq w_{\max}$, то решая неравенство при фиксированном i , в последовательности получаем $s_{\max} = \left\lfloor \log_2 \frac{m}{2i-1} \right\rfloor + 2$ членов. Будем различать наименьший и наибольший члены этой

последовательности. Каждая последовательность есть цепочка разложений наибольшей образующей этой последовательности на левые составляющие разложений. Это разложение можно продлить на один шаг вниз, полагая $s = 0$, тогда получим $x_0 = 4l$, т. е. первую половину вершин первого уровня. Аналогично рассуждая, приходим к выводу, что максимальные значения последовательностей составляют остаточные элементы, превышающие $n + 1$, но их порядок зависит от конкретного значения m . Однако каждый элемент множества $v_i \in V$ разлагается на образующую $4i$ и на конечный элемент последовательности, начальный элемент которой $x_0 = 4j$. Так как разница между $4i$ и этим конечным элементом должна быть $n - 1 = 4m + 2$, то j определяем из уравнения

$$4i + 4m + 2 = (4j) \cdot 2^s - 2^{s+1} + 2 \quad (s > 0), \quad (i = 1, 2, \dots, m). \quad (2.36)$$

Отсюда находим $2j - 1 = \frac{i + m}{2} = \mu_2(i + m)$, так как $2j - 1$ — нечетное число. В результате $j = \frac{\mu_2(i + m) + 1}{2}$.

Рассмотрим теперь отображение $i \Rightarrow \frac{\mu_2(i + m) + 1}{2}$. Докажем, что оно является перестановкой из S_m , т. е. при изменении i от 1 до m j пробегает разные значения. Для $m = 2, 3$ это можно проверить непосредственно. Это перестановки (2,1) и (1,3,2). Пусть утверждение справедливо для произвольного m . Докажем то же самое для $m + 1$. Так как $i + m = (i - 1) + (m + 1)$, то, начиная с $i = 2$ и до $i = m$, элементы в f_m равны соответствующим элементам в f_{m+1} , начиная с $i = 1$ и до $i = m - 1$. Все они по индукции различны. Остается определить два элемента для $i = m$ и $i = m + 1$.

Первый элемент равен $\frac{\mu_2(m + m + 1) + 1}{2} = \frac{2m + 1 + 1}{2} = m + 1$, а второй — $\frac{\mu_2(m + 1 + m + 1) + 1}{2} = \frac{\mu_2(m + 1) + 1}{2}$, т. е. первому элементу в f_m . Оба эти элемента еще не появлялись прежде, поэтому имеем всегда дело с перестановкой. В рассмотренном доказательстве приведен способ построения всех перестановок для произ-

вольного m по индукции. Для того чтобы записать все f_m , считая f_2 и f_3 заданными, необходимо следовать таким правилам:

- переписать все, кроме первого, элементы из f_{m-1} ;
- записать элемент m ;
- записать первый элемент из f_{m-1} .

Все эти перестановки для $m = 2, 3, \dots, 20$ приведены в табл. 2.1, а их представление в виде циклов — в табл. 2.2 (для $m \leq 16$).

Нетрудно заметить общие закономерности табл. 2.1:

- 1) номер числа m находится на $(m - 1)$ -м месте в перестановке;
- 2) число i в следующей перестановке находится на месте, номер которого на $1 \pmod{m}$ меньше, чем в предыдущей перестановке.

Этих двух правил достаточно, чтобы построить полную табл. 2.1.

Теперь число циклов или компонент на множестве вершин остаточного множества определяется числом циклов в соответствующей перестановке. Еще одну компоненту в $R_1(n)$ дает образующая $n + 1 = 4(m + 1)$, которая разлагается на две нечетных образующих $u_1 = 2m + 3$ и $u_2 = 2(m + 1) + n = 6m + 5$, что в сумме составляет

Т а б л и ц а 2.1

m	Перестановки при $2 \leq m \leq 20$
2	2, 1
3	1, 3, 2
4	3, 2, 4, 1
5	2, 4, 1, 5, 3
6	4, 1, 5, 3, 6, 2
7	1, 5, 3, 6, 2, 7, 4
8	5, 3, 6, 2, 7, 4, 8, 1
9	3, 6, 2, 7, 4, 8, 1, 9, 5
10	6, 2, 7, 4, 8, 1, 9, 5, 10, 3
11	2, 7, 4, 8, 1, 9, 5, 10, 3, 11, 6
12	7, 4, 8, 1, 9, 5, 10, 3, 11, 6, 12, 2
13	4, 8, 1, 9, 5, 10, 3, 11, 6, 12, 2, 13, 7
14	8, 1, 9, 5, 10, 3, 11, 6, 12, 2, 13, 7, 14, 4
15	1, 9, 5, 10, 3, 11, 6, 12, 2, 13, 7, 14, 4, 15, 8
16	9, 5, 10, 3, 11, 6, 12, 2, 13, 7, 14, 4, 15, 8, 16, 1
17	5, 10, 3, 11, 6, 12, 2, 13, 7, 14, 4, 15, 8, 16, 1, 17, 9
18	10, 3, 11, 6, 12, 2, 13, 7, 14, 4, 15, 8, 16, 1, 17, 9, 18, 5
19	3, 11, 6, 12, 2, 13, 7, 14, 4, 15, 8, 16, 1, 17, 9, 18, 5, 19, 10
20	11, 6, 12, 2, 13, 7, 14, 4, 15, 8, 16, 1, 17, 9, 18, 5, 19, 10, 20, 3

цепь длиной 3. Циклам в перестановке из f_m соответствует цикл в графе $R_1(n)$, если вместо одного элемента перестановки брать соответствующую последовательность вершин. Теперь можно выбирать любые образующие для регулярного графа. Если взять нечетную образующую, то ее дополнением может быть четная образующая либо типа $4i$, либо из остаточного множества. Второй случай исключается, следовательно, остается $4i$, которая разлагается на две нечетные. Всего получается 4 образующих и граф будет регулярным степени 2. Если же взять четную образующую типа $4i$, то вместе с дополняющей нечетной и двумя нечетными по разложению получатся те же 4, что также дает регулярный граф степени 2. Если же взять четную образующую из остаточного множества, то необходимо брать все образующие одной компоненты, что дает регулярный граф степени $2z$, где z — число вершин в цикле. Используя теорему и таблицы, легко можно построить граф $R_1(n)$ для любого $n \equiv 1 \pmod{2}$.

Рассмотрим простой пример: $m = 3$, $n = 15$. По табл. 2.1 и 2.2 определяем перестановку и ее представление в циклах $(1^3)(2^2, 3^1)$.

Т а б л и ц а 2.2

m	Коды циклов
2	$(1^3, 2^1)$
3	$(1^3)(2^2, 3^1)$
4	$(1^4, 3^1, 4^1)(2^2)$
5	$(1^4, 2^2, 4^1, 5^1, 3^2)$
6	$(1^4, 4^1, 3^2, 5^1, 6^1, 2^3)$
7	$(1^4)(2^3, 5^1)(3^2)(4^2, 6^1, 7^1)$
8	$(1^5, 5^1, 7^1, 8^1)(2^3, 3^2, 6^1, 4^2)$
9	$(1^5, 3^2, 2^3, 6^1, 8^1, 9^1, 5^2, 4^2, 7^1)$
10	$(1^5, 6^1)(2^3)(3^3, 7^1, 9^1, 10^1)(4^2)(5^2, 8^1)$
11	$(1^5, 2^3, 7^1, 5^2)(3^3, 4^2, 8^1, 10^1, 11^1, 6^2, 9^1)$
12	$(1^5, 7^1, 10^1, 6^2, 5^2, 9^1, 11^1, 12^1, 2^4, 4^2)(3^3, 8^1)$
13	$(1^5, 4^2, 9^1, 6^2, 10^1, 12^1, 13^1, 7^2, 3^3)(2^4, 8^1, 11^1)(5^2)$
14	$(1^5, 8^1, 6^2, 3^3, 9^1, 12^1, 7^2, 11^1, 13^1, 14^1, 4^3, 5^2, 10^1, 2^4)$
15	$(1^5)(2^4, 9^1)(3^3, 5^2)(4^3, 10^1, 8^1)(6^2, 11^1, 7^2)(8^2, 12^1, 14^1, 15^1)$
16	$(1^6, 9^1, 13^1, 15^1, 16^1)(2^4, 5^2, 11^1, 14^1, 8^2)(3^3, 10^1, 7^2, 12^1, 4^3)(6^2)$

Граф $R_1(15)$ состоит из трех компонент. Для $i = 1$ находим образующую $v_1 = 8i - 2 = 6$. Вес элемента 1 равен 3, т.е. цепочка длиной 3 составляет цикл. Находим его элементы: $v_2 = 2v_1 - 2 = 10$, $v_3 = 2v_2 - 2 = 18$. Первая компонента составляет цикл из остаточных образующих (6,10,18) и всех образующих после их разложения. Для второй компоненты соответственно тоже находим $i = 2$, $v_1 = 8i - 2 = 14$. Эта цепочка состоит из двух вершин, поэтому $v_2 = 2v_1 - 2 = 26$. Для третьей вершины $i = 3$, $v_3 = 8i - 2 = 22$. Таким образом, вторая компонента состоит из цикла (14, 26, 22) и образующих, полученных от их разложения. Третья компонента состоит из образующей $n+1=16$ и ее разложения 9 и 23. Граф $R_1(15) = Gr(R_1(29))$, $R_0(8) = Gr(R_1(15))$, $m = 3$ представлен на рис. 2.12.

Рассмотрим теперь случай $n \equiv 0 \pmod{2}$. Так как нечетная образующая имеет своим дополнением также нечетную образующую, то степень регулярности графа может быть любой, если выбирать только нечетные образующие. Если же взять четную образующую, то для выяснения вопроса о существовании регулярных графов необходимо построить граф разложения образующих $R_0(n)$, который строится по тому же принципу, что и $R_1(n)$. Каждая четная образующая разлагается обязательно на одну четную и одну нечетную, так как разница между их значениями равна $n - 1$, т.е. нечетному числу.

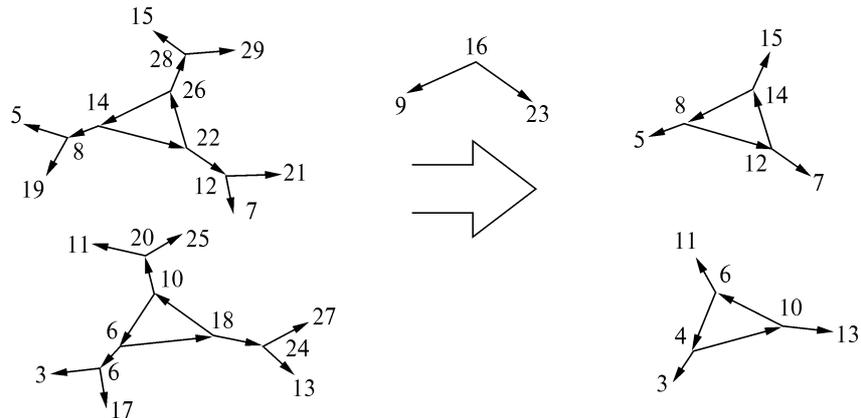


Рис. 2.12

Теорема 2.11. Граф разложений $R_0(2m+2)$ состоит из $p+1$ компонент связности, из которых одна является вершиной $n-1$, а остальные компоненты содержат ровно один цикл из вершин остаточного множества. Число p равно числу циклов в перестановке $f_m \in S_m$, $f_m = \{i \Rightarrow \frac{\mu_2(m+i)+1}{2}\}$, а длина каждого цикла в графе равна сумме весов элементов соответствующего цикла в f_m . При этом $m = \frac{n-2}{2}$, а вес элемента определяется так же, как и в $R_1(n)$.

Образует последовательности такого же типа, как и для $R_1(n)$: $x_s = x_1 2^{s-1} - 2^s + 2$, где в качестве x_1 возьмем образующую $4i$. Наибольшее значение образующей равно $2n-1$, поэтому $i = 1, 2, \dots, \frac{n}{2} - 1$. Нетрудно показать, что $x_s \neq 4i$ при любом s, i и

$k \geq 1$. Обозначим $m = \frac{n}{2} - 1$ и, как и прежде, будем называть его кардинальным числом графа $R_0(n)$. Тогда получаем m разных непересекающихся последовательностей, таких же, как и для $R_1(n)$, с единственным отличием, что здесь x_1 принадлежит последовательности. Здесь x_s не должно превышать максимального значения четных образующих, т. е. $(4i)2^s - 2^{s+1} + 2 \leq 4m + 2$.

Отсюда длина цепочки $\lambda(i) = s = \left\lfloor \log \frac{m}{2i-1} \right\rfloor + 2$. Так как начальный элемент цепочки $4i$ разлагается на нечетную образующую $2i+1$ и четную образующую $2i+n = 2(i+m)+2$, которая должна быть максимальным элементом другой цепочки, то решив уравнение

$$2(i+m)+2 = 4ij \cdot 2^s - 2^{s+1} + 2, \quad (2.37)$$

находим $2j-1 = [i+m]/2^s = \mu_2(i+m)$. Поскольку $2j-1$ — нечетное число, то тогда $j = \frac{\mu_2(i+m)+1}{2}$, и мы приходим к тому же результату, что и в теореме 2.10.

Таким образом, для определения структуры графа $R_0(n)$ можно воспользоваться теми же таблицами, которые составлены

для $R_1(n)$, выбирая строку с заданным m . Рассмотрим граф $R_0(n)$ для $n = 8$. При этом $m = 3$ и в табл. 2.2 находим соответствующую перестановку $(1, 3, 2)$, состоящую из двух циклов. Подставим в них веса элементов: $\lambda(1) = 3, \lambda(2) = 2, \lambda(3) = 1$. В результате получаем граф (см. рис. 2.12, справа). Из рис. 2.12 видно, что этот граф получен из графа $R_1(n)$ для $m = 3$ путем радиального гомоморфизма.

Следствие. $Gr(R_1(4m + 3)) = R_0(2m + 2)$.

Имея перед собой графы разложения $R_1(n)$ и $R_0(n)$, можно решать вопрос о существовании регулярных графов, содержащих любые образующие. Из рис. 2.11 видно, что любой однородный граф, содержащий хотя бы одну образующую из остаточного множества, должен включать в себя и все остальные вершины компоненты. Однородный граф степени 2 — фактороид, и его можно получить различными способами. Для этого надо взять образующую типа $4k$, ее разложение $2k + 1$ и $2k + n$ и дополнение $4k + n$ (нечетное число). Согласно теореме 2.10 это будет фактороид. Все остальные степени однородности можно лишь складывать из таких подграфов, т.е. в любом случае она может быть только четной.

При переходе к четному числу вершин картина немного иная. Здесь можно построить граф степени 1, что соответствует любой нечетной образующей и ее дополнению $n + u$, которое тоже будет нечетным. Поэтому можно построить однородный граф любой степени.

Таким образом, вопрос о построении однородных графов для заданного u решается непосредственно с помощью табл. 2.1, 2.2. Очевидно, что строить такие таблицы для больших n довольно хлопотно. Поэтому возникает вопрос, как аналитическим путем описать структуру графов разложения для произвольного n ? Прежде всего, следует научиться определять циклы, на которые разбивается подстановка.

Пусть необходимо найти условия существования цикла длиной k для заданного n или заданного m . Элемент под номером i определяется по формуле

$$a_m(i) = \frac{\mu_2(m + i) + 1}{2}. \quad (2.38)$$

Тогда для цикла (i_1, i_2, \dots, i_k) должна выполняться система равенств

$$\begin{aligned}
 i_2 &= [\mu_2(m + i_1) + 1] / 2, \\
 i_3 &= [\mu_2(m + i_2) + 1] / 2, \\
 &\dots\dots\dots \\
 i_k &= [\mu_2(m + i_{k-1}) + 1] / 2, \\
 i_1 &= [\mu_2(m + i_k) + 1] / 2.
 \end{aligned}
 \tag{2.39}$$

Равенство (2.38) для определенного $\alpha \geq 0$ равносильно следующему:

$$m + i = 2^\alpha [2a_m(i) - 1]. \tag{2.40}$$

Тогда систему (2.39) для определенного вектора $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k)$ ($\alpha_i \geq 0$) записываем таким образом:

$$\begin{aligned}
 m + i_1 &= 2^{\alpha_1} [2(i_2) - 1], \\
 m + i_2 &= 2^{\alpha_2} [2(i_3) - 1], \\
 &\dots\dots\dots \\
 m + i_{k-1} &= 2^{\alpha_{k-1}} [2(i_k) - 1], \\
 m + i_k &= 2^{\alpha_k} [2(i_1) - 1].
 \end{aligned}
 \tag{2.41}$$

Или в стандартном виде:

$$\begin{aligned}
 -i_1 + i_2 2^{\alpha_1 + 1} &= m + 2^{\alpha_1}, \\
 -i_2 + i_3 2^{\alpha_2 + 1} &= m + 2^{\alpha_2}, \\
 &\dots\dots\dots \\
 -i_{k-1} + i_k 2^{\alpha_{k-1} + 1} &= m + 2^{\alpha_{k-1}}, \\
 i_1 2^{\alpha_k + 1} \dots\dots - i_k &= m + 2^{\alpha_k}.
 \end{aligned}
 \tag{2.42}$$

Пусть $\sum_{i=1}^k \alpha_i = s$, тогда определитель этой системы равен $\Delta = (-1)^k (2^{s+k} - 1) \neq 1$. Решение системы существует всегда, остается найти такой вектор α , для которого оно будет целочисленным. На этот вектор существуют два ограничения:

$$i_1 \neq i_2 \text{ (условие невырожденности цикла)}, \tag{2.43}$$

$$i_l \leq m \quad (l = 1, 2, \dots, k). \tag{2.44}$$

Задача определения циклов достаточно сложная, и в этой работе не ставилась цель решить ее полностью.

Для начала рассмотрим условия существования цикла длиной 1, т. е. отображение элемента перестановки в себя. Это равносильно условию

$$m + i = 2^\alpha(2i - 1). \quad (2.45)$$

Отсюда $m = i(2^{\alpha+1} - 1) - 2^\alpha$. Подставляя последовательно разные значения i и α , получаем номера перестановок, в которых есть тождественные подстановки. Вычислим вес такого элемента:

$$\lambda(i) = \left\lfloor \log_2 \left(\frac{[2^\alpha(2i - 1) - i]}{(2i - 1)} \right) \right\rfloor + 2 = \alpha + 1. \quad (2.46)$$

Значения m приведены в табл. 2.3 для $i \leq 6$ и $\alpha \leq 7$.

Табл. 2.3 можно продолжить и дальше, не обязательно выполняя все сложные вычисления. Обозначим ее элемент для произвольных (i, α) , $m(i, \alpha)$. Тогда, кроме заданной очевидной закономерности $m(i, \alpha + 1) = 2m(i, \alpha) + i$, можно заметить следующую, которая проверяется непосредственно:

$$m(i + 1, \alpha) = m(i, \alpha) + m(1, \alpha + 1). \quad (2.47)$$

Это позволяет заполнить только первую строку таблицы, затем по столбцам заполнить остальные клетки, выполняя только одну операцию сложения. В табл. 2.3 выделены значения m , для которых по данным табл. 2.1, 2.2 можно убедиться в справедливости полученных результатов. Например, в табл. 2.3 имеется по два одинаковых элемента $m(1,3) = m(3,1) = 7$. Это означает, что для $m = 7$ в табл. 2.2 имеются два тождественных отображения для $i = 1$ с весом $\alpha + 1 = 4$ и $i = 3$ с весом $\alpha + 1 = 2$. Аналогично для $m = 10$

Таблица 2.3

i	α						
	1	2	3	4	5	6	7
1	1	3	7	15	31	63	127
2	4	10	22	46	94	190	382
3	7	17	37	77	157	317	617
4	10	24	52	108	220	444	892
5	13	31	67	139	283	571	1147
6	16	38	82	170	346	698	1402

имеются такие же два отображения для $i = 2$ с весом 3 и $i = 4$ с весом 2.

Рассмотрим условия существования циклов (i_1, i_2) длиной 2. Из (2.42) получаем систему

$$\begin{aligned} -i_1 + i_2 2^{\alpha_1+1} &= m + 2^{\alpha_1}, \\ i_1 2^{\alpha_2+1} - i_2 &= m + 2^{\alpha_2}. \end{aligned} \quad (2.48)$$

Отсюда определяем $\Delta = 2^{\alpha_2+\alpha_1+2} - 1$ и такие решения:

$$\begin{aligned} i_1 &= \frac{m(2^{\alpha_1+1} + 1) + 2^{\alpha_2+\alpha_1+1} + 2^{\alpha_1}}{\Delta}, \\ i_2 &= \frac{m(2^{\alpha_2+1} + 1) + 2^{\alpha_2+\alpha_1+1} + 2^{\alpha_2}}{\Delta}. \end{aligned} \quad (2.49)$$

Условие (2.44) явно выполняется, а (2.43) приводится к виду $2^{\alpha_2}(2m+1) \neq 2^{\alpha_1}(2m+1)$, что равносильно

$$\alpha_1 \neq \alpha_2. \quad (2.50)$$

Теорема 2.12. Для $i_1 = 1$ справедливы соотношения

$$m = 2^{\alpha_1} \sum_{k=1}^{2\gamma} (-1)^k 2^{(\alpha_1+1)k} - 1 \quad (\alpha_1 \geq 0, \quad \gamma \geq 1), \quad (2.51)$$

$$i_2 = \sum_{k=1}^{2\gamma} (-1)^k 2^{(\alpha_1+1)k-1} + 1, \quad (2.52)$$

$$\lambda(i_1) = (2\gamma + 1)(\alpha_1 + 1); \quad \lambda(i_2) = \alpha_1 + 1. \quad (2.53)$$

Доказательство. Выразим m через i_1 из выражения (2.49):

$$m = \frac{i_1(2^{\alpha_1+\alpha_2+2} - 1) - 2^{\alpha_1+\alpha_2+1} - 2^{\alpha_1}}{2^{\alpha_1+1} + 1}. \quad (2.54)$$

Отсюда для $i_1 = 1$

$$m = \frac{2^{\alpha_1+\alpha_2+1} - 2^{\alpha_1} - 1}{2^{\alpha_1+1} + 1}. \quad (2.55)$$

Для наименьшего значения $\alpha_2 = \alpha_1$ получаем деление нацело:

$$m = \frac{2^{\alpha_1+\alpha_2+1} - 2^{\alpha_1} - 1}{2^{\alpha_1+1} + 1} = \frac{(2^{\alpha_1+1} - 1)(2^{\alpha_1+1} + 1)}{2^{\alpha_1+1} + 1} = 2^{\alpha_1+1} - 1.$$

Пусть $\alpha_2 = \alpha_1 + \delta$ ($\delta \geq 1$), тогда

$$m = \frac{2^{2\alpha_1 + \delta + 1} - 2^{\alpha_1} - 1}{2^{\alpha_1 + 1} + 1} = \frac{2^{\alpha_1 + 1}(2^\delta - 1)}{2^{\alpha_1 + 1} + 1} + 2^{\alpha_1} - 1.$$

Все действия сводятся к делимости выражения $2^\delta - 1$ на $p = 2^{\alpha_1 + 1} - 1$, т. е. к решению уравнения $2^\delta \equiv -1 \pmod{p}$. Так как при $\delta = \alpha_1 + 1$ имеем $2^\delta \equiv 1 \pmod{p}$, то $\delta = 2(\alpha_1 + 1)$. Поэтому

$$\alpha_2 = \alpha_1 + 2\gamma(\alpha_1 + 1) \quad (\gamma \geq 1). \quad (2.56)$$

Тогда $m = \frac{2^{\alpha_1}[2^{(2\gamma+1)(\alpha_1+1)} + 1]}{2^{\alpha_1+1}} - 1.$

Полученная дробь делится нацело, в результате получаем соотношение (2.51). Значение i_2 находим после подстановки значения m и $i_1 = 1$ в выражение (2.48). Определим $\lambda(1)$. Для этого в (2.51) найдем положительное слагаемое с наибольшей степенью двойки. Это первый член, у которого степень равна $\alpha_1 + 2\gamma(\alpha_1 + 1)$. Далее следуют знакопеременные члены, меньшие по значению. Поэтому

$$\lambda(1) = \lfloor \log_2 m \rfloor + 2 = \alpha_1 + 2\gamma(\alpha_1 + 1) - 1 + 2 = (2\gamma + 1)(\alpha_1 + 1).$$

Для определения $\lambda(i_2)$ найдем

$$2i_2 - 1 = \sum_{k=1}^{2\gamma} (-1)^k 2^{(\alpha_1+1)k} + 1 = \sum_{k=0}^{2\gamma} (-1)^k 2^{(\alpha_1+1)k}.$$

Тогда $\lambda(i_2) = \lfloor \log_2 m(2i_2 - 1) \rfloor + 2 = \alpha_1 + 1.$

Для подтверждения полученных результатов выполним некоторые расчеты:

$\alpha_1 = 0,$	$\gamma = 0,$	$m = 0,$	-	-	-	;
	$\gamma = 1,$	$m = 2,$	$i_2 = 2,$	цикл (1,2),	$\lambda(1) = 3,$	$\lambda(2) = 1;$
	$\gamma = 2,$	$m = 10,$	$i_2 = 6,$	цикл (1,6),	$\lambda(1) = 5,$	$\lambda(6) = 1;$
	$\gamma = 3,$	$m = 42,$	$i_2 = 22,$	цикл (1,22),	$\lambda(1) = 7,$	$\lambda(22) = 1;$
	$\gamma = 4,$	$m = 170,$	$i_2 = 86,$	цикл (1,86),	$\lambda(1) = 9,$	$\lambda(86) = 1;$
$\alpha_1 = 1,$	$\gamma = 0,$	$m = 1,$	-	-	-	;
	$\gamma = 1,$	$m = 25,$	$i_2 = 7,$	цикл (1,7),	$\lambda(1) = 6,$	$\lambda(7) = 2;$
	$\gamma = 2,$	$m = 409,$	$i_2 = 103,$	цикл (1,103),	$\lambda(1) = 10,$	$\lambda(103) = 2;$
	$\gamma = 3,$	$m = 6553,$	$i_2 = 1639,$	цикл (1,1639),	$\lambda(1) = 14,$	$\lambda(1639) = 2.$

Аналогичную картину можно проследить и для $i_1 = 2$. Тогда

$$m = \frac{2^{\alpha_1 + \alpha_2 + 3} - 2^{\alpha_1 + \alpha_2 + 1} - 2^{\alpha_1} - 2}{2^{\alpha_1 + 1} + 1} = \frac{3 \cdot 2^{\alpha_1 + \alpha_2 + 1} - 2^{\alpha_1} - 2}{2^{\alpha_1 + 1} - 1}. \quad (2.57)$$

Выполним необходимые расчеты:

$$\begin{aligned} \alpha_1 = 0, \quad m &= (3 \cdot 2^{\alpha_2 + 1}) / 3 = 2^{\alpha_2 + 1} - 1, \quad -, \quad m = 1, 3, 7, 15, \dots; \\ \alpha_1 = 1, \quad m &= (3 \cdot 2^{\alpha_2 + 2} - 4) / 5, \quad \alpha_2 = 1 \pmod{4}, \quad m = 4, 76, 1270, \dots; \\ \alpha_1 = 2, \quad m &= (3 \cdot 2^{\alpha_2 + 3} - 2) / 3, \quad \alpha_2 = 0 \pmod{2}, \quad m = 2, 10, 42, \dots; \\ \alpha_1 = 3, \quad m &= (3 \cdot 2^{\alpha_2 + 4} - 10) / 7, \quad \alpha_2 = 3 \pmod{8}, \quad m = 22, 5782, \dots; \\ \alpha_1 = 4, \quad m &= (3 \cdot 2^{\alpha_2 + 5} - 18) / 33, \quad \alpha_2 = 4 \pmod{10}, \quad m = 46, 47662, \dots; \\ \alpha_1 = 5, \quad m &= (3 \cdot 2^{\alpha_2 + 6} - 34) / 65, \quad \alpha_2 = 5 \pmod{12}, \quad m = 94, \dots \end{aligned}$$

За исключением $\alpha_1 = 2$, решением для целых m является $\alpha_2 \equiv \alpha_1 \pmod{2\alpha_1 + 2}$. Для всех $\alpha_1 \equiv 0 \pmod{2}$ выражение (2.57) делится на 3 и тогда возможны упрощения.

Теорема 2.13. Для циклов длиной 2 справедливы соотношения

$$m = i_1 \sum_{k=0}^{2\gamma+1} (-1)^{k+1} 2^{(\alpha_1+1)k} - 2^{\alpha_1} \sum_{k=0}^{2\gamma} (-1)^k 2^{(\alpha_1+1)k} \quad (\alpha_1 \geq 0, \gamma \geq 1), \quad (2.58)$$

$$i_2 = (i_1 + 2^{\alpha_1}) \sum_{k=0}^{2\gamma} (-1)^k 2^{(\alpha_1+1)k} - 2^{\alpha_1 + 2\gamma(\alpha_1+1)}, \quad (2.59)$$

$$\lambda(i_1) = (2\gamma + 1)(\alpha_1 + 1) \quad \lambda(i_2) = \alpha_1 + 1. \quad (2.60)$$

2.7. НЕОБХОДИМЫЕ И ДОСТАТОЧНЫЕ УСЛОВИЯ СВЯЗНОСТИ \mathcal{NA} -ГРАФОВ

Для графов, задаваемых обычным способом, существуют алгоритмы, которые позволяют определить, являются ли эти графы h -связными для любого $h > 0$. Разумеется, эти алгоритмы пригодны и для \mathcal{NA} -графов, однако часто можно установить h -связность \mathcal{NA} -графов, анализируя только множество образующих U .

Определение 2.9. Интервалом определения $\beta(u)$ образующей u называется максимальный отрезок натурального ряда $[i, j]$, для которого $i + j = u$.

Для всех $u \leq n + 1$ таким интервалом является $\beta(u) = [1, u - 1]$, а для $u \geq n + 1$ — $\beta(u) = [u - n, n]$. В общем случае

$$\beta(u) = [u - n + |n - u + 1|, n - |n - u + 1|]. \quad (2.61)$$

Условие 1. Необходимым условием связности NA -графа с m образующими является

$$\bigcup_{i=1}^m \beta(u_i) = N_n. \quad (2.62)$$

Следует отметить, что для нечетных u все вершины интервала $\beta(u)$ образуют паросочетание, а для четных u одна вершина с номером $u/2$ остается изолированной. Если бы допускались петли, то в этой вершине была бы петля, так как $u/2 + u/2 = u$.

Лемма 2.14. Число компонент связности NA -графа с образующими $U = \{u_1, u_2\}$ равно

$$p = \left\lfloor \frac{u_2 - u_1}{2} \right\rfloor + 1 - u_1 u_2 \pmod{2} + (u_1 - n - 1) \left[1 + \operatorname{sgn}(u_1 - n - 1) \right] / 2 + (n + 1 - u_2) \left[1 + \operatorname{sgn}(n + 1 - u_2) \right] / 2. \quad (2.63)$$

Если $u_1, u_2 < n + 1$, то начиная с u_2 и дальше все вершины — изолированные. В этом случае предпоследнее слагаемое в формуле (2.60) равно 0, а последнее слагаемое — числу этих изолированных вершин. Если же $u_1, u_2 > n + 1$, то последнее слагаемое будет равно нулю, а предпоследнее слагаемое — числу изолированных вершин от 1 до $u_1 - n - 1$. Последний случай можно свести к первому, если сделать двойственную замену: $x'_i = n + 1 - x_i$, $u'_i = 2n + 2 - u_i$. В общем случае считаем, что $u_1, u_2 < n + 1$. Удаляя изолированные вершины, приходим к случаю, когда $n' = u_2 - 1$. Для него необходимо доказать первую часть формулы (2.60).

В графе при двух образующих циклов нет и все вершины имеют степень 0, 1 или 2. Для целого значения x введем обозначения:

$$\delta(x) = (x + 1) \pmod{2} = 1 - x \pmod{2} = \left[1 + (-1)^x \right] / 2.$$

Все вершины в графе, начиная с номера u_1 , имеют степень 1, за исключением $\delta(u_2)$, которая имеет степень 0. Все вершины от

1 до $u_1 - 1$ имеют степень 2, за исключением $\delta(u_1)$, которая имеет степень 1. Все компоненты графа либо изолированные вершины, либо цепи, число которых равно половине числа вершин со степенью 1. В результате имеем

$$p = \frac{u_2 - 1 - [u_1 - 1 - \delta(u_1)]}{2} + \delta(u_2) = \frac{u_2 - u_1 + \delta(u_1) + \delta(u_2)}{2}.$$

Подставляя в эту формулу различные значения 0 или 1 для $\delta(x)$, получаем первую часть выражения (2.63).

Из доказательства леммы 2.14 вытекает следующее условие.

Условие 2. Необходимым условием связности NA -графа с m образующими является

$$\min_{1 \leq i \leq m} \{u_i\} \leq n + 1, \max_{1 \leq i \leq m} \{u_i\} \geq n + 1. \quad (2.64)$$

Это условие превращает в нуль последние два слагаемых в формуле (2.63).

Условие 3. Необходимым условием связности NA -графа с двумя образующими $U = \{u_1, u_2\}$ является

$$n - 1 \leq u_1 \leq n + 1. \quad (2.65)$$

Это следует из леммы 2.14, если положить $p = 1$. Тогда последние слагаемые равны нулю и $\lfloor (u_2 - u_1) / 2 \rfloor = u_2 u_1 \pmod{2}$. Если $u_1 \equiv u_2 \equiv 0 \pmod{2}$, то в левой части должно быть $u_1 = u_2$, что невозможно. Если одна из образующих — четная, а другая — нечетная, то $u_2 - u_1 = 1$. Если обе образующие — нечетные, то $u_2 - u_1 = 2$. Вычитая эти равенства из неравенства $u_2 \geq n + 1$, получаем необходимое условие.

Рассмотрим для NA -графа матрицу образующих $A = (a_{ij})$, где $a_{ij} = i + j$; $a_{ii} = 0$; $i, j = \overline{1, n}$. Эта матрица симметрична относительно обеих диагоналей.

Теорема 2.14. Число компонент связности NA -графа, у которого $U = \{u_1, u_2\}$, равно

$$p = \frac{|n + 1 - u_1| + |n + 1 - u_2| + \delta(u_1) + \delta(u_2)}{2}. \quad (2.66)$$

Для доказательства необходимо определить, сколько ребер в графе соответствуют одной образующей. В матрице A каждому ребру соответствует два элемента $a_{ij} = a_{ji} = u$. В силу симметрии число таких элементов равно

$$r_n(u) = r_n(2n+2-u). \quad (2.67)$$

В работе [36] показано, что

$$r_n(u) = 2 \cdot \left\lfloor \frac{n - |n+1-u|}{2} \right\rfloor. \quad (2.68)$$

Если u — нечетное, то в (2.68) внешние скобки можно опустить, так как в них получится четное выражение. Если u — четное, то в скобках будет нечетное число, поэтому можно вычесть в числителе 1, чтобы получить четное число. Так как $\delta(u) = 0$ для u нечетного и $\delta(u) = 1$ для u четного, можно записать

$$r_n(u) = n - |n+1-u| - \delta(u). \quad (2.69)$$

Пусть m — число ребер графа, λ — его цикломатическое число. По формуле Эйлера $p = n - m + \lambda$. На рис. 2.13 ($X = N_{19}$, $U = \{14, 20\}$) верхние ребра соответствуют u_1 , а нижние ребра — u_2 .

Очевидно, что для двух образующих в графе циклы не образуются, иначе существовала бы пара из верхнего и нижнего ребер, соединяющая две вершины, что возможно лишь при $u_1 = u_2$. Это означает, что $\lambda = 0$, тогда

$$p = n - [r_n(u_1) - r_n(u_2)] / 2.$$

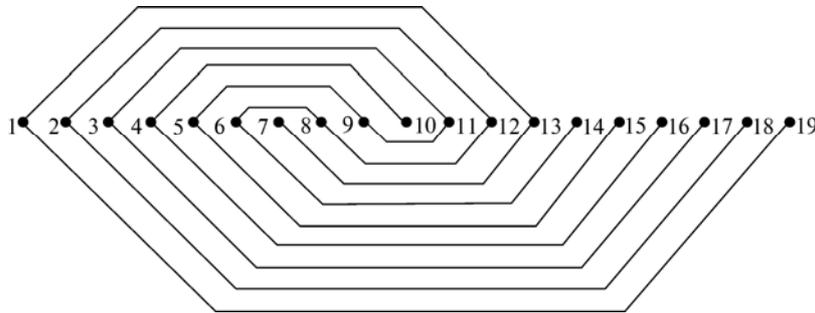


Рис. 2.13

Подставляя в это выражение формулу (2.69), получаем утверждение теоремы.

Из матрицы A видно, что если граф имеет только одну образующую, то число изолированных вершин равно $n - r_n(u)$. Если для каждого u обозначить $p(\dot{u})$ — число вершин, на которые не действует образующая u , т. е.

$$p(\dot{u}) = |n + 1 - u| + \delta(u), \quad (2.70)$$

то получим

$$p = [p(\dot{u}_1) + p(\dot{u}_2)] / 2. \quad (2.71)$$

Исследуем теперь вопрос, при каких образующих $u_1 < u_2$ NA -граф связан. Для этого решим уравнение (2.66) для $p = 1$, которое приводится к виду

$$|n + 1 - u_1| + |n + 1 - u_2| = 1 - \frac{(-1)^{u_1} + (-1)^{u_2}}{2}. \quad (2.72)$$

Если $u_1 \equiv u_2 \equiv 0 \pmod{2}$, то правая часть уравнения (2.72) равна 0, и решением будут значения $u_1 = u_2 = n + 1$, что невозможно.

Пусть $u_1 \not\equiv u_2 \pmod{2}$. Тогда правая часть уравнения (2.72) равна 1 и необходимо рассмотреть два случая:

$$\begin{aligned} \text{а) } & \begin{cases} |n + 1 - u_1| = 0, \\ |n + 1 - u_2| = 1. \end{cases} \text{ Решение: } \begin{cases} u_1 = n + 1, \\ u_2 = n + 2; \end{cases} \\ \text{б) } & \begin{cases} |n + 1 - u_1| = 1, \\ |n + 1 - u_2| = 0. \end{cases} \text{ Решение: } \begin{cases} u_1 = n, \\ u_2 = n + 1. \end{cases} \end{aligned}$$

Пусть $u_1 \equiv u_2 \equiv 1 \pmod{2}$. Тогда правая часть уравнения (2.72) равна 2 и необходимо рассмотреть три случая:

$$\begin{aligned} \text{а) } & \begin{cases} |n + 1 - u_1| = 0, \\ |n + 1 - u_2| = 2. \end{cases} \text{ Решение: } \begin{cases} u_1 = n + 1, \\ u_2 = n + 3; \end{cases} \quad (n \text{ — четное}) \\ \text{б) } & \begin{cases} |n + 1 - u_1| = 1, \\ |n + 1 - u_2| = 1. \end{cases} \text{ Решение: } \begin{cases} u_1 = n, \\ u_2 = n + 2; \end{cases} \quad (n \text{ — нечетное}) \end{aligned}$$

$$в) \begin{cases} |n+1-u_1|=2, \\ |n+1-u_2|=0. \end{cases} \text{ Решение: } \begin{cases} u_1 = n-1, \\ u_2 = n+1. \end{cases} \quad (n - \text{четное})$$

Тем самым доказана следующая теорема.

Теорема 2.15. *NA-граф с образующими $U = \{u_1, u_2\}$ связан тогда и только тогда, когда U принимает значения $\{n, n+1\}$, $\{n+1, n+2\}$ для произвольных n , $\{n-1, n+1\}$, $\{n+1, n+3\}$ — для четных n и $\{n, n+2\}$ — для нечетных n .*

Если граф удовлетворяет условию 2, то в нем отсутствуют изолированные вершины, находящиеся на рисунках слева или справа от графа с ребрами. Обозначим $r = u_2 - u_1$.

Лемма 2.15. Число компонент связности *NA-графа*, удовлетворяющего условию 2, с двумя образующими равно числу решений уравнения

$$i + j \equiv u \pmod{r}, \text{ где } u \equiv u_1 \pmod{r}. \quad (2.73)$$

Действительно, если граф удовлетворяет условию 2, то в нем не будет изолированных вершин ни справа, ни слева от графа с ребрами. Тогда путем добавления фиктивных вершин, не нарушающих связности графа и не увеличивающих числа его компонент, можно добиться, чтобы $u_2 = n' + 1$. Если разбить числа от 1 до n' на r классов вычетов по модулю r — S_1, S_2, \dots, S_r , то образующие $u_1 \equiv u_2 \pmod{r}$ объединяют пары таких классов: (S_1, S_{u-1}) , (S_2, S_{u-2}) и т.д. Как показано на рис. 2.14, число таких пар равно числу решений (2.73), при этом возникает случай, когда u — четное. Тогда решение принадлежит одному классу с индексом $u/2$, а в случае четного r — классу с индексом $(r+u)/2$. В зависимости от значений r или u (все случаи показаны на рис. 2.14) можно определить число таких решений:

$$p = \frac{r + \delta(u) + \delta(r+u)}{2}.$$

Нетрудно убедиться, что эта формула совпадает с (2.63), если в нее подставить $u_2 = n + 1$.

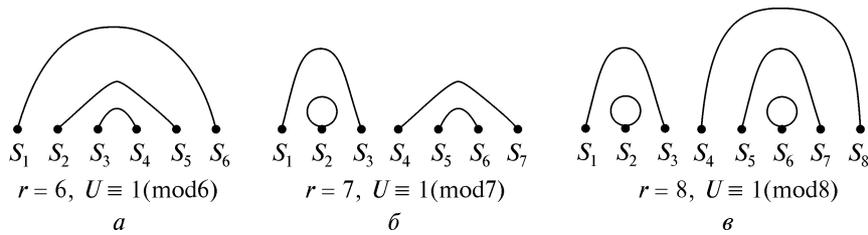


Рис. 2.14

Рассмотрим NA -граф с тремя образующими $U = \{u_1, u_2, u_3\}$. Пусть $r_1 = u_2 - u_1, r_2 = u_3 - u_2, D$ — наибольший общий делитель r_1 и r_2 .

Теорема 2.16. NA -граф с множеством трех образующих $U = \{u_1, u_2, u_3\}$ связан тогда и только тогда, когда

- а) $u_1 \leq n + 1, u_3 \geq n + 1$;
- б) $u_3 - u_2 - u_1 - u_3 \pmod{2} - u_2 \pmod{2} - u_1 \pmod{2} + 2 \leq 0$;
- в) $D = 1$ или $D = 2$ при u_1 нечетном.

Условие а) — это перенесенное условие 2. Если оно выполняется, то значение u_2 не играет роли. Путем удаления или добавления висячих фиктивных вершин, не нарушая связности графа, можно получить $u_2 = n' + 1$, где n' — новое число вершин. На интервале $\beta(u_1)$, который является частью $\beta(u_2)$, все вершины, за исключением $\delta(u_1)$, имеют степень 2. Аналогично на интервале $\beta(u_3)$, который является частью интервала $\beta(u_2)$, все вершины, за исключением $\beta(u_3)$, имеют степень 2. Степень 1 имеют те вершины, которые попадают между интервалами $\beta(u_1)$ и $\beta(u_3)$, если $\beta(u_1) \cap \beta(u_3) = \emptyset$. Число таких вершин равно $u_3 - (n' + u_1)$. Так как вершины со степенью 3 отсутствуют, то граф будет несвязен, если число вершин степени 1 превышает 2. Поэтому для связности графа необходимо выполнение условия

$$u_3 - (n' + u_1) + \delta(u_3) + \delta(u_2) + \delta(u_1) \leq 2.$$

Подставляя в это выражение $n' = u_2 - 1$ и раскрывая символы δ , получаем

$$u_3 - u_2 - u_1 + 1 + 3 - u_3 \pmod{2} - u_2 \pmod{2} - u_1 \pmod{2} \leq 2,$$

что и дает нам условие б).

Покажем теперь, что при $D > 2$ граф несвязен. Так как $r_1 = \alpha_1 D$, а $r_2 = \alpha_2 D$, то $u_3 \equiv u_2 \equiv u_1 \pmod{D}$. Любая последовательность вершин использует только два числа из D классов вычетов по модулю D . Все оставшиеся вершины графа, представляющие $D - 2$ класса вычетов, не смежны с ними, так как $D \geq 3$.

Пусть $D = 2$ и u_1 — нечетная образующая. Не нарушая общности, полагаем $r_1 > r_2$. В противном случае путем перенумерации вершин $x'_i = n + 1 - x_i$ этого всегда можно добиться. Составим прямоугольную матрицу размером $r_2 \times r_1$. Расположим в ней все числа от 1 до n так, чтобы каждое x находилось в строке с номером $i \equiv x \pmod{r_2}$ и столбце с номером $j \equiv x \pmod{r_1}$. Так как $D = 2$, то всегда $i + j \equiv 0 \pmod{2}$, и числа в таблице располагаются в шахматном порядке. В зависимости от значения n возможны некоторые различия таблицы. Пусть $\beta \equiv n \pmod{r_1} = n - r_1 \lfloor n/r_1 \rfloor$.

$$1) \beta = r_1 - r_2.$$

Рассмотрим столбцы 1 и β . В первом столбце расположены все числа от 1 до $kr_1 + 1$, где $k = \lfloor n/r_1 \rfloor$. В столбце β расположены все числа от $\beta = n - kr_1$ до n . Составим последовательность $n, 1, n - r_1, 1 + r_1, \dots, \beta, n - \beta + 1$. Сумма двух соседних чисел равна $n + 1$ или $n + 1 - r_1 = u_2 - r_1 = u_1$. Это означает, что соответствующие вершины составляют цепь. Нетрудно убедиться, что таким свойством обладают и другие пары столбцов $(2, \beta - 1), (3, \beta - 2), \dots, (\beta/2, \beta/2 + 1)$. Возьмем теперь столбцы $\beta + 1$ и r_1 . В первом столбце расположены все числа, начиная от $\beta + 1$ до $(k - 1)r_1 + \beta + 1 = n + 1 - r_1 = u_1$, а в последнем столбце — числа от r_1 до kr_1 . Здесь также последовательность чисел $kr_1, \beta + 1, (k - 1)r_1, r_1 + \beta + 1, \dots, u_1$ соответствует цепи с образующими $n + 1$ и u_1 . Этим свойством обладают и пары столбцов $(\beta + 2, r_1 - 1), (\beta + 3, r_1 - 2), \dots, \lfloor (u_1 - 1)/2, (u_1 + 1)/2 \rfloor$.

Теперь рассмотрим столбцы 1 и r_1 . В первом столбце можно найти число $1 + r_1$, а в последнем — kr_1 . Их сумма составляет $kr_1 + r_1 + 1 = n - \beta + r_1 + 1 = n + 1 - (r_1 - r_2) + r_1 = n + 1 + r_2 = u_3$. Аналогичным свойством обладают и пары столбцов $(2, r_1 - 1)$, $(3, r_1 - 2)$, ..., $(r_1/2, r_1/2 + 1)$. Сделаем гомоморфное отображение: множество вершин, записанных в i -м столбце, стянем в одну i -ю вершину. Получаем r_1 — вершинный граф H , а его образующими пусть будет множество $V = \{ \beta + 1, r_1 + 1, r_1 + \beta + 1 \}$, где $\beta + 1$ — нечетное число, а r_1 — четное число.

Теперь вопрос о связности графа G сводится к вопросу о связности графа H , который легко решается.

По теореме 2.11 граф H представляет собой фактороид. Он будет связан только тогда, когда будет гамильтоновым. Для этого необходимо, чтобы $\beta/2$ и $r_1/2$ были взаимно простыми числами. Это действительно так, ибо $\beta = r_1 - r_2$, $\beta/2 = r_1/2 - r_2/2$. Но $(r_1/2, r_2/2) = 1$, поэтому H — гамильтонов цикл, а граф G — связан.

$$2) \quad 2 \leq \beta < r_1 - r_2.$$

Аналогично рассуждая, приходим к выводу, что и в данном случае вершины, соответствующие числам в столбцах i и j , составляют цепь, если $i + j \equiv (\beta + 1) \pmod{r_1}$. При этом образующими будут числа u_1 и $n + 1$.

Выберем в столбце $r_2 + \beta$ это же число. В первом столбце есть число $kr_1 + \beta + r_2 + 1 = n + 1 + r_2 = u_3$. Аналогичным свойством обладают и пары столбцов $(2, r_2 + \beta - 1)$, $(3, r_2 + \beta - 2)$, ..., $[(r_2 + \beta)/2, (r_2 + \beta)/2 + 1]$. То же справедливо и в оставшихся столбцах, если взять пары $(r_2 + \beta + 1, r_1)$, $(r_2 + \beta + 2, r_1 - 1)$, ..., $[(r_2 + r_1 + \beta)/2, (r_2 + r_1 + \beta)/2 + 1]$. Таким образом, здесь можно сделать гомоморфные отображения графа G на граф H с образующими $V = \{ \beta + 1, r_2 + \beta + 1, r_1 + \beta + 1, r_1 + r_2 + \beta + 1 \}$. Этот граф является

гамильтоновым, так как полуразность первых двух образующих и $r_1/2$ — взаимно простые числа. И в этом случае граф G связан.

$$3) r_1 - r_2 < \beta \leq r_1.$$

В этом случае при подобных рассуждениях получаем гомоморфные отображения графа G на граф H с аналогичными образующими $V = \{\beta - r_1 + r_2 + 1, \beta + 1, r_1 + \beta + 1, r_2 + \beta + 1\}$. Полуразность между первыми двумя образующими равна $r_1/2 - r_2/2$, как и в случае 1), поэтому граф H — гамильтонов, что равносильно связности графа G .

Так как случай $\beta = 0$ равносильен $\beta = r_1$, то рассмотрены все случаи, когда $D = 2$. Для доказательства теоремы необходимо еще рассмотреть случай $D = 1$ при произвольных образующих. Вначале докажем одно утверждение.

Лемма 2.16. *NA-граф G с множеством из четырех образующих $U = \{u_1, u_2, n + u_1, n + u_2\}$ ($u_1, u_2 < n - 1$) изоморфен графу H с образующими $V = \{u_2 - \Delta, n + u_1 - \Delta, n + u_2 - \Delta\}$, где $\Delta = u_1 - 2 + u_1 \pmod{2}$.*

Будем изображать граф G в виде горизонтального ряда вершин, ребра, соответствующие образующим u_2 и $n + u_2$, показаны в верхней части рисунка (см. рис. 2.9), а остальные ребра — в нижней части. Возьмем вершину 1 и вместе со смежными ей ребрами переместим на место вершины $n + 1$. Естественно, граф от этого не изменится. Если теперь перенумеруем вершины графа по правилу ($1 \rightarrow n, i \rightarrow i - 1$), то получим изоморфный *NA-граф* с образующими $U' = \{u_1 - 2, u_2 - 2, n + u_1 - 2, n + u_2 - 2\}$. Эти операции можно продолжать до тех пор, пока позволит значение u_1 . Если u_1 — нечетное, то можно переместить вправо все вершины от 1 до $(u_1 - 1)/2$. Если же u_1 — четное, то вершина $u_1/2$ — висячая и в конце концов она станет первой. В первом случае максимальное значение вычитаемой величины Δ равно $2 \lceil (u_1 - 1)/2 \rceil = u_1 - 1$, а во втором — $2(u_1/2 - 1) = u_1 - 2$, что и требовалось доказать.

Как и для $D = 2$, строим аналогичную таблицу, содержащую все числа от 1 до k . Рассмотрим два случая.

а) $1 \leq \beta < r_1 - r_2$.

Определим пары столбцов (i, j) , номера которых являются решениями уравнения $i + j \equiv (\beta + 1) \pmod{r_1}$. При этом, учитывая произвольность значений β , в качестве решений для $\beta \equiv 1 \pmod{2}$ берем значения $i = j = \beta/2$, а при $\beta \equiv 0 \pmod{2}$ и $r_1 \equiv 1 \pmod{2}$ — значения $i = j = (r_1 + \beta + 1) / 2$. В результате действия гомоморфизма получаем модульный граф H с образующими $V = \{\beta + 1, r_2 + \beta + 1, r_1 + \beta + 1, r_1 + r_2 + \beta + 1\}$, где $\beta + 1$ может быть четным или нечетным. По лемме 1.19 этот граф с четырьмя образующими изоморфен графу H' с образующими

$$V' = \{r_2 + 1 + \beta_0 \pmod{2}, r_1 + 1 + \beta_0 \pmod{2}, r_1 + r_2 + 1 + \beta_0 \pmod{2}\},$$

где $\beta_0 = \lceil n \pmod{r_1} \rceil \pmod{2}$. Таким образом, проблема связности исходного графа с параметрами (n, r_1, r_2) свелась к той же проблеме, но уже для графа с меньшими параметрами (n, r_1, r_2) , где

$$n' = r_1 + \lceil n \pmod{r_1} \rceil \pmod{r_2}, r'_1 = \max\{r_1 - r_2, r_2\},$$

$$r'_2 = \min\{r_1 - r_2, r_2\};$$

б) $r_1 - r_2 \leq \beta < r_1$.

В этом случае аналогичные рассуждения приводят к построению гомоморфного образа — графа H с четырьмя образующими $V = \{\beta - r_1 + r_2 + 1, \beta + 1, r_2 + \beta + 1, r_1 + \beta + 1\}$. Применяя лемму 2.16, получаем изоморфный граф H' , у которого множество образующих есть

$$V' = \{r_1 - r_2 + 1 + \gamma_0, r_1 + 1 + \gamma_0, 2r_1 - r_2 + 1 + \gamma_0\},$$

где $\gamma_0 = \lceil n \pmod{r_1} - r_1 + r_2 \rceil \pmod{2}$. Таким образом, здесь проблема также свелась к той же проблеме, но с меньшими параметрами (n', r'_1, r'_2) , где

$$n' = r_1 + \lceil n \pmod{r_1} - r_1 + r_2 \rceil \pmod{2},$$

$$r'_1 = \max \{ r_1 - r_2, r_2 \}, r'_2 = \min \{ r_1 - r_2, r_2 \}.$$

Случаи, когда $\beta = r_1 - r_2$ (или $\beta = r_1$), сразу же приводят к гомоморфному графу с тремя образующими и с меньшими параметрами $V = \{ \beta + 1, r_1 + 1, r_1 + \beta + 1 \}$, у которого r'_1 и r'_2 имеют такие же значения.

Последовательность гомоморфизмов приводит к наименьшему графу с тремя образующими, которые нельзя преобразовать, т. е. к одному из типов:

$$V_1 = \{ 3, n + 1, n + 3 \}, V_2 = \{ 3, n + 1, n + 2 \}, V_3 = \{ 4, n + 1, n + 4 \}$$

и

$$V_4 = \{ 4, n + 1, n + 3 \}.$$

Последняя образующая в этих графах зависит от второй составляющей в значениях n' . Значения $r_1^{(k)}$ и $r_2^{(k)}$ после k шагов получаются по алгоритму Эвклида при нахождении $\text{НОД}(r_1, r_2)$, поэтому всегда $\text{НОД}(r_1^{(k)}, r_2^{(k)}) = 1$. Первый граф является гамильтоновым циклом, т.е. связан.

Второй граф без первой образующей, как было показано, представляет собой цепь длиной n , поэтому он также связан.

В третьем графе первая образующая связывает вершины 1 и 3. Вершина 2 — висючая и является началом цепи, соответствующей образующим $n + 1$ и $n + 4$. Ее вершины образуют последовательность $2, n - 1, 5, n - 4, 8, \dots$, в которой операции выполняются по модулю n . Граф несвязен, если на каком-то шаге будут равны два соседних члена последовательности. Это возможно для значений $n = 6, 9, 12, \dots$. Но тогда $r_1 \equiv r_2 \equiv 0 \pmod{3}$, что противоречит начальным условиям. Следовательно, $n \equiv 0 \pmod{3}$ и тогда последовательность пробегает все вершины, что равносильно связности графа.

В четвертом графе последовательность имеет вид $2, n - 1, 4, n - 3, 6, \dots$. Если она обрывается раньше, чем пробегает все вершины, то $n \equiv 1 \pmod{2}$, откуда $r_1 \equiv r_2 \equiv 0 \pmod{2}$, что также невозможно. Этим завершается доказательство леммы.

Рассмотрим произвольный NA -граф с тремя образующими и исследуем все случаи. Если $u_i \geq n + 1$, то появляются изолиро-

ванные вершины, коды которых начинаются с 1. Если же $u_1 \leq n+1$, то изолированные вершины имеют коды n и меньше. Общее их число равно

$$\frac{u_1 - u_3 + |n+1 - u_1| + |n+1 - u_3|}{2}.$$

Назовем граф неплотным, если $\Delta u = u_3 - u_2 - u_1 + 1 > 0$. В этом случае граф не имеет вершин со степенью 3 и число компонент равно половине числа вершин со степенью 1. Величина Δu это число определяет с точностью до тех вершин, которые имеют коды $u_i/2$ для четных образующих. В сумме оно равно $\Delta u + \delta(u_1) + \delta(u_2) + \delta(u_3)$. Существенную роль играет отношение $\max\{\gamma_1, \gamma_2\} / \max\{r_1, r_2\}$. Если оно равно целому числу, то в графе существует $\lfloor \min\{u_1, 2u_2 - u_3\} / 2 \rfloor$ компонент, представляющих вложенные друг в друга циклы (самый внутренний цикл может вырождаться в цепь).

Теорема 2.17. Число компонент связности NA -графа с множеством $U = \{u_1, u_2, u_3\}$ равно

$$\frac{|n+1 - u_1| + |n+1 - u_3| - u_2 - u_1 \pmod{2} - u_2 \pmod{2} - u_3 \pmod{2}}{2} + 2,$$

если же $\max\{u_3 - u_2, u_2 - 1\} / \min\{u_3 - u_2, u_2 - u_1\}$ есть целая величина, то это число увеличивается на

$$\left\lfloor \frac{2u_2 - u_3 + u_1 + 2 - |u_3 + u_1 - 2u_2|}{4} \right\rfloor - 1.$$

Эта формула получается после суммирования всех перечисленных выше компонент и элементарных преобразований.

Вопрос о связности произвольных NA -графов завершает утверждение. Число компонент связности плотного NA -графа равно

$$\frac{u_1 - u_3 + |n+1 - u_1| + |n+1 - u_3|}{2} + \left\lfloor \frac{D - u_1 \pmod{2}}{2} \right\rfloor + 1, \quad (2.74)$$

где D — наибольший общий делитель чисел $u_3 - u_2$ и $u_2 - u_1$.

Доказательство этого утверждения почти идентично доказательству теоремы 2.16.

2.8. ПРЕДСТАВЛЕНИЕ ОДНОРОДНЫХ ДЕРЕВЬЕВ ПЕРВОГО РАНГА

Представление даже одного из простейших деревьев первого ранга, которое иначе называется *звездой*, в виде NA -графа невозможно, в чем можно непосредственно убедиться, перебирая все случаи кодирования для $n = 4$. При $n = 3$ звезда вырождается в цепь, которую еще можно представить в виде NA -графа. Так как любой граф можно представить в виде арифметического графа (A -графа), то возникает задача об оптимальном представлении.

Обозначим максимальный код вершины в графе N , а n , как и раньше, пусть обозначает число вершин графа. В оптимальном представлении необходимо минимизировать N . Очевидно, что N всегда должно участвовать в оптимальном представлении.

Лемма 2.17. В оптимальном представлении в виде A -графа n -вершинной звезды

$$N \leq 2n - 3.$$

Прежде всего покажем, что в оптимальном представлении всегда присутствует вершина с кодом 1. Если ее нет, то переходя к двойственной кодировке $x'_i = N + 1 - x_i$ и $u'_i = 2N + 2 - u_i$, где N — максимальный код, всегда получаем для наименьшего числа α наибольшее число $N' = N + 1 - \alpha < N$. Это означает, что первая кодировка не была оптимальной.

Рассмотрим матрицу образующих для данного графа $A = (a_{ij})$ размером $N \times N$. Пусть оптимальной кодировкой будет последовательность $x_1 = 1, x_2, x_3, \dots, x_n = N$. Число образующих графа должно быть равным числу ребер $n - 1$. Значение $N = 2n - 3$ достигается при следующей кодировке: всем периферийным (висячим) вершинам присваиваем коды от 1 до $n - 1$, а центральной — код $2n - 3$. Тогда множество образующих будет следующим: $U = \{2n - 2, 2n - 1, \dots, 3n - 4\}$. Так как все суммы кодов периферийных вершин не превышают $2n - 3$, то это будет допустимая кодировка. Двойственная кодировка дает центральной вершине код 1, а периферийным — $2n - 3, 2n - 2, 2n - 1, \dots, n - 1$. На рис. 2.15 приведена кодировка звезды при $n = 8$.

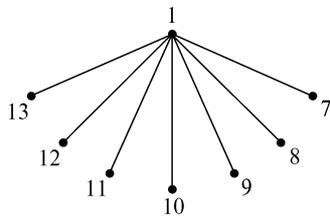


Рис. 2.15

Двойственная кодировка дает центральной вершине код 1, а периферийным — $2n - 3, 2n - 2, 2n - 1, \dots, n - 1$. На рис. 2.15 приведена кодировка звезды при $n = 8$.

Лемма 2.18. Если центр n -вершинной звезды имеет код 1 или $2n - 3$, то кодировка звезды однозначна.

Доказательство. Если код центральной вершины равен 1, то одна из периферийных вершин имеет код $2n - 3$, т. е. имеется одна образующая $u_1 = 2n - 2$. Построим на N -вершинном множестве граф $H(u)$, в котором две вершины смежны, если их коды в сумме дают число $2n - 2$, что автоматически исключает совместное присутствие этих кодов в звезде, так как в ней уже есть соответствующее ребро. Этот граф показан на рис. 2.16, а.

Рассмотрим в таком графе первое ребро $(2, 2n - 4)$. В оптимальную кодировку может войти только один из этих кодов. Допустим, что выбран код 2. Это означает, что в дальнейшем нельзя одновременно выбирать смежные коды k и $k + 1$, так как тогда ребро $(1, k + 1)$ имеет дубликат $(2, k)$. Соединяя ребром последовательные коды, получаем граф, показанный на рис. 2.16, б. В этом графе, кроме вершины 2, необходимо выбрать вершинно-независимое множество мощностью $n - 3$. Но это невозможно, так как число оставшихся вершин равно $2n - 7$, а выбранные вершины требуют удаления не меньшего количества вершин, откуда следует $2n - 6 > 2n - 7$. Следовательно, код 2 в оптимальном выборе не участвует, и остается код $2n - 4$. В результате появляется образующая $u_2 = 2n - 3$, что влечет за собой появление в графе $H(u)$ ребер $(2, 2n - 5), (3, 2n - 6), \dots, (n - 2, n - 1)$, как показано на рис 2.16, в. В этом графе вершинно-независимое множест-

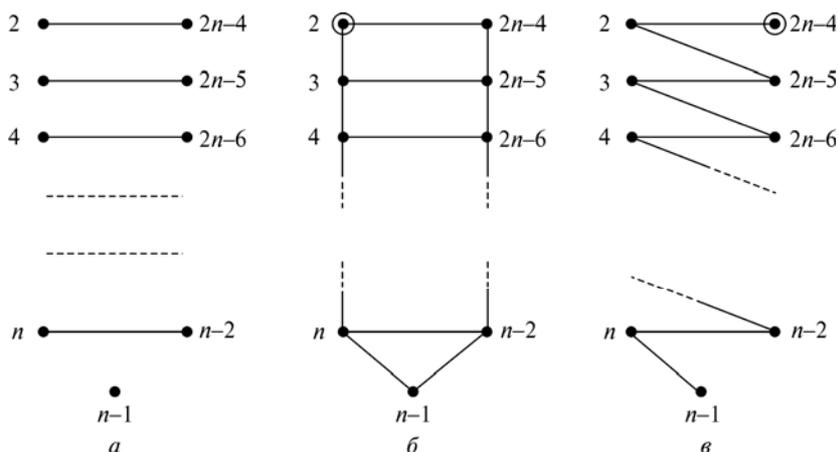


Рис. 2.16

во мощности $n - 2$ выбирается единственным образом, что дает кодировку, как в лемме 2.17.

Теорема 2.18. В оптимальном представлении n -вершинной звезды

$$N = 2n - 3.$$

Для доказательства теоремы докажем, что если код центральной вершины не равен 1 или $2n - 3$, то путем перебора всех кодировок этой вершины нельзя уменьшить оценку леммы 2.17. Доказательство разбивается на части.

1. Пусть код центральной вершины равен $2k$ ($k \geq 1$). Достаточно ограничиться случаем $2k \leq n - 1$, так как иначе можно к нему возвратиться после замены $x'_i = N + 1 - x_i$. Этот код задает две образующие $u_1 = 2k + 1$ и $u_2 = 2n - 3 + 2k$. Построим граф типа графа $H(u)$ в лемме 2.17. Это будет граф, где соединены ребрами вершины, коды которых в сумме равны $2n - 3 + 2k$ или $2k + 1$. Будем обозначать на рисунках такие ребра горизонтальными линиями.

Кроме того, ребрами надо соединить те вершины, коды которых дают разность $2k - 1$ или $2n - 3 - 2k$. Действительно, если существует в оптимальной кодировке код y и $y + 2k - 1$, то образующая $y + 2k$, соответствующая ребру $(y, 2k)$, соединяет вершины 1 и $y + 2k - 1$, что недопустимо. Все такие коды образуют арифметическую прогрессию с разностью $d = 2k - 1$. Так как $2n - 3 - 2k \equiv [(2k + 1) \bmod (2n - 4)]$, то будем считать ее естественным продолжением для чисел, больших $2n - 4$, в классе вычетов по этому модулю. На рисунках будем изображать эти ребра вертикальными линиями.

Если $2k \neq n - 1$, то существует код, который заведомо не используется. Его можно найти из соотношения $2k + x = 2n - 2$, и это равно сумме $1 + N$. Такой код равен $2n - 2k - 2$. Вершина с этим кодом соединена горизонтальным ребром с вершиной, код которой $2n - 3 + 2k - (2n - 2k - 2) = 4k - 1$. Проследим, начиная с этой вершины, куда ведет вниз цепь из вертикальных ребер, соответствующая арифметической прогрессии. Покажем, что она ведет к вершине $n - 1$. Для этого необходимо решить уравнение

$$4k - 1 + (2k - 1)t \equiv (n - 1) \pmod{2n - 4}. \quad (2.75)$$

Это уравнение всегда имеет решение, в чем можно убедиться, подставив значение $t = n - 4$. В результате несложных преобразований получим истинное соотношение

$$(k-1)(2n-4) \equiv 0 \pmod{2n-4}.$$

Вершина $(n-1)$ связана горизонтальным ребром с вершиной $2n-3+2k-(n-1) = n-2+2k$. Но код этой вершины отличается от кода вершины $n-1$ на величину $2k-1$, т. е. арифметическую прогрессию можно продолжить через горизонтальное ребро и далее вверх до вершины с кодом $2n-3+2k-(4k-1+2k-1) = 2n-4k-1$.

Если $\text{НОД}(2k-1, n-2) = 1$, то $t = n-4$ является наилучшим решением (2.75), тогда граф $H(u_1, u_2)$ состоит только из одной компоненты (рис. 2.17). В нем занято $1 + 2(n-4) = 2n-7$ вершин, что с вершинами $1, 2n-3, 2k, 2n-2-2k$ составляет исходное число $2n-3$. В графе $H(u_1, u_2)$ для оптимальной кодировки необходимо выбрать $n-3$ попарно несмежных вершин.

Очевидно, это можно сделать единственным образом, начиная с вершины $4k-1$. Удаляя смежные вершины, далее выбираем $2n-4k-1, 8k-3$ и т.д. В результате в оптимальной кодировке окажутся все нечетные вершины от 1 до $2n-3$. Таким образом, все образующие в звезде будут нечетными, поэтому ни одна пара висячих вершин не будет соединена, что и требовалось.

Пусть теперь $\text{НОД}(2k-1, n-2) = \alpha > 1$. Тогда уравнение (2.75) при $2k-1 = \alpha s$ и $2n-4 = 2\alpha q$ преобразуется в следующее:

$$s(t+2) = q \pmod{2q}. \quad (2.76)$$

Решением уравнения (2.76) является $t = q - 2 = (n-2)/\alpha - 2$. В этом случае граф H состоит из $(\alpha+1)/2$ компонент. В компоненте $p(1)$, начинающейся с вершины $4k-1$, содержатся все коды, равные $1 \pmod{\alpha}$. Возьмем вершину с кодом 2. Она связана радиальным ребром с вершиной $2k-1$. Во внешней круговой цепи будут перечислены все коды, равные $2 \pmod{\alpha}$, а во внутренней круговой цепи — все коды, равные $0 \pmod{\alpha}$, так как $2k-1 = 0 \pmod{\alpha}$. Обозначим эту компоненту графа $p(2,0)$. Уравнение $st \equiv 0 \pmod{2q}$ имеет только одно решение $t = 2q$, поэтому длина этих цепей равна $2q$ и они замыкаются в цикл, что вместе с внутренним таким же циклом дает круговую лесенку (рис. 2.18). Аналогично по-

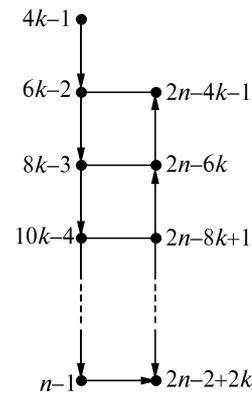


Рис. 2.17

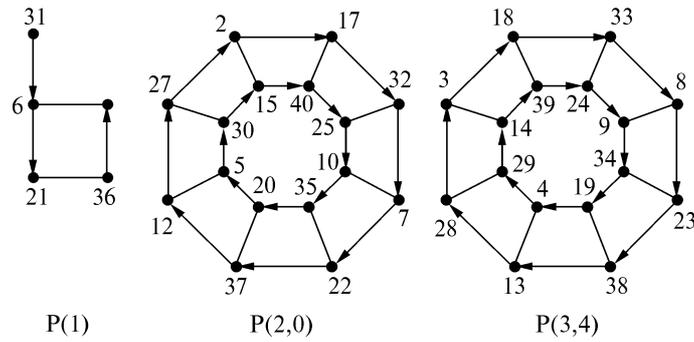


Рис. 2.18

лучаем еще компоненты $p(3, \alpha - 1)$, $p(4, \alpha - 2)$, ..., $p[(\alpha + 1)/2, (\alpha + 3)/2]$.

Рассмотрим пример на рис. 2.18, где $n = 22$, $k = 8$. В этом графе выбор $n - 3$ взаимно несмежных вершин уже не очевиден. В компоненте $p(1)$ это выполняется, как и раньше, однозначно. В других компонентах $p(i, j)$ необходимо выбрать либо все четные коды, либо все нечетные.

В компоненте $p(2, 0)$ в оптимальную кодировку входит либо код 2, либо код $2k - 1$. Допустим, что вначале выбран код 2. Это означает, что в графе H надо соединить ребрами вершины, коды которых дают сумму $2k + 2$ или разность $2k - 2$.

Рассмотрим теперь компоненту $p[(\alpha + 1)/2, (\alpha + 3)/2]$. Во внешнем ее цикле перечисляются все коды, не превышающие $2n - 4$ и равные $(\alpha + 1)/2 \pmod{\alpha}$. Во внутреннем цикле — такие же коды, равные $(\alpha + 3)/2 \pmod{\alpha}$. Это означает, что во внутреннем цикле находятся все коды, превышающие коды внешнего цикла на 1.

Возьмем вершину $(\alpha + 1)/2$ и следующую за ней $2k - 1 + (\alpha + 1)/2$. Последнюю вершину необходимо соединить ребром с вершиной $(\alpha + 3)/2$ внутреннего цикла, так как разница их кодов равна $2k - 2$. Эти коды одинаковой четности, поэтому их нельзя выбрать для оптимальной кодировки, т. е. для выбора остается код $(\alpha + 1)/2$. С другой стороны, во внутреннем цикле есть вершина с кодом $2k - 1 + (\alpha + 3)/2$, которую необходимо соединить с вершиной $4k - 2 + (\alpha + 1)/2$. Но последняя вершина одинаковой четности с $(\alpha + 1)/2$, что обуславливает невозможность ее выбора для оптимальной кодировки. Это противоречие делает невозможным первоначальный выбор вершины 2 в $p(2,0)$.

Остается взять код $2k - 1$, что автоматически выбирает все вершины с нечетными кодами в этой компоненте, в том числе смежную с вершиной 2 вершину $2k + 1$. Это означает, что в дальнейшем нельзя выбирать соседние коды. Поэтому в компоненте $p(3, 2k - 2)$ надо выбирать код 3 и все нечетные коды. В компоненте $p(4, 2k - 3)$ уже нельзя выбирать код 4, а надо взять код $2k - 3$ и все нечетные коды.

Рассуждая подобным образом, приходим к выводу, что если код центральной вершины меньше $n - 1$ и равен $2k$, то единственной оптимальной кодировкой висячих вершин звезды является последовательность всех нечетных кодов от 1 до $2n - 3$.

2. Код центральной вершины равен $2k + 1 < n - 1$ ($k \geq 1$).

Основное уравнение, которое связывает вершину $4k + 1$ и запрещенную вершину $2n - 2k - 3$, имеет вид

$$4k + 1 + 2kt \equiv (2n - 2k - 3) \pmod{(2n - 4)}. \quad (2.77)$$

Оно преобразуется к следующему:

$$k(t + 3) \equiv 0 \pmod{(n - 2)}. \quad (2.78)$$

Всегда существует решение $t = (n - 2)/\text{НОД}(k, n - 2) - 3 = \Delta - 3$.

Теперь рассмотрим цепи, представляющие арифметическую прогрессию и соединяющие вершины $n - 1$, $k + 1$ и $n + k - 1$ в графе H , которые мы назовем *срединными*, так как они являются средним арифметическим уже заданных вершин 1, $2k + 1$ и $2n - 3$. Вершины $k + 1$ и $n + k - 1$ в графе $H(u)$ принадлежат треугольным граням. Например, $k + 1$ связана с $3k + 1$, эта же вершина связана с вершиной, код которой $2n + 2k - 2 - (3k + 1) = 2n - k - 3$, а последняя, если прибавить к ней код $2k$, связана с вершиной $2n - k - 3 + 2k = k + 1 + (2n - 4) \equiv (k + 1) \pmod{(2n - 4)}$. Аналогично убеждаемся в том, что составляют треугольник и вершины с кодами $n + k - 1$, $n + 3k - 1$ и $n + k - 1$.

Рассмотрим уравнение цикла, определяющего арифметическую прогрессию:

$$2kt \equiv 0 \pmod{(2n - 4)}, \quad (2.79)$$

которое равносильно следующему: $kt \equiv 0 \pmod{(n - 2)}$. Очевидно, что его решением есть $t = \Delta$. При построении замкнутого цикла, являющегося арифметической прогрессией, используются повороты цепей (на рисунках) в вершинах, принадлежащих только трем элементам. Эти элементы — два треугольника с кодами $k + 1$ и $n + k - 1$, а также горизонтальное ребро $(n - 1, n + 2k - 1)$. В последнем сумма кодов вершин равна сумме максимального кода

$2n - 3$ и центрального кода $2k + 1$; с другой стороны, их разница равна $2k$, т. е. коды ребра принадлежат арифметической прогрессии. Вершины $4k + 1$ и $k + 1$ связаны цепью с вершиной $n - 1$, если имеет решение одно из уравнений:

$$\begin{aligned} 2k(t + 2) &\equiv (n - 2) \pmod{(2n - 4)}, \\ k(2t + 1) &\equiv (n - 2) \pmod{(2n - 4)}. \end{aligned} \quad (2.80)$$

Если Δ — четное число, то $t = \Delta/2 - 2$, и связанными будут вершины $4k + 1$ и $n - 1$, если же Δ — нечетное число, то $t = (\Delta + 1)/2$ и связанными будут вершины $k + 1$ и $n - 2$. В первом случае два треугольника принадлежат одной компоненте и всего таких компонент будет $\Delta + 1$. Во втором случае число компонент также равно $\Delta + 1$, но треугольники принадлежат разным компонентам. Таким образом, граф $H(u)$ состоит из $2n - 7$ вершин, и в нем необходимо выбрать вершинно-независимое множество мощности $n - 4$. Однако, ввиду отсутствия треугольников этого сделать нельзя. Это равносильно утверждению о несуществовании оптимальной кодировки, если код центральной вершины нечетный.

3. Остается доказать существование оптимальной кодировки, если код центральной вершины равен $n - 1$. В этом случае граф $H(u)$ состоит из $\lfloor n/2 \rfloor - 1$ компонент, каждая из которых представляет собой связный квадрат с такими кодами вершин: $(i, n - i, n + i - 2, 2n - i - 2)$ ($i = 2, 3, \dots, \lfloor (n - 1)/2 \rfloor$). Если n — четное, то последняя компонента есть вертикальное ребро с кодами $(n/2, 3n/2 - 2)$.

Пусть $n \equiv 1 \pmod{2}$ (рис. 2.19, $n = 15$), тогда центральная вершина имеет четный код.

Возьмем для оптимальной кодировки в графе $H(u)$ вершину 2. Это означает, что в графе $H(u)$ надо соединить ребрами вершины, разность кодов которых равна $n - 3$. В последнем квадрате появится диагональ, соединяющая вершины $(n + 1)/2$ и $(3n - 5)/2$ (на рис. 2.19 вершины 8 и 20), т. е. в этом квадрате можно выбрать

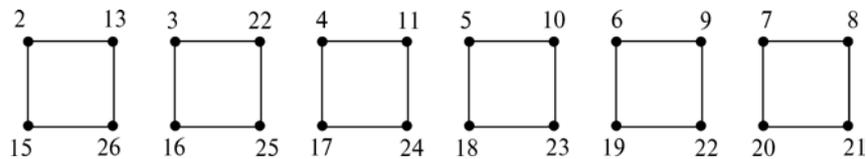


Рис. 2.19

только вершину $(n - 1)/2 = 7$. Эта вершина соединена с левой нижней вершиной (код которой $(3n - 7)/2 = 19$) предыдущего квадрата, поэтому в нем можно выбрать одну вершину $(n - 3)/2 = 6$.

Рассуждая таким образом и далее, приходим к выводу, что оптимальной кодировкой является выбор в квадратах левых верхних и правых нижних вершин, что дает единственные коды $2, 3, \dots, (n - 1)/2$ и $2n - 3, 2n - 4, \dots, (3n - 3)/2$. Кроме того, как было показано раньше, оптимальной кодировкой является набор всех нечетных чисел от 1 до $2n - 3$.

Пусть теперь $n \equiv 0 \pmod{2}$. Если мы выберем вершину 2 в первом квадрате, то так же, как и прежде, в графе $H(u)$ надо выбрать те же вершины в квадратах, а на ребре можно выбрать одну любую вершину, ибо они являются двойственными относительно кода $2n - 2$. Получаются две оптимальные кодировки: $2, 3, \dots, n/2, 3n/2 - 1, 3n/2, \dots, 2n - 3$, при этом вторая получается из этой заменой кода $n/2$ на двойственный $3n/2 - 2$.

Возьмем теперь в первом квадрате два других кода $n - 2$ и n . Это означает, что в графе $H(u)$ нужно соединить все вершины, коды которых являются соседними. По этой причине верхняя вершина одинокого ребра соединится с двумя верхними, а нижняя — с двумя нижними вершинами предыдущего квадрата. Тем самым коды этого одинокого ребра не могут входить в оптимальную кодировку, что невозможно. Следовательно, для четного n существует только одна оптимальная кодировка.

Следствие. Число оптимальных кодировок n -вершинной звезды равно

$$n - n \pmod{2}.$$

Действительно, число четных кодов, которые присваиваются центральной вершине, равно $n - 2$. При четных n еще добавляется две кодировки, когда код центральной вершины равен $n - 1$, а для нечетных n — только одна кодировка.

2.9. ОПТИМАЛЬНАЯ КОДИРОВКА ОДНОРОДНЫХ ДЕРЕВЬЕВ ВТОРОГО РАНГА

Напомним, что *рангом дерева* называется длина максимального пути от центра к периферийной (висячей) вершине. Часто центр дерева выбирают в качестве корневой вершины. Будем рассматривать однородные деревья степени ρ , у которых все висячие вершины находятся на расстоянии k от корня. Иначе эти вершины называются *вершинами верхнего яруса*.

Пусть $k = 2$. Обозначим корень дерева как y_n , где n — число всех вершин, вершины первого яруса — y_i ($i = 1, 2, \dots, \rho$), остальные вершины второго (верхнего) яруса — y_j ($j = \rho + 1, \rho + 2, \dots, n - 1$).

Известно [38], что набор цепей можно закодировать с помощью двух образующих. Если сделать правильную раскраску ребер дерева (в нашем случае это делается однозначно с точностью до перестановки цветов), то понадобится ρ красок. Если поставить в соответствие каждой краске одну образующую, то возникает вопрос о построении соответствующей кодировки.

Для того чтобы дать ответ на этот вопрос, рассмотрим одну проблему из теории чисел.

Задача о разностях. Для каждого $\rho \geq 2$ найти целые числа $x_\rho > x_{\rho-1} > \dots > x_1 = 1$ такие, что:

- 1) для любых $1 \leq i, j \leq \rho$ ни одна разность $|x_i - x_j|$ не повторяется;
- 2) x_ρ — минимальное.

В общем виде эта задача еще не решена, хотя для $\rho \leq 11$ с помощью ЭВМ удалось определить все такие числа. При этом получаются неединственные решения.

В табл. 2.4 [74] приведены все результаты этих решений. Здесь до $\rho = 7$ включительно указаны все варианты решений, а дальше приведено только по одному варианту. В третьем столбце вычислены разности между соседними числами последовательности x_i .

Возьмем $\rho = 6$ и рассмотрим матрицу A размерностью $(\rho - 1) \times (\rho - 1)$, у которой на главной диагонали расположены элементы из третьего столбца (последовательные разности):

$$A = \begin{pmatrix} 1 & 4 & 10 & 12 & 17 \\ & 3 & 9 & 11 & 16 \\ & & 6 & 8 & 13 \\ & & & 2 & 7 \\ & & & & 5 \end{pmatrix}.$$

Ниже диагонали все $a_{ij} = 0$, а для a_{ij} ($j > i$) элементы образуются по правилу

$$a_{ij} = a_{ii} + a_{i+1, i+1} + \dots + a_{jj}.$$

Таблица 2.4

ρ	x_ρ	Разность	Последовательность
2	2	1	1,2
3	4	1,2	1,2,4
4	7	1,3,2	1,2,5,7
5	12	1,3,5,2	1,2,5,10,12
6	18	2,5,1,3	1,3,8,9,12
		1,3,6,2,5	1,2,5,11,13,18
		1,3,6,5,2	1,2,5,11,16,18
		1,7,4,2,3	1,2,9,12,14,18
7	26	1,7,3,2,4	1,2,9,13,15,18
		1,3,6,8,5,2	1,2,5,11,19,24,26
		1,6,4,9,3,2	1,2,8,12,21,24,26
		1,10,5,3,4,2	1,2,12,17,20,24,26
		2,1,7,6,5,4	1,3,4,11,17,22,26
		2,5,6,8,1,3	1,3,8,14,22,23,26
8	35	1,3,5,6,7,10,2	1,2,5,10,16,23,33,35
9	45	1,4,7,13,2,8,6,3	1,2,6,13,26,28,36,42,45
10	56	1,5,4,13,3,8,7,12,2	1,2,7,11,24,27,35,42,54,56
11	73	1,3,9,15,5,14,7,10,6,2	1,2,5,14,29,34,48,55,65,71,73

Покажем, что все ненулевые элементы матрицы A не повторяются. Для этого заметим, что по существу $a_{ij} = x_{i+1} - x_i$. Тогда

$$a_{ij} = (x_{i+1} - x_i) + (x_{i+2} - x_{i+1}) + \dots + (x_{j+1} - x_j) = x_{j+1} - x_i.$$

По построению x_i такие, что никакие их разности не совпадают, значит, все a_{ij} различны. Следовательно, любая сумма последовательных элементов главной диагонали матрицы A дает нам неповторимое число. Рассмотрим матрицу

$$B = \begin{pmatrix} 1 & 2 & 5 & 11 & 13 & \underline{18} \\ 6 & 7 & 10 & 16 & \underline{18} & 23 \\ 8 & 9 & 12 & \underline{18} & 20 & 25 \\ 14 & 15 & \underline{18} & 24 & 26 & 31 \\ 17 & \underline{18} & 21 & 27 & 29 & 34 \\ \underline{18} & 19 & 22 & 28 & 30 & 35 \end{pmatrix}.$$

В этой матрице в первой строке записана последовательность x_i . Во второй строке записаны те же элементы, увеличенные на последнее значение разности (т.е. на 5). В третьей строке записаны элементы второй строки, увеличенные на предпоследнее значе-

ние разности (т. е. на 2) и т.д. Как видно, в матрице все элементы, за исключением подчеркнутых, различны. Подчеркнутые элементы образуют диагональ и равны x_p . Эта диагональ обуславливает симметрию для элементов, что обнаруживается и при образовании матрицы:

$$a_{ij} + a_{n+1-j, n+1-i} = 2x_p.$$

Очевидно, что последовательность x_i , построенная для вектора разностей (1, 3, 6, 2, 5), можно построить и для обратного вектора (5, 2, 6, 3, 1). Будем называть такую последовательность *двойственной*, в матрице B ей соответствует первый столбец. Возьмем два произвольных элемента матрицы, одновременно не принадлежащих подчеркнутой диагонали, и покажем, что они различны. Если они находятся в одной строке или в одном столбце, то они различны всегда. Пусть их строки и столбцы не совпадают, т.е. сравниваем a_{ij} и a_{kl} , где $l > j$.

Возможны два случая:

1) $i > k$,

тогда

$$a_{ij} = a_{kj} + d_1, \quad a_{kl} = a_{kj} + d_2.$$

Здесь d_1 и d_2 — сумма последовательных элементов диагонали матрицы A , т. е. различные величины, что равнозначно несовпадению элементов a_{ij} и a_{kl} ;

2) $i < k$,

тогда

$$a_{ij} = a_{kj} - d_1, \quad a_{kl} = a_{kj} - d_2.$$

Здесь d_1 и d_2 имеют те же свойства, что и в случае 1), поэтому всегда a_{ij} не равно a_{kl} .

Вернемся к однородному дереву второго ранга для $\rho = 6$ (рис. 2.20). Представим, что получена кодировка вершин этого дерева, соответствующая оптимальному представлению.

Относительно этой кодировки справедлива следующая теорема.

Теорема 2.19. Для оптимального представления однородного дерева второго ранга степени k справедливо неравенство

$$\max_{i,j} |y_i - y_j| \leq 4(x_p - 1),$$

где x_p — минимальное значение задачи о разностях.

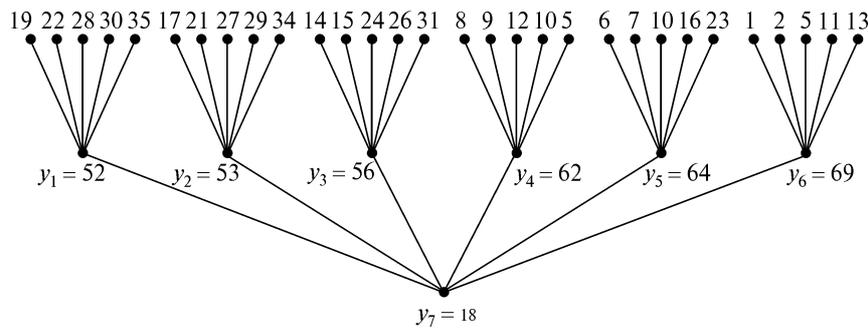


Рис. 2.20

Доказательство. Сделаем перекодировку дерева по правилу $y'_i = y_i - y_n$ для всех вершин. Тогда $y'_n = 0$ и образующие ребер, смежных с корнем, будут иметь вид $u_i = y'_i$ ($i = 1, 2, \dots, \rho$). Те же образующие должны быть и для ребер, соединяющих вершины первого и второго ярусов. Коды висячих вершин, связанных с первой вершиной, будут иметь вид $y'_k = y_i - y_1$. В общем случае коды висячих вершин, связанных с j -й вершиной первого яруса ($j = 1, 2, \dots, \rho$), будут иметь вид $y'_k = y_i - y_j$ ($j \neq i, k = \rho + 1, \rho + 2, \dots, n - 1$).

Таким образом, коды висячих вершин будут представлять всевозможные разности между кодами первых ρ вершин, связанных с корнем дерева, в том числе и отрицательные. Не определяя коды y_i ($i = 1, 2, \dots, \rho$), зафиксируем коды висячих вершин. Прибавим снова к ним число, равное $\max_{i,j} |y_i - y_j| + 1$. Из табл. 2.4 нам известно, что оно равно 18. Таким образом, корень дерева имеет вид $y_n = 18$, а висячие вершины приобретают коды, расположенные в строках матрицы B . При этом висячим вершинам, связанным с k -й вершиной ($k = 1, 2, \dots, \rho$), соответствуют коды строки под номером $(7 - k)$, исключая подчеркнутые элементы, относящиеся к корню дерева.

2.10. О ГАМИЛЬТОНОВОСТИ АРИФМЕТИЧЕСКИХ ГРАФОВ

Если в арифметическом графе образующая $u < n + 1$, то вершина n не охвачена этой образующей; если $u > n + 1$, то вершина 1 не охвачена этой образующей. Вопрос о существовании в

арифметическом графе гамильтонова цикла упирается в анализ образующих этого графа, так как степень каждой вершины при этом должна быть ≥ 2 . В этом случае особую роль приобретает образующая $u = n + 1$, которая охватывает обе вершины 1 и n . Найдем минимальное количество образующих, для которых граф будет гамильтоновым. Очевидно, что для любых двух образующих граф не будет гамильтоновым, так как при этом либо вершина 1, либо вершина n будет иметь степень ≤ 1 .

Теорема 2.20. Арифметический граф с образующими

$$U = \left\{ n, n + 1, n + \left\lfloor \frac{n + 1}{2} \right\rfloor \right\}$$

гамильтонов.

Доказательство. Первые две образующие представляют собой цепь, начинающуюся в вершине n , и образуют последовательность $n, 1, n - 1, 2, n - 2, \dots$. Если $n = 2k$, то цепь заканчивается в вершине k , а если $n = 2k + 1$, то цепь заканчивается в вершине $k + 1$. Чтобы образовать гамильтонов цикл, необходимо эту конечную вершину соединить с вершиной n . Для этого и необходима образующая $u = n + \left\lfloor \frac{n + 1}{2} \right\rfloor$.

Следствие. Двойственный арифметический граф будет иметь образующие

$$U = \left(n + 1, n + 2, \left\lfloor \frac{n + 1}{2} \right\rfloor + 1 \right).$$

Действительно, тогда соответствующая цепь будет иметь конечные вершины 1 и $\left\lfloor \frac{n + 1}{2} \right\rfloor$, чем и определяется последняя образующая. Из теоремы 2.20 и следствия логично сделать также вывод о том, что любой гамильтонов граф с минимальным числом образующих должен всегда иметь образующую $u = n + 1$. На рис. 2.21 приведен пример гамильтонова графа для $n = 11$ (A -граф с $U = (11, 12, 17)$) и двойственного к нему (с $U = (7, 12, 13)$). Будем обозначать Δ — разницу между образующей $u = n + 1$ и ближайшей образующей к нему. В теореме 2.20 были рассмотрены графы с $\Delta = 1$. Рассмотрим графы с $\Delta = 2$, т. е. графы с $u = n + 1$ и $u = n - 1$. Здесь возможны различные случаи:

а) пусть $n = 2k$. В этом случае образующие обеспечивают получение одной цепи $n, 1, n - 2, 3, n - 4, 5, \dots, 2, n - 1$. Тогда до-

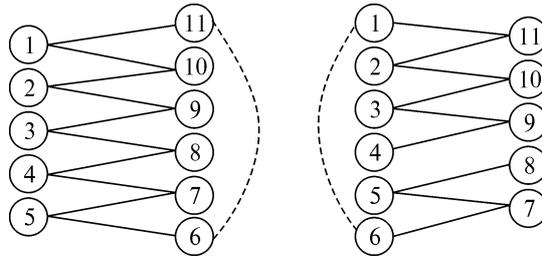


Рис. 2.21

статочно одной образующей $u = 2n - 1$, чтобы объединить эту цепь в гамильтонов цикл;

б) $n = 2k + 1$. В этом случае образующие создают две цепи — одну с четными номерами, одну — с нечетными. В зависимости от значения k это приводит к двум вариантам:

б₁) $n = 4l + 1$. При этом нечетные номера образуют цепь $4l + 1, 1, 4l - 1, 3, 4l - 3, 5, \dots, 2l + 1$, а четные номера образуют цепь $4l, 2, 4l - 2, 4, 4l - 4, 6, \dots, 2l$. Здесь достаточно добавить одну образующую $u = 6l + 1$, чтобы соединить две цепи в гамильтонов цикл. При этом соединятся максимальный номер одной цепи с минимальным номером другой;

б₂) $n = 4l + 3$. При этом нечетные номера образуют цепь $4l + 3, 1, 4l + 1, 3, 4l - 1, 5, \dots, 2l + 1$, а четные номера — цепь $4l + 2, 2, 4l, 4, 4l - 2, 6, \dots, 2l + 2$. Здесь не существует одной образующей, достаточной для того, чтобы объединить две цепи в гамильтонов цикл. Поэтому необходимо две образующие: либо $u_1 = 6l + 3$, $u_2 = 6l + 5$, либо $u_1 = 8l + 5$, $u_2 = 4l + 3$. Однако последний случай сводится к случаю $\Delta = 1$, поэтому он отпадает. Остается первый случай. Таким образом, доказана следующая теорема.

Теорема 2.21. При $\Delta = 2$ для гамильтоновости графа достаточно трех образующих, за исключением $n = 4l + 3$, когда требуется четыре образующих.

Для двойственного графа имеем те же случаи. На рис. 2.22 приведен пример графа для $n = 13$ (A -граф с $n = 13$, $U = (12, 14, 19)$).

Рассмотрим теперь A -графы с $\Delta = 3$.

Теорема 2.22. Для гамильтоновости A -графа с $\Delta = 3$ необходимо и достаточно четных образующих.

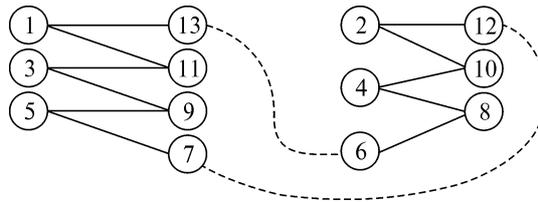


Рис. 2.22

Доказательство. В этом случае две первые образующие имеют вид $u_1 = n + 1, u_2 = n - 2$. Они образуют две цепи, для преобразования их в гамильтонов цикл понадобятся еще две образующих. Рассмотрим три случая:

а) $n \equiv 0 \pmod{3}$. Первую цепь составляют вершины $n, 1, n - 3, 4, \dots, 3, n - 2$. Вторую цепь составляют вершины, номера которых равны $-1 \pmod{3}$. Начальный отрезок цепи $n - 1, 2, n - 4, 5, \dots$. Конец цепи зависит от значения n . Если $n = 2k$, то конец цепи равен $k - 1$, а если $n = 2k + 1$, то $-k + 1$;

б) $n \equiv 1 \pmod{3}$. Первая цепь состоит из вершин, номера которых равны $1 \pmod{3}$. Начальный отрезок цепи $n, 1, n - 3, 4, \dots$, а конечная вершина находится так же, как и в случае а). Вторая цепь состоит из вершин $n - 1, 2, n - 4, 5, \dots, 3, n - 2$;

в) $n \equiv 2 \pmod{3}$. Первую цепь составляет последовательность вершин $n, 1, n - 3, 4, \dots, 2, n - 1$. Вторая цепь состоит из вершин, номера которых равны $0 \pmod{3}$. Начальный отрезок цепи $n - 2, 3, n - 5, 6, \dots$. А конечная вершина определяется так: для $n = 2k$ конец цепи равен $k + 2$, а для $n = 2k + 1$ конец цепи равен $k + 1$.

Во всех случаях для образования гамильтонова цикла необходимо добавить еще две образующие, при этом меньшим их количеством нельзя обойтись. На рис. 2.23 приведен пример для A -графа с $n = 16, U = (14, 17, 21, 31)$. Рассмотрим теперь A -графы с $\Delta = 4$. Для них справедлива следующая теорема.

Теорема 2.23. Для гамильтоновости A -графов с $\Delta = 4$ при $n = 4k, 4k + 3$ достаточно четырех образующих, при $n = 4k + 2$ достаточно трех образующих и при $n = 4k + 1$ необходимо 5 образующих.

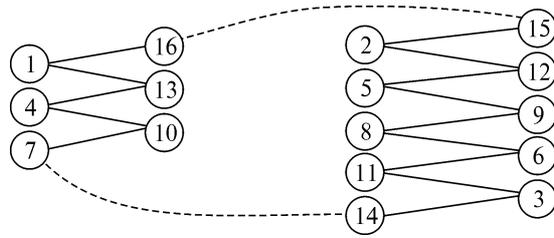


Рис. 2.23

Доказательство. Рассмотрим последовательно все случаи, учитывая то, что образующие равны $u_1 = n + 1$, $u_2 = n - 3$:

а) $n = 4k$. Образующие составляют две цепи. Первая проходит по вершинам $n, 1, n - 4, 5, \dots, 4, n - 3$. Вторая цепь проходит по вершинам $n - 1, 2, n - 5, 6, \dots, 3, n - 2$. Чтобы объединить эти цепи в гамильтонов цикл, необходимо добавить две образующие: $u_1 = 2n - 1$, $u_2 = 2n - 5$ либо $u_1 = 2n - 2$, $u_2 = 2n - 4$;

б) $n = 4k + 3$. Образующие составляют три цепи. Первая цепь проходит по вершинам $n, 1, n - 4, 5, \dots, 3, n - 2$. Вторая цепь проходит по вершинам $n - 1, 2, n - 5, 6, \dots, 2k + 2$. А третья цепь представляет собой последовательность $n - 3, 4, n - 7, 8, \dots, 2k$. Здесь существуют два способа добавления двух образующих, чтобы получить гамильтонов цикл. Первый способ: $u_1 = 2n - 3$, $u_2 = 4k + 2$. Но последняя образующая равна $n - 1$, и тогда приходим к случаю $\Delta = 2$, так как по теореме 2.21 для гамильтоновости графа достаточно четырех образующих. Второй способ: $u_1 = n + 2k$, $u_2 = 8k + 2$. Вследствие чего имеем четыре образующие;

в) $n = 4k + 2$. В этом случае две образующие составляют две цепи. В первой цепи чередуются вершины с номерами $1(\bmod 4)$ и $2(\bmod 4)$. Во второй цепи чередуются вершины с номерами $3(\bmod 4)$ и $0(\bmod 4)$. Первая цепь имеет вид $n, 1, n - 4, 5, \dots, 2, n - 1$, а вторая имеет вид $n - 2, 3, n - 7, 7, \dots, 4, n - 3$. Очевидно, что здесь достаточно одной образующей $u = 4n - 3$, чтобы объединить две цепи в гамильтонов цикл;

г) $n = 4k + 1$. В этом случае образующие составляют три цепи. В первой цепи находятся все вершины, номера которых равны $1(\bmod 4)$, а именно: $n, 1, n - 4, 5, \dots, 2k + 1$. Во второй цепи чере-

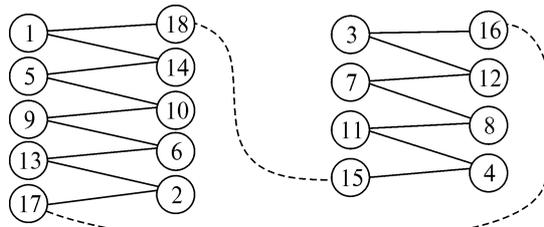


Рис. 2.24

дуются вершины, номера которых равны $2 \pmod{4}$ и $0 \pmod{4}$, а именно: $n-1, 2, n-5, 6, \dots, 4, n-3$. В третьей цепи находятся все вершины, номера которых равны $3 \pmod{4}$, а именно: $n-2, 3, n-5, 7, \dots, 2k-1$. Существует единственная возможность объединить три цепи в гамильтонов цикл с помощью двух образующих. Это $u_1 = 2n-3, u_2 = 4k$. Но последняя образующая равна $n-1$, а это случай $\Delta = 2$, вследствие чего по теореме 2.2 достаточно трех образующих. Следовательно, необходимо добавить три образующие. Итого, в сумме получаем пять образующих.

На рис. 2.24 приведен пример для A -графа с $n=18$ ($U = (15, 19, 33)$). Можно продолжать исследования для A -графов с большим числом Δ , используя те же приемы. Вопрос сводится к перечислению цепей, где встречаются различные вершины с номерами $i \pmod{\Delta}$.

2.11. ОБ ИЗОМОРФИЗМЕ NA -ГРАФОВ

Рассмотрим самые простейшие числовые графы — натуральные арифметические графы с одной образующей, т. е. числовые графы, у которых $X = N_n, U = \{u\}$, а $F(x_i, x_j) = x_i + x_j$. Для них вопрос об изоморфизме решает следующая теорема.

Теорема 2.24. В классе NA -графов с одной образующей каждому графу $G = (X, u)$ с образующей $u \leq n+1$ соответствует множество ему изоморфных, состоящее из:

- а) трех графов с образующими $u_1 = u - (-1)^u, u_2 = 2n + 2 - u, u_3 = 2n + 2 - u + (-1)^u$ для $u < n$;
- б) $3 - u \pmod{2}$ графов тех же типов, где граф u_3 может не существовать при $u = n$;

в) $1 + (-1)^u$ графов первых двух типов, которые могут не существовать для $u = n + 1$.

Доказательство. При распознавании изоморфных графов используются инварианты графа, среди которых наиболее важными являются: 1) число вершин; 2) число ребер; 3) вектор степеней вершин $S = (s_1, s_2, \dots, s_n)$, выписанный в порядке неубывания $s_1 \leq s_2 \leq \dots \leq s_n$. Так как число вершин у рассматриваемых графов совпадает по условию, а степени вершин у NA -графов с одной образующей равны 0 или 1, то достаточно проверить совпадение у всех графов числа ребер.

Рассмотрим матрицу $A = (a_{ij})$ образующих n -вершинного полного NA -графа, в которой $a_{ii} = 0$, а $a_{ij} = i + j$ ($0 < i, j \leq n$):

$$A = \begin{pmatrix} 0 & 3 & 4 & 5 & \dots & n+1 \\ 3 & 0 & 5 & 6 & \dots & n+2 \\ 4 & 5 & 0 & 7 & \dots & n+3 \\ 5 & 6 & 7 & 0 & \dots & n+4 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ n+1 & n+2 & n+3 & n+4 & n+5 & 0 \end{pmatrix}. \quad (2.81)$$

Каждой образующей $u = i + j$ соответствует диагональ (линия), ортогональная основной диагонали, все элементы которой равны u . Исключение составляют четные u , линия которых пересекается с главной диагональю с нулевыми элементами. Обозначим $r(u)$ — число ребер, соответствующих образующей u . Ранее [48] было показано, что $r(u) = r(2n + 2 - u)$. Образующая $u' = 2n + 2 - u$ называется *двойственной* к u . Для $u \leq n + 1$ справедливо уравнение

$$r(u) = \left\lfloor \frac{u-1}{2} \right\rfloor = k. \quad (2.82)$$

Если решить это уравнение относительно u , то получим

$$u \in \{2k + 1, 2k + 2\}. \quad (2.83)$$

Нетрудно убедиться, что элементы в скобках выражаются один через другой по формуле

$$u_i = u_j - (-1)^{u_j}, \quad j = 1, 2. \quad (2.84)$$

Таким образом, если NA -граф с одной образующей u имеет k ребер, то столько же ребер имеет и NA -граф с образующей $u - (-1)^u$. Если еще взять NA -графы с соответствующими двойственными образующими, то получим еще 2 графа с тем же количеством ребер. Все четыре графа имеют k ребер и $n - 2k$ изолированных вершин. Очевидно, что все они изоморфны, что и требовалось доказать.

Пусть $u = n$. Если $n \equiv 0 \pmod{2}$, то число ребер графа равно $\frac{n}{2} - 1$. Такое же число ребер дают и образующие $u_1 = n - 1$, $u_2 = 2n + 2 - n = n + 2$ и $u_3 = 3n + 2 - (n - 1) = 2n + 3$. В результате получим четыре изоморфных графа. Если $n \equiv 1 \pmod{2}$, то число ребер графа равно $\frac{n-1}{2}$. Такое же число ребер дает и образующая $u_1 = n + 1$. Но последняя образующая двойственна сама себе, поэтому добавляется только один изоморфный граф с образующей $u_3 = 2u + 2 - n = n + 2$. Итого, в сумме имеем только три изоморфных графа, а всего к исходному добавляется $3 - u \pmod{2}$ графов.

Осталось рассмотреть случай $u = n + 1$. Если $n \equiv 0 \pmod{2}$, то граф содержит $\frac{n}{2}$ ребра и ни одной изолированной вершины.

Если уменьшить значение u , то число ребер уменьшится. Если увеличить u , то двойственная образующая уменьшится, т. е. опять число ребер уменьшится. Так как $u = n + 1$ — самодвойственная образующая, то ей будет соответствовать единственный граф. Если $n \equiv 1 \pmod{2}$, то этот случай сводится к $u = n$ и $n \equiv 1 \pmod{2}$, т. е. получается всего три изоморфных графа. В общем случае к исходному графу добавляется $1 + (-1)^u$ изоморфных графов. Этим и завершается доказательство теоремы.

На рис. 2.25 приведен пример изоморфизмов NA -графа с $n = 10$ и $u = 8$.

Теорема 2.24 дает исчерпывающий ответ об изоморфизме NA -графов с одной образующей. Однако можно предположить, что NA -граф с одной образующей может быть изоморфным другому графу с несколькими образующими, если число ребер одного графа равно сумме ребер другого, а степени вершин обо-

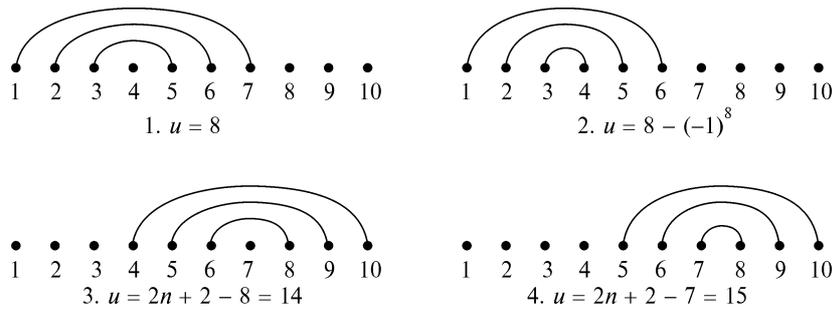


Рис. 2.25

их графов равны 0 или 1. Некоторые пояснения в этот вопрос вносит следующая лемма.

Лемма 2.19. *NA-граф с одной образующей не может быть изоморфным NA-графу с числом образующих больше 2.*

Действительно, в этом случае во втором графе найдутся две образующие v_1 и v_2 , которые либо обе меньше $n + 2$, либо обе больше n . В первом случае существуют ребра $(1, v_1 - 1)$ и $(1, v_2 - 1)$, а во втором случае — ребра $(n, v_1 - n)$ и $(n, v_2 - n)$. Это означает, что во втором графе либо вершина 1, либо вершина n имеют степень, превышающую 1. А это противоречит тому, что первый граф таких вершин не имеет.

NA-графы с двумя образующими при определенных условиях могут иметь вершины, степень которых не превышает 1. Как следствие леммы 2.19 можно считать, что для них $v_1 \leq n + 1$, а $v_2 \geq n + 1$.

Лемма 2.20. *Необходимыми и достаточными условиями того, что NA-граф с двумя образующими $V = \{v_1, v_2\}$ имеет степени вершин не больше 1, есть следующие:*

- а) $v_1 \leq n - 1$;
- б) $v_2 \geq n + 3$;
- в) $v_2 - v_1 > n - 1$. (2.85)

Первое условие вытекает из того, что если v_2 соответствует только одному ребру, то это ребро $(n - 1, n)$. Тогда максимальное значение v_1 соответствует ребру $(1, n - 2)$, т. е. $v_1 \leq 1 + (n - 2) = n - 1$. Аналогично, если v_1 может представлять только одно ребро,

а именно $(1, 2)$, то минимальное v_2 соответствует ребру $(3, n)$, откуда $v_2 \geq n + 3$. Максимальный номер для v_1 соответствует ребру $(1, v_1 - 1)$, а минимальный номер вершины для v_2 — ребру $(v_2 - n, n)$. Чтобы ребра не были инцидентными, необходимо выполнение условия $v_2 - n > v_1 - 1$ или $v_2 - v_1 > n - 1$, что и требовалось доказать.

Пусть k — количество ребер в NA -графе с одной образующей u , т. е. $k = \left\lfloor \frac{u-1}{2} \right\rfloor$. На основании двух лемм можно доказать более сильный результат.

Теорема 2.25. В классе NA -графов $G = (X, V)$ с двумя образующими $V = \{v_1, v_2\}$ каждому NA -графу $G = (X, u)$ с одной образующей $5 \leq u \leq n + 1$ соответствует множество ему изоморфных, состоящее из:

а) $4(k - 1)$ графов с образующими

$$V^{(1)} = \{2i + 1, 2n - 2k + 2i + 1\}, V^{(2)} = \{2i + 1, 2n - 2k + 2i\},$$

$$V^{(3)} = \{2i + 2, 2n - 2k + 2i + 1\}, V^{(4)} = \{2i + 2, 2n - 2k + 2i\},$$

$$(i = 1, 2, \dots, k - 1) \text{ для } u < n;$$

б) $[4 - u(\bmod 2)](k - 1)$ графов тех же типов, где граф с $V^{(4)}$ может не существовать, для $u = n$;

в) $[2 + (-1)^u](k - 1)$ графов первых трех типов, где последние два типа могут не существовать, для $u = n + 1$.

Доказательство. Пусть в NA -графе с одной образующей $u < n$, и по условию число ребер в нем $k \geq 2$. Это число можно разбить на $k - 1$ сумму из двух чисел: $(1, k - 1)$, $(2, k - 2)$, $(3, k - 3)$, ..., $(k - 1, 1)$. Возьмем какую-либо пару из этого разбиения $(i, k - i)$ и поставим в соответствие каждой составляющей две образующие v_1 и v'_2 , которые в точности соответствуют i ребрам и $k - i$ ребрам соответственно. Как было показано ранее, это может быть при условии $v_1 \in \{2i + 1, 2i + 2\}$ и $v'_2 \in \{2(k - i) + 1, 2(k - i) + 2\}$. При таких значениях $v_1, v'_2 \leq n + 1$ и по лемме 2.19 граф с такими образующими не может быть изоморфным NA -графу с одной образующей.

Для этого необходимо заменить v'_2 на двойственную образующую $v_2 = 2n + 2 - v'_2$ или $v_2 \in \{2n - 2k + 2i, 2n - 2k + 2i + 1\}$. В этом случае полученный граф будет иметь степени вершин не более единицы, а число ребер будет равно k . Комбинируя значения v_1 и v_2 , получаем для фиксированного значения i четыре различных изоморфных графа, а всего таких графов будет ровно $4(k - 1)$.

Пусть $k = n$. В этом случае значения двух образующих могут не удовлетворять условиям (2.6). Легко проверяются условия а) и б), которые выполняются.

Рассмотрим последовательно все типы множеств образующих $V^{(j)}$ ($j = 1, 2, 3, 4$) и проверим для них условие в). При этом воспользуемся значениями $k = \left\lfloor \frac{n-1}{2} \right\rfloor$ и $2k = n - 2 + n(\bmod 2)$. Получаем

неравенства

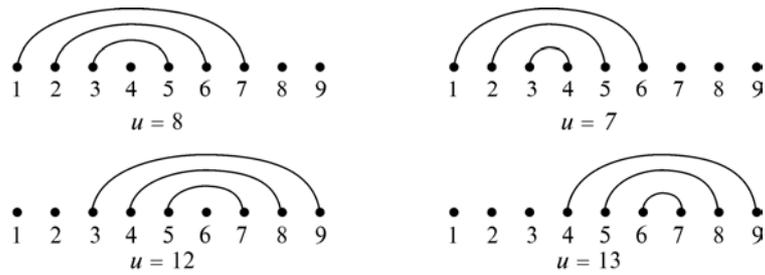
$$\begin{aligned} j = 1: & \quad n + 2 - n(\bmod 2) > n - 1; \\ j = 2: & \quad n + 1 - n(\bmod 2) > n - 1; \\ j = 3: & \quad n + 1 - n(\bmod 2) > n - 1; \\ j = 4: & \quad n - n(\bmod 2) > n - 1. \end{aligned} \quad (2.86)$$

Как видно, первые три неравенства выполняются всегда, а четвертое — лишь при $n \equiv 0(\bmod 2)$. Это означает, что из четырех типов изоморфных графов, приведенных в пункте а), один тип графа с множеством образующих $V^{(4)}$ при нечетном n не существует. Общее количество изоморфных графов при фиксированном i в этом случае можно выразить как $4 - u(\bmod 2)$, что и требовалось доказать.

Пусть $u = n + 1$. Очевидно, что в этом случае трудностей с построением графов будет больше. Проверим условие (2.85,в) для каждого типа образующих $V^{(j)}$ ($j = 1, 2, 3, 4$). При этом подставим значения

$k = \left\lfloor \frac{n}{2} \right\rfloor$ и $2k = n - n(\bmod 2)$. Получаем неравенства типа (2.86):

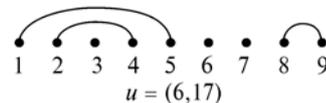
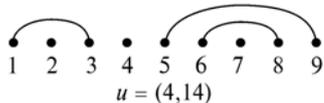
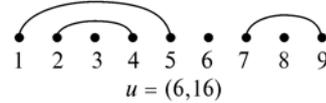
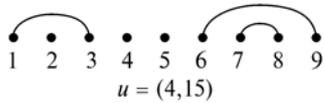
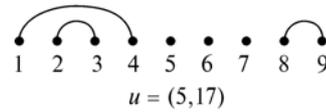
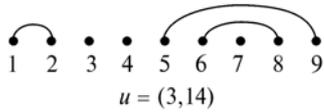
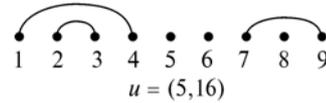
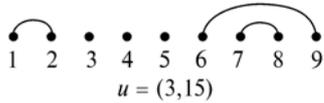
$$\begin{aligned} j = 1: & \quad n + n(\bmod 2) > n - 1; \\ j = 2: & \quad n + n(\bmod 2) - 1 > n - 1; \\ j = 3: & \quad n + n(\bmod 2) - 1 > n - 1; \\ j = 4: & \quad n + n(\bmod 2) - 2 > n - 1. \end{aligned} \quad (2.87)$$



Изоморфные графы с одной образующей

1. Разбиение (1,2)

2. Разбиение (2,1)



Изоморфные графы с двумя образующими

Рис. 2.26

Здесь четвертое неравенство не выполняется ни при каких n . Второе и третье неравенства выполняются лишь для $n \equiv 1 \pmod{2}$, а первое неравенство выполняется всегда. Это означает, что при четном n существует единственный изоморфный граф с множеством образующих $V^{(1)}$. При нечетном n таких графов уже 3, которые имеют множества образующих $V^{(1)}, V^{(2)}, V^{(3)}$ соответственно. В общем случае количество таких графов при фиксированном i равно $2 - (-1)^n$, что и завершает доказательство теоремы.

Рассмотрим пример на рис. 2.26 для NA -графов, изоморфных графу $G = (X, u)$, $n = 9$, $u = 8$.

Объединив теоремы 2.24 и 2.25, можно получить следующий вывод.

Следствие. Каждому *NA*-графу с одной образующей $u \leq n + 1$ соответствует множество изоморфных *NA*-графов, состоящее из:

- а) $4k$ графов для $u < n$;
- б) $[4 - u(\bmod 2)]k$ графов для $u = n$;
- в) $[2 - (-1)^n]k$ графов для $u = n + 1$, где $k = \left\lfloor \frac{u-1}{2} \right\rfloor$.

Очевидно, что алгоритм проверки изоморфизма для *NA*-графов с одной образующей является полиномиальным.

**МОДУЛЬНЫЕ ГРАФЫ (M-ГРАФЫ)
И ИХ СВОЙСТВА**

3.1. ПРЕДСТАВЛЕНИЕ МОДУЛЬНЫХ ГРАФОВ

Как и в случае с арифметическими графами, здесь возникает вопрос о представлении графов в виде M -графов.

Лемма 3.1. Любой конечный граф можно представить в виде определенного M -графа.

Возьмем опять какое-либо число $k > 1$ и закодируем каждую вершину графа $x_i = k^{i-1}$ ($1 \leq i \leq n$). Каждому ребру графа (x_i, x_j) , $i, j \in N_n$, поставим в соответствие число $u_{ij} = |k^{i-1} - k^{j-1}|$. Тогда граф $G = (X, U)$ с $X = \{1, k, k^2, \dots, k^{n-1}\}$ и $U = \{u_{ij} | (i, j) \text{ — ребро между вершинами } k^{i-1} \text{ и } k^{j-1} \text{ будет одним из искомым } M\text{-графов. Здесь также каждое ребро представлено единственной образующей. Если это не так, то существует пара ребер } (i, j) \text{ и } (s, r) \text{ таких, что}$

$$|k^{i-1} - k^{j-1}| = |k^{r-1} - k^{s-1}|.$$

Переставим в прямых скобках слагаемые так, чтобы разности были положительными. Не нарушая общности, будем считать, что $i < j < r < s$. Тогда

$$k^{j-1} - k^{i-1} = k^{s-1} - k^{r-1}.$$

Отсюда $k^{i-1}(k^{s-i} + 1) = k^{i-1}(k^{j-i} + k^{r-i})$. После сокращения на k^{i-1} это выражение равносильно следующему: $1 \equiv 0 \pmod{k}$, что невозможно и подтверждает справедливость леммы.

По аналогии с NA -графами назовем M -графы, у которых $X = \{1, 2, \dots, n\} = N_n$, *натуральными модульными графами (NM-графами)*.

Рассмотрим матрицу $A = (a_{ij})$, где $a_{ij} = |i - j|$, $1 \leq i, j \leq n$. Эта матрица соответствует произвольному полному натуральному мо-

дульному графу, который имеет n вершин и всевозможные образующие от минимальной $u = 1$ до максимальной $u = n - 1$:

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & \dots & n-1 \\ 1 & 0 & 1 & 2 & \dots & n-2 \\ 2 & 1 & 0 & 1 & \dots & n-3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ n-1 & n-2 & n-3 & n-4 & \dots & 0 \end{pmatrix}. \quad (3.1)$$

Очевидно, что матрица представляет указанный граф однозначно, так как у него множество образующих состоит из отрезка натурального ряда $U = \{1, 2, \dots, n-1\}$ или $U = N_{n-1}$. Любое подмножество этого множества определяет некоторый NM -граф $G = (X, U)$. В дальнейшем без исключения все NM -графы будем считать n -вершинными.

Определение 3.1. Матрицей образующих для произвольного NM -графа $G = (X, U)$ называется матрица $A(G) = (a_{ij})$, у которой $a_{ij} = |i - j|$, если существует такое $u \in U$, что $u = |i - j|$, и $a_{ij} = 0$ для всех остальных значений i и j ($1 \leq i, j \leq n$).

В этой матрице каждый ненулевой элемент и ему симметричный соответствует одному ребру графа. Нетрудно заметить, что каждой образующей соответствует множество ребер, число которых равно

$$r_n(u) = n - u. \quad (3.2)$$

Элементы матрицы, соответствующие образующей u , расположены параллельно главной диагонали. Будем называть их совокупность линией u в матрице. Число линий, пересекающих i -ю строку (столбец) матрицы, равно степени вершины x_i . Наибольшее число ребер соответствует образующей $u = 1$.

В дальнейшем нам часто придется использовать выражения $x \pmod{a}$, где a — целое положительное число, а x — целое. При этом всегда будут подразумеваться только положительные вычеты.

Лемма 3.2. NM -граф $G = (X, U)$ с одной образующей $U = \{u\}$ состоит из u компонент связности, из которых $\left\lceil \frac{n}{u} \right\rceil u - n$ являются цепями из $\left\lceil \frac{n}{u} \right\rceil - 1$ вершин, остальные — цепями из $\left\lfloor \frac{n}{u} \right\rfloor$ вершин.

Здесь $\lceil x \rceil$ — ближайшее целое, не меньшее x . Действительно, если $n \equiv 0 \pmod{u}$, то $n = ku$, и получаем u цепей из k вершин, которые содержат следующие последовательные вершины: $\{1, u + 1, 2u + 1, \dots, (k - 1)u + 1\}$, $\{2, u + 2, 2u + 2, \dots, (k - 1)u + 2\}$, ..., $\{u, 2u, 3u, \dots, ku\}$. Каждая i -я цепь ($1 \leq i \leq u$) содержит все коды $i \pmod{u}$. Здесь $\left\lceil \frac{n}{u} \right\rceil = k$, $\left\lceil \frac{n}{u} \right\rceil u - n = 0$, поэтому цепей длиной $k - 1$ нет. Если же $n \not\equiv 0 \pmod{u}$, тогда из этого списка часть последних цепей на одну вершину урезается, $n \pmod{u}$ цепей состоят из $\left\lceil \frac{n}{u} \right\rceil$ вершин, остальные цепи содержат на одну вершину меньше. И таких цепей, если подсчитать, $u - n \pmod{u}$ или $\left\lceil \frac{n}{u} \right\rceil u - n$ в общем случае. Легко видеть, что минимальный код правого конца цепей равен $n - u + 1$. Можно вычислить число всех ребер графа, учитывая то, что в каждой цепи ребер на единицу меньше, чем вершин:

$$r_n(u) = \left(\left\lceil \frac{n}{u} \right\rceil u - n \right) \left(\left\lceil \frac{n}{u} \right\rceil - 2 \right) + \left(u + n - \left\lceil \frac{n}{u} \right\rceil u \right) \left(\left\lceil \frac{n}{u} \right\rceil - 1 \right) = n - u, \quad (3.3)$$

что соответствует выражению (3.2).

На рис. 3.1 приведен *NM*-граф для $n = 23$, $u = \{5\}$. При $u = 1$ по лемме 3.2 граф должен представлять одну цепь, и в этом можно непосредственно убедиться.

Рассмотрим теперь *NM*-графы с двумя образующими, у которых $U = \{u_1, u_2\}$ и $u_2 \geq u_1$. Прежде всего изучим простые графы, у

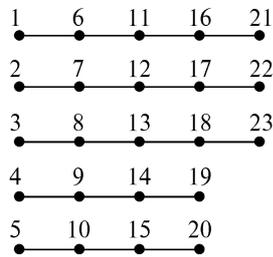


Рис. 3.1

которых степени вершин не превышают 2. Найдем условия, при которых это требование выполняется. Для этого рассмотрим вершину 1 и ее ближайшие вершины $a = u_1 + 1$ и $b = u_2 + 1$. Так как $a \leq b$, то необходимо, чтобы $a + u_2 \geq n$, иначе вершина a будет обязательно смежной с вершиной $a + u_1$ и ее степень будет равной 3. Поэтому все вершины имеют степень не больше 2 при условии $u_1 + u_2 \geq n$.

А. Рассмотрим случай, когда $u_1 + u_2 = n$.

Если $n \equiv 0 \pmod{u_1}$, то $\frac{n}{u_1} = k$

и $u_2 = (k - 1)u_1$. Тогда граф является фактороидом, состоящим из u циклов длиной k . Действительно, любая вершина i ($1 \leq i \leq u$) связана цепью из $k - 1$

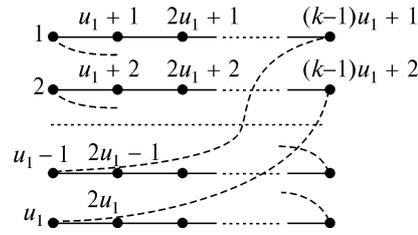


Рис. 3.2

ребер с помощью образующей u_1 с вершиной $(k - 1)u_1 + 1$, но они смежны благодаря образующей u_2 , что вместе создает цикл.

Если $n \not\equiv 0 \pmod{u_1}$, то $n = ku_1 + r$ ($1 \leq r < u$) и $u_2 = (k - 1)u_1 + r$.

Изобразим граф в виде параллельных цепей, соответствующих образующей u_1 (рис. 3.2). С помощью образующей u_2 соединяются пары вершин $[1, (k - 1)u_1 + r + 1]$, $[2, (k - 1)u_1 + r + 2], \dots, [u_1 - r + 1, ku_1 + 1], \dots, [u_1, ku_1 + r = n]$.

Таким образом, все левые концы цепей соединяются с правыми концами. Это означает, что степени всех вершин графа равны 2, и граф является фактороидом. Цикл, который начинается в вершине 1, соединяется с правым концом цепи под номером r , затем левый конец последней цепи — с правым концом цепи под номером $2r$ и т. д., пока не закончится в правой вершине первой цепи $ku_1 + 1$. Число цепей, которые проходит данный цикл, является решением уравнения

$$l \cdot r \equiv 0 \pmod{u_1}. \quad (3.4)$$

Если r и u — взаимно простые, т. е. не имеют общих делителей, то $l = u_1$, и граф представляет собой гамильтонов цикл. Если же они имеют общий делитель, то существует решение для $l \leq u_1$. Тогда граф представляет собой несколько циклов. Очевидно, что в уравнение (3.4) можно вместо r подставлять n , так как $n \equiv r \pmod{u_1}$. Тем самым доказана следующая лемма.

Лемма 3.3. *NM*-граф с двумя образующими $U = \{u_1, u_2\}$ и условием $u_1 + u_2 = n$ представляет собой набор p циклов длиной $\frac{n}{p}$, где $p = \text{НОД}(n, u_1)$ — наибольший общий делитель чисел n и u_1 .

В теории чисел [14] известна функция Эйлера $\varphi(x)$, которая равна количеству чисел, взаимно простых с x и не превышающих его.

Следствие. NM -граф с двумя образующими $U = \{u_1, u_2\}$ может быть представлен $\frac{\varphi(n)}{2}$ способами как гамильтонов цикл. При этом $U = \{u, n - u\}$ и $\text{НОД}(n, u) = 1$.

Здесь берется половина функции, так как пары образующих упорядочены $u_2 \geq u_1$.

Б. Рассмотрим случай, когда $u_1 + u_2 = n + 1$.

Этот случай легко свести к предыдущему, если ввести фиктивную вершину $n + 1$. Тогда $n' = n + 1$, $u_1 + u_2 = n'$ и можно доказать аналогичные утверждения, а затем удалить фиктивную вершину.

На рис. 3.3 показан такой граф для $n = 24$, $u_1 = 7$, $u_2 = 18$. Фиктивная вершина 25 соединена пунктирными ребрами с соответствующими вершинами. Удаление фиктивной вершины приводит к тому, что один из циклов превращается в цепь.

Лемма 3.4. NM -граф с двумя образующими $U = \{u_1, u_2\}$ при условии $u_1 + u_2 = n + 1$ представляет собой набор из $\rho - 1$ циклов длиной $\frac{n+1}{\rho}$ и одной цепи длиной $\frac{n+1}{\rho} - 1$, где $\rho = \text{НОД}(u_1, n + 1)$.

Если граф вместе с фиктивной вершиной является гамильтоновым циклом, то удаление последней приводит к образованию гамильтоновой цепи.

Следствие. NM -граф с двумя образующими $U = \{u_1, u_2\}$ может

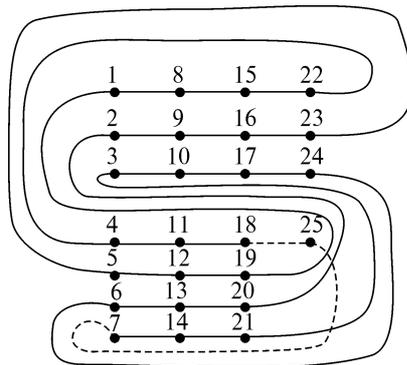


Рис. 3.3

быть представлен $\frac{\varphi(n+1)}{2} - 1$ способами как гамильтонова цепь. При этом $U = \{u, n - u + 1\}$ и $\text{НОД}(n + 1, u) = 1$.

Здесь в отличие от следствия леммы 3.2 вычитается единица, так как пара образующих $(1, n)$ невозможна. Например, на рис. 3.3 имеем: $\varphi(n + 1) = \varphi(25) = \varphi(5^2)$. Следуя [14], проводим вычисления: $\varphi(5^2) = 5(5 - \frac{1}{5}) = 20$,

$\frac{\varphi(25)}{2} - 1 = 9$. Перечислим те пары образующих, которые представляют гамильтонову цепь: (2,23), (3,22), (4,21), (6,19), (7,18), (8,17), (9,16), (11,14), (12,13). Можно непосредственно убедиться, что это соответствует действительности.

3.2. О СВЯЗНОСТИ НАТУРАЛЬНЫХ МОДУЛЬНЫХ ГРАФОВ (*MM*-ГРАФОВ)

В настоящее время числовые графы в связи с поиском эффективных алгоритмов на графах привлекают все большее внимание исследователей. Оказалось, что в вычислительном смысле представление графов в виде числовых по таким параметрам, как быстродействие и объем памяти, дает несомненное преимущество по сравнению с традиционными способами.

Кроме [22—35], появилось много публикаций, где в отличие от арифметических рассмотрен широкий класс других числовых графов. Еще в работе [38] были указаны несколько классов числовых графов, изучение которых имело бы важное практическое значение.

В параграфе 3.1 описаны *MM*-графы с одной образующей, а также некоторые *MM*-графы с двумя образующими. Для полного описания таких графов определим ряд характерных для них свойств, которые устанавливает следующая теорема.

Теорема 3.1. Пусть задан *MM*-граф $G = (X, U)$, у которого $|X| = n$ и $U = \{u_1, u_2, \dots, u_m\}$. Тогда γ графов G можно представить как *MM*-граф $\Gamma = (X, Y)$, у которого $X = \{1, 2, \dots, n, n+1, \dots, \gamma n\} = N_{\gamma n}$, а $Y = \{u_1, u_2, \dots, u_m\}$.

Доказательство. Покажем, что определенная нумерация γn вершин для Γ образует γ несвязных графов. Пусть в графе G вершины имеют код $\alpha = 1, 2, \dots, n-1, n$. Каждому значению α поставим в соответствие в графе Γ код $\alpha_\beta = (\alpha-1)\gamma + \beta$ ($1 \leq \beta \leq \gamma$). Для фиксированного β получаем β -ю копию графа G с кодами $\beta, \gamma + \beta, 2\gamma + \beta, \dots, (n-1)\gamma + \beta$. Если в графе G вершины α_1 и α_2 смежные, то $|\alpha_1 - \alpha_2| \in U$. В графе Γ этим вершинам соответствуют две вершины $\alpha_\beta^1 = (\alpha_1-1)\gamma + \beta$ и $\alpha_\beta^2 = (\alpha_2-1)\gamma + \beta$. С одной стороны, они — смежные, так как $|\alpha_\beta^1 - \alpha_\beta^2| = |\alpha_1 - \alpha_2| \gamma \in Y$. С

другой стороны, для $\beta_1 \neq \beta_2$ любые вершины и $(\alpha_2 - 1)\gamma + \beta_2$ — несмежные. Это следует из того, что абсолютная разница их кодов равна $|(\alpha_1 - \alpha_2)\gamma + \beta_1 - \beta_2|$ и никогда не может быть равной γu_1 или γu_2 , так как $1 \leq |\beta_1 - \beta_2| < \gamma$.

Теорема 3.1 дает возможность изучать только те *NM*-графы, для которых наибольший общий делитель образующих равен 1. Одной из важнейших характеристик любых графов является связность.

Следствие. *NM*-граф $G = (X, U)$ с m образующими, для которых $\text{НОД}(u_1, u_2, \dots, u_m) = \gamma > 0$, несвязен.

Действительно, если закодировать все вершины такого графа кодами $\alpha_\beta = (\alpha - 1)\gamma + \beta$ ($1 \leq \beta \leq \gamma$), то они примут все значения от 1 до n , и для разных значений β все вершины будут несмежные, т. е. принадлежать разным компонентам связности.

В общем случае для *NM*-графов с одной образующей вопрос о связности разрешается легко: граф связан только для $u = 1$, и тогда он является цепью. Для *NM*-графов с двумя образующими справедлива следующая теорема.

Теорема 3.2. *NM*-граф $G = (X, U)$ с множеством $U = \{u_1, u_2\}$ связан тогда и только тогда, когда:

- 1) $\text{НОД}(u_1, u_2) = 1$;
- 2) $u_1 + u_2 \leq n + 1$.

Первое условие следует из теоремы 3.1. Необходимость второго условия вытекает из следующих рассуждений. Для связности вершин любого графа G необходимо не менее $n - 1$ ребро. Так как каждой образующей u соответствует ровно $n - u$ ребер, то получаем зависимость $(n - u_1) + (n - u_2) \geq n - 1$, откуда и следует условие 2). Для доказательства его достаточности построим сначала граф $G' = (X, U')$, где $U' = \{u\}$, а $u = \min\{u_1, u_2\}$. Поскольку $u \leq \left\lfloor \frac{n}{2} \right\rfloor$, то этот граф не имеет изолированных вершин и представляет набор u цепей. Каждая цепь содержит только вершины с кодом $i \pmod{u}$ для $1 \leq i \leq u$. Добавим к графу G' образующую $v = \max\{u_1, u_2\}$. Ей соответствует не менее $u - 1$ ребро, поэтому ее можно записать в виде $v = n - \lambda$, где $\lambda \geq u - 1$. Возьмем ровно $u - 1$ ребро, соответствующих образующей v , инцидентных вершинам n ,

$n - 1, \dots, n - u + 2, n - 1, \dots, n - u + 2$. Если стянуть каждую цепь в одну вершину, то останутся только эти ребра, и связность графа не нарушится. Докажем, что в результате стягивания получится цепь, т. е. исходный граф G связан. Если это не цепь, то среди $u - 1$ ребра найдутся k таких, которые образуют цикл, что соответствует уравнению

$$(n - \lambda)k \equiv vk \equiv 0 \pmod{u_1}. \quad (3.5)$$

Так как $1 \leq k \leq u - 1$, то это возможно лишь тогда, когда v и u имеют общий делитель, что противоречит условию 1).

Следствие 1. Если в *NM*-графе $G = (X, U)$ с m образующими ($m \geq 2$) найдутся такие $u, v \in U$, что $\text{НОД}(u, v) = 1$ и $u + v \leq n + 1$, то граф связан.

Для указанных *NM*-графов первое условие является достаточным, но не необходимым. На рис. 3.4 приведен пример *NM*-графа с $n = 16$ и $U = \{6, 10, 15\}$, в котором для двух любых его образующих u_i и u_j ($1 \leq i, j \leq 3$) $\text{НОД}(u_i, u_j) \neq 1$, тем не менее, как можно непосредственно убедиться, граф связан.

Следствие 2. Необходимым условием связности *NM*-графа $G = (X, U)$ с m образующими является

$$\sum_{i=1}^m u_i \leq (m - 1)n + 1. \quad (3.6)$$

Действительно, каждая образующая u дает ровно $n - u_i$ ребер. Среди связанных графов наименьшее число ребер, равное $n - 1$, содержит цепь. Поэтому

$$\sum_{i=1}^m (n - u_i) \geq n - 1, \quad (3.7)$$

откуда после упрощений получаем (3.6). В частном случае для $m = 1$ имеем $u \leq 1$, что возможно только при $u = 1$. Если выполняется условие (3.6), то с учетом следствия 1 из теоремы 3.2 условие 2) выполняется автоматически.

Для графов с числом образующих больше двух ответ на вопрос о связности не так очевиден. Подходящие примеры на рисунках уже проверять доволь-

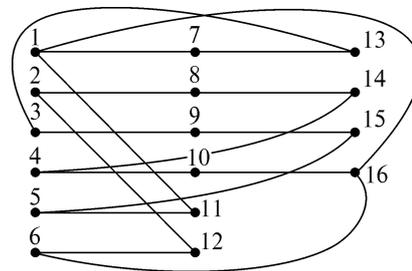


Рис. 3.4

но сложно. В NM -графе с $n = 106$ и множеством образующих $U = \{20, 42, 70, 105\}$ любые три образующие имеют общий делитель, при этом граф остается связным. Об этом свидетельствует следующая теорема.

Теорема 3.3. NM -граф $G = (X, U)$ с m образующими ($m \geq 1$) связан, если:

- 1) $\text{НОД}(u_1, u_2, \dots, u_m) = 1$;

- 2) выполняется условие (3.6) следствия 2 из теоремы 3.2.

Доказательство. Пусть λ — максимальное число образующих, для которых существует общий делитель, равный d . Очевидно, что $2 \leq \lambda \leq m - 1$, иначе выполнить условие 1) теоремы 3.3 невозможно. Не нарушая общности, полагаем, что ими являются первые λ образующих, т. е.

$$\text{НОД}(u_1, u_2, \dots, u_{\lambda-1}, u_\lambda) = d \geq 1. \quad (3.8)$$

Граф $G' = (X, U')$, у которого $U' = \{u_1, u_2, \dots, u_\lambda\}$, состоит из d компонент связности, как утверждает следствие из теоремы 3.2. В силу условия 2) теоремы 3.2 всегда найдется такое $u_i \leq n - d + 1$ ($i \geq \lambda$), которое не делится на d , иначе было бы $\lambda + 1$ таких образующих, что противоречит соглашению о максимальности λ . Образует граф G'' , добавив $d - 1$ ребро, соответствующих образующей u_i и инцидентных вершинам $n, n - 1, n - 2, \dots, n - d + 2$. Эти ребра соединяют пары вершин из разных компонент графа G' . Если стянуть каждую компоненту в вершину, то связность графа G'' не нарушится. В результате получаем цепь из d вершин, что свидетельствует о связности графа G'' . Если это не так, то образуется цикл длиной меньше d . Но это равносильно тому, что существует решение уравнения

$$u_i k \equiv 0 \pmod{d} \quad (1 \leq k \leq d). \quad (3.9)$$

Это возможно только тогда, когда u_i и d имеют общий делитель, например $c \geq 1$. Но тогда

$$\text{НОД}(u_1, u_2, \dots, u_\lambda, u_i) = c \geq 1,$$

и максимальное число образующих, имеющих общий делитель, составит $\lambda + 1$, что противоречит предположению. Это и завершает доказательство теоремы.

Последний пример NM -графа теперь можно легко исследовать. Здесь $\lambda = 3$, поэтому $\text{НОД}(30, 42, 70) = 2$. Так как $\text{НОД}(2, 105) = 1$, то граф связан.

3.3. О ЦИКЛОМАТИЧЕСКОМ ЧИСЛЕ NM -ГРАФОВ

Рассмотрим распределение степеней вершин для произвольного NM -графа $G = (X, U)$, где $X = N_n$, $U = \{u_1, u_2, \dots, u_m\}$. Каждой образующей u_i соответствует ровно $n - u_i$ ребер, однако не всякая вершина инцидентна ребрам каждой образующей. Все образующие можно разделить на две части:

1. $u_i \leq \left\lfloor \frac{n}{2} \right\rfloor$. В этом случае ребра, соответствующие данной

образующей, инцидентны всем вершинам и дают прибавление к их степеням, равное 1 или 2, в таком порядке: вершинам с номерами от 1 до u_i и от $n - u_i + 1$ до n — единицу, остальным вершинам — двойку.

2. $u_i \geq \left\lceil \frac{n}{2} \right\rceil$. В этом случае вершины с номерами от $n - u_i$ до u_i

не инцидентны ребрам, соответствующим образующей u_i , остальные вершины получают прибавку к степени, равную 1. Здесь также первое множество вершин может быть пустым, если $n - u_i + 1 = u_i + 1$, что возможно лишь при четном n и $u_i = \frac{n}{2}$.

В теореме 3.3 описаны необходимые условия связности NM -графа. В общем случае эти условия не являются достаточными. На рис. 3.5 показан NM -граф с $n = 23$, и $U = \{8, 12, 21\}$, у которого $\text{НОД}(8, 12, 21) = 1$, $8 + 12 + 21 \leq 2 \cdot 23 + 1$, т. е. выполняются условия 1) и 2), но граф не связан, он состоит из двух компонент, одна из которых — цикл (4, 16, 8, 20, 12, 4).

Нетрудно увидеть, что если увеличить число вершин графа до 24, то появится ребро (3, 24), которое свяжет две компоненты, и граф станет связным.

Допустим, что в графе приведены все ребра, соответствующие набору образующих из $U = (v_1, v_2, \dots, v_{k-1})$, для которых $\text{НОД}(v_1, v_2, \dots, v_{k-1}) = \lambda \geq 1$, и существует в U образующая v_k , для которой $\text{НОД}(v_k, \lambda) = 1$. Тогда граф G' на множестве из n вершин и с набором указанных $k - 1$ образующих будет состоять из λ

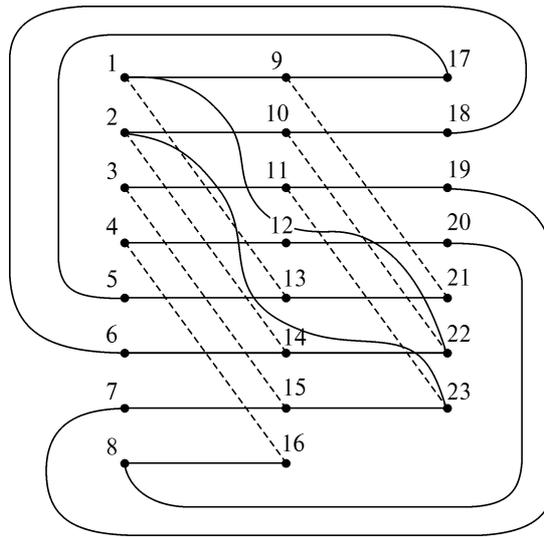


Рис. 3.5

компонент связности, а вершины с номерами от 1 до λ будут представлять разные компоненты. Действительно, если это не так, то какая-то пара вершин i, j из этого множества принадлежит одной компоненте связности. Это означает, что существует такая последовательность:

$$i \pm u_{\alpha_1} \pm u_{\alpha_2} \pm \dots \pm u_{\alpha_r=j} \quad (u_{\alpha_s} \subset U, s = 1, 2, \dots, r). \quad (3.10)$$

Поскольку $u_{\alpha_s} \equiv u_{\alpha_1} \pmod{\lambda}$, то $i \equiv j \pmod{\lambda}$, что невозможно. Добавим к графу G' образующую v_k . К графу G' добавятся новые ребра, и λ из них $(1, v_k + 1), (2, v_k + 2), \dots, (\lambda, v_k + \lambda)$ должны связать все компоненты графа G' в одну. Это может не произойти по двум причинам. Первая состоит в том, что числа типа $r_1 v_k + i$ ($1 \leq r, i \leq \lambda$) не все разные по $\text{mod } \lambda$. Тогда образующая v_k не обеспечивает связности всего графа G' . Но это равносильно справедливости равенства

$$r_1 v_k + i \equiv (r_2 v_k + i) \pmod{\lambda} \quad (1 \leq r_1, r_2 < \lambda) \quad (3.11)$$

или $(r_1 - r_2)v_k \equiv 0 \pmod{\lambda}$. Так как $(r_1 - r_2) \leq \lambda$, то $\text{НОД}(v_k, \lambda) \neq 1$, что противоречит первоначальному предположению.

Вторая причина заключается в том, что не хватает ребер, соответствующих образующей v_k , для связывания λ компонент. Это возможно только при $v_k \geq n - \lambda + 1$. Тем самым доказана следующая теорема.

Теорема 3.4. Для связности NM -графа $G = (X, U)$ с n вершинами и m образующими ($m \geq 1$), $U = \{u_1, u_2, \dots, u_m\}$ необходимо и достаточно, чтобы нашлось хотя бы одно такое подмножество образующих $V = \{v_1, v_2, \dots, v_k\} \subseteq U$ ($k \geq 1$), у которого:

- 1) $\text{НОД}(v_1, v_2, \dots, v_k) = 1$;
- 2) $\sum_{i=1}^m u_i \leq (m-1)n + 1$;
- 3) $v_k \leq n - \text{НОД}(v_1, v_2, \dots, v_{k-1}) + 1$.

Последнее условие теоремы существенно, так как большинство утверждений в теории графов звучит по-разному, в зависимости от того, связан граф или несвязен. Так как связность графа зависит от величины $\text{НОД}(u_1, u_2, \dots, u_m) = \lambda_m$, то условие 3) будет относиться к образующей u_m .

Назовем *дефицитом* графа $\Delta(G)$ величину, которая определяется следующим образом:

$$\Delta(G) = \begin{cases} 0, & \text{если } u_m \leq n - \lambda_m, \\ u_m - n + \lambda_m & \text{в остальных случаях.} \end{cases} \quad (3.12)$$

Выражение (3.12) можно записать в виде формулы

$$\Delta(G) = \frac{u_m - n + \lambda_m + |u_m - n + \lambda_m|}{2}. \quad (3.13)$$

Граф, у которого $\Delta(G) = 0$, будем называть *бездефицитным*.

Теорема 3.5. Цикломатическое число NM -графа с n вершинами и m образующими ($m \geq 1$) равно

$$\chi(G) = (m-1)n - \sum_{i=1}^m u_i + \frac{u_m - n + 3\lambda_m + |u_m - n + \lambda_m|}{2}. \quad (3.14)$$

Докажем это утверждение для бездефицитного графа. Тогда число компонент связности графа равно $P(G) = \lambda_m$. В этом случае верна известная формула Эйлера для графа с n вершинами и r ребрами:

$$\chi(G) = r - n + P(G). \quad (3.15)$$

Подставляя сюда $r = \sum_{i=1}^m (n - u_i)$, получаем уравнение (3.14), где последнее слагаемое будет λ . Пусть теперь дефицит графа $\Delta(G) \geq 0$. Удалим в графе ребра, соответствующие образующей u_m . Получим бездефицитный граф G' с образующими $U = \{u_1, u_2, \dots, u_{m-1}\}$ и с числом компонент $P(G') = \text{НОД}(u_1, u_2, \dots, u_{m-1}) = \lambda_{m-1}$. Возвращение удаленных ребер уменьшает число этих компонент на величину, равную числу новых ребер. Если число этих ребер равно $\text{НОД}(\lambda_{m-1}, u_m)$, то $P(G) = \lambda_m$, а иначе число таких ребер равно $\lambda_m - n + u_m$. В общем случае число компонент становится равным $2\lambda_m - n + u_m$, что и соответствует (3.14).

Исследуем условия, необходимые для существования в NM -графе эйлерова цикла или цепи. Известно, что для первого необходимо и достаточно, чтобы степени всех вершин графа были четными числами. Из изложенного в параграфе 3.2 вытекает, что число образующих графа должно быть четным.

Теорема 3.6. Для того чтобы в связном NM -графе существовал эйлеров цикл, необходимо и достаточно, чтобы множество его образующих имело вид

$$U = \{u_1, u_2, \dots, u_k, n - u_k, n - u_{k-1}, \dots, n - u_2, n - u_1\}. \quad (3.16)$$

При этом граф будет однородным степени $2k$.

Действительно, если все образующие графа соответствуют только условию 1), то в графе не может быть эйлерова цикла, ибо вершины с номерами $u_1 + 1, u_3 + 1$ и все остальные вершины с номерами $2l + 1$ имеют нечетную степень, равную $2l + 1$. Пусть в U встречаются образующие, удовлетворяющие условию 2). Для $k = 1$ очевидно, что граф типа (3.16) содержит эйлеров цикл, он же гамильтонов, так как степень каждой его вершины равна 2. Пусть теорема 3.6 справедлива для заданного k . Докажем ее для $k + 1$. Добавим к графу образующую u_{k+1} , удовлетворяющую условию 1) и еще какую-нибудь $u_{k+2} \geq u_{k+1}$. Если u_{k+2} удовлетворяет условию а), то вершина $u_{k+1} + 1$ имеет нечетную степень. Пусть u_{k+2} удовлетворяет условию 2). Тогда образующие u_{k+1} и u_{k+1} добавляют к степени каждой вершины с номерами от 1 до u_{k+1} ровно два ребра. Если $u_{k+2} \geq n - u_{k+1}$, то вершина $u_{k+1} + 1$ имеет нечетную степень, равную $2k + 1$. Единственно возмож-

ный вариант, чтобы все вершины имели четную степень, это когда $u_{k+2} = n - u_{k+1}$. Теперь, если каждая образующая u_i прибавляет к вершинам по одному ребру, то второе ребро добавляет образующая $n - u_i$, а там, где u_i прибавляет к вершинам два ребра, образующая $n - u_i$ не дает ни одного. В результате число ребер, инцидентных каждой вершине, равно числу образующих, поэтому степень каждой вершины равна $2k$, что и требовалось доказать.

Следствие 1. Для того чтобы в связном и бездефицитном *MM*-графе существовала эйлерова цепь, необходимо и достаточно, чтобы его множество образующих имело вид $U = \{U_0, u_{k+1}, u_{k+1} + 1\}$, где U_0 — множество типа (3.16).

Действительно, в графе содержатся только две вершины нечетной степени $u_{k+1} + 1$ и $n - u_{k+1}$, остальные вершины имеют четную степень. В этом случае эйлерова цепь начинается в одной из этих вершин и заканчивается в другой.

Следствие 2. Любой бездефицитный связный *MM*-граф с образующими типа (3.16) можно разложить на k гамильтоновых циклов.

Это очевидно, так как любая пара образующих u_i и $n - u_i$ образует гамильтонов цикл.

Построим на координатной плоскости функциональную зависимость добавления к степени вершины, зависящей от номера вершины и значения образующей (рис.3.6). Обозначим эту величину $\rho(i)$. Ее значения в соответствии с параграфом 3.2 легко вычислить:

$$\rho(i) = \begin{cases} 1, & \text{если } (i - u_k)(n - u_k - i) \leq 0; \\ 2 - 2 \left\lfloor \frac{2u_k}{n+1} \right\rfloor & \text{в остальных случаях.} \end{cases} \quad (3.17)$$

Учитывая характер четырех областей, изображенных на рис. 3.5, чтобы не возникало разночтений при вычислении формул (3.17), прямые, которые делят эту координатную плоскость, сдвинуты на 0,5 единицы.

Теперь, если взять произвольное i_0 , то можно определить его степень, складывая значения $\rho(i_0)$ на пересечении вертикали $i = i_0$ и горизонтали $u = u_k$ ($k = 1, 2, \dots, m$). Например, на рис. 3.6 для $i = 8$ вычисляем $\rho(8) = 2$ при $u = 4$ и $u = 7$; $\rho(8) = 1$ при $u = 9$; $\rho(8) = 0$ при $u = 13$. Тогда степень вершины 8 равна 5. Назовем

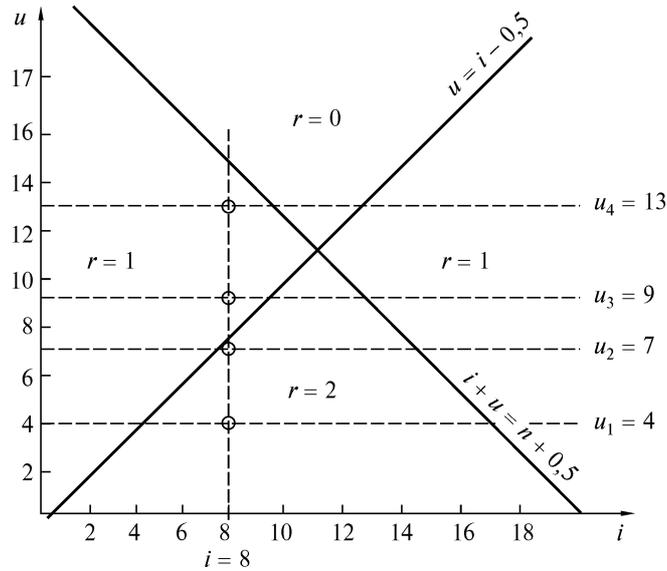


Рис. 3.6

множество $U = \{u_1, u_2, \dots, u_m\}$ сжатым, если в нем проведены следующие преобразования:

- 1) все образующие $u_i \geq \left\lceil \frac{n}{2} \right\rceil$ заменяются образующими $u'_i = n - 1$;
- 2) все образующие упорядочиваются по возрастанию.

Полученное множество обозначим так: $\varphi = \{\varphi_1, \varphi_2, \dots, \varphi_m\}$.

Лемма 3.6. Связный бездефицитный NM -граф с $2l$ вершинами можно покрыть q цепями, где q определяется из соотношений

$$q = \sum_{j=0}^m \varphi_{2j+1} - \sum_{j=1}^m \varphi_{2j} \quad \text{для нечетных } m,$$

$$q = \sum_{j=1}^m \varphi_{2j} - \sum_{j=1}^m \varphi_{2j+1} \quad \text{для четных } m.$$
(3.18)

Это вытекает из того, что между двумя соседними значениями φ_i и φ_{i+1} число вершин, имеющих нечетную степень, равно разности $\varphi_{i+1} - \varphi_i$. В зависимости от четности m получаются разные результаты.

3.4. СТРУКТУРА МНОЖЕСТВА NM -ГРАФОВ С ДВУМЯ ОБРАЗУЮЩИМИ

Рассмотрим натуральные модульные графы (NM -графы), у которых степени вершин не превышают число 2. В дальнейшем речь будет идти только о таких графах, которые для краткости будем называть 2-графами. Очевидно, что NM -графы с множеством $U = \{u_1\}$, т. е. с одной образующей, являются

простейшими 2-графами. Пусть дальше $a = \left\lfloor \frac{n}{u_1} \right\rfloor$, $b \equiv n \pmod{u_1}$,

при этом будут браться только положительные вычеты. Тогда число вершин такого графа $n = au_1 + b$. Нас будут интересовать такие NM -графы, которые после добавления второй образующей остаются 2-графами. Так как все компоненты этих графов состоят из вершин со степенями 1 и 2, то весь граф является набором цепей и циклов.

Пусть P_m — простая цепь из m вершин, а C_m — простой цикл из m вершин. Если граф G состоит из r цепей и s циклов, то его можно представить в виде

$$G = \{P_{t_1}^{\alpha_1}, P_{t_2}^{\alpha_2}, \dots, P_r^{\alpha_r}; C_{q_1}^{\beta_1}, C_{q_2}^{\beta_2}, \dots, C_{q_s}^{\beta_s}\}, \quad (3.19)$$

где α_i — число цепей с количеством вершин t_i ($i = 1, 2, \dots, r$), а β_j — число циклов с количеством вершин q_j ($j = 1, 2, \dots, s$).

Рассмотрим простейший NM -граф $G = (X, U)$, где $U = \{u_1\}$, $n = au_1$, ($a \geq 2$), а $b = 0$. Так как число вершин у такого графа кратно значению первой образующей, назовем его *кратным* и исследуем вопрос, при каких значениях новой образующей u_2 граф останется 2-графом.

Теорема 3.7. Кратный граф G будет оставаться 2-графом, если вторая образующая принадлежит отрезку $[(a-1)u_1; n-1]$, при этом:

$$1) \text{ для } u = (a-1)u_1 \quad (a \geq 2) \quad G = \{C_a^{u_1}\}; \quad (3.20)$$

$$2) \text{ для } u_2 = (a-1)u_1 + k \quad (1 \leq k \leq u_1) \quad G = \{P_c^{u_1 \pmod{k}}; P_d^{k - u_1 \pmod{k}}\},$$

где $c = \left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1 \right) a$, $d = \left\lfloor \frac{u_1}{k} \right\rfloor a$.

Доказательство. Как известно из параграфа 3.1, NM -граф с одной образующей u_1 и $n = au_1$ есть набор u_1 цепей с числом вершин a . Он будет оставаться 2-графом при добавлении новой образующей u_2 тогда и только тогда, когда u_2 будет соединять его висячие вершины. Это вершины с номерами $1, 2, \dots, (a-1)u_1 + 1, (a-1)u_1 + 2, \dots, au_1 = n$, и их число равно $2u_1$. Наименьшая разница номеров среди них равна $(a-1)u_1$, а наибольшая — $n-1$. Это и определяет диапазон значений u_2 . Если $u_2 = (a-1)u_1$, то все цепи графа с одной образующей преобразуются в циклы длиной a (при условии $a \geq 2$), что и доказывает пункт 1 теоремы 3.7. Если $u_2 = (a-1)u_1 + 1$, т. е. $k=1$, то получаем цепь с числом вершин n , так как u_2 соединяет u_1 цепей по парам вершин $[1, (a-1)u_1 + 2], [2, (a-1)u_1 + 3], \dots, [u_1 - 1, au_1 = n]$. В этом случае $u_1 \equiv 0 \pmod{1}$ и получаем $G = \{P_d^1\}$, где $d = \begin{bmatrix} u_1 \\ 1 \end{bmatrix} a = au_1 = n$.

Рассмотрим теперь произвольное $1 \leq k \leq n-1$. Проведем стягивание графа G таким образом, что его i -я компонента ($i = 1, 2, \dots, u_1$) стягивается в i -ю вершину нового графа. Новый граф $G' = (X', U')$ будет состоять из вершин $X' = \{1, 2, \dots, u_1\}$ и $U' = \{k\}$. Действительно, $u' = k$ связывает две вершины i и $i+k$, что в графе G соответствует связыванию двух компонент с номерами i и $i+k$ образующей $(a-1)u_1 + k$ через вершины i и $i+k + (a-1)u_1$. Для графов с одной образующей справедлива лемма 3.2.

Заметим, что всегда $\left\lfloor \frac{n}{u} \right\rfloor u = n - n \pmod{u}$. Если $n \equiv 0 \pmod{u}$, то $\left\lfloor \frac{n}{u} \right\rfloor = \left\lceil \frac{n}{u} \right\rceil$, иначе $\left\lceil \frac{n}{u} \right\rceil = \left\lfloor \frac{n}{u} \right\rfloor + 1$. С учетом этого, подставляя $n = u_1$, $u = k$, получаем при $u_1 \equiv 0 \pmod{k}$ ровно k цепей из $\frac{u_1}{k}$ вершин, а при $u_1 \not\equiv 0 \pmod{k}$ — соответственно $k - u_1 \pmod{k}$ цепей с числом вершин $\left\lfloor \frac{u_1}{k} \right\rfloor$ и $u_1 \pmod{k}$ цепей с числом вершин $\left\lceil \frac{u_1}{k} \right\rceil + 1$. Если вернуться теперь к исходному графу G , то число вершин каждой из полученных цепей необходимо умножить на a , что и доказывает теорему 3.7.

Теперь лемму 3.7 можно перефразировать так: *NM*-граф с n вершинами и одной образующей $U = \{u\}$ представляется в виде набора цепей двух типов:

$$G = \{P_c^{n(\bmod u)}; P_d^{u-n(\bmod u)}\}, \quad (3.21)$$

где $c = \left\lfloor \frac{n}{u} \right\rfloor + 1$, $d = \left\lfloor \frac{n}{u} \right\rfloor$.

Рассмотрим *NM*-графы с одной образующей, у которых $n = au_1 + 1$, т. е. $b = 1$, и будем добавлять вторую образующую u_1 . Рассуждая так же, как и для кратных графов, приходим к выводу, что диапазон ее изменения, не выводящий новый граф из класса 2-графов, есть отрезок $[(a-1)u_1 + 1, n-1]$. Рассмотрим последовательное изменение u_2 и представим новый граф с образующими $U = \{u_1, u_2\}$. Для этого выполним две операции:

1) вершины одной компоненты $[i, i + u_1, i + 2u_1, \dots, (a-1)u_1 + i]$ стянем в одну вершину с номером i и эти вершины назовем *новыми* (на рис. 3.7 изображены в виде кружков);

2) вершину с номером n перенумеруем в вершину с номером $u_1 + 1$ и назовем ее *старой* вершиной (на рис. 3.7 показана в виде точки).

Тем самым граф $G(X, U)$ преобразовался в граф $G' = (X', U)$, в котором $n' = u_1 + 1$, а образующая u_1 связывает новую вершину 1

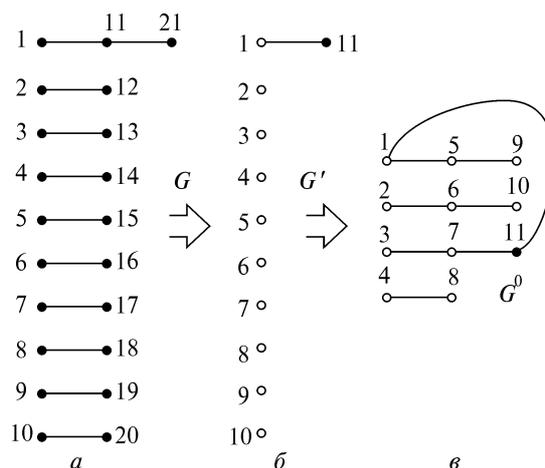


Рис. 3.7

и старую вершину $u_1 + 1$ (рис.3.7, а, б, $G \Rightarrow G' \Rightarrow G^0$; $n = 21$, $u = 10$, $k = 4$).

Нетрудно убедиться, что новая образующая $u_2 = (a - 1)u_1 + k$ ($1 \leq k \leq u_1$) для графа G будет действовать в графе G' как образующая $u'_2 = k$. Эта образующая преобразует граф G' в граф $G^0(X', U')$, где $U' = \{u_1, k\}$. Новые и одна старая вершины графа G^0 образуют k компонент связности. Если старая вершина попадает в первую компоненту, что бывает при равенстве $u_1 + 1 \equiv 1 \pmod{k}$ или $u_1 \equiv 0 \pmod{k}$, то первая компонента благодаря образующей u_1 является циклом. В нем $\left\lfloor \frac{u_1}{k} \right\rfloor$ новых вершин и одна старая.

Остальные компоненты (их число $k - 1$) будут цепями из $\left\lfloor \frac{u_1}{k} \right\rfloor$ новых вершин.

Если старая вершина попадает в другие (не последнюю) компоненты, то граф G^0 разбивается на цепи трех типов (рис. 3.7, в).

Одна цепь благодаря образующей u_1 состоит из $2 \left\lfloor \frac{u_1}{k} \right\rfloor + 1$ новых вершин и одной старой, $u_1 \pmod{k} - 1$ цепей состоят из $\left\lfloor \frac{u_1}{k} \right\rfloor + 1$ новых вершин и $k - 1 - u_1 \pmod{k} - 1$ цепей из $\left\lfloor \frac{u_1}{k} \right\rfloor$ новых вершин.

И если, наконец, старая вершина принадлежит последней компоненте, что бывает только при $u_1 + 1 \equiv 0 \pmod{k}$, то граф G^0 состоит из цепей двух типов. Одна цепь состоит из $2 \left\lfloor \frac{u_1}{k} \right\rfloor + 1$ новых вершин и одной старой и $k - 2$ цепей из $\left\lfloor \frac{u_1}{k} \right\rfloor + 1$ новых вершин.

Заметим, что при $u_1 + 1 \equiv 0 \pmod{k}$ имеет место $u_1 = (k - 1) \pmod{k}$, поэтому последний случай можно свести к предыдущему, когда количество третьих типов цепей равно $k - 1 - (k - 1) = 0$. Так как новые вершины кратны a вершинам графа G , то все вышеприведенные рассуждения нетрудно применить к исходному графу G . Тем самым доказана следующая теорема.

Теорема 3.8. Граф $G(X, U)$ с одной образующей $U = \{u\}$ и числом вершин $n = au + 1$ принадлежит классу 2-графов со второй образующей u_2 тогда и только тогда, когда $u_2 = (a - 1)u_1 + k$ ($1 \leq k \leq u_1 - 1$), при этом:

$$1) \text{ если } u_1 \equiv 0(\text{mod } k), \text{ то } G = \{P_{u_1 a / k}^{k-1}; C_{u_1 a / k+1}^1\}; \quad (3.22)$$

2) если $u_1 \not\equiv 0(\text{mod } k)$, то

$$G = \left\{ P_{2\left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1\right)a+1}; P_{\left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1\right)a}^{u_1(\text{mod } k)-1}; P_{\left\lfloor \frac{u_1}{k} \right\rfloor a}^{k-1-u_1(\text{mod } k)} \right\}.$$

Рассмотрим произвольный граф $G(X, U)$ с одной образующей, у которого $n = au_1 + b$ ($2 \leq b \leq u_1 - 1$). Из теоремы 3.8 вытекает, что новая образующая u_2 , которая не выводит граф из класса 2-графов, должна иметь вид $u_2 = (a - 1)u_1 + k$ ($b \leq k \leq u_1 - 1$). Рассмотрим последовательно два случая:

1) $u_1(\text{mod } k) + b \leq k$ (рис. 3.8, а).

Особый случай занимает соотношение $u_1 \equiv 0(\text{mod } k)$. Тогда, очевидно, граф будет состоять из b циклов и $k - b$ цепей. Число вершин в циклах будет равно $\frac{u_1 a}{k} + 1$, а в цепях — $\frac{au_1}{k}$. Пусть теперь справедливо $u_1 \not\equiv 0(\text{mod } k)$. Если $u_1(\text{mod } k) < b$, то из всего графа можно выделить подграф на вершинах первых $u_1(\text{mod } k) + b$ горизонтальных компонент. Если каждую компоненту стянуть в одну вершину, то получим граф $G^*(X^*, U^*)$ с одной образующей, где $n^* = b + u_1(\text{mod } k)$, а $u^* = u_1(\text{mod } k)$. Согласно лемме 3.2 этот граф состоит из $n^*(\text{mod } u^*)$ цепей с $\left\lfloor \frac{n^*}{u^*} \right\rfloor + 1$

вершинами и $u^* - n^*(\text{mod } u^*)$ цепей с $\left\lfloor \frac{n^*}{u^*} \right\rfloor$ вершинами. Если подставить сюда исходные параметры, то после упрощений получим $n^*(\text{mod } u^*) = b[\text{mod } u_1(\text{mod } k)]$, $\left\lfloor \frac{n^*}{u^*} \right\rfloor = 1 + \left\lfloor \frac{b}{u_1(\text{mod } k)} \right\rfloor$.

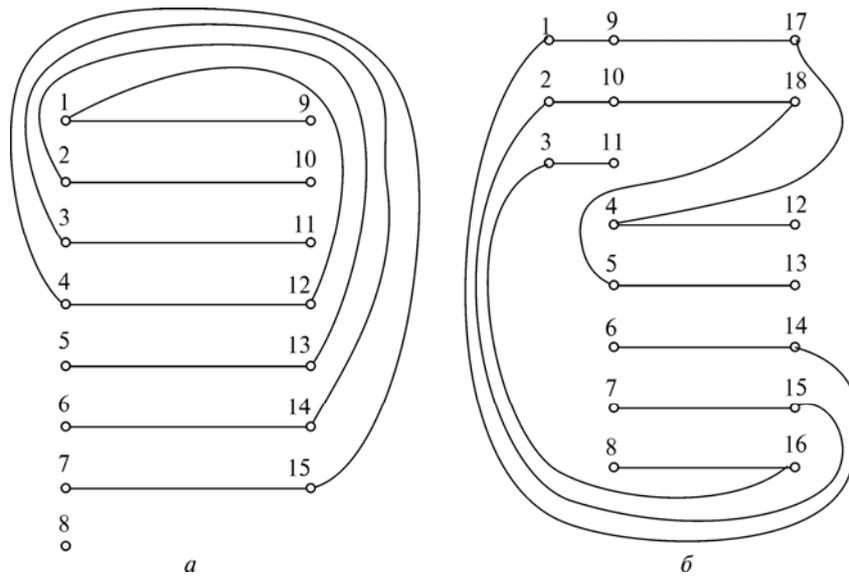


Рис. 3.8

Учитывая, что вершины были разные, приходим к выводу, что первое слагаемое — единица — относится к круглым вершинам, а второе — к точкам. В результате число вершин в цепях первого типа будет равным $\left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1\right)a + \left(\left\lfloor \frac{u_1}{k} \right\rfloor a\right)\left(\left\lfloor \frac{b}{u_1(\text{mod } k)} \right\rfloor\right)$, в цепях второго типа — $\left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1\right)a + \left(\left\lfloor \frac{u_1}{k} \right\rfloor a + 1\right)\left(1 + \left\lfloor \frac{b}{u_1(\text{mod } k)} \right\rfloor\right)$, а исходный граф $G(X, U)$ можно представить в виде

$$G = \left\{ P_c^{b[\text{mod } u_1(\text{mod } k)]}; P_d^{u_1(\text{mod } k) - b[\text{mod } u_1(\text{mod } k)]}; P_e^{k - b - u_1(\text{mod } k)} \right\}, \quad (3.23)$$

где

$$d = \left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1\right)a + \left(\left\lfloor \frac{u_1}{k} \right\rfloor a + 1\right)\left(\left\lfloor \frac{b}{u_1(\text{mod } k)} \right\rfloor\right),$$

$$c = d + \left\lfloor \frac{u_1}{k} \right\rfloor a + 1, \quad e = \left\lfloor \frac{u_1}{k} \right\rfloor a.$$

Если $u_1(\text{mod } k) \geq b$, то образующая $u_1(\text{mod } k)$ связывает только две компоненты подобного графа. Одна из них имеет $\left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1\right)a$ вершин, а другая — $\left\lfloor \frac{u_1}{k} \right\rfloor + 1$ вершин. Таким образом, в этом случае граф $G(X, U)$ можно представить в виде

$$G = \left\{ P^b_{\left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1\right)a+1}; P^{k-2b}_{\left\lfloor \frac{u_1}{k} \right\rfloor a} \right\}; \quad (3.24)$$

2) $u_1(\text{mod } k) + b > k$ (рис. 3.8, б).

Из рис. 3.8 видно, что в графе $G^0(X', U')$ можно выделить подграф на b первых горизонтальных компонентах. Если каждую компоненту стянуть в одну вершину, то у полученного графа $G^*(X^*, U^*)$ число $n^* = b$, а $U^* = \{u_1(\text{mod } k) = u_1^*, u_2^* = k - u_1(\text{mod } k)\}$. Так как $b \leq u_1(\text{mod } k)$, то вторая образующая не нужна, и граф можно представить в виде

$$G = \left\{ P_c^{b[\text{mod } u_1(\text{mod } k)]}; P_d^{u_1(\text{mod } k) - b[\text{mod } u_1(\text{mod } k)]} \right\}, \quad (3.25)$$

где

$$c = \left(\left\lfloor \frac{b}{u_1(\text{mod } k)} \right\rfloor + 1 \right) \left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1 \right) a + \left\lfloor \frac{u_1}{k} \right\rfloor a + 2,$$

а

$$d = \left\lfloor \frac{b}{u_1(\text{mod } k)} \right\rfloor \left(\left\lfloor \frac{u_1}{k} \right\rfloor + 1 \right) a + \left\lfloor \frac{u_1}{k} \right\rfloor a + 1.$$

3.5. ИЗОМОРФИЗМ НАТУРАЛЬНЫХ МОДУЛЬНЫХ ГРАФОВ

Натуральные модульные графы представляют интересный класс числовых графов, в которых функция смежности задается модулем разности на множестве вершин, коды которых задаются натуральными числами. Для таких графов базовые алгоритмы из теории графов могут быть намного менее емкие как по времени, так и по памяти. Потому интересной для рассмотрения есть проблема поиска изоморфных графов в классе *NM*-графов.

Как известно, изоморфные графы имеют ряд совпадающих параметров (инвариантов), среди которых такие простейшие: а) количество вершин, б) количество ребер, в) вектор степеней вершин.

В этом параграфе, если не указано иначе, рассматриваются графы с количеством образующих, не превышающих 2. В предыдущем параграфе показан алгоритм нахождения изоморфизма для натуральных арифметических графов с количеством образующих меньше 2, а также проведено перечисление изоморфных компонент. Что касается натуральных модульных графов, то известны некоторые их свойства, например связность [43], цикломатическое число [41] и другие. Эти свойства позволяют проводить исследование изоморфизма таких графов и даже осуществлять перечисление изоморфных компонент.

Для начала рассмотрим *NM*-графы с одной образующей. Пусть $G = (X, U)$, $X \in N$, $|X| = n$, а $U = \{u\}$. Из [43] вытекает, что для каждой образующей $u \in U$ существует ровно $n - u$ ребер. Поскольку количество ребер в изоморфных графах совпадает, то это условие для *NM*-графов с одной образующей можно изложить в виде следующего утверждения.

Лемма 3.7. Два *NM*-графа с одной образующей $G_1 = (X, u)$ и $G_2 = (X, v)$ изоморфны тогда и только тогда, когда $u = v$.

Таким образом, можно перечислить все неизоморфные *NM*-графы с n вершинами и одной образующей.

В лемме 3.2 [51] доказано, что *NM*-граф $G = (X, u)$ состоит из u компонент связности, среди которых $\left\lceil \frac{n}{u} \right\rceil u - n$ являются цепями из

$\left\lceil \frac{n}{u} \right\rceil - 1$ вершин каждая, а остальные — цепями из $\left\lfloor \frac{n}{u} \right\rfloor$ вершин каждая. Здесь $\lceil x \rceil$ — ближайшее целое, не меньшее x . Для графов с двумя образующими имеет место следующая лемма.

Лемма 3.8. Два *NM*-графа с двумя образующими будут изоморфными при условии, что сумма их образующих совпадает.

Доказательство. В данном случае речь идет о совпадении второго условия инвариантов. Действительно, пусть $G_1 = (X, U)$, $G_2 = (X, V)$, где $U = \{u_1, u_2\}$, $V = \{v_1, v_2\}$ изоморфны. Тогда количество ребер у них должно совпадать, т. е.

$$(n - u_1) + (n - u_2) = (n - v_1) + (n - v_2).$$

Раскрыв скобки, получаем $u_1 + u_2 = v_1 + v_2$.

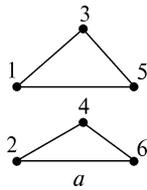


Рис. 3.9

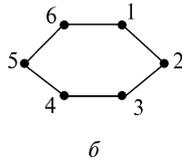
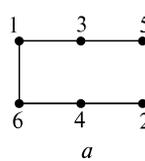


Рис. 3.10



Нетрудно заметить, что при небольшом изменении лемма 3.8 может быть применима и для графов с большим количеством образующих. Иначе говоря, лемма 3.8 является следствием более общего утверждения.

Лемма 3.9. Если два *NM*-графа с одинаковым количеством образующих изоморфны, то сумма их образующих совпадает.

Это условие не является достаточным в общем случае. На рис. 3.9 показаны графы с шестью вершинами и образующими $U = \{2, 4\}$ (рис. 3.9, а), $V = \{1, 5\}$ (рис. 3.9, б). Эти графы не будут изоморфными, хотя их образующие удовлетворяют условию леммы 3.9. С другой стороны, графы с образующими $\{3, 4\}$ и $\{2, 5\}$ будут изоморфны (рис. 3.10).

Таким образом, поиск достаточных условий не столь очевиден, поскольку одинаковое количество ребер для натуральных модульных графов не гарантирует изоморфности.

Для упрощения записи обозначим $G_n(u_1, u_2)$ — *NM*-граф с n вершинами и множеством образующих $U = \{u_1, u_2\}$.

Как известно [88], у связного графа с двумя образующими наибольший общий делитель $\text{НОД}(u_1, u_2) = 1$, а $u_1 + u_2 \leq n + 1$. Исходя из этих условий, можно доказать следующее утверждение.

Теорема 3.9 Графы $G_n(u_1, u_2)$, $G_n(v_1, v_2)$ — изоморфны, если:

- 1) $u_1 + u_2 = v_1 + v_2 \in \{n, n + 1\}$;
- 2) $\text{НОД}(u_1, u_2) = \text{НОД}(v_1, v_2) = 1$.

Доказательство. Графы, удовлетворяющие этим условиям, будут либо гамильтоновым циклом ($u_1 + u_2 = n$), либо гамильтоновой цепью, следовательно, их изоморфность очевидна.

Теорема 3.10. Графы $G_n(u_1, u_2)$, $G_n(v_1, v_2)$ изоморфны, если

$$u_1 + u_2 = v_1 + v_2, \text{НОД}(u_1, u_2) = \text{НОД}(v_1, v_2) = 1 \text{ и } u_1 + u_2 = n - 1.$$

Доказательство. Графы с такими свойствами состоят из двух граней, содержащих соответственно четыре вершины и $n-1$ вершин. Наложим четырехугольные грани одна на другую так, чтобы вершины со степенью 3 одного графа (таких две) наложились на такие же вершины другого графа. Остались неуложенными $n-4$ вершин. Но эти вершины соединены в цепь как в одном, так и в другом графе. Следовательно, наложив эти цепи, получим взаимнооднозначное соответствие между графами, т. е. эти графы изоморфны.

Теорема 3.11. Графы с двумя образующими $G_n(u_1, u_2)$, $G_n(v_1, v_2)$ не будут изоморфными, если

$$u_1 + u_2 = v_1 + v_2, \text{НОД}(u_1, u_2) = \text{НОД}(v_1, v_2) = 1 \text{ и } u_1 + u_2 < n - 1.$$

Доказательство. Пусть $G_n(u_1, u_2)$ и $G_n(v_1, v_2)$ — два графа, для которых выполняются условия теоремы и они изоморфны. Пусть $\varphi: X_1 \rightarrow X_2$ — взаимнооднозначная функция, переводящая вершины первого графа в вершины второго. Имеем грань длиной $u_1 + u_2$, которая состоит из $u_1 + u_2$ вершин вида $1, 1 + u_1, 1 + 2u_1, \dots, 1 + ku_1 = u_1 + u_2, u_1, 2u_1, ku_1$, где k — решение уравнения $(k-1)u_1 = u_2 - 1$. Тогда в изоморфном графе эта грань имеет вид

$$\varphi(1), \varphi(1 + u_1), \varphi(1 + 2u_1), \dots, \varphi(1 + ku_1 = u_1 + u_2), \varphi(u_1), \varphi(2u_1), \varphi(ku_1).$$

Однако эта грань во втором графе образуется только тем же способом, что и в первом, т. е. $1, 1 + v_1, 1 + 2v_1, \dots, 1 + lv_1 = v_1 + v_2, v_1, 2v_1, lv_1$, где l — решение соответствующего уравнения $(l-1)v_1 = u_2 - 1$. Поскольку $u_1 + u_2 = v_1 + v_2$, то $ku_1 = lv_1$, $ku_1 + ku_2 = lv_1 + lv_2$, следовательно, $k = l$. Это означает, что образующие $u_1 = v_1$, т. е. такие графы совпадают. Теорема 3.11 доказана.

Теорема 3.12. Графы с двумя образующими $G_n(u_1, u_2)$, $G_n(v_1, v_2)$ не будут изоморфными, если

$$u_1 + u_2 = v_1 + v_2, \text{НОД}(u_1, u_2) = \text{НОД}(v_1, v_2) = 1 \text{ и } u_1 + u_2 > n + 1.$$

Доказательство. Такие графы не будут связными, более того, в таких графах не будет совпадать вектор степеней вершин ввиду того, что количество вершин степени 0, т. е. количество изолированных вершин, зависит от величины большей образующей.

Однако не все несвязные графы будут неизоморфными. Для некоторых из них справедлива следующая теорема.

Теорема 3.13. Графы с двумя образующими $G_n(u_1, u_2)$, $G_n(v_1, v_2)$ у которых $u_1 + u_2 = v_1 + v_2$, $\text{НОД}(u_1, u_2) = \text{НОД}(v_1, v_2) = c > 1$, изоморфны тогда и только тогда, когда графы $G_{\lfloor \frac{n}{c} \rfloor}(\frac{u_1}{c}, \frac{u_2}{c})$ и $G_{\lfloor \frac{n}{c} \rfloor}(\frac{v_1}{c}, \frac{v_2}{c})$ изоморфны.

Доказательство. Графы, указанные в условии теоремы 3.13, состоят из c компонент связности. Поэтому изоморфизм таких графов возможен лишь при условии изоморфизма компонент связности исходных графов. Эти компоненты связности представляют собой $n \pmod{c}$ графов с числом вершин $\lfloor \frac{n}{c} \rfloor$ и $c - n \pmod{c}$ графов с числом вершин $\lfloor \frac{n}{c} \rfloor$. Если графы с числом вершин $\lfloor \frac{n}{c} \rfloor$ изоморфны, то изоморфны и графы с количеством вершин $\lfloor \frac{n}{c} \rfloor$, поскольку последние являются подграфами первых.

Определение 3.2. Пусть заданы две матрицы инцидентности вершин графов, из которых A_1 соответствует графу G_1 , а A_2 — графу G_2 . Эти графы будут изоморфными ($G_1 \cong G_2$), если найдется такая перестановочная матрица P , для которой справедливо

$$A_2 = PA_1P^T.$$

Матрице P соответствует перестановка $p = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ такая, что если на множестве вершин графа G_2 сделать перестановку p , то полученный граф станет полной копией графа G_1 .

Рассмотрим матрицу образующих полного *NM*-графа. Каждой образующей $1 \leq u \leq n-1$ в матрице A :

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & \dots & n-1 \\ 1 & 0 & 1 & 2 & \dots & n-2 \\ 2 & 1 & 0 & 1 & \dots & n-3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ n-1 & n-2 & n-3 & n-4 & \dots & 0 \end{pmatrix} \quad (3.26)$$

соответствует две последовательности чисел u , расположенных параллельно над и под главной диагональю, состоящей из нулей. Матрица образующих произвольного NM -графа отличается от матрицы (3.26) тем, что на месте несуществующих образующих стоят нули. Поэтому степень i -й вершины s_i в таких графах равна количеству ненулевых элементов в i -й строке (столбце) матрицы образующих. Построим график степеней вершин графа, исходя из указанных свойств матрицы образующих:

1) если $2u \leq n - 1$, то образующая u добавляет к степени вершины j величину

$$\Delta_j(u) = \begin{cases} 1 & \text{для } 1 \leq j \leq u; \\ 2 & \text{для } u + 1 \leq j \leq n - u; \\ 1 & \text{для } n - u + 1 \leq j \leq n; \end{cases} \quad (3.27)$$

2) если $2u > n - 1$, то образующая u добавляет к степени вершины j величину

$$\Delta_j(u) = \begin{cases} 1 & \text{для } 1 \leq j \leq n - u; \\ 0 & \text{для } n - u + 1 \leq j \leq u; \\ 1 & \text{для } u + 1 \leq j \leq n. \end{cases} \quad (3.28)$$

Единственная образующая при $n \equiv 0 \pmod{2}$, которая добавляет всегда единицу к степени произвольной вершины, это $u = \frac{n}{2}$. Граф с множеством образующих $U = \{u_1, u_2, \dots, u_m\}$ имеет вектор степеней $S = (s_1, s_2, \dots, s_n)$, где

$$s_j = \sum_{u \in U} \Delta_j(u); \quad j = 1, 2, \dots, n. \quad (3.29)$$

Построим графики образующих, используя выражения (3.27) и (3.28) для $n = 22$, $U = \{7, 16\}$ (рис. 3.11: $a - u_1 = 7$, $b - u_2 = 16$).

Путем наложения таких графиков для каждой образующей получим суммарный график функции степеней вершин, которую обозначим $S(G)$. Очевидно, что если графики образующих имеют центральную ось симметрии, то и график $S(G)$ тоже будет симметричным. Поэтому все свойства таких графиков будут изучаться только для их левой половины. Графики образующих для (3.27) имеют подъем в точке $j = u$, а для образующих (3.28) —

спуск в точке $j = n - u$. При построении графика функции $S(G)$ некоторые подъемы могут накладываться на спуски и нейтрализовать друг друга. Это возможно только в случае, если $u_k + u_l = n$ ($k \neq l$). Если таких образующих нет, то число подъемов функции $S(G)$ будет равно числу образующих типа (3.27), а число спусков — числу образующих типа (3.28). Как пример рассмотрим график $S(G)$ на рис. 3.12.

Подсчитав число подъемов и спусков графика (напоминаем, что все делается для левой половины графика, т. е. $1 \leq j \leq 11$), находим, что оно равно 5 (три спуска и два подъема). Это означает, что должно быть не меньше 5 образующих. Так как $\min S(G) = 3$, а $\max S(G) = 5$, то число образующих должно быть в этих пределах, что определяет окончательно число образующих, равное 5. Подъемы на графике присутствуют в точках $j = 6, 8$, что

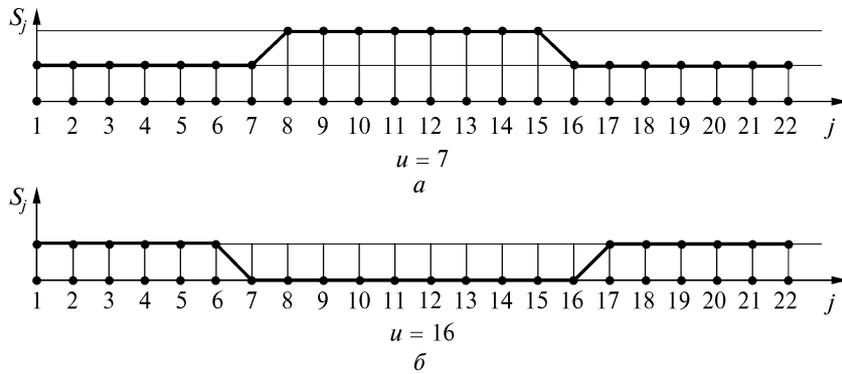


Рис. 3.11

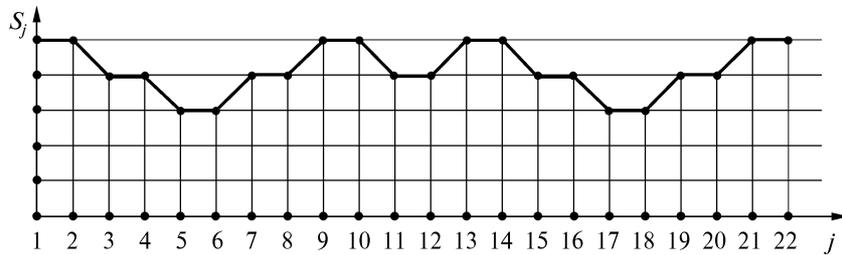


Рис. 3.12

соответствует образующим $u_1 = 6, u_2 = 8$. Спуски присутствуют в точках $j = 2, 4, 10$. Это соответствует отношениям $n - u_3 = 10$, $n - u_4 = 4$, $n - u_5 = 2$, откуда $u_3 = 12$, $u_4 = 18$ и $u_5 = 20$. Непосредственно можно убедиться, что эти образующие и соответствуют данному графику.

Вектор степеней графа $S = (3^4, 4^{10}, 5^8)$, где верхний индекс указывает число вершин с данной степенью. Если вектор считать одним из инвариантов графа, то этому вектору соответствует много NM -графов. Назовем график функции $S(G)$ для заданного вектора S *каноническим*, если он является монотонно возрастающим (рис. 3.13).

Граф, соответствующий каноническому графику функции $S(G)$, назовем *каноническим*. Здесь число подъемов равно 2, а спусков не будет никогда по правилу построения. Но число образующих должно быть, по крайней мере, три. Третья образующая не должна иметь ни подъемов, ни спусков, и такая образующая существует для четных n и имеет вид $u_3 = \frac{n}{2}$. Таким образом, канонический график $S(G)$ строится единственным образом с помощью трех образующих $u_1 = 2$ (точка подъема $j = 2$), $u_2 = 7$ (точка подъема $j = 7$) и $u_3 = 11$. Очевидно, что число образующих канонического графа равно $\min S(G)$. Если значения графика увеличить всюду на единицу, то тогда пришлось бы использовать четыре образующих, хотя подъемов было бы по-прежнему 2. В этом случае две образующие в сумме должны не допускать ни подъемов, ни спусков. Такие образующие существуют и имеют вид u_3 и $u_4 = n - u_3$, но при этом канонический график строится не единственным

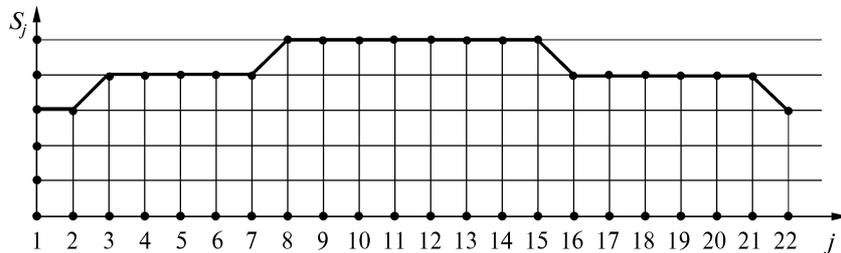


Рис. 3.13

образом. Все полученные результаты можно подытожить в виде утверждений.

Утверждение 3.1. Для изоморфных *NM*-графов число образующих не является инвариантом.

Утверждение 3.2. Канонический граф, реализующий заданный вектор степеней $S = (s_1, s_2, \dots, s_n)$, содержит наименьшее число образующих.

В процессе исследования проблемы изоморфизма *NM*-графов приходится использовать график степеней вершин, при этом часть графика может принадлежать образующей $u = \frac{n}{2}$ (для четных n) или набору пар образующих типа u и $n - u$. Остальные образующие являются надстройкой над ними. Сами эти пары образующих, отдельно взятые в различных комбинациях, представляют собой регулярные графы. Действительно, для них любой график степеней вершин не содержит ни подъемов, ни спусков, т. е. является константой, что и есть определением регулярности графа. Тем самым доказана следующая лемма.

Лемма 3.10. Все регулярные *NM*-графы степени $2k$ имеют множество образующих вида $U = \{u_1, u_2, \dots, u_k, n - u_k, \dots, n - u_2, n - u_1\}$, где $1 \leq u_i \leq \left\lfloor \frac{n-1}{2} \right\rfloor$, $(i = 1, 2, \dots, k)$. Регулярный *NM*-граф степени $2k + 1$ возможен лишь при четном числе вершин и отличается от графа степени $2k$ дополнительной образующей $u = \frac{n}{2}$.

Отсюда вытекает, что регулярный граф с одной образующей существует только для четного числа вершин. Рассмотрим регулярные графы степени 2, множества образующих которых представлены в виде $U = \{u, n - u\}$, где $1 \leq u \leq n - 1$. Таких множеств $\left\lfloor \frac{n-1}{2} \right\rfloor$, но некоторые из них могут соответствовать изоморфным графам. Известно, что если u_1 и u_2 — взаимно простые, а также $u_1 + u_2 = n$, то такой граф является гамильтоновым циклом.

Лемма 3.11. Число *NM*-графов с двумя образующими, являющихся гамильтоновыми циклами, равно $\frac{\varphi(n)}{2}$, где $\varphi(n)$ — функция Эйлера.

Доказательство. Очевидно, что если $\text{НОД}(u, n-u) = 1$, то и $\text{НОД}(u, n) = 1$, а всего таких значений u есть $\varphi(n)$. Среди пар $(u, n-u)$ всегда $u < n-u$, поэтому количество таких пар, обе образующие которых взаимно простые, равно $\frac{\varphi(n)}{2}$. Покажем, что существует такая перестановочная матрица P , которая переводит любой гамильтонов цикл с образующими $U = \{u, n-u\}$ в такой же цикл с образующими $U = \{1, n-1\}$. Этой матрице соответствует перестановка $p = \binom{1+(k-1)u}{k}$, где $k = 1, 2, \dots, n$. Действительно, любая линейная форма $u(k-1)+1$ при $\text{НОД}(u, n) = 1$ пробегает все вычеты по $\text{mod } u$, если k принимает значения от 1 до n .

Следствие. Если для двух NM -графов $G_n(u, n-u)$ и $G_n(v, n-v)$ $\text{НОД}(u, n) = \text{НОД}(v, n) = c > 1$, то такие графы изоморфны и число

их равно $\frac{\varphi\left(\frac{n}{c}\right)}{2}$.

Действительно, согласно результату предыдущего параграфа [67] такие графы распадаются на c компонент связности с $\frac{n}{c}$ вершинами. Если к каждой компоненте применить лемму 3.11, то получим указанный результат.

Теперь можно полностью описать структуру регулярных графов с двумя образующими.

Теорема 3.14. Граф $G_n(u_1, u_2)$ — плоский граф; если $n \geq u_1 + u_2$, то он состоит из $n - u_1 - u_2 + k$ циклов, из которых k циклов имеют длину $\frac{u_1 + u_2}{k}$ и $n - u_1 - u_2 - k$ циклов имеют длину 4, где $k = \text{НОД}(u_1, u_2)$.

Доказательство. Если $n < u_1 + u_2$, то граф является подграфом фактор-графа, поэтому он — плоский. Пусть $n \geq u_1 + u_2$.

Рассмотрим подграф $G_{u_1+u_2}(u_1, u_2)$ графа $G_n(u_1, u_2)$. Он состоит из k циклов $C_i(1, 2, \dots, k)$, где $k = \text{НОД}(u_1, u_2)$. Цикл C_i состоит из последовательности вершин $(i + tu_1) \pmod{(u_1 + u_2)}$, где $t = 0, 1, \dots$

..., $\frac{u_1 + u_2}{k} - 1$. Каждая новая вершина с номером $j + u_1 + u_2$ ($j \geq 1$) добавляется к внешней стороне цикла C_i ($j \equiv i \pmod{[u_1 + u_2]}$) и окружает вершину j , образуя новый цикл длиной 4 с вершинами $(j + u_1 + u_2, j + u_1, j, j + u_2)$. В результате длина внешнего цикла C_i не изменится, а вершина j закроется вершиной $j + u_1 + u_2$. И этот процесс может быть продолжен для всех циклов C_i , пока j не достигнет $n - u_1 - u_2$.

В итоге имеем k циклов длиной $\frac{u_1 + u_2}{k}$ и $n - u_1 - u_2$ циклов длиной 4.

Пример. $U = \{6, 9\}$. Для $n = 15$ получаем (рис. 3.14, ребра показаны полужирными линиями) три цикла длиной 5. Добавляя вершины (увеличивая n) до 25, имеем

- вершина 16 окружает вершину 1, образуя цикл (16, 7, 1, 10);
- вершина 17 окружает вершину 2, образуя цикл (17, 8, 2, 11);
- вершина 23 окружает вершину 8, образуя цикл (23, 14, 8, 17);
- вершина 24 окружает вершину 9, образуя цикл (24, 15, 9, 18);
- вершина 25 окружает вершину 10, образуя цикл (25, 16, 10, 19).

Таким образом, получаем еще $25 - 15 = 10$ четырехвершинных цикла.

Теорема 3.14 позволяет построить алгоритм плоской укладки *NM*-графа с двумя образующими.

В предыдущем параграфе полностью решена проблема изоморфизма для *NM*-графов с двумя произвольными образующими. Очевидно, что регулярные *NM*-графы степени 2 при n простом всегда изоморфны, так как их всех можно представить в виде n -вершинного гамильтонова цикла.

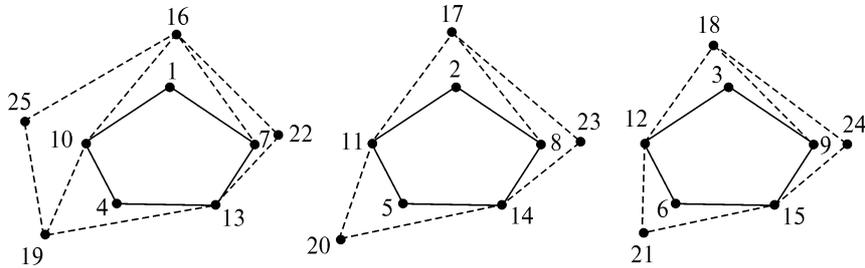


Рис. 3.14

Рассмотрим регулярные NM -графы степени 4. В зависимости от значений n возможны два случая.

Пусть n — простое число. Тогда все пары образующих $(i, n-i)$ ($i = 1, 2, \dots, \frac{n-1}{2}$) представляют собой гамильтоновы циклы. Обозначим каждый такой цикл C_i . Теперь каждый регулярный NM -граф степени 4 можно представить как коммутативную композицию двух таких циклов $C_i C_j$ ($i \neq j$). Поскольку C_i и C_j изоморфны, то существует перестановка S , которая переводит C_j в C_i .

Лемма 3.12. Для преобразования цикла C_j в C_i ($i \neq j$) необходимо применить перестановку

$$S(C_j \rightarrow C_i) : k \rightarrow \begin{cases} [(k-1)j^{-1}i + 1] \pmod{n}, & \text{или} \\ [n - (k-1)j^{-1}i + 1] \pmod{n}, & k = 1, 2, \dots, n. \end{cases} \quad (3.30)$$

Доказательство. Непосредственно можно убедиться, что S есть перестановка, т. е. для двух разных чисел $k_1 \neq k_2$ результаты перестановок также будут разными. Найдем сначала перестановку для перевода C_j в C_1 , затем перестановку, переводящую C_1 в C_i . Для этого нужно перевести 1 в 1, $1+j$ — в 2 и в общем случае для любого $2 < l \leq n$ необходимо $(l-1)j+1$ перевести в l . Решая уравнение $\left\lfloor \frac{n-1}{4} \right\rfloor$ относительно l , получаем искомую перестановку:

$$S(C_j \rightarrow C_1) : k \rightarrow [(k-1)j^{-1} + 1] \pmod{n}, \quad k = 1, 2, \dots, n. \quad (3.31)$$

Теперь для перевода C_1 в C_i необходимо 1 перевести в 1, 2 перевести в $1+i$ и в общем случае число $2 < l \leq n$ перевести в $1+(l-1)i$. После чего имеем перестановку

$$S(C_1 \rightarrow C_i) : k \rightarrow [(k-1)i + 1] \pmod{n}, \quad k = 1, 2, \dots, n. \quad (3.32)$$

Последовательно применяя перестановки (3.31) и (3.32), получаем цепочку

$$k \rightarrow [(k-1)j^{-1} + 1] \pmod{n} \rightarrow [(k-1)j^{-1}i + 1] \pmod{n},$$

что и требовалось доказать. Вторая перестановка в (3.30) тождественна первой, если цикл просматривать не по часовой стрелке, а против нее.

Следствие. Перестановки (3.31) и (3.32) можно записать в общем виде:

$$k \rightarrow [1 \pm (k-1)j^{-1}i](\text{mod } n). \quad (3.33)$$

Следует учесть, что при всех описанных и дальнейших преобразованиях вершина с номером $0(\text{mod } n)$ отождествляется с вершиной n . Исследуем проблему изоморфизма сначала среди графов типа C_1C_j ($i = 1, 2, \dots, \frac{n-1}{2}$). Казалось бы, среди них нет изоморфных, так как если накладывать на граф C_1C_i граф C_1C_j , $j > i$, по одноименным вершинам, то цикл первого графа $(1, 2, \dots, i+1, 1)$ всегда меньше цикла $(1, 2, \dots, j+1, 1)$ и графы никогда не совпадут. Однако преобразование $C_j \rightarrow C_1$ может привести к преобразованию $C_1 \rightarrow C_i$ в том же графе, что в результате преобразует второй граф в C_iC_1 , который изоморфен первому.

Лемма 3.13. Два *NM*-графа $G_1 = C_1C_j$ и $G_2 = C_1C_i$ изоморфны, если выполняется условие

$$ij \equiv \pm 1(\text{mod } n). \quad (3.34)$$

Поскольку $i \neq j$, то графы будут изоморфными, если при переходе $C_1 \rightarrow C_i$ в графе G_2 цикл C_j перейдет в C_1 . Этому процессу соответствует перестановка (3.31). В то же время в цикле C_j номера вершин составляют арифметическую прогрессию $1, 1+j, \dots, [1+j(k-1)](\text{mod } n)$ для $k = 1, 2, \dots, n$. Применяя к этой последовательности перестановку (3.32), получаем последовательность номеров $1, 1+ij, \dots, [1+ij(k-1)](\text{mod } n)$ для тех же значений k . Если использовать соотношение (3.34), то получим либо последовательность $(1, 2, \dots, n)$, либо $(1, n, n-1, \dots, 2)$, что соответствует циклу C_1 . Это и подтверждает справедливость леммы 3.13.

Теорема 3.15. Два *NM*-графа $G_1 = C_iC_j$ и $G_2 = C_pC_q$ изоморфны, если выполняется одно из условий:

$$\begin{aligned} qi &\equiv \pm pj(\text{mod } n); \\ pi &\equiv \pm qj(\text{mod } n). \end{aligned} \quad (3.35)$$

Доказательство. Два регулярных *NM*-графа могут быть изоморфными только в двух случаях:

- 1) если C_p перевести в C_i , то C_q перейдет в C_j ;
- 2) если C_p перевести в C_j , то C_q перейдет в C_i .

В первом случае это достигается с помощью перестановки (3.33) $k \rightarrow [1 \pm (k-1)p^{-1}i](\text{mod } n)$. Тогда вершины цикла C_q , которые образуют последовательность $[1 + (k-1)q](\text{mod } n)$, перейдут в вершины $[1 \pm (k-1)qp^{-1}i](\text{mod } n)$. Поскольку при этом $C_q \rightarrow C_j$, то должно выполняться равенство $1 \pm (k-1)qp^{-1}i \equiv [1 + (k-1)j](\text{mod } n)$.

После преобразований получим первое равенство из формулы (3.35). Второе равенство из (3.35) получим, если граф $C_p C_q$ представить как $C_q C_p$, как следствие первого.

Следствие. Множество всех неизоморфных регулярных NM -графов степени 4 принадлежит множеству $\{C_1 C_i\}$, $i = 2, 3, \dots, \frac{n-1}{2}$.

Действительно, если взять произвольный граф $C_i C_j$ ($i \neq 1, j \neq 1$), то обязательно найдется такой граф $C_1 C_x$, который ему изоморфен. Это следует из теоремы 3.15, потому что должно выполняться одно из равенств:

$$xi \equiv \pm j(\text{mod } n) \text{ или } xj \equiv \pm i(\text{mod } n).$$

Поскольку n — простое, то решение этих равенств существует всегда. Оно равно

$$x \equiv \pm ji^{-1}(\text{mod } n) \text{ или } x \equiv \pm ij^{-1}(\text{mod } n). \quad (3.36)$$

С другой стороны, два изоморфных графа $C_i C_j$ и $C_p C_q$ можно преобразовать в графы $C_1 C_s$ и $C_1 C_t$, и тогда следствие становится очевидным.

Лемма 3.14. Число всех неизоморфных NM -графов степени 4 равно $\left\lfloor \frac{n-1}{4} \right\rfloor$.

Рассмотрим все пары $C_1 C_i$ ($i = 2, 3, \dots, \frac{n-1}{2}$) и найдем для каждого i обратный элемент $i^{-1} \equiv \lambda(\text{mod } n)$. По лемме 3.13 графы $C_1 C_i$ и $C_1 C_\lambda$ изоморфны. Если $\lambda \leq \frac{n-1}{2}$, то C_λ — это NM -граф с образующими $(\lambda, n-\lambda)$. Если $\lambda > \frac{n-1}{2}$, то $i(n-\lambda) \equiv -1(\text{mod } n)$ и

изоморфными будут графы C_1C_i и $C_1C_{n-\lambda}$. Всего графов $\left\lfloor \frac{r+1}{2} \right\rfloor$ насчитывается $\frac{n-3}{2} = r$. Если это четное число, то неизоморфных графов будет $\frac{r}{2}$, если r — нечетное, то найдется такой граф C_1C_α , для которого $\alpha(n-1) \equiv 1 \pmod{n}$ или $\alpha^2 \equiv -1 \pmod{n}$. У этого графа нет изоморфных среди графов C_1C_i . Для обоих случаев число неизоморфных графов равно $\left\lfloor \frac{r+1}{2} \right\rfloor$ или C_1C_6 , что и требовалось доказать.

Пример. Пусть $n = 17$. Перечислим графы: C_1C_2 , C_1C_3 , C_1C_4 , C_1C_5 , C_1C_6 , C_1C_7 , C_1C_8 , всего 7 графов или $\frac{17-3}{2} = 7$. Находим $2^{-1} = 9$, $3^{-1} = 6$, $4^{-1} = 13$, $5^{-1} = 7$, $6^{-1} = 3$, $7^{-1} = 5$, $8^{-1} = 15$. Среди этих элементов существуют три, которые больше 8, это 9, 13 и 15. Заменим их на 8, 4 и 2. В результате получаем три пары изоморфных графов:

$$C_1C_2 \cong C_1C_8; C_1C_3 \cong C_1C_6; C_1C_5 \cong C_1C_7.$$

Граф C_1C_4 не имеет изоморфной пары. Всего получаем $\left\lfloor \frac{17-1}{2} \right\rfloor = 4$ типа неизоморфных графов. На рис. 3.15 показаны два изоморфных графа C_1C_4 и C_3C_5 , для которых выполняются соотношения (3.35), так как $1 \cdot 3 \equiv 4 \cdot 5 \pmod{17}$.

Пусть в каноническом разложении

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}, \quad (3.37)$$

где p_1, p_2, \dots, p_l — разные простые делители числа n . Тогда можно утверждать, что все делители числа n исчерпываются всеми числами:

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_l^{\beta_l}, \quad (3.38)$$

где

$$0 \leq \beta_1 \leq \alpha_1, \quad 0 \leq \beta_2 \leq \alpha_2, \dots, \quad 0 \leq \beta_l \leq \alpha_l. \quad (3.39)$$

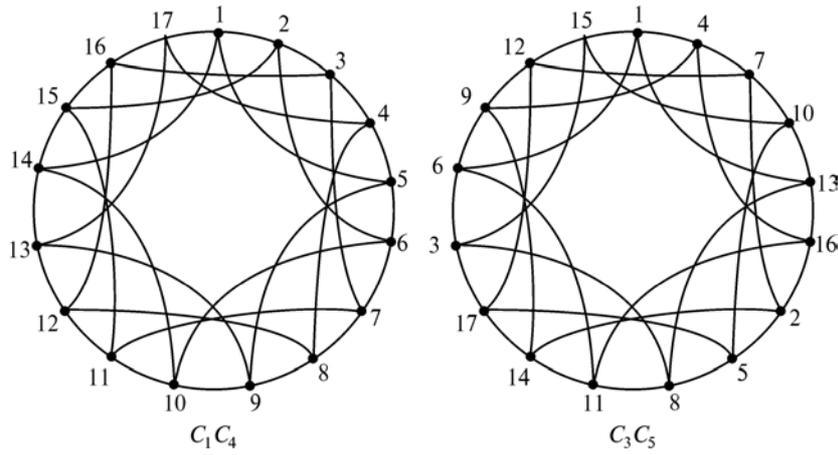


Рис. 3.15

Действительно, с одной стороны, всякое d такого вида является делителем n . С другой стороны, всякое число d , которое делит n , не может иметь простых множителей, отличных от p_1, p_2, \dots, p_l , а их показатели степени не могут противоречить условиям (3.39).

Рассмотрим простейший случай $d = 1$. Тогда все C_i , для которых $\text{НОД}(i, n) = 1$, представляют собой гамильтонов цикл. Поскольку $i \leq \left\lfloor \frac{n-1}{2} \right\rfloor$, то таких циклов ровно $\frac{\varphi(n)}{2}$, где $\varphi(n)$ — функция Эйлера.

Если $d > 1$, то граф с образующими $(d, n-d)$ состоит из d циклов длиной $\frac{n}{d}$, т. е. является 2-фактором из d компонент связности. Поэтому каждый граф для фиксированного n , заданного в виде (3.37), с образующими $(i, n-i)$, где $i = 1, 2, \dots, \left\lfloor \frac{n-1}{2} \right\rfloor$, будем обозначать F_i . Упорядочим множество всех делителей d_s типа (3.38) с условием (3.39) в порядке возрастания. Очевидно, что общее число таких делителей равно $\prod_{j=1}^l (\alpha_j + 1)$. Из этого количества необходимо изъять множитель $d = n$, когда $\beta_j = \alpha_j$, а

при $n \equiv 0 \pmod{2}$ — и $d = \frac{n}{2}$, так как эти множители не будут входить в значения образующих. Общее количество упомянутых графов F_i можно разбить на классы по признаку $\text{НОД}(i, n) = d_s$ ($s = 1, 2, \dots$).

Лемма 3.15. Число *NM*-графов s -класса при фиксированном s равно $\frac{\varphi(n)}{2d_s}$.

Это легко показать для 1-класса, где графы F_i имеют индексы, взаимно простые с n , т. е. их значения пробегают первую половину приведенной системы вычетов по модулю n и образуют множество $J_1 = \{1 = i_1, i_2, \dots, i_\lambda\}$, где $\lambda = \frac{\varphi(n)}{2}$.

Графы F_i s -класса имеют индексы i , для которых $\text{НОД}(i, n) = d_s$. Если разделить эти индексы на d_s , то получим нижние индексы $j = \frac{i}{d_s}$, для которых $\text{НОД}(\frac{i}{d_s}, \frac{n}{d_s}) = 1$. Если обозначить $n' = \frac{n}{d_s}$, то получим 1-класс для n' , где значения индексов графов F_j пробегают первую половину приведенной системы вычетов J' по модулю n' и где $\lambda = \frac{\varphi(n')}{2}$. Это означает, что число графов s -класса

равно $\frac{\varphi(\frac{n}{d_s})}{2} = \frac{\varphi(n)}{2d_s}$, что и требовалось доказать.

Лемма 3.15 позволяет изучать проблему изоморфизма среди графов, полученных композицией двух графов из s -класса, который можно представить в виде

$$F^s = \{F_j\}, \quad j = i_r d_s; \quad r = 1, 2, \dots, \lambda; \quad i_r \in J_s, \quad \lambda = \frac{\varphi(n)}{2}. \quad (3.40)$$

Очевидно, что *NM*-графы фиксированного s -класса изоморфны. Рассмотрим теперь композицию из двух графов F_i и F_j , которая образует регулярный *NM*-граф степени 4. Начнем с s -класса для $d = 1$. Так же, как и для простого n , можно утверждать о справедливости следствия теоремы 3.14 о том, что все графы типа $F_i F_j$ изоморфны определенному графу $F_1 F_x$ ($x \neq 1$). Поэтому

можно констатировать, что в 1-классе необходимо исследовать проблему изоморфизма для графов F_1F_i , где $i \in J_1 \setminus \{1\}$.

Рассмотрим два графа $G_1 = F_1F_i$ и $G_2 = F_1F_j$ ($i \neq j$). Если они изоморфны, то для них должно выполняться условие (3.36). Однако для непростого n могут встретиться такие графы F_1F_x , для которых справедливо условие

$$x^2 \equiv \pm 1 \pmod{n}. \quad (3.41)$$

Это означает, что такие графы не имеют себе изоморфных. Поэтому необходимо все такие графы обнаружить и перечислить. Для этого представим число n в виде

$$n = 2^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}; \quad \alpha_1 \geq 0; \alpha_i \geq 1; \quad i = 2, 3, \dots, k. \quad (3.42)$$

Здесь предполагается, что $p_1 = 2$, но в отличие от других множителей он может отсутствовать.

Известно [66], что сравнение $x^2 \equiv a \pmod{n}$ равносильно системе сравнений

$$\begin{aligned} x^2 &\equiv a \pmod{2^{\alpha_1}}, \\ x^2 &\equiv a \pmod{p_2^{\alpha_2}}, \\ &\dots\dots\dots \\ x^2 &\equiv a \pmod{p_k^{\alpha_k}}. \end{aligned} \quad (3.43)$$

Число a в зависимости от существования или отсутствия решения системы (3.43) называется *квадратичным вычетом (невывчетом)* по модулю n .

Лемма 3.16. Число (-1) является квадратичным вычетом системы (3.43) при условии

$$\left| \frac{3}{\alpha_1 + 2} \right| \prod_{i=2}^k \frac{p_i + 1}{2} \equiv 1 \pmod{2}. \quad (3.44)$$

Вначале покажем, что сравнение $x^2 \equiv -1 \pmod{2^{\alpha_1}}$ не может иметь решение для $\alpha_1 > 1$. Очевидно, что если такое решение существует, то оно должно быть нечетным числом. Пусть $x = 2r + 1$. Тогда $x^2 + 1 \equiv 0 \pmod{2^{\alpha_1}}$. Подставим значение x и получим $(2r + 1)^2 + 1 \equiv 0 \pmod{2^{\alpha_1}}$ или $2(2r^2 + 2r + 1) \equiv 0 \pmod{2^{\alpha_1}}$. В скобках стоит нечетное число, поэтому $\alpha_1 = 1$, что и требовалось.

Таким образом, для $\alpha_1 = 0$ или 1 первый множитель в (3.44) равен 1, а для $\alpha_1 > 1$ он равен нулю. Для других модулей известно [66], что (-1) может быть квадратичным вычетом по простому модулю p , если $p \equiv 1 \pmod{4}$. Если хотя бы один из простых множителей в системе (3.43) отличен от $1 \pmod{4}$, то при $a = -1$ система не имеет решения. Составим выражение: $\varepsilon = \prod_{i=2}^k \left(\frac{p_i + 1}{2} \right) \pmod{2}$.

Легко определить, что если найдется хотя бы один множитель $p_j \equiv 3 \pmod{4}$ $j = 2, 3, \dots, k$, то $\varepsilon \equiv 0 \pmod{2}$. Вместе с ограничением на α_1 это и дает условие (3.44).

Определим теперь количество решений системы (3.43) для заданного числа a , если решение существует. Составим для всех $i = 1, 2, \dots, k$ числа $M_i = \frac{n}{p_i}$ и M'_i при условии $M_i M'_i \equiv \pm 1 \pmod{p_i^{\alpha_i}}$.

Пусть $\pm x_i$ есть решение сравнения $x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$. Тогда общее решение системы (3.43) согласно [10] будет иметь вид

$$x \equiv \pm x_1 M_1 M'_1 \pm x_2 M_2 M'_2 \pm \dots \pm x_k M_k M'_k \pmod{n}. \quad (3.45)$$

Определим вид этого решения для $a = -1$. Если $\alpha_1 = 0$, то первое слагаемое в (3.45) отсутствует. Остается еще случай $\alpha_1 = 1$.

Тогда $x_1 \equiv 1 \pmod{2}$, а $M_1 M'_1 = \frac{n}{2} \equiv 1 \pmod{2}$. Поскольку $\frac{n}{2} \equiv -\frac{n}{2} \pmod{n}$, то первое слагаемое будет равно $\frac{n}{2}$. В итоге варьировать знаками в (3.45) можно только для оставшихся $k-1$ множителей, откуда получаем 2^{k-1} решений (3.45). Поскольку для построения графов выбираются только $x \leq \left\lfloor \frac{n-1}{2} \right\rfloor$, то окончательное число графов, соответствующих правой части $a = -1$, будет равно

$$\left\lfloor \frac{3}{\alpha_1 + 2} \right\rfloor \prod_{i=2}^k \left(\frac{p_i + 1}{2} \right) \pmod{2} \cdot 2^{k-2}. \quad (3.46)$$

Для $a = 1$ проблема существования решения системы (3.43) разрешается проще. Известно, что $(+1)$ является квадратичным

вычетом для любой степени простого модуля, и есть очевидное решение $x_i = \pm 1 \pmod{p_i^{\alpha_i}}$ ($i = 1, 2, \dots, k$). Но для степени двойки, кроме указанных решений, при $\alpha_1 \geq 3$ появляются два дополнительных решения $y = 2^{\alpha_1-1} \pm 1$. Действительно, в этом случае $y^2 \equiv 2^{2\alpha_1-2} \pm 2^{\alpha_1} + 1 \equiv 1 \pmod{2^{\alpha_1}}$. Общее число решений сравнения $x^2 \equiv 1 \pmod{2^{\alpha_1}}$ можно записать в виде $2^{2-f(\alpha_1)}$, где $f(0) = f(1) = 2$, $f(2) = 1$ и $f(\alpha_1 \geq 3) = 0$. Такой подходящей функцией является

$$f(\alpha_1) = \left\lfloor \frac{4}{\alpha_1^2 - \alpha_1 + 2} \right\rfloor; \quad \alpha_1 \geq 0. \quad (3.47)$$

Используя остальные множители, отличные от 2^{α_1} , получаем 2^{k-1} решений системы (3.43), которые в отличие от (3.45) записываем в виде

$$x = (\pm 1 \pm 2^{\alpha_1-1})M_1M'_1 \pm M_2M'_2 \pm \dots \pm M_kM'_k \pmod{n}. \quad (3.48)$$

Здесь параметры M_i и M'_i вычисляются по тем же формулам, что и для решения (3.45). Общее число решений системы (3.43) будет равно $2^{k+1-f(\alpha_1)}$.

Из этого количества для построения графов отбирают только $x \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ и исключают решение $x \equiv 1 \pmod{n}$. Окончательное число графов, соответствующее правой части $a = 1$, будет равно

$$2^{k-f(\alpha_1)} - 1. \quad (3.49)$$

Это позволяет доказать следующую теорему.

Теорема 3.16. Число неизоморфных NM -графов 1-класса F_1F_i , где $i \in J \setminus \{1\}$, равно

$$\frac{\varphi(n)}{4} + \left\lfloor \frac{3}{\alpha_1 + 2} \right\rfloor \prod_{j=2}^k \left(\frac{p_j + 1}{2} \right) \pmod{2} \cdot 2^{k-3} + 2^{k-1-f(\alpha_1)} - 1. \quad (3.50)$$

Действительно, из общего числа $\frac{\varphi(n)}{2} - 1$ образованных пар F_1F_i необходимо вычесть число обособленных графов, не имеющих себе изоморфных, это (3.36) и (3.49). В результате останутся графы, имеющие ровно по одному себе изоморфных. Это коли-

чество необходимо разделить пополам и добавить (3.36) и (3.49). В результате несложных преобразований получаем (3.50).

Пример. Для $n = 130 = 2 \cdot 5 \cdot 13$ вычисляем $\varphi(130) = 130 \times \left(\frac{1}{2} \cdot \frac{4}{5} \cdot \frac{12}{13}\right) = 48$.

Находим

$$J = \{1, 3, 7, 9, 11, 17, 19, 21, 23, 29, 31, 33, 37, 41, 43, 47, 49, 51, 53, 57, 59, 61, 63\},$$

$$\left\lfloor \frac{3}{\alpha_1 + 2} \right\rfloor = 1; \quad \varepsilon = \frac{5+1}{2} \cdot \frac{13+1}{2} = 21 \equiv 1 \pmod{2}.$$

Следовательно, (-1) является квадратичным вычетом для заданного n .

Сравнение $x_2^2 \equiv -1 \pmod{5}$ дает решение $x_2 \equiv \pm 2 \pmod{5}$, а сравнение $x_3^2 \equiv -1 \pmod{13}$ — соответственно $x_3 \equiv \pm 5 \pmod{13}$.

Находим $M_2 = \frac{130}{5} = 26$; $M'_2 = 1$; $M_3 = \frac{130}{13} = 10$; $M'_3 \equiv 4 \pmod{13}$.

В результате общее решение записываем так: $x \equiv 65 \pm 2 \cdot 26 \pm \pm 5 \cdot 40 \pmod{130}$.

Получаем четыре решения: $x_1 = 47$, $x_2 = 57$, $x_3 = 83$, $x_4 = 73$. Последние два решения отбрасываем, так как они больше $\left\lfloor \frac{130-1}{2} \right\rfloor = 64$. Графы F_1F_{47} и F_1F_{57} не имеют себе изоморфных на множестве F_1F_x , где $x \in J \setminus \{1\}$. Для правой части $a = 1$ получаем общее решение: $x = 65 \pm 26 \pm 40 \pmod{130}$.

Здесь также четыре решения $x_1 = 1$, $x_2 = 51$, $x_3 = 79$, $x_4 = 129$. Два последних решения отбрасываем, так как они больше чем 64. Из двух оставшихся $x_1 = 1$ неприемлемо. В результате получаем $x = 51$, а соответствующий граф F_1F_{51} не имеет себе изоморфных. Остальные пары имеют себе изоморфные графы по правилу (3.34):

$$F_1F_3 \cong F_1F_{43} \Leftarrow 3 \cdot 43 = 129 \equiv -1 \pmod{130};$$

$$F_1F_7 \cong F_1F_{37} \Leftarrow 7 \cdot 37 = 259 \equiv -1 \pmod{130};$$

$$F_1F_9 \cong F_1F_{29} \Leftarrow 9 \cdot 29 = 261 \equiv 1 \pmod{130};$$

$$F_1F_{11} \cong F_1F_{59} \Leftarrow 11 \cdot 59 = 649 \equiv -1 \pmod{130};$$

$$F_1F_{17} \cong F_1F_{23} \Leftarrow 17 \cdot 23 = 391 \equiv 1 \pmod{130};$$

$$F_1F_{19} \cong F_1F_{41} \Leftarrow 19 \cdot 41 = 779 \equiv -1 \pmod{130};$$

$$F_1F_{21} \cong F_1F_{31} \Leftarrow 21 \cdot 31 = 651 \equiv 1 \pmod{130};$$

$$F_1F_{27} \cong F_1F_{53} \Leftarrow 27 \cdot 53 = 1431 \equiv 1 \pmod{130};$$

$$F_1F_{49} \cong F_1F_{61} \Leftarrow 49 \cdot 61 = 2989 \equiv -1 \pmod{130}.$$

Всего получили 13 неизоморфных графов. Если подставить $n = 130$ в выражение (3.50), то найдем: $\frac{48}{4} + 2^{3-3} + 2^{3-1-2} - 1 = 13$.

Распространим это исследование на произвольное четное количество образующих. В этом случае максимальное число образующих составит $n - 1$, при котором граф будет полным. Более того, существует единственный полный граф для заданного n , что соответствует единственному способу задания его образующих. Пусть $|U| = m = 2l, l < \left\lfloor \frac{n}{2} \right\rfloor$. В этом случае графы для простого n также будут представлять собой композицию из l гамильтоновых циклов. Для таких графов проверка изоморфизма осуществляется таким же способом — соответствующие циклы графов приводятся к C_1 и сравниваются. По сути, необходимо провести преобразование массива образующих и сравнить их. Длина этого массива — l , образующие в нем лишь те, которые меньше $\left\lfloor \frac{n}{2} \right\rfloor$.

Для графов с составным n используется подобный подход. Для случаев, когда среди образующих графа есть взаимно простые с n , применяем метод сравнения массивов образующих, приведенных к единичному гамильтонову циклу, а в случае отсутствия таковых — граф разбивается на семейство изоморфных компонент связности, каждая из которых соответствует одному из вышеприведенных подходов. Еще один вид графов, который содержит множество попарно взаимно простых образующих, не имеет изоморфных, поскольку сводится к графам вида (3.41).

ПРОБЛЕМЫ ПОСТРОЕНИЯ ЭФФЕКТИВНЫХ АЛГОРИТМОВ НА ЧИСЛОВЫХ ГРАФАХ

В этой главе исследуется важная проблема об оценке сложности алгоритмов на числовых графах. Получены результаты, которые позволяют в дальнейшем на этих графах для некоторых сложных задач строить эффективные алгоритмы.

4.1. ОБ ОБЩЕМ ПРЕДСТАВЛЕНИИ ЧИСЛОВЫХ ГРАФОВ

Из всех числовых графов натуральные арифметические (*NA*-графы) и натуральные модульные (*NM*-графы) графы по способу задания являются самыми простыми. Уже обычные арифметические (*A*-графы) и модульные (*M*-графы) требуют задания способа (функции), по которому из натурального ряда чисел изымаются те, которые соответствуют вершинам, не принадлежащим множеству X . В общем случае в зависимости от вида числового графа существуют два принципиально различных способа их задания.

Первый, наиболее общий способ, задается следующим образом.

Числовым графом $G = (X, U, F, g)$ называется n -вершинный граф, представленный двумя множествами $X = \{1, 2, \dots, n, \dots, N\} = N_n$ — множеством вершин и $U \in N$ — множеством образующих, функцией смежности $F(x_i, x_j)$ и функцией исключения $g(x)$. Вершина $x_k \notin X$, если $g(x_k) = 0$, а вершины $x_i, x_j \in X$ смежны, если $F(x_i, x_j) \in U$.

Если $F(x_i, x_j) = x_i + x_j$, то такой числовой граф называется *арифметическим*, если же $F(x_i, x_j) = |x_i - x_j|$, то — *модульным*. Относительно функции $g(x)$ никаких определенных свойств не предполагается, в конце концов, она может просто перечислять множество вершин, не принадлежащих X .

В большинстве случаев, когда заданный граф имеет определенную структуру, в частности, несколько осей симметрии или периодически повторяющиеся части, задание функций $F(x_i, x_j)$ и $g(x)$ не представляет труда.

Применение теории графов в различных областях практической деятельности человека показало, что подавляющее большинство графов, которые при этом использовались, носили именно такую специфическую структуру. Можно перечислить множество работ из области распознавания образов, математического моделирования параллельных процессов, теоретических основ создания информационных технологий и многих других, где рассматриваются графы, которые можно представить в виде числовых графов указанным выше способом.

Рассмотрим пример из работы [16, с. 42, рис. 2.4]. Здесь уравнение распознаваемой реализации сигнала x_i с эталоном слова производилось с помощью графа, представленного (в уменьшенном виде) на рис. 4.1. По своей структуре это довольно простой граф, который можно представить в виде числового графа следующим образом (рис. 4.2). В данном случае получаем граф с числом вершин $n = 39$, т. е. $X = \{1, 2, \dots, 39\}$, $F(x_i, x_j) = x_j - x_i$, $g(x) \equiv 0 \pmod{8}$, а $U = \{1, 8, 9\}$. Таким образом, информация о гра-

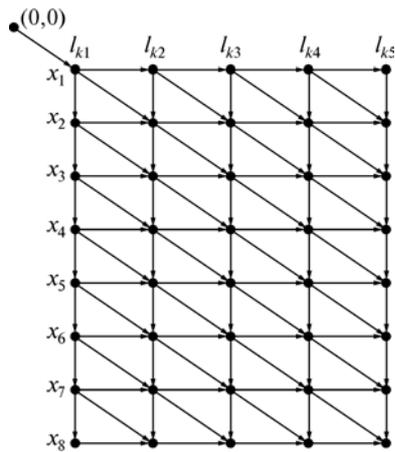


Рис. 4.1

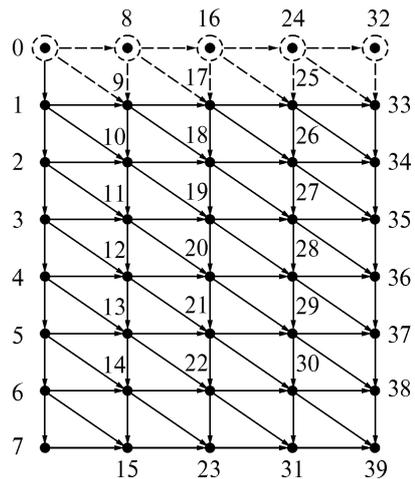


Рис. 4.2

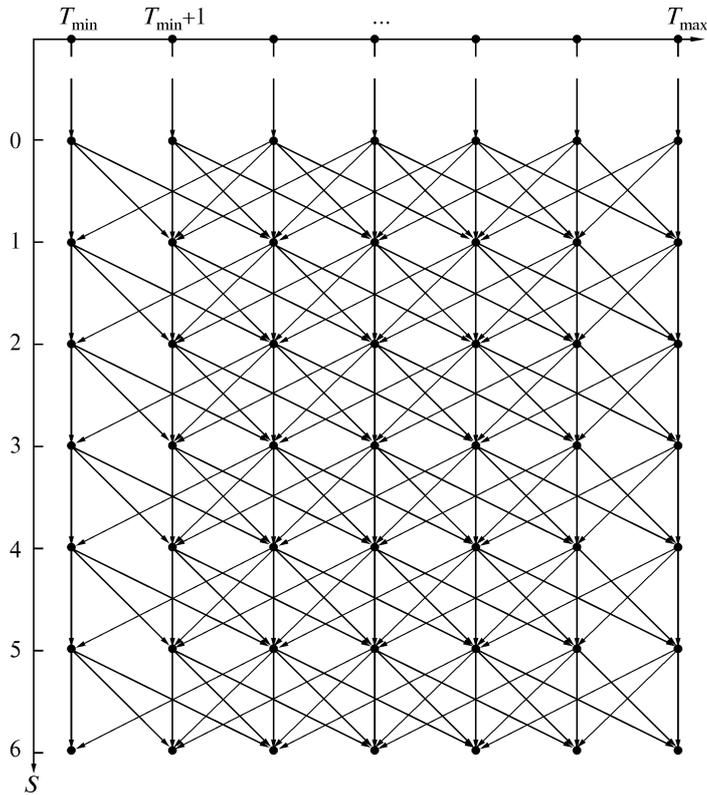


Рис. 4.3

фе укладывается в 6 чисел. В [16] граф по размерам больше, он по вертикали имеет 21 вершину и по горизонтали — 14 вершин, т. е. всего 294. Числовой граф, на рис. 4.2 (с учетом добавленных фиктивных вершин) будет иметь $n = 308$ вершин и задаваться таким образом:

$$X = \{1, 2, \dots, 308\}, F(x_i, x_j) = x_j - x_i, g(x) \equiv 0 \pmod{22}, U = \{1, 22, 23\}.$$

Аналогичное представление допускает и граф решения задачи о мгновенном периоде основного тона, приведенный на рис. 4.3 [16, с.185, рис. 9.6]. Этот граф можно представить в виде числового графа с той же самой порождающей функцией, что и в предыдущем примере, т. е. $F(x_i, x_j) = x_j - x_i$, но с другим множеством образующих.

Реализация предыдущего графа в виде числового показана на рис. 4.4. Здесь на рисунке сохраняются все стрелки, что и на основном рисунке, но они для удобства лишь обозначены. Граф представлен в виде $n = 62$, т. е. $X = \{1, 2, \dots, 62\}$, $F(x_i, x_j) = x_j - x_i$, $g(x) \equiv 0 \pmod{9}$, $U = \{-17, -8, 1, 10, 19\}$; поскольку $F(x_i, x_j)$ — функция несимметричная, то граф ориентирован. Если бы он

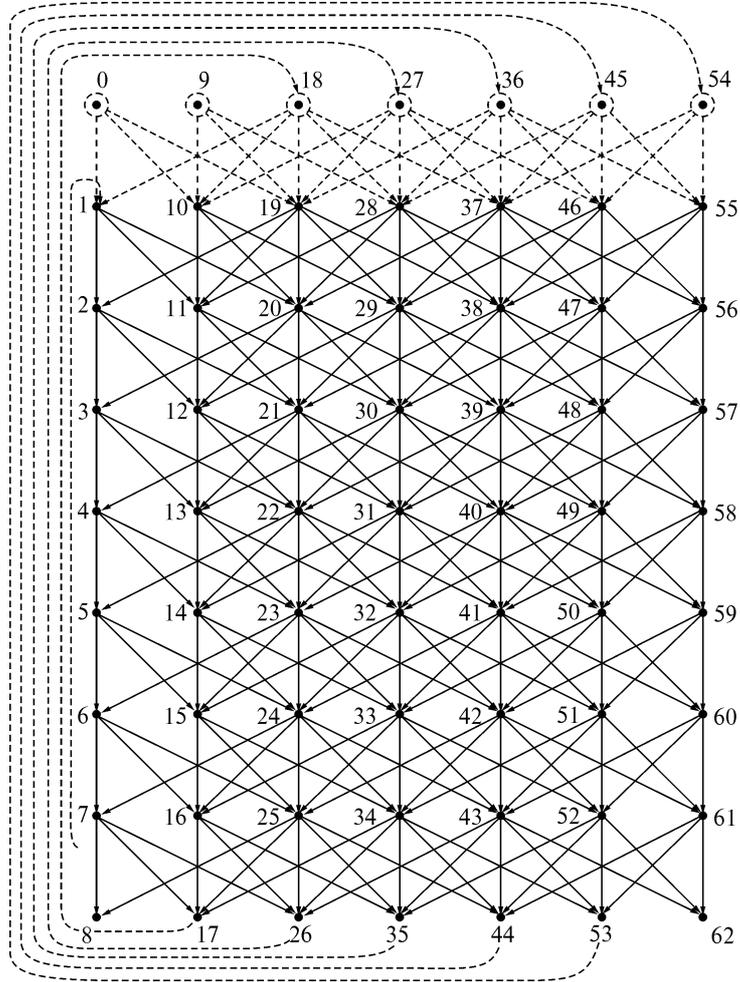


Рис. 4.4

не был ориентированным, то его можно было бы представить и другой функцией — $F_1(x_i, x_j) = |x_j - x_i - 1|$, а $U = \{0, 9, 18\}$.

Рассмотрим еще один пример из той же работы [16, с. 159, рис. 8.1], где функция смежности не является элементарной. На рисунке нанесены пунктиром стрелки, которые соединяют вершины целочисленной решетки по правилам:

- а) вершину $(0, 0)$ с вершинами $(1, i)$, $1 \leq i \leq 8$;
- б) вершину (i, j) с вершинами $(i + 1, k)$, $8 \geq k \geq j \geq 1$;
- в) вершины $(8, j)$ с вершиной $(9, 9)$.

Чтобы реализовать этот граф в виде числового графа, рассмотрим следующий граф из 80 вершин, который представляет собой 10 колонок по 8 вершин в каждой. Нумерация вершин начинается с нуля до 79, идет снизу вверх.

Вершины $\{1, 2, \dots, 7\}$ и $\{72, 73, \dots, 78\}$ будут фиктивными. Вершина 0 соответствует вершине $(0, 0)$ на рис. 4.5 (граф для оценивания оператора настройки S), а вершина 79 — вершине $(9, 9)$. Остальные связи легко переносятся на новый граф. В результате получаем граф на рис. 4.6. Граф представлен следующим образом:

$$n = 79, \quad g(x) = \{1, 2, \dots, 7; 72, 73, \dots, 78\}, \quad U = \{8, 9, 10, 11, 12, 13, 14, 15\}.$$

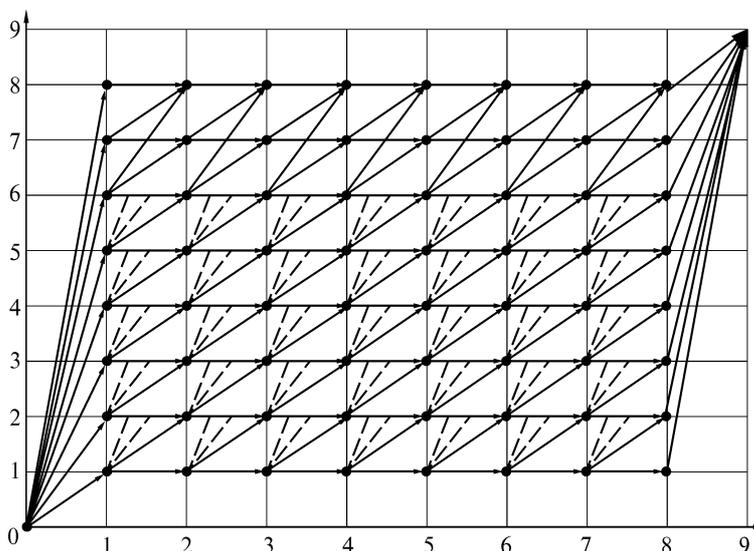


Рис. 4.5

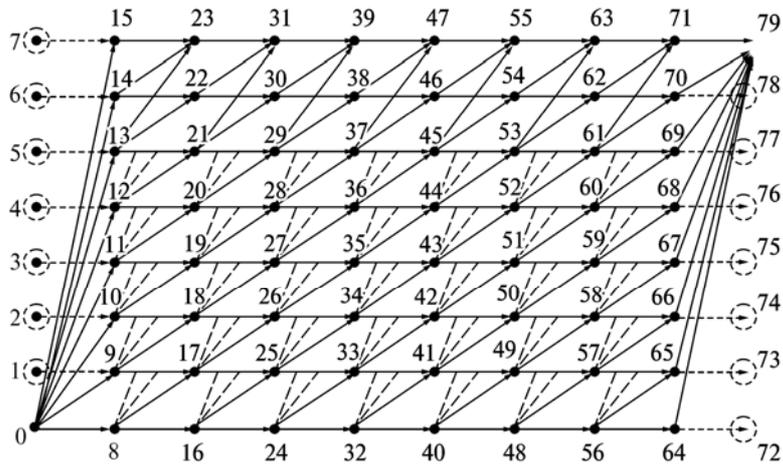


Рис. 4.6

Покажем, что любой подобный граф, у которого $n = st$, можно реализовать в виде числового графа со следующими параметрами:

$$n = st - 1, \quad X = \{0, 1, \dots, st - 1\},$$

$$g(x) = \{1, 2, \dots, s - 1; (s - 1)t, (s - 1)t + 1, \dots, st - 1\},$$

$$U = \{s, s + 1, \dots, 2s - 1\}.$$

Действительно, U представляет собой образующие, которые связывают вершины двух соседних столбцов, минимальная разность кодов которых равна s . Номер каждого столбца, в котором находится вершина x_i , равен ks (номера начинаются с нуля). Поэтому если найдутся две вершины x_i и x_j , разность которых принадлежит U , но они находятся не в соседних столбцах, то множитель k будет больше 1, и тогда $|F(x_j, x_i)| \geq 2s$, т. е. вершины графа x_i и x_j будут несмежными.

Во многих монографиях, посвященных построению и исследованию математических моделей параллельных вычислительных систем, особенно успешным оказалось использование графов, в частности при описании графов систем, реализующих заданный алгоритм. В той или иной мере графы для этих целей применяются давно, однако их использование носило фрагментарный характер и не получило должного развития. Это происходило из-за того, что сравнение систем и алгоритмов на уровне графов неизбежно приводит к необходимости исследовать графы на

изоморфизм, гомоморфизм. Кроме того, многие задачи на графах являются *NP*-полными. Если алгоритм записывается произвольным графом, то отсюда возникают пессимистические выводы о невозможности решить задачу эффективными методами и необходимости привлекать для этого полный перебор вариантов.

В основе этих выводов лежит методологическая ошибка, связанная с предположением о произвольности графа алгоритма. На самом деле графы алгоритмов таковыми не являются, многие из них, как правило, обладают такими свойствами, как симметричность, периодичность или подобие отдельных частей. В этом отношении числовые графы и способы их представления могут быть полезными, идет ли речь об объеме компьютерной памяти или быстродействии алгоритмов.

Рассмотрим в качестве примера элементарный двумерный решетчатый граф, который повсеместно использован в [17, с. 153, рис.15.1] (рис. 4.7).

Очевидно, что такой граф легко реализовать с помощью *M*-графа, используя только две образующие. В частности, можно использовать представление, показанное на рис. 4.2, где подобный граф отличается от решетчатого наличием диагональных дуг. Существуют алгоритмы, графы которых можно задавать решетчатыми графами размерностью 3. К такому алгоритму может привести задача об умножении двух прямоугольных матриц. Указанный алгоритм приведен в работе [17, с. 70, рис. 6.2].

На рис. 4.8 показана реализация трехмерного решетчатого графа в виде *M*-графа. Здесь $n = 71$, $X = \{0, 1, 2, \dots, 71\}$, $g(x) \equiv 0 \pmod{4}$, $F(x_i, x_j) = x_i - x_j$, $U = \{1, 4, 12\}$. Фиктивные вершины, которые составляют верхний слой, легко определяются свойством делимости на 4.

Одним из перспективных направлений повышения производительности и эффективности параллельных вычислительных систем является их специализация на классе решаемых задач. Возрастающие требования к скорости решения современных задач и связанный с этим переход к новейшим технологиям сверхбольших интегральных схем (СБИС) привели к разработке специализированных локально связанных систем. В частности, это относит-

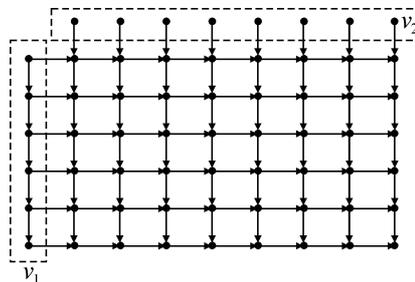


Рис. 4.7

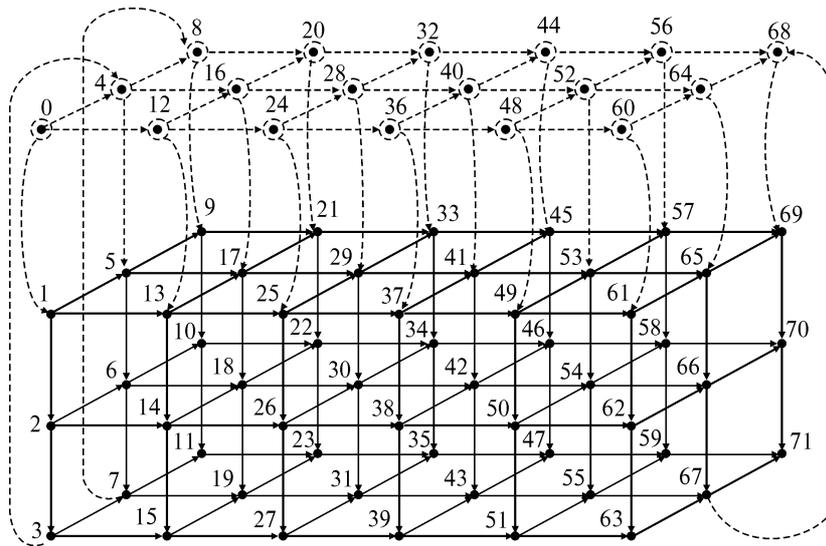


Рис. 4.8

ся к систолическим массивам [73], обладающих высоким уровнем быстродействия, который достигается благодаря тому, что структура систолического массива адекватна структуре реализуемого им параллельного алгоритма и максимально учитывает особенности технологии СБИС [74].

Примеры реализации быстрого алгоритма для умножения матриц и синтеза новых архитектур систолических массивов приведены в [52, 53], где использованы трехмерные решетчатые графы, а также в [16], где используемые графы можно легко представить в виде числовых графов. Однако по мере усложнения структуры графов, это, как указывалось раньше, не всегда возможно. Существует более сложный способ представления числовых графов, отличный от описанного ранее. В этом случае функция исключения имеет в качестве аргумента не вершины, а образующие. Обозначим ее $h(u)$. При этом $h(u_i)$ указывает те вершины, к которым нельзя применять данную образующую. В качестве иллюстрации рассмотрим пример систолического массива на рис. 4.9 [17, с. 236, рис. 23.7]. На этом рисунке дуги, идущие слева направо вниз, не всюду имеют место. То же самое относится и к дуге, идущей справа налево вниз. Если этим дугам поставить в соответствие образующие, то для некоторых вершин эти образу-

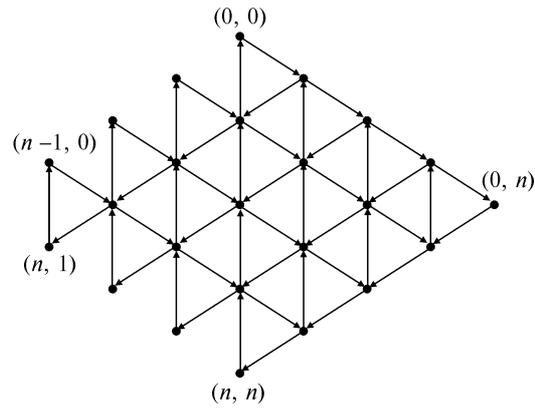


Рис. 4.9

ющие не могут быть применены, хотя вершины и не фиктивные. В этом случае используем функцию g для указанных образующих.

С учетом изложенного получаем числовой граф (рис. 4.10) в

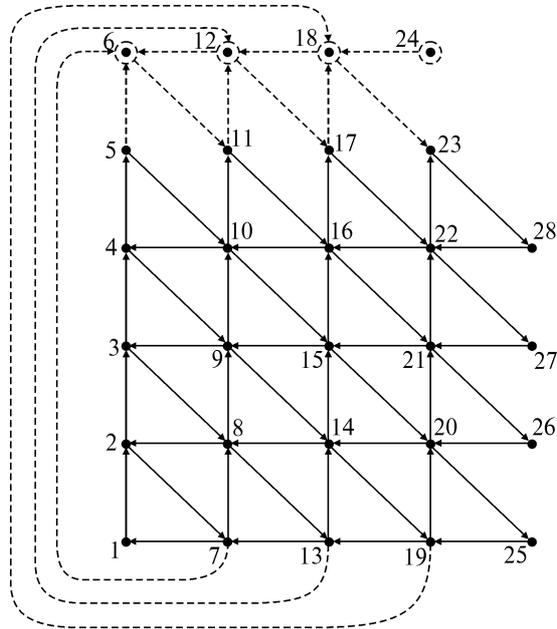


Рис. 4.10

виде некоторого решетчатого графа. Этот граф можно реализовать в виде M -графа с параметрами: $n = 28$, $X = \{1, 2, \dots, 28\}$, $g(x) \equiv 0 \pmod{6}$, $F(x_i, x_j) = |x_i - x_j|$, $U = \{-6, 1, 5\}$, $h(1) = \{x > 25\}$, $h(-6) = \{x \equiv 5 \pmod{6}\}$. Здесь введена функция $h(u)$, которая применяется к двум образующим. Она запрещает проводить горизонтальные дуги на пятой горизонтали. Аналогично запрещаются вертикальные дуги на последней вертикали.

Приведенные примеры показывают, что числовые графы можно успешно использовать в различных областях научных исследований, а также при решении прикладных задач.

4.2. ОЦЕНКА СЛОЖНОСТИ БАЗОВОГО АЛГОРИТМА ПОИСКА В ГЛУБИНУ НА M -ГРАФАХ

Понятие числового графа, введенное в [23], получило широкое применение. Все известные алгоритмы на графах построены с учетом традиционных представлений графов. То же относится и к оценке трудоемкости этих алгоритмов. Поскольку представление графов в виде числовых графов отличается от известных представлений, возникает необходимость построить для них наиболее целесообразные алгоритмы и оценить их относительную сложность.

Опишем вкратце один из таких типичных алгоритмов, каким является поиск в глубину. Цель этого алгоритма — построение остовного леса для данного графа. Для этого рассмотрим следующее прохождение вершин неориентированного графа. Выбираем и посещаем начальную (произвольную) вершину графа x_0 . Затем выбираем произвольное ребро (x_0, x_i) , инцидентное x_0 , и посещаем вершину x_i . Вообще, пусть x — последняя посещенная вершина. Выбираем какое-нибудь не рассмотренное ребро (x, y) , инцидентное x . Если вершина y уже посещалась, то ищем новое ребро, инцидентное x . Если y не посещалось, то идем в вершину y и начинаем поиск с нее. В случае невозможности продвижения вперед возвращаемся к вершине x (к вершине, от которой мы пришли к y) и начинаем поиск с нее. В итоге вернемся к вершине x_0 и обнаружим невозможность продолжать от нее поиск. Ищем теперь новую, ранее не посещаемую вершину x_i и вновь ведем от нее поиск. Поиск закончится, если посетим таким образом все вершины графа.

Этот метод обхода называется *поиском в глубину*, поскольку процесс идет в направлении вперед (вглубь) до тех пор, пока это возможно.

Поиск в глубину в неориентированном графе $G = (X, U)$ разбивает ребра U на два множества T и B . Ребро $u_i = (x, y)$ помещается в T только в том случае, если в процессе поиска мы прошли по этому ребру. Подграф $G' = (X, T)$ представляет собой лес, который называется *глубинным остовным лесом*. Если лес состоит из единственного дерева, то G' будем называть *глубинным остовным деревом*. В этом случае вершина x_0 , с которой начинается обход, является *корнем* этого дерева.

Оценка трудоемкости описанного алгоритма для натуральных арифметических графов (*НА-графов*) приведена в [42]. В данном параграфе приводится такая оценка для натуральных модульных графов (*НМ-графов*). Наиболее часто применяемое представление графов осуществляется в виде списков смежностей.

В качестве примера рассмотрим граф на рис. 4.11, *a*, где номера вершин записаны внутри кружков. Заданный граф будет представлен массивом НАЧАЛО размерностью n и двумя массивами КОНЕЦ и СЛЕДУЮЩИЙ размерностью $2m$ (рис. 4.12).

В i -ячейке массива НАЧАЛО указан номер ячейки массива КОНЕЦ, с которой начинается запись конечных вершин j для всех ребер (i, j) . Конец записи отмечается нулем в ячейке массива СЛЕДУЮЩИЙ.

Теперь можно сформулировать задачу.

ПОИСК В ГЛУБИНУ на неориентированном графе.

Вход: граф $G = (X, U)$, представленный таблицами списка смежностей с помощью массивов НАЧАЛО, КОНЕЦ и СЛЕДУЮЩИЙ.

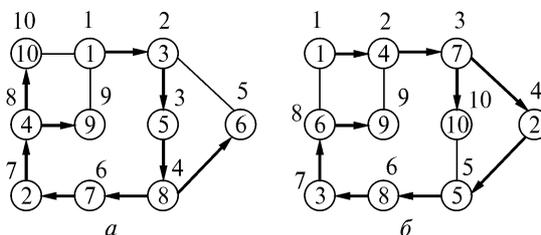


Рис. 4.11

Вершины		Ребра	
НАЧАЛО		КОНЕЦ	СЛЕДУЮЩИЙ
1	1	1	3
2	4	2	9
3	6	3	10
4	9	4	4
5	12	5	7
6	14	6	1
7	16	7	5
8	18	8	6
9	21	9	2
10	23	10	9
		11	10
		12	3
		13	8
		14	3
		15	8
		16	2
		17	8
		18	5
		19	6
		20	7
		21	1
		22	4
		23	1
		24	4

Рис. 4.12

Выход: разбиение множества U на два множества T и B .

При работе алгоритма, реализующего решение этой задачи, будет использована рекурсивная процедура ПОИСК (x). Процедура ПОИСК(x) добавляет ребро (x, y) в T , если вершина y впервые достигнута во время прохождения по ребру из вершины x . Все вершины графа первоначально помечены как «новые».

ПРОЦЕДУРА ПОИСК (x)

- 1) пометить вершину x как «старую»;
- 2) найти очередную вершину y , смежную с x ;
- 3) если вершина y помечена как «старая», перейти к 2;

- 4) добавить ребро (x, y) к T ;
- 5) перейти к ПОИСК (y);
- 6) если не все вершины, смежные с x , рассмотрены, перейти к 2;
- 7) конец.

Общий алгоритм, решающий задачу, выглядит так:

- 1) $T \leftarrow \emptyset$;
- 2) пометить все вершины графа как «новые»;
- 3) найти вершину x , отмеченную как «новая»;
- 4) ПОИСК (x);
- 5) если не все вершины графа «старые», перейти к 3;
- 6) конец.

Это описание алгоритма пригодно для всех структур исходных данных.

Конкретный алгоритм (алгоритм P) расписан детальнее в [47] и состоит из 24 шагов. Этот алгоритм по смысловой нагрузке можно разбить на три части. К первой части можно отнести шаги 1—7, где выполняется предварительная обработка. Вторая, основная, часть охватывает шаги 8—19, где осуществляется обход по вершинам графа. Третья часть алгоритма (шаги 20—24) работает в том случае, если граф не связан. Тогда для каждой компоненты графа поиск (обход вершины графа) начинается заново.

После работы алгоритма массив T содержит ребра остовного дерева исходного графа, отмеченные на рис. 4.11, *a* полужирными линиями. Эти ребра имеют вид $w_i = (T[i], i)$, где $2 \leq i \leq n$, т. е. $w_2 = (6, 2)$, $w_3 = (1, 3)$, $w_4 = (2, 4)$, $w_5 = (3, 5)$, $w_6 = (8, 6)$, $w_7 = (8, 7)$, $w_8 = (5, 8)$, $w_9 = (4, 9)$, $w_{10} = (4, 10)$. Стрелки на этих ребрах и порядковые номера вне кружков указывают порядок обхода вершин графа. К множеству B относятся оставшиеся ребра, а именно: $B = [(9, 1), (10), (3, 6)]$.

Рассмотрим тот же алгоритм, но записанный для другой структуры исходных данных. Пусть задан тот же граф, но нумерация вершин будет такой, как на рис. 4.11, *б* (номер вершины — в кружке). Его можно представить в виде NM -графа с множеством вершин $X = \{1, 2, \dots, 9, 10\}$ и множеством образующих $U = \{3, 5\}$.

Поиск в глубину можно организовать различным способом, все зависит от порядка выбора смежных вершин. Будем полагать, что в данном алгоритме продвижение в глубину идет как можно дальше вдоль ребер, соответствующих первой образующей u_1 .

Алгоритм Q (Поиск в глубину). Натуральный модульный граф $G = (X, U)$ с n вершинами и p образующими задан массивом $U(2p)$, где $U = \{-5, -3, 3, 5\}$. Используются два рабочих массива $S(n)$ и $T(n)$; первый — для отметок вершин графа, второй — для получения ребер множества T . Используются четыре переменных r, r_1, r_2 и r_3 . Как и в алгоритме P , предполагается, что $n \geq 1, p \geq 1$. Алгоритм предназначен для поиска T -остовного леса заданного графа. Первые части алгоритмов P в [47] и Q совпадают буквально, третья часть алгоритма Q (шаги 23—25) соответствует шагам 20—24 алгоритма P , поэтому приводится только основная часть Q алгоритма. В r_1 первоначально находится номер первой вершины, $r_1 = 1, r_2 = p$.

8. Установить $r_3 = n$.
9. [Отмечается вершина как «старая». В качестве отметки будем использовать число 1]. $S[r_1] = 1$.
10. [Начальная установка] $i = 1$.
11. [Пропуск образующей, использованной на предыдущем шаге]. Если $i = T[i]$, то перейти к шагу 14.
12. [Определение смежной вершины] $r = u[i] + r_1$.
13. [Отрицательная вершина ?] Если $r > 0$, то перейти к шагу 19.
14. [Продвижение] $i = i + 1$.
15. [Использованы все образующие ?] Если $i \leq r_2$, то вернуться к шагу 11. В противном случае возвращаемся по ребру множества T в предыдущую вершину.
16. [Вернулись в начальную вершину ?] Если $T[r_1] = 0$, что является признаком того, что вернулись в начальную вершину, от которой никуда нельзя продвинуться, то необходимо поискать «новую» начальную вершину. Для этого надо перейти к шагу 23.
17. [Продолжение поиска предыдущей вершины] $i = T[r_1]$.
18. [Восстановление номера предыдущей вершины]. Если $T[r_1] = 0$, то перейти к шагу 25. Установить $r_1 = r_1 - u[i]$ и вернуться к шагу 14.
19. [Превышает ли номер вершины максимальный номер ?] Если $r > r_3$, то вернуться к шагу 18.
20. [Пропуск «старой» вершины]. Если $S[r] = 1$, то вернуться к шагу 14.

21. [Добавление ребра в T]. $T[r] = i$.
22. [Начало поиска с «новой» вершины]. Установить $r_1 = r$ и вернуться к шагу 9.
23. [Продвижение] $i = i + 1$.
24. [Пропуск «старой» вершины]. Если $S[r] = 1$, то вернуться к шагу 14.
25. Конец.

После работы алгоритма Q массив T содержит информацию о ребрах остовного дерева исходного графа, отмеченных на рис. 4.11, б полужирными линиями. Эти ребра имеют вид $w_i = (i - u[T[i]], i)$, где $2 \leq i \leq n$. Для придания им вида, соответствующего виду массива T в алгоритме P , надо выполнить следующие операции.

01. [Начальная установка]. Установить $i = 2$.
02. [Расшифровка первой вершины ребра]. Установить $T[i] = i - u[T[i]]$.
03. [Продвижение]. Увеличить i на 1.
04. [Конец массива T ?] Если $i \leq r_3$, то вернуться к шагу 02.
05. Конец.

В результате получаем ребра вида $w_i = (T[i], i)$, т.е. $w_2 = (7, 2)$, $w_3 = (8, 3)$, $w_4 = (1, 4)$, $w_5 = (2, 5)$, $w_6 = (3, 6)$, $w_7 = (4, 7)$, $w_8 = (5, 8)$, $w_9 = (6, 9)$, $w_{10} = (7, 10)$. Оставшиеся ребра принадлежат множеству $B = [(1, 6), (4, 9), (5, 10)]$. Порядковые номера возле кружков и направление стрелок указывают порядок обхода вершин графа.

Попытаемся провести сравнительную оценку двух описанных алгоритмов. Двумя важными мерами сложности алгоритмов являются временная и емкостная сложности, рассматриваемые как функции от размера исходных данных. Чтобы точно определить временную и емкостную сложности, надо указать время, необходимое для выполнения каждого шага алгоритма, и объем памяти, используемый для исходных данных и рабочих массивов. Существует несколько весовых критериев для оценки алгоритмов. Воспользуемся логарифмическим весовым критерием, описанным в [6], суть которого заключается в следующем. Пусть $e(i)$ — логарифмическая функция на целых числах, заданная равенствами для всех остальных i .

Логарифмический весовой критерий основан на допущении, что цена выполнения операции (ее вес) пропорциональна длине ее операндов. В работе [47] определено время поиска начального

Таблица 4.1

Номер шага	Алгоритм P	Число выполнений	Алгоритм Q	Число выполнений
08	$e(M_3) + e(r_1) + 1$	n	$e(p)$	1
09	$e(M_4) + e(r_1)$	n	$e(M_3) + e(r_1) + 1$	n
10	$e(M_1) + e(r)$	n	1	$n - 1$
11	$e(M_2) + e(r)$	m	$e(M_4) + e(i) + e(i)$	m
12	$e(M_4) + e(r_1) + 1$	m	$e(M_7) + e(r_1) + e(i)$	m
13	$e(M_6) + e(r_1) + e(r)$	$n - 1$	$e(r) + 1$	m
14	$e(M_3) + e(r_2) + e(r_1)$	$n - 1$	$e(i) + 1$	$n - 1$
15	$e(r_2)$	$n - 1$	$e(i) + e(p)$	m
16	$e(r) + 1$	m	$e(M_4) + e(r_1) + 1$	$n - 1$
17	$e(M_3) + e(r_1) + 1$	$n - 1$	$e(M_4) + e(r_1) + e(i)$	$n - 1$
18	$e(M_3) + e(r_1)$	$n - 1$	$e(M_7) + e(r_1)$	m
19	$e(M_6) + e(r_1)$	$n - 1$	$e(n) + e(r)$	m
20	—	—	$e(M_3) + e(r) + 1$	$n - 1$
21	—	—	$e(M_4) + e(r) + e(i)$	$n - 1$
22	—	—	$e(r)$	$n - 1$

адреса массивов НАЧАЛО, КОНЕЦ, СЛЕДУЮЩИЙ, S , T , SS , U — соответственно $e(M_1)$, $e(M_2)$, $e(M_3)$, $e(M_4)$, $e(M_5)$, $e(M_6)$ и $e(M_7)$, которые являются постоянными величинами.

Чтобы вычислить суммарное время, необходимо оценить значения, которые принимают параметр i и переменные r , r_1 , r_2 .

Оказывается, что их среднее значение равно $\frac{n+1}{2}$. Тогда можно с очень малой погрешностью принять $e(i) = e(r) = e(r_1) = e(r_2) = e(r_3) = e(n) - 1$. Подставляя эти значения в табл. 4.1 и суммируя, получаем оценки для алгоритмов P и Q :

$$t_1 = e(n)(11n + 3m - 8) + n[4e(M_3) + 2e(M_4) + e(M_1) + e(M_2) + 2e(M_6) - 9] + m[e(M_4) + e(M_2) - 1] + 7;$$

$$t_2 = e(n)(9n + 9m - 8) + \\ + n[2e(M_3) + 3e(M_4) - 4] + m[e(M_4) + e(M_7)e(p) - 7] + e(p) + 4.$$

Теперь нетрудно определить временную сложность для общих частей алгоритмов:

$$e(n)(9n - 1) + n[3e(M_3) - 1] + 3.$$

Окончательно получаем оценки временной сложности алгоритмов:

$$t(P) = e(n)(20n + 3m - 9) + n[7e(M_3) + 2e(M_4) + e(M_2) + 2e(M_6) - 10] + \\ + m[e(M_4) + 2e(M_2) - 1] + 10;$$

$$t(Q) = e(n)(18n + 9m - 9) + \\ + n[5e(M_3) + 3e(M_4) - 5] + m[e(M_4) + 2e(M_7)e(p) - 7] + e(p) + 7.$$

Для вычисления емкостной сложности алгоритмов будем считать, что она равна сумме величин $e(x_i)$ по всем используемым элементам памяти, где x_i — наибольшее число, хранящееся в этой памяти. Очевидно, что это число равно n . Таким образом, для алгоритма P требуется память объемом $n + 4m + n + n + n = 4(n + m)$ ячеек. Отсюда получаем оценку $V(P) = 4(n + m)e(n)$. Для алгоритма Q требуется память объемом $2n + p$, т. е. $V(Q) = e(n)(2n + p)$.

Можно сделать вывод, что в вычислительном смысле алгоритм Q немного лучше алгоритма P , но по емкостной оценке он намного превышает алгоритм P , потому что $p \approx \frac{4m}{n}$.

Мы выполнили оценку алгоритма Q для поиска в глубину на MM -графах, однако эта оценка справедлива и для M -графов. Это видно из того, что алгоритм Q работает и для M -графов, если в массиве S вначале пометить номера несуществующих вершин как «старые».

Различие структур данных приводит к разным оценкам трудоемкости и других алгоритмов. В алгоритмах на графах наиболее часто встречаются следующие операции, которые приводят к разным оценкам:

- P_1 — для вершины x найти очередную смежную с ней вершину;
- Q_1 — проверить, являются ли вершины x и y смежными.

Оценим эти операции для первой структуры данных. Поиск начала массивов для алгоритма P_1 имеет вес

$$[e(M_4) + e(x)] + [e(M_5) + e(r_1)].$$

Если необходимо определить очередную вершину, смежную с x , то вес этих операций равен $[e(M_5) + e(r)] + [e(r_2) + e(r)]$.

Для второй структуры поиск первой смежной вершины достигается путем поиска такого числа u_i , что $u_i + x > 0$. Отсюда вес алгоритма P равен

$$1 + \frac{p+1}{2} [e(i) + e(U[i]) + e(r) + e(x) + e(M_1) + 2].$$

Оценим теперь операцию Q_1 для двух случаев. Для первой структуры данных каждый шаг в среднем повторяется $\frac{n+1}{2}$ раз, поэтому общий вес алгоритма Q_1 равен

$$1 + \frac{n+1}{2} [e(M_3) + e(M_4) + e(M_5) + 2e(r) + 2e(r_1) + e(x) + e(y) + 1].$$

Для структуры M -графа вес алгоритма Q_1 с учетом того, что шаги повторяются в среднем $\frac{p+1}{2}$ раз, будет равен

$$1 + e(x + y) + \frac{p+1}{2} [e(M_1) + e(U[i]) + 2e(i) + e(i + 1) + e(p)].$$

Для окончательной оценки веса алгоритмов учтем, что средние значения величин x, y, r, r_1 и $U[i]$ равны $\frac{n+1}{2}$, а переменной i — $\frac{p+1}{2}$. Подставляя эти числа, получаем

$$e(x) = e(y) = e(r_1) = e(r) = e(U[i]) \approx \log_2 n.$$

В формуле определения весов алгоритмов есть множитель $\frac{p+1}{2}$, который получается как среднее число шагов при последовательном поиске. Однако, ввиду упорядоченности множества U , можно организовать поиск со средним числом шагов, равным $\log_2 p$.

При сравнении двух структур данных можно заметить, что веса $t(P_1)$ для двух структур данных одного порядка. Если же p зависит от n , то P_1 несколько лучше для традиционных структур данных. Однако Q_1 значительно лучше для NM -графов. Даже полагая, что $p \approx O(\sqrt{n})$, получаем порядки трудоемкости алгоритма Q_1 соответственно $O(n \log_2 n)$ и $O(\log_2^2 n)$, т.е. для NM -графов выигрыш значительный. Для определения емкостной сложности алгоритмов будем считать, что она равна сумме величин $e(x_i)$ по всем используемым элементам памяти, где x — наибольшее число, хранимое в этой памяти. Очевидно, что это число равно n . Таким образом, для алгоритма поиска в глубину для первой структуры данных требуется память объемом $n + 4m + 3n = 4(n + m)$ ячеек. Откуда имеем оценку $V_1 = 4(n + m) \log_2 n$.

Для второй структуры данных требуется память объемом $2n + p$, т. е.

$$V_2 = (2n + p) \log_2 n.$$

Можно сделать вывод о том, что в вычислительном смысле представление графа в виде NM -графов по всем параметрам имеет несомненное преимущество по сравнению с традиционными способами представления. Этот вывод справедлив и для M -графов.

Здесь показано преимущество представления графов в виде M -графов для алгоритмов, разработанных и применяемых на графах с традиционным представлением в виде списков смежностей. Однако можно построить такие же алгоритмы специально для M -графов, которые имеют еще больше преимуществ по сравнению с рассмотренными.

4.3. ОПТИМАЛЬНЫЙ АЛГОРИТМ ПОИСКА В ГЛУБИНУ НА NM -ГРАФАХ С ДВУМЯ ОБРАЗУЮЩИМИ

Основное преимущество числовых графов по сравнению с обычными состоит в том, что для них проблема размещения данных решается значительно проще, особенно это относится к натуральным графам, множество вершин которых можно задавать одним числом. Как было доказано ранее [85], в силу различных законов изоморфизма для произвольных числовых графов можно

так модифицировать множество их вершин, что оно будет представлено как натуральный ряд, за исключением некоторых чисел. Однако множество образующих в общем случае может иметь произвольный объем. На практике оно значительно меньше множества вершин, и это обуславливает большое преимущество по сравнению с обычным представлением графов в виде списков смежностей, где объем памяти пропорционален сумме чисел вершин и ребер. Преимущество это проявляется при разработке на графах различных алгоритмов. Можно привести сравнение типичных алгоритмов, записанных для графов, представленных в виде списков смежностей и в виде числовых графов. Такими типичными алгоритмами являются алгоритмы, в основе которых лежит систематический просмотр всех вершин графа, при этом каждая вершина просматривается ровно один раз. Такими алгоритмами, которые являются базовыми для конструкции более сложных алгоритмов, являются алгоритмы поиска в глубину и поиска в ширину.

Первое такое сравнение для арифметических графов алгоритма поиска в глубину было проведено в [42], где и подтвердилось преимущество числовых графов. Затем в [47] была проделана аналогичная работа для модульных графов и с тем же результатом. В обеих работах алгоритм был записан в том виде, в каком он был раньше разработан для обычных графов, т. е. преимущество числовых графов было чисто техническим за счет удобной записи исходных данных и меньшего времени работы алгоритма. В работе [47] была приведена гипотеза о том, что многие алгоритмы для числовых графов не нужно строить в привычном понимании, а можно благодаря специфической структуре данных выдать готовое решение поставленной задачи. Тогда сложность алгоритма будет оцениваться только временем вычисления некоторых простых параметров и записи ответа. Здесь этот результат рассмотрен для алгоритма поиска в глубину на натуральных модульных графах.

Общая идея алгоритма для связного графа состоит в том, что, начиная с какой-либо фиксированной вершины, по ребру переходим на новую вершину и от нее продолжаем поиск новых вершин. Если это невозможно, то возвращаемся пройденным путем до тех пор, пока появится возможность перейти на новую вершину. Процесс заканчивается, когда окажемся в исходной вершине и нет возможности продолжить поиск. В результате работы алгоритма выдается список пар вершин исходного графа,

которые в совокупности представляют ориентированное остовное дерево, корнем которого является начальная вершина поиска.

Таким образом, поиск в глубину в неориентированном графе $G=(X,U)$ разбивает ребра на два множества T и B . Ребро r помещается в T в том и только в том случае, если в процессе поиска мы прошли по этому ребру. Подграф $H=(X,T)$ называется *глубинным остовным деревом*, поэтому алгоритм заканчивается построением множества T , состоящего из $n-1$ ориентированных ребер вида $r[i]=(x_i, y_i)$.

Рассмотрим произвольный связный NM -граф. Известно [87], что связность его обеспечивает наименьшее количество образующих $(u_{i_1}, u_{i_2}, \dots, u_{i_k}), (k \leq m)$, наибольший общий делитель которых есть 1. Рассмотрим сначала случай $k=2$. Пусть это образующие u_1 и u_2 , где $u_1 \leq u_2$, и они взаимно просты. Подграф $G'=(X, Y')$, где $U=\{u_1, u_2\}$, является связным графом, степени вершин которого не больше 4. Поэтому в алгоритме поиск новых вершин не всегда имеет альтернативу, что упрощает решение задачи.

В процессе поиска ребра остовного дерева будем помещать вершины в двумерный массив T . Номер первого элемента этого массива будем называть *текущим номером*, а значение второго элемента — *текущим кодом вершины*. Кроме того, используем массив S объемом u_1 .

Вычислим параметры $s = u_1 + u_2$, $p = \left\lfloor \frac{n}{s} \right\rfloor$, $k = \left\lfloor \frac{u_2}{u_1} \right\rfloor$ и положи-

тельный вычет $\Delta = -u_2 \pmod{u_1}$. Назовем *шагом вперед* сложение текущего кода вершины с образующей u_1 и *шагом назад* вычитание из текущего кода вершины образующей u_2 . Рассмотрим алгоритм Q , который состоит из такой последовательности операций.

1. [Начальная установка]. В качестве текущего кода установим $i = 1$, текущий код вершины установим $l = 1$, $j = 1$, $v(1) = 1$.

2. [Прямой шаг]. Вычислить $r = v(i) + u_1$.

3. [Заполнение массива T]. Установить $T[i] = (v(i), r)$, $i = i + 1$, $v(i) = r$.

4. [Сравнить]. Если $r \leq u_2$, то перейти к шагу 2.

5. [Запомнить]. Установить $S[j] = r$, $j = j + 1$.

6. [Обратный шаг]. Вычислить $r = \nu(i) - u_2$. Если $r > 1$, перейти к шагу 3.

7. Конец.

Лемма 4.1. В результате работы алгоритма Q получится цикл Z , в котором перечисляются все вершины интервала $[1, 2, \dots, u_1 + u_2]$.

Доказательство. Цикл получится ввиду того, что код текущей вершины в конце алгоритма становится равным 1. Так как u_1 и u_2 взаимно просты, то это относится и к Δ с u_1 . По условию шага 2 код вершины не должен быть больше $u_1 + u_2$. В начале алгоритма идет перечисление всех кодов, равных $1 \pmod{u}$. Затем идет переход (после шага назад) к множеству кодов $(1 + \Delta) \pmod{u_1}$ и т. д. Так как Δ и u_1 взаимно просты, то линейная форма $(1 + c\Delta) \pmod{u_1}$ при подстановке в нее вместо c положительных вычетов $0, 1, \dots, u_1 - 1$ также пробегает все эти вычеты. В сумме это и дает весь интервал $[1, 2, \dots, u_1 + u_2]$.

Лемма 4.2. Последовательность $[1, 2, \dots, u_1 + u_2]$ в цикле Z занимает места, номера которых составляют арифметическую прогрессию по $\text{mod}(u_1 + u_2)$ с началом $a = 1$ и разницей $d > k$.

Доказательство. Поскольку обход графа начинается с вершины 1, то к вершине 2 мы придем через a прямых и b обратных шагов, тогда a и b являются решением диофантова уравнения:

$$au_1 - bu_2 = 1. \quad (4.1)$$

Так как u_1 и u_2 взаимно просты, то решение этого уравнения существует.

Чтобы найти его, можно использовать представление дроби $\frac{u_2}{u_1}$ в виде конечной непрерывной дроби [78]. В результате решения получаем $d = a + b$. Очевидно, $d > k$, что определяется самим алгоритмом Q , где сначала выполняется не меньше k прямых шагов и один обратный. Сделав d шагов, придем в вершину 2. Понятно, что после αd ($\alpha > 1$) шагов придем в вершину $\alpha + 1$, если продвижение будет осуществляться по циклу Z . Если сделать $1 + u_1$ шагов, то окажемся во второй точке цикла. Это равносильно соотношению

$$du_1 = (u_1 + u_2)x + 1. \quad (4.2)$$

Если подставить в (4.2) $d = a + b$ и $x = b$, то получим уравнение (4.1), что доказывает справедливость леммы 4.2.

В результате работы алгоритма Q мы придем в вершину $1 + u_2$. Если теперь к ее коду прибавить образующую u_1 , то получим вершину $1 + u_1 + u_2$, которая является следующей после наибольшей вершины в цикле Z . Согласно лемме 4.1, применяя алгоритм Q , получаем обход всех вершин в интервале $[1 + u_1 + u_2, \dots, 2u_1 + 2u_2]$. Этот алгоритм можно применить p раз и получить обход всех вершин графа от 1 до $p(u_1 + u_2)$. Определить

p можно из условия $p(u_1 + u_2) < n$, откуда $p = \left\lfloor \frac{n}{u_1 + u_2} \right\rfloor$. Для того чтобы использовать это свойство, заменим шаги 3 и 7 алгоритма Q на последовательность операций, которая организует соответствующий цикл.

Покажем на примере (рис. 4.13) как работает алгоритм. Здесь $n = 51$, $U = \{4, 17\}$. Вычислим $s = u_1 + u_2 = 21$. Отсюда $p = \left\lfloor \frac{51}{21} \right\rfloor = 2$. За первый цикл алгоритм проходит цепь, в которой перечисляются вершины от 1 до 21. Во втором цикле перечисляются вершины от 22 до 42. На рис. 4.13 эти два множества вершин определяют разрезы (а) и (б).

В результате работы алгоритма Q и двух указанных замен получим в массиве T цепь из $p(u_1 + u_2)$ ориентированных ребер с начальной вершиной 1 и конечной $p(u_1 + u_2) - u_1 + 1$. Если номер последней вершины меньше n , то остаются еще непосещенные вершины.

Чтобы их посетить (узнать порядок обхода вершин при поиске в глубину), применим новый алгоритм R , описанный ниже и результат работы которого показан на рис. 4.14.

1. [Начальная установка]. Установить $i = 1, j = ps$.
2. [Найти начало ветви дерева]. Вычислить $v = S[i] + k$.
3. [Прямой шаг]. Установить $i = i + 1$, вычислить $r = v + u_1$.
4. [Сравнить]. Если $r < n$, то перейти к шагу 6.
5. [Текущие установки]. Положить $T[j] = (v, r), v = r, j = j + 1$ и перейти к шагу 3.

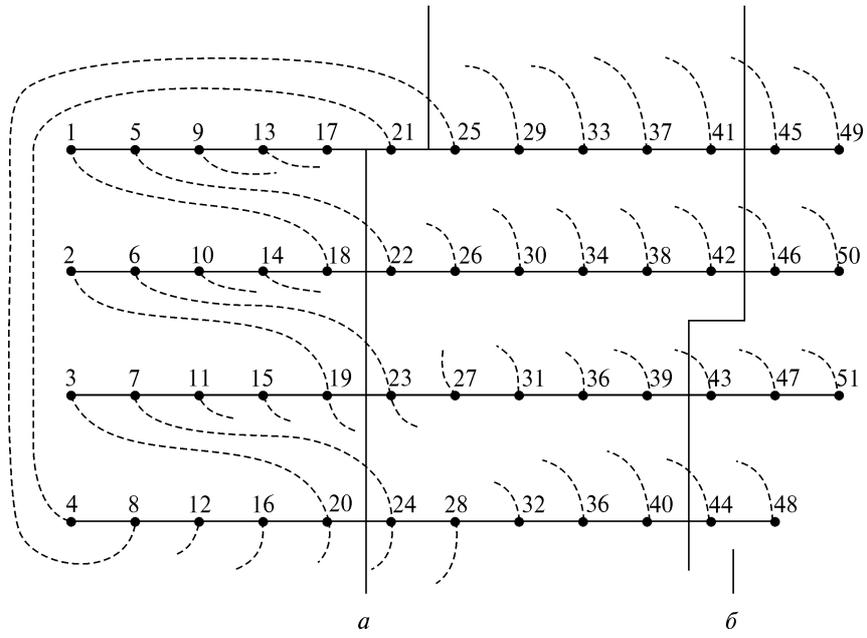


Рис. 4.13

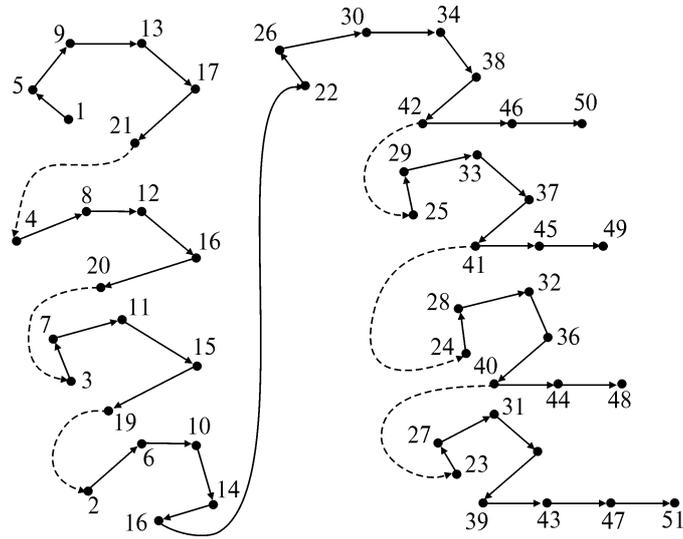


Рис. 4.14

6. [Сравнить]. Если $i < u_1$, то перейти к шагу 2.

7. Конец.

О корректности приведенного алгоритма утверждает следующая теорема.

Теорема 4.1. Для модульного графа, у которого существуют две образующие, обеспечивающие его связность, алгоритм Q с расширениями и алгоритм R выдают решение задачи о поиске в глубину.

Если модульный граф содержит l образующих ($l > 2$), обеспечивающих его связность, то для него решение задачи поиска в глубину достигается немного сложнее, но почти с тем же объемом вычислительных операций.

4.4. ОПТИМАЛЬНЫЙ АЛГОРИТМ ПОИСКА В ГЛУБИНУ ДЛЯ ПРОИЗВОЛЬНЫХ NM -ГРАФОВ

Обычно при построении алгоритма поиска в глубину довольствуются предъявлением двух множеств ребер — множества T , представляющего остовное дерево, и множества B , представляющего остальные ребра графа. Сам алгоритм в основном зависит от способа выбора смежных вершин на каждом шаге.

Алгоритм, описанный в параграфе 4.3, определяется тем, что доминирующим предпочтением при таком выборе является первая образующая NM -графа из двух возможных.

Чтобы воспользоваться полученными результатами, необходимо еще составить порядок обхода вершин NM -графа. Для этого изобразим дерево, соответствующее множеству T (рис. 4.15).

В алгоритме Q из предыдущего параграфа в массиве S сохраняются номера тех вершин, в которых дерево T разветвляется.

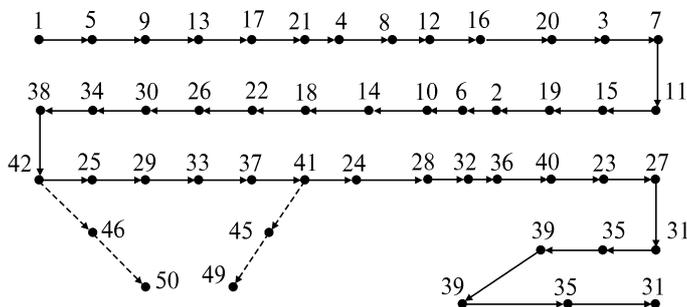


Рис. 4.15

В нашем примере это вершины (в порядке обхода) 42, 41, 40, 39. Обозначим их $S(i)$, $i = 1, 2, 3, \dots, u_1$. Тогда от вершины $S(i)$ идет

ветвь длиной $\lambda_i = \left\lfloor \frac{n - S(i)}{u_1} \right\rfloor$, заканчивающаяся висячей вершиной

$S(i) + \lambda_i u_1$. Чтобы продолжить обход, необходимо вернуться по этой ветви в вершину $S(i)$. Все вершины цепи обозначены первыми в массиве ребер T . Таким образом весь обход представляется последовательностью соответствующих вершин, если после вершины $S(i)$ вставить вершины ветви в прямом и обратном порядке, за исключением последней ветви, где заканчивается обход.

В нашем примере она имеет такой вид: $L = [1, 5, 9, 13, 17, 21, 4, 8, 12, 16, 20, 3, 7, 11, 15, 19, 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, (46, 50, 46, 42), 25, 29, 33, 37, 41, (45, 49, 45, 41) 24, 28, 32, 36, 40, (44, 48, 44, 40), 23, 27, 31, 35, 39, 43, 47, 51]$.

Каждый раз при построении алгоритма поиска в глубину на любом графе возникает дилемма: либо легко представить остовое дерево T , которое, может быть, неудобно обходить, либо очень сложно представить указанное дерево, но которое очень легко обходить. В последнем случае самым удобным деревом является гамильтонова цепь. Но вопрос о том, существует ли в NA -графе гамильтонова цепь, пока остается открытым. Вопрос об уменьшении числа вершин, принадлежащих ветвям в дереве T , полученным с помощью алгоритма Q в предыдущем параграфе, можно частично решить с помощью такого приема. Увеличим на единицу длину каждой цепи, полученной благодаря применению только образующей u_1 . На рис. 4.14 первая цепь заканчивается в 21.

Продлим ее до 25. Следующая цепь в том же столбце будет начинаться не с вершины 4, а с вершины 8 ($25 - 17 = 8$) и заканчиваться вершиной 24. Точно также будут пропущены вершины 3 и 2. Они будут висячими по отношению к основной цепи. На рис. 4.13 это отмечено переносом разреза (a) на один интервал правее. Если проделать ту же операцию с аналогичными цепями во втором столбце на рис. 4.14, то получим висячие вершины 26, 27 и 28, а разрез (b) передвинется на два интервала правее. И останется еще одна висячая вершина — 51. Всего получим 7 вершин, не принадлежащих основной цепи, что на две меньше, чем на рис. 4.15.

Таким образом, если алгоритм Q дает решение в виде основной цепи $p(u_1 + u_2)$ и $n - p(u_1 + u_2)$ вершин на ответвлениях, то с

помощью описанного приема можно получить основную цепь с $p(u_1 + u_2 + 1)$ вершинами и на p вершин меньше на ответвлениях. Последовательность L преобразуется в $L_1 = [1, 5, 9, 13, 17, 21, 25, 8, (4, 8), 12, 16, 20, 24, 7, (3, 7), 11, 15, 19, 23, 6, (2, 6), 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 33, (29, 33), 37, 41, 45, 49, 32, (28, 32), 36, 40, 44, 48, 31, (27, 31), 35, 39, 43, 47, 51]$.

Самый простой способ построения остоного дерева T определяет следующая теорема.

Теорема 4.2. Следующий набор ребер NM -графа с двумя образующими определяет остоное дерево: $[i + (\lambda - 1)u_1, i + \lambda u_1]$, где i — вершины, а также ребра $(i, i + u_2)$ для $i = 1, 2, \dots, u_1 - 1$.

Действительно, для каждого фиксированного i эта последовательность определяет цепь с началом в вершине i и которая заканчивается максимально большим номером. Последние $u_1 - 1$ ребер связывают эти цепи в общее остоное дерево. Очевидно, что образующие u_2 в этих ребрах не образуют цикл, иначе существовало бы ненулевое решение уравнения

$$au_2 \equiv 0 \pmod{u_1}, 0 < a \leq u_1 - 1. \quad (4.3)$$

Но это возможно тогда и только тогда, когда u_1 и u_2 имеют общий множитель, что противоречит начальным условиям.

Для этого дерева легко организовать обход по всем вершинам, хотя в нем проходы вперед и возвраты занимают больше вершин, чем в предыдущих решениях. Для этого обозначим $\alpha_i = (\alpha_{i-1} + u_2) \pmod{u_1} > 0$, $\alpha_0 = 1$, ($i = 1, 2, \dots, u_1 - 1$), а $\beta_i = \max_k \{\alpha_i + ku_1\} \leq n$. Тогда последовательность обхода вершин

NA -графа будет схематически выглядеть так:

$$L_3 = \beta_0 \rightarrow 1 \rightarrow \bigcup_{i=1}^{u_1-1} [\alpha_{i-1} + u_2 \rightarrow \beta_i \rightarrow \alpha_i]. \quad (4.4)$$

Здесь стрелками обозначен путь вдоль цепи с помощью образующей u_1 . Для примера (см. рис. 4.13) вычислим параметры:

$$\beta_0 = 49, \alpha_1 \equiv (1 + 17) \pmod{4} = 2,$$

$$\beta_1 = 50, \alpha_2 = 2 + 17 \equiv 3 \pmod{4}, \beta_2 = 51, \alpha_3 = 3 + 17 \equiv 4 \pmod{4}.$$

В результате обход всех вершин будет осуществляться по маршруту: $L_4 = [49, 45, 41, 37, 33, 29, 25, 21, 17, 13, 9, 5, 1, 18, (22, 26, 30, 34, 38, 42, 46, 50, 42, 38, 34, 30, 26, 22, 18), 14, 10, 6, 2, 19,$

(23, 27, 31, 35, 39, 43, 47, 51, 47, 43, 35, 31, 27, 23, 19), 15, 11, 7, 3, 20, (24, 28, 32, 36, 40, 44, 48, 44, 36, 28, 24, 20), 16, 12, 8, 4].

Теперь, когда получены два способа построения остовных деревьев и, соответственно, два способа обхода всех вершин NM -графа, можно перейти к построению остовных деревьев и их обходов для NM -графов с произвольным числом образующих, большим двух.

Пусть задан связный натуральный модульный граф, у которого $U = \{u_1, u_2, \dots, u_m\}$, из которых l — максимальное число образующих, обеспечивающих связность. Рассмотрим подграф G' на подмножестве этих образующих, которые перенумеруем $U' = \{u'_1, u'_2, \dots, u'_l\}$. По теореме 3.3 граф G' также будет связным и для него справедливы условия

$$\begin{aligned} \text{а) } \text{НОД}(u_1, u_2, \dots, u_l) &= 1; \\ \text{б) } \text{НОД}(u_{i_1}, u_{i_2}, \dots, u_{i_k}) &= d > 1; \quad k < l. \end{aligned} \quad (4.5)$$

Возьмем наименьшие образующие u_1 и u_2 . Обозначим $\text{НОД}(u_1, u_2) = d(1, 2) > 1$. Это означает, что подграф на множестве образующих $\{u_1, u_2\}$ будет состоять из $d(1, 2)$ компонент. Построим на каждой из этих компонент остовное дерево по алгоритму Q , т. е. по типу, как на рис. 4.15. Каждое i -е дерево ($i = 1, 2, \dots, d(1, 2)$) содержит все вершины $i[\text{mod } d(1, 2)]$, и каждое такое дерево содержит $\frac{u_1}{d(1, 2)}$ поддеревьев, образованных одной образующей u_1 . Добавление третьей образующей u_3 приведет к уменьшению компонент связности до числа, равного наибольшему общему делителю $\text{НОД}(u_1, u_2, u_3) = d(1, 2, 3)$. И в каждой такой компоненте будет $\frac{d(1, 2)}{d(1, 2, 3)}$ поддеревьев, образованных с помощью образующих u_1 и u_2 . Продолжая ввод новых образующих, все время уменьшаем число компонент связности получаемого графа. На j -м шаге при вводе образующей u_j получаем $d(1, 2, \dots, j)$ компонент связности, а в каждой из них по $\frac{d(1, 2, \dots, j-1)}{d(1, 2, \dots, j)}$ поддеревьев, образованных с помощью образующих u_1, u_2, \dots, u_{j-1} . И наконец, при вводе образующей u_j получаем связный граф.

Эти рассуждения помогут нам последовательно построить остовное дерево. Для этого докажем следующую теорему.

Теорема 4.3. Следующий набор из l типов ребер MM -графа, у которого l образующих, обеспечивающих связность, определяет остовное дерево:

$$1) [i + (\lambda - 1)u_1, i + \lambda u_1], i = 1, 2, \dots, u_1; \quad \lambda = 1, 2, \dots, \left\lfloor \frac{n-i}{u_1} \right\rfloor;$$

$$2) (i, i + u_2), \quad i = 1, 2, \dots, u_1 - d(1, 2);$$

$$3) (i, i + u_3) \quad i = 1, 2, \dots, d(1, 2) - d(1, 2, 3);$$

.....
 $l) (i, i + u_l), \quad i = 1, 2, \dots, d(1, 2, \dots, l) - 1.$

Доказательство теоремы 4.3 вытекает из способа построения остовного дерева, описанного выше.

ПОСТРОЕНИЕ ДИСКРЕТНЫХ ОБРАЗОВ

ВВЕДЕНИЕ

В течение последних лет возрастает интерес к проблемам распознавания образов. Термином «распознавание образов» обозначается обширное поле деятельности, связанной как с реальными жизненными потребностями (распознаванием людьми и животными «образов» в окружающей их среде), так и с решением научных и технических задач (распознаванием людьми или автоматическими системами треков в пузырьковых камерах, считыванием символов, классификацией хромосом и т. д.). Особого внимания заслуживает тот факт, что распознавание образов, зарождение которого было обусловлено необходимостью решения задач зрительного анализа, ныне в основном не имеет прямого отношения к этим задачам. Широко известные методы распознавания, такие как метод обобщенного портрета [15], потенциальных функций [2], алгоритмы Бонгарда [9, 10] и Розенблатта [52], были ориентированы именно на задачи зрительного анализа. Эти методы успешно применяются для решения многих задач: медицинской диагностики, прогнозирования долговечности приборов, распознавания нефтеносных и водоносных пластов [23]. Однако распознавание изображений находится вне этой сферы. Достижения в применении систем распознавания изображений обусловлены в значительно меньшей степени рекомендациями общей теории, чем учетом специфических особенностей каждой отдельной прикладной задачи. Это свидетельствует об определенном разрыве между теорией распознавания образов, сформировавшейся к настоящему времени, и существующей практикой распознавания изображений.

Все разнообразие известных методов и направлений в современном распознавании образов заключается в той или иной

формализации указанного неформального требования. Наиболее глубокие и вместе с тем обширные исследования выполнены в школах, руководимых Ю.И. Журавлевым [28—31], В.Н. Вапником [15, 16], Ш.Ю. Раудисом [50, 51], Н.Г. Загоруйко [32—34], В.А. Ковалевским [7, 36—38, 45, 60, 61], В.А. Якубовичем [62], и приведены в ранних работах М.А. Айзермана, Э.М. Бравермана, Л.И. Розоноэра [1], А.Г. Ивахненко [35], Розенблатта [52], К.С. Фу [56, 57] и др. Совокупность результатов исследований, изложенных в указанных работах, сформировала современную теорию обучения распознавания образов, плодотворность которой прошла длительную и многостороннюю проверку на большом количестве прикладных задач медицины, геологии, социологии и других не математических наук.

Распознавание образов всегда предполагает наличие некоторой системы обработки данных (информации), имеющей вход и выход. На вход системы данные могут поступать от множества различных источников: физического объекта, находящегося в некоторой среде, некоторого процесса или как результат эксперимента, или как метеорологические, экономические, или просто некоторые отвлеченные данные. Данные, поступающие на вход системы распознавания, как правило, весьма сложны и включают сигналы, которые часто являются пространственными или временными функциями. Выходная информация сравнительно проста: она сводится к указанию одного из нескольких классов. Например, если входной информацией служат результаты измерения коэффициента отражения некоторой поверхности, полученные сканированием, то выходная информация указывает названия символов, нанесенных на эту поверхность.

Результатом распознавания человеком лиц, голосов и т. д. часто является идентификация некоторого определенного объекта. Под идентификацией в данном случае понимается присвоение рассматриваемому объекту надлежащего и однозначного названия. Человеку в процессе идентификации совсем не обязательно явным образом определять характерные признаки объекта. Имеет значение, в сущности, только окончательный результат процесса наблюдения, восприятия и распознавания. Автоматические системы, заменяющие распознавание посредством органов чувств человека, должны осуществлять такую же идентификацию, как и человек, сталкивающийся с определенным объектом. Однако распознающие системы должны явным образом использовать характерные признаки объекта.

Классификация включает все процессы, заканчивающиеся указанием некоторого класса (или принадлежности классу) для рассматриваемых объектов или данных. Результат распознавания тоже можно представить как подобное указание класса — в таком смысле распознавание образов является одной из разновидностей классификации. Классификация включает также простые процессы, в основе которых лежит, например, использование некоторого измеренного и некоторого порогового значений (для определения того, находится ли значение температуры в безопасных пределах). И снова традиция (а также область приложения) определяет, является ли данная классификация достаточно сложной для того, чтобы считать ее распознаванием. В тех случаях, когда каждый класс содержит только один объект, классификация эквивалентна идентификации.

Классы, возникающие в результате реализации процесса распознавания, могут быть *дискретными* (объект либо является, либо не является элементом некоторого класса) или *нечеткими* (объектам ставятся в соответствие функции принадлежности классу). В случае нечетких классов некоторый объект может характеризоваться принадлежностью к одному или нескольким классам, значение которой может задаваться в пределах 0—1. Иногда результатом процесса распознавания является присвоение аналоговой (непрерывной) переменной некоторого значения с помощью интерполяции между дискретными классами.

В большинстве задач распознавания, решавшихся до сих пор, классы были дискретными.

Существует целый ряд методов принятия решений, пригодных для отнесения объекта к одному из нескольких классов по заданным признакам и с учетом изменчивости образов. Эти методы существенно зависят от типов признаков и соотношения собственной и межклассовой изменчивости соответствующих образов. В дополнение к специализированным и эвристическим можно выделить два обширных семейства методов принятия решений.

1. *Методы статистической теории решений* применимы при работе с объектами, признаками которых служат числовые значения, причем эти значения у объектов, принадлежащих одному классу, неодинаковы. Априорные сведения являются существенными для выбора признаков; сведения об отклонениях значений признаков у объектов одного и того же класса должны собираться с использованием статистического анализа. Эти разновиднос-

ти сведений способствуют формированию решающих функций, обеспечивающих классификацию.

2. *Лингвистические методы* (называемые также *структурными* или *синтаксическими*) применимы при работе с объектами, признаками которых служат непроеизводные элементы (или конгломераты непроеизводных элементов) и их отношения. Некоторая грамматика определяет правила построения образа из непроеизводных элементов. Используется множество типов грамматик (в том числе стохастические), обладающих различной широтой грамматического описания и сложностью. Такие грамматики часто удается определять на основе априорных сведений об образах; в противном случае для их получения приходится прибегать к грамматическому выводу по значительной выборке образов. Выполнение классификации при заданных непроеизводных элементах и их отношениях требует грамматического разбора.

Целесообразно применение комбинаций этих двух методов.

При выполнении некоторых условий изменчивость образа и различия между образами можно определить строго. Если рассматриваемые образы можно охарактеризовать некоторым набором k признаков, каждый из которых принимает непрерывные или дискретные значения, то можно задать k -мерное векторное пространство, каждая координата которого представляет один признак (признаковое пространство). В этом случае образ задается некоторой точкой k -мерного пространства. Если ввести понятие расстояния (евклидова, прямоугольного, кварталы и т. д.), то образы, находящиеся на небольшом расстоянии друг от друга, можно считать сходными, а образы, разделенные значительным расстоянием, — различными. Образ, обладающий малой изменчивостью, т. е. малыми вариациями значений признаков различных представлений данного образа, определяется небольшим характеристическим объемом в k -мерном пространстве (центром этого объема могут служить, например, средние значения признаков). Иногда предполагается, что все представления некоторого образа должны располагаться в пределах подобного малого объема (*гипотеза «компактности»*) при условии правильного выбора признаков. Шумы, связанные с измерением и передачей данных, приводят к увеличению характеристического объема.

Если различные образы далеко отстоят друг от друга и занимают непересекающиеся характеристические объемы, то очень простое решение задачи распознавания состоит в классификации предъявленного образа в соответствии с положением облас-

ти k -мерного пространства, в которой находится представляющая этот образ точка. Практически, однако, эти объемы часто не являются малыми, а области, соответствующие различным образам, пересекаются. Значения признаков иногда можно рассматривать как случайные переменные (с учетом случайной природы шумов, возникающих в системах измерения и каналах связи). В этом случае соответствующие области можно считать плотностью распределения образов. Следует найти оптимальные разделяющие поверхности, обеспечивающие классификацию образов с неизвестной классовой принадлежностью. Кроме интерпретации как плотности распределений признаки можно задавать с помощью нечетких понятий; в этом случае также можно ввести меры сходства.

Если рассматриваемые образы представить некоторой последовательностью двоичных символов (например, нулей и единиц), то в качестве расстояния между образами можно использовать *расстояние Хэмминга* (число несовпадений соответствующих символов обеих последовательностей). Как и прежде, чем меньше расстояние Хэмминга, разделяющее образы, тем большим сходством они обладают.

Выше были рассмотрены задачи распознавания, в которых максимум сходства по параметрам можно было найти простейшими средствами. Эта простота достигалась за счет того, что характер зависимости сходства от оптических мешающих параметров позволяет найти максимум аналитическим приемом. Число других, не оптических параметров было невелико, так что можно было осуществить полный перебор их значений.

Существует много других практически важных случаев, когда изображения или вообще сигналы зависят от большого числа не оптических параметров. Например, изображение написанной от руки «печатной» буквы может быть охарактеризовано такими параметрами, как высота и ширина буквы, координаты концов прямолинейных отрезков и дуг, из которых состоит это изображение, углы наклона отрезков, кривизны дуг, толщина линий и т. п. Можно предложить различные способы разложения сложного изображения на составные части, но при этом всегда сложное изображение будет характеризоваться большим числом параметров, причем при изменении значений одних параметров изменяются ограничения, накладываемые на допустимые значения других параметров. В таких случаях для нахождения максимума сходства по всем параметрам необходимо применять специаль-

ные математические методы, например, динамическое программирование.

В случае сложных изображений возникают практически важные задачи их анализа, которые нецелесообразно рассматривать как классификацию. В.А. Ковалевский [39—44] и Р. Нарасимхан [47, 48] предложили рассматривать задачу *описания изображений*, суть которой состоит в автоматическом получении нужных геометрических характеристик сложного изображения. В качестве примера приведем очень важную для физических исследований задачу автоматической обработки фотографий следов частиц, получаемых с помощью пузырьковых камер. На фотографии необходимо выделить на фоне помех следы (треки) частиц и определить такие их параметры, как направление, кривизна, длина, угол разветвления и т. д. Аналогичным путем предлагается анализировать изображения букв, чтобы, получив описание изображения в определенных геометрических терминах, распознать его затем на основе этого описания.

В основе анализа сложных изображений лежат формальные правила, по которым сложные различные изображения могут быть составлены из определенных элементарных частей. Эти правила являются разновидностью формальных грамматик и налагают определенные ограничения как на получаемые с их помощью изображения, так и на те описания изображений, которые должны быть получены в результате решения задачи. Таким образом, формальный язык для описания изображений связан со структурой изображений рассматриваемого класса.

Для того чтобы представить двумерное изображение в виде последовательности, необходимо рассмотреть процесс составления сложного изображения из элементарных изображений или элементов. Элементы, которые нужно дорисовывать в определенном порядке один за другим для получения некоторого сложного изображения, образуют соответствующую этому изображению последовательность. Можно представить, что заранее заготовлен некоторый набор тонких прозрачных пластинок стандартного размера, и на каждой из них нарисовано некоторое элементарное изображение. Каждому терминальному символу b данного алфавита соответствует определенное элементарное изображение, причем b является параметром, характеризующим это изображение. Правила грамматики указывают, какую пластинку разрешается взять и наложить на стопку взятых раньше пластинок. В результате наложения всех выбранных пластинок получится

сложное изображение E , построенное в соответствии с данным набором правил.

Развитые в последние годы методы обучения машин распознаванию образов, как правило, основаны на предположении, что различным образам непосредственно в пространстве рецепторов [4] соответствуют достаточно удаленные друг от друга множества [3, 4, 62]. Поэтому, несмотря на значительное разнообразие таких методов, все они применимы лишь в том случае, когда образы, которые машина должна научиться распознавать, сравнительно просты. Кроме того, в этих методах предполагается, что предъявляемые изображения нормированы и центрированы, т. е. имеют приблизительно одинаковый размер и расположены приблизительно в одной и той же части поля рецепторов.

Одним из возможных путей решения более сложных задач обучения машин распознаванию образов является выработка в процессе обучения небольшого числа признаков объектов, с помощью которых можно составлять экономные описания этих объектов.

В работе И.Б. Мучника [8] разработаны и экспериментально исследованы алгоритмы автоматического формирования простейших признаков («уголок», «палочка»). Предполагается, что в дальнейшем из этих простейших признаков будут конструироваться более сложные признаки — «выражения», например такие, которые указывают взаимное расположение простейших признаков («уголок справа от вертикальной палочки», «горизонтальная палочка в центре овала» и т. д.). Специально организованные «фразы» — утверждения, составленные из признаков — «выражений», рассматриваются как возможные описания образов, и, таким образом, процесс распознавания сводится к определению того, какое описание больше подходит для анализируемого изображения.

В этой работе предполагается, что для достаточно широкого класса зрительных образов в качестве простейших можно принять признаки, которые характеризуют только отдельные участки изображений.

Возможность использования для целей автоматического распознавания отдельных участков изображений подробно описана в литературе.

В работах [3, 62] изложен ряд методов активного осмотра изображения, позволяющих фиксировать участки сильного изменения кривизны линии. На основе этих методов были сконст-

руированы макеты машин для распознавания рукописных цифр, проведено экспериментальное опробование работы этих устройств. К этому же периоду относятся работы, в которых рассматриваются алгоритмы обнаружения и анализа таких участков изображения, как скачки градиента зачерненности изображения, пересечение нескольких контуров и т. п. Дальнейшее развитие эти исследования получили в [26, 27].

В работах [12—14] приведены примеры систем, приспособляющихся в результате обучения двигаться вдоль контура изображения и вырабатывающих некоторые признаки, характеризующие как особенности движения развертки, так и свойства небольшой окрестности изображения вдоль траектории ее движения. Этим исследованиям посвящена работа [47].

Вопросам обработки специальных участков изображений уделено большое внимание в работах по телевизионной технике, а также по психологии и физиологии процессов зрительного восприятия.

Человек, описывая изображения, часто использует такие слова, как «уголок», «закругление», «перекрест». Они употребляются для характеристики не целого изображения, а отдельных его элементов. Такие фрагменты, как правило, относятся к участкам сильного изменения формы или контрастности. Будем предполагать, что именно такие участки являются важными для описания изображений и что именно они должны быть, прежде всего, использованы для формирования простейших признаков. Такие участки называются *информативными фрагментами*.

В связи с этим возникает задача разработки методов нахождения информативных фрагментов.

Распознавание на основе данных, воспринимаемых органами чувств, часто приводит к результатам, которые человек в состоянии получать посредством прямого наблюдения. Люди еще далеки от возможности добывать с помощью систем распознавания образов все знания, доступные органам чувств человека. Существуют, однако, и исключения; при контроле быстро перемещающихся поверхностей может возникнуть необходимость замены людей-контролеров на распознающие системы.

Значительно более фундаментальный характер имеет проблема распознавания на основе данных произвольного характера. Применение методов распознавания для установления происхождения кремневых орудий первобытного человека позволяет получить сведения, которые невозможно или очень трудно получить другими способами.

Кластерный анализ и другие методы поиска регулярностей в данных, применяемые при распознавании образов, могут также обеспечить получение новых знаний. Анализ точности статистической системы распознавания, в процессе которого определяется *ошибка классификации*, свойственная этой системе (вероятность ошибки при классификации новых объектов), позволяет обнаружить существование определенных границ для этой ошибки и, следовательно, для приобретаемого в процессе распознавания знания. Ошибка классификации зависит от размера обучающего множества, числа признаков и применяемого статистического метода. Можно показать [29], что при некотором фиксированном объеме обучающего множества увеличение числа признаков приводит к возрастанию ошибки классификации; интересным следствием является необходимость иногда ограничивать число переменных (признаков), значения которых измеряются и используются при статистическом анализе.

Распознавание образов можно использовать для автоматизации некоторых рутинных наблюдений, например при анализе простых треков в пузырьковой камере или в материаловедении для подсчета и определения размеров частиц и различных включений, число которых очень велико. Методы распознавания можно применять для изучения сложных данных в астрономии, метеорологии, спектральном анализе и т. д. Как указывалось ранее, некоторые результаты распознавания могут быть использованы для планирования эксперимента при наличии ограничений на возможности сбора данных. Изложены также предположения о возможности применения методов распознавания образов при использовании квантовомеханического подхода к изучению молекул [58]. Ранее приведены примеры применения распознавания образов в физике.

Для решения многих задач распознавания требуются знания в области физики классифицируемых объектов, фона (в случае изображений), датчиков и ошибок измерений. Успеху процесса распознавания могут существенно способствовать эксперименты, проводимые с целью нахождения признаков, адекватность которых определяется их связями с физическими характеристиками рассматриваемых образов.

Можно указать на связь теории распознавания образов и с другими науками и выделить два аспекта таких связей: в распознавании образов используются знания и технические приемы других дисциплин, а другие дисциплины используют распознавание образов для решения некоторых своих задач.

Из изложенного выше следует, что, в частности, статистика и физика вносят свой вклад в решение задач распознавания образов; то же самое относится и к теории автоматов, теории множеств, теории управления, теории информации, кибернетике, искусственному интеллекту, информатике, обработке изображений, лингвистике, формальным языкам, теории нервных сетей, биологии, теории восприятия и психологии. При разработке реальных систем распознавания образов необходимо использовать многочисленные технические достижения оптики, механики и электроники.

Специалисты в области распознавания стремятся объединить знания и средства, заимствованные из всех этих областей науки и техники, а также собственные результаты исследований для того, чтобы получить необходимые решения задач распознавания. Можно утверждать, что распознавание образов представляет собой междисциплинарное направление, объединяющее информатику, математику, физику и технику; эти направления, сливаясь, образуют междисциплинарное ядро распознавания, обеспечивающее систематическую основу для решения всех типов задач распознавания.

Распознавание можно использовать во многих дисциплинах как для замены органов чувств человека (или в качестве вспомогательного средства), так и для анализа сложных структур данных. Решение стандартных задач диагностики и контроля в технике и медицине может постепенно быть передано устройствам распознавания образов; кроме того, решение некоторых задач такого рода может стать возможным лишь в результате использования соответствующих устройств распознавания. Иногда после перестройки системы можно отказаться от использования устройств распознавания. Так, при сборке можно организовать хранение элементов собираемой конструкции таким строго фиксированным и упорядоченным образом, что применение методов распознавания для сортировки и ориентации деталей станет излишним.

Ранее упоминалось об *обработке и описании изображений*. Существуют сильные зависимости между распознаванием образов, обработкой изображений и родственной им *машинной графикой*. Многие задачи распознавания связаны с образами, присутствующими в изображениях, и поэтому блоки предварительной обработки должны осуществлять обработку изображений и выделение признаков (например, производных элементов). Эксперимен-

тальные, экономические и другие данные иногда преобразуются в зрительную форму — кривые, наборы изолированных точек — и могут служить отправной точкой для распознавания образов. Кроме того, промежуточные данные, возникающие в процессе распознавания, можно представлять в виде некоторого изображения с тем, чтобы облегчить работу оператора в интерактивном режиме и использовать в процессе распознавания опыт человека и свойственные ему способы принятия решений.

Если обработка изображений является целью, то решение задачи распознавания возлагается на человека. Поскольку датчики вносят искажения в сканируемое изображение, в процессе обработки изображения можно улучшить его качество («восстановление») при помощи обратной фильтрации и снижения уровня шумов. Вследствие улучшения качества изображения повышается его контрастность, выделяются края и контуры и т. д., тем самым человек сможет лучше увидеть необходимый объект. Восстановление и улучшение качества изображений эффективны в качестве предварительной обработки для распознавания.

При этом допускаются некоторые локальные преобразования в обработке изображений. Представим, что изображение можно описать через единственную функцию $f(x,y)$. Хотя такой функцией можно представлять различные величины (например, яркость, интенсивность, плотность, светимость), преобразования, которым она подвергается, часто оказываются подобными. Эту функцию называют *зачерненностью*. Пространственное квантование и квантование по зачерненности — необходимые условия для обработки изображения с помощью компьютеров. В результате квантования строится целочисленная матрица, элементами которой являются значения зачерненности. Точки выборки могут образовывать прямоугольную решетку (обычно используемую) или шестиугольную.

Кроме решетки, образованной точками выборки, можно построить решетку из линий, которые представляют собой границы, разделяющие выборочные точки и проведенные посередине между ними. Эта сетка дополняет каждую выборочную точку элементом изображения, называемым *пикселем* (*pixel*). Таким образом, вся площадь изображения оказывается разделенной на элементы, центром каждого из которых служит одна из выборочных точек.

Изменение масштаба значений зачерненности можно использовать для повышения контрастности изображения. Помимо растяжения и сжатия уровней зачерненности ее значения могут

быть подвергнуты новому квантованию с тем, чтобы обеспечить равномерность гистограммы зачерненности. Если после нового квантования необходимо обеспечить равную вероятность K значений зачерненности, то кумулятивную гистограмму (прежней) зачерненности следует разделить ровно на K равных частей. Поскольку кумулятивная гистограмма состоит из ступенек, то новый вариант квантования не обеспечивает точного равенства ступенек квантования в преобразованной кумулятивной гистограмме. Известно несколько методов, с помощью которых можно уменьшить эффект повторного квантования [55]. Рассмотрим некоторые из них.

Сегментация. Часто изображение состоит из частей, называемых компонентами и подлежащих анализу, и фона. Под сегментацией понимается отнесение каждого элемента изображения либо к компонентам, либо к фону. Можно выделить три метода сегментации.

1. *Разделение по порогу.* Сегментация осуществляется исключительно на основе значения зачерненности каждого элемента изображения. Если это значение больше некоторого (локального) порогового, то соответствующий элемент изображения классифицируется как компонента, если значение зачерненности оказывается меньше порогового, то элемент относится к фону (либо наоборот). Известно несколько методов определения порогового значения по гистограмме зачерненности изображения.

2. *Обнаружение края.* Если граница между компонентой и фоном характеризуется изменением значения зачерненности, то эти изменения можно использовать для выделения компонент. Обнаружение краев осуществляется прямым вычислением производной функции зачерненности, высокочастотной фильтрацией, оцениванием границы статистическими методами или с помощью специальных процедур. Ложные края или утраченные части краев можно обнаружить, используя априорную информацию.

3. *Разделение изображения на области.* Изображение разбивается на простейшие области, образованные соединенными между собой элементами изображения с одинаковыми значениями зачерненности. Затем соседние элементарные области объединяются с учетом различия зачерненности вдоль общей границы объединяемых областей и относительной длины общей границы. При объединении областей также можно использовать априорную информацию.

Кроме *сегментации* используют и другие локальные преобразования в обработке информации, типа *преобразования сегменти-*

рованных изображений, контур, поверхностное разрушение (сжатие, прорезживание) и наращивание (расширение, распространение), остовы, серединные оси.

В теории нечетких множеств приходится вводить новые определения для объединения и пересечения множеств.

Метки, указывающие принадлежность объектов обучающего множества к соответствующим классам, могут быть нечеткими. Это означает, что специалист должен классифицировать объект с учетом всех возможных классов. Так, кардиограмма определенного характера может соответствовать нескольким разновидностям сердечных заболеваний, а также здоровому сердцу. Это обстоятельство отражает значения принадлежности ко всем классам заболеваний и к классу нормы. Отметим, что значения принадлежности соответствуют «возможностям», но не вероятностям.

Если при распознавании вместо «классических» меток, указывающих принадлежность точно к одному классу, использовать нечеткие метки, то результаты классификации будут более точными, поскольку на этапе обучения задействован больший объем информации. Кроме того, отпадает необходимость «чистки» обучающего множества, поскольку все объекты, в том числе сомнительные случаи и «выбросы», могут быть помечены. Все это обеспечивает возможность работать с более определенным обучающим множеством.

Еще одна возможность проявления нечеткости связана с «размыванием» признаков. Обычно признаки представляют собой результаты каких-то объективных измерений и не содержат нечеткостей. Значения признаков, однако, могут быть нечеткими вследствие отображения на интервал $[0,1]$.

С помощью описанных выше процедур вычисляют значения принадлежности для всех классов. Нечеткость результата классификации можно устранить, относя объект к тому классу, которому соответствует наибольшее значение принадлежности. Существует, однако, и другая возможность — рассматривать значения принадлежности как окончательный результат процесса распознавания. В этом случае для принятия решения следует применить иные методы или доверить его вынесение человеку, который должен использовать при этом вычисленные значения принадлежности.

Нечеткие классификации такого рода можно использовать в кластерном анализе при формировании критерия выделения кластеров [5]. В этом, как и во многих других случаях, теория

нечетких множеств применяется для получения гибкого и исчерпывающего описания используемой стратегии.

В лингвистическом подходе к распознаванию признаками служат подобразы, называемые *непроизводными элементами*, а также отношения между ними, характеризующие структуру образа. Для описания образов через непроизводные элементы и их отношения можно использовать некоторый «язык» образов. Правила такого языка, позволяющие составлять образы из непроизводных элементов, называются *грамматикой*. При этом образ представляется некоторым предложением в соответствии с действующей грамматикой. Для распознавания некоторого образа необходимо в первую очередь определить его непроизводные элементы и отношения между ними, после чего следует провести (синтаксический) анализ с тем, чтобы установить, согласуется ли описание образа с грамматикой, которая могла бы его породить; такой анализ часто называют *грамматическим разбором*. Синтезировать грамматику можно, опираясь на априорные сведения об образах или на результаты анализа некоторого конечного множества образов.

Будем считать, что изображения описываются N -мерными векторами, компоненты которых выражают почернение ячеек сетчатки прямоугольного поля размером $N = m \times n$. Составление сложного изображения из элементарных изображений осуществляется с помощью покомпонентной операции.

Роль операции может играть обычное сложение компонент или их дизъюнкция, если компоненты двоичные, или какая-либо другая операция.

Эти представления о теории распознавания образов взяты из работ Р. Нарасимхана и В.А. Ковалевского. Данная монография и посвящена развитию этих представлений. В ней впервые формализованы принципы построения сложных изображений на прямоугольном поле при заданной операции объединения (сложения) элементарных изображений, которые называются *эталонами* или *шаблонами*. Предлагается новое направление в этой области, проведен структурный анализ построения дискретных изображений на плоскости, в результате чего задача сводится к решению системы линейных сравнений по конечному модулю, значение которого совпадает с числом цветов. При этом решается вопрос о возможности или невозможности решения задачи для некоторого множества шаблонов.

ПОСТРОЕНИЕ ЛИНЕЙНОЙ МОЗАИКИ

1.1. ЗАДАЧА ПОСТРОЕНИЯ ЦВЕТНОЙ МОЗАИКИ

Эта задача в том или ином виде может возникнуть в тех областях науки, где используется прямоугольная метрика. Всякое изображение на плоскости можно ограничить прямоугольником, затем разбить горизонтальными и вертикальными прямыми на маленькие клеточки, которые можно считать раскрашенными одним цветом.

Определение 1.1. Поле зрения $\Pi = (\pi_{ij})_{m,n}$ называется прямоугольником, разбитый на $N = mn$ клеток, где m — число клеток по горизонтали (строк), а n — число клеток по вертикали (столбцов).

Пусть задано некоторое множество шаблонов $S = \{s_1, s_2, \dots, s_p\}$ из p связанных фигур (без повторений), каждая из которых состоит из k_i ($i = 1, 2, \dots, p$) клеток, и число горизонтальных клеток каждой фигуры не превышает n , а вертикальных — m . Две клетки считаются связными, если они имеют одну или две общих вершины. Иногда, когда есть только второе, будем рассматривать сильную связность. Каждую фигуру s_i ($i = 1, 2, \dots, p$) логично представить в виде графа с k_i вершинами, если каждую пару вершин, соответствующих связным клеткам, соединить ребром. Фигура будет связной, если связан соответствующий граф. В дальнейшем не ограничиваем в общих случаях число копий каждого шаблона.

Пусть задано множество целых чисел $Q = \{0, 1, \dots, K-1\}$, которое назовем *множеством красок*. Каждой клетке шаблона s_i ($i = 1, 2, \dots, p$) поставлена в соответствие определенная краска $q \neq 0$ или $q \in Q \setminus \{0\}$. Это задается с помощью отражения $f = (f_1, f_2, \dots, f_p)$, где $f_i : s_i \rightarrow Q \setminus \{0\}$.

Первоначально полагаем, что поле Π раскрашено в цвет 0. Задано множество раскрасок B поля зрения Π (в дальнейшем — поля), которое называется *множеством образов (мозаик)*. На поле можно в допустимых пределах последовательно накладывать ша-

блонь без ограничения на место, порядок и повторение некоторых из них. Окончательный цвет каждой клетки поля будет равен сумме цветов тех клеток всех шаблонов, которые накладывались на данную клетку.

На множестве Q введена бинарная коммутативная операция \oplus сложения цветов, которая произвольным $a \in Q$ и $b \in Q$ ставит в соответствие некоторое $c \in Q$. Эта операция действует для каждой клетки поля при наложении шаблонов на него и удовлетворяет некоторым условиям. Наиболее часто такой операцией является сложение чисел по конечному модулю. Задача о построении дискретного образа состоит в следующем: при заданных S , Q и f найти такое семейство шаблонов и разместить их на поле так, чтобы в результате получить заданную раскраску $B = F: \Pi \rightarrow Q$, которая называется *образом* или *мозаикой*. В зависимости от исходных данных задача может быть неразрешимой.

Для математической постановки задачи необходимо определить, как однозначно фиксировать положение произвольного шаблона на поле. Это тем более необходимо, если учитывать, что любой шаблон можно размещать на плоскости еще в трех положениях (кроме заданного), которые получаются после поворота шаблона в плоскости на 90° , 180° и 270° . Иногда новые положения можно получить после поворота шаблона вокруг горизонтальной или вертикальной оси. Самое простое — считать новое положение шаблона, отличное от заданного, новым типом шаблона. Тогда множество S расширится до $\bar{S} = \{s_1, s_2, \dots, s_L\}$, где каждый шаблон имеет уникальный вид независимо от места, которое он занимает на поле.

Теперь в каждом шаблоне можно выделить одну постоянную клетку, относительно которой все остальные клетки шаблона определяются однозначно. Назовем такую клетку *меткой* соответствующего шаблона. Занумеруем все клетки поля по строкам от 1 до N . Тогда любая клетка поля π_{ij} будет иметь номер $l = n(i - 1) + j$ ($i = 1, 2, \dots, m; j = 1, 2, \dots, n - 1$). Если какой-то шаблон расположить на поле таким образом, чтобы его метка совпала с клеткой l , то координаты остальных клеток шаблона определяются однозначно, через l .

Рассмотрим пример шаблона из 9 клеток на поле 3×4 , где метка шаблона заштрихована (рис. 1.1).

Записываем уравнение шаблона, которое состоит из координат всех его клеток, выраженных через

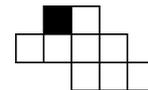


Рис. 1.1

координаты его метки l :

$$s = (l, l+1, l+n-1, l+n, l+n+1, l+n+2, l+2n+1, l+2n+2, l+2n+3). \quad (1.1)$$

Двигая горизонтально или вертикально шаблон на поле, находим допустимые пределы его положения, которые выражаются в виде ограничений на параметр l : $\alpha \leq l \leq \beta$ для первой строки и $\alpha + n\gamma \leq l \leq \beta + n\gamma$ ($i \leq \gamma \leq m-3$) для остальных строк с номером $\gamma - 1$.

Множество положений шаблона s_t на поле определяется множеством координат его меток $X(t) = \{x_1^{(t)}, x_2^{(t)}, \dots, x_M^{(t)}\}$ ($t = 1, 2, \dots, L$).

Каждая координата $x_i^{(t)} = \lambda$ ($1 \leq \lambda \leq r-1$) определяет число экземпляров шаблона s_t , наложенных друг на друга, метки которых имеют эту координату. Заданный образ, который необходимо построить, можно определить как $B = (b_1, b_2, \dots, b_N)$, где $b_i \in Q$ ($i = 1, 2, \dots, N$).

Обозначим $\Theta'(l)$ — окрестность клетки l относительно шаблона s_t ($t = 1, 2, \dots, L$), т. е. подмножество координат $X(t)$, для которых этот шаблон содержит клетку l . Так же, как и уравнение шаблона (1.1), зададим его раскраску $s_i(q) = \{q_1, q_2, \dots, q_{k_i}\}$ ($i = 1, 2, \dots, L$), где цвета расположены в том же порядке, что и клетки в (1.1). Очевидно, что в окрестность клетки l любого шаблона входит и сама клетка l . Для некоторых пар (t, l) множество $\Theta'(l)$ может быть пустым. Сформулируем задачу для произвольных операций сложения.

Постановка задачи. Пусть заданы множества шаблонов S и цветов Q и операция сложения цветов \oplus . Необходимо найти такое подмножество $S' \subseteq S$ и так наложить эти шаблоны на поле, чтобы в результате сложения цветов получить мозаику $b \in B$, где $b = \{b_1, b_2, \dots, b_N\}$.

Учитывая все обозначения, основную задачу можно свести к решению уравнений такого типа:

$$\sum_{\Theta'(l) \neq \emptyset} \sum_{i \in \Theta'(l)} x_i^{(t)} q_i^{(t)} \equiv b_l \pmod{K} \quad (l = 1, 2, \dots, N), \quad (1.2)$$

где все решения $x_i^{(t)} \neq 0$ определяют положение и количество тех шаблонов, которые в сумме дают заданный образ B . В общем

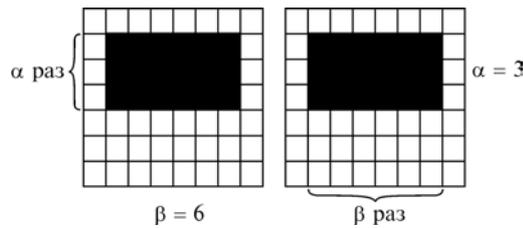


Рис. 1.2

виде эта задача довольно сложная, так как число переменных в ней существенно превышает число уравнений. При этом возникают проблемы с определением ранга системы, что во многом зависит от типов шаблонов и множества красок.

Кроме уравнения (1.2) можно вывести несколько зависимостей между шаблонами, если их накладывать на поле различными способами.

Самая простейшая зависимость получается для одинаковых линейных шаблонов, т. е. шаблонов, представляющих набор β горизонтальных клеток или α вертикальных клеток, окрашенных одинаково (рис. 1.2). Нетрудно увидеть, что все вертикальные положения линейных шаблонов являются линейно зависимыми от горизонтальных шаблонов. Если взять α горизонтальных шаблонов длиной β , расположенных строго один под другим, то это равносильно β вертикальным шаблонам длиной α , расположенных в ряд строго один за другим. Таких зависимостей может быть очень много и для других разновидностей шаблонов; обнаружить их не всегда возможно из-за большого количества уравнений и больших размеров поля.

1.2. ПОСТРОЕНИЕ БАЗИСА РЕШЕНИЙ ЗАДАЧИ ДЛЯ ДВУХ ОДНОЦВЕТНЫХ ШАБЛОНОВ

Здесь решается простая задача для набора прямолинейных шаблонов как последовательности клеток, окрашенных разным цветом. Самые простые шаблоны — окрашенные цветом 1 и длиной s_t ($t \geq 1$), а множество $Q = \{0, 1\}$. Самое простое поле зрения — поле размером $1 \times n$ или просто строка длиной n .

Определение 1.2. Будем считать выделенной клеткой (меткой) в каждом шаблоне самую крайнюю левую клетку. Номер клетки, на котором расположена метка шаблона, назовем его координатой.

Координаты клеток поля определяются как числа натурального ряда $1, 2, \dots, n$. Координаты меток шаблонов зависят от их размеров. Они представляют также натуральные числа $1, 2, \dots, n - k_t + 1$, где k_t — размер (длина) шаблона s_t ($t = 1, 2, \dots, L$). Множество шаблонов можно представлять как множество векторов, например:

$$s_t = \{q_1^{(t)}, q_2^{(t)}, \dots, q_{k_t}^{(t)}\},$$

где $q_i^{(t)} \in Q \setminus \{0\}$.

В качестве операции сложения выберем сложение по mod 2.

Если сложить шаблон длиной $d + 1$ ($d \geq 2$) с координатой j с шаблоном длиной d и координатой $j + 1$, то получим единицу в j -й клетке.

Пронумеруем клетки поля от 1 до n . Образом на таком поле будет произвольное множество черных клеток. Общее число образов (без учета пустого, окрашенного белым цветом) равно $2^n - 1$. Множество типов шаблонов $S = \{s_1, s_2, \dots, s_p\}$ ($s_i \neq s_j; 1 \leq i, j \leq p$) будем задавать как множество чисел, где s_i равно числу соответствующих окрашенных подряд в черный цвет клеток. Легко убедиться, что шаблон s_i ($i = 1, 2, \dots, p$) может разместиться на поле $n - s_i + 1$, если двигать его последовательно слева направо. Будем считать, что у нас есть $n - s_i + 1$ копий шаблона s_i .

Приходим к выводу, что достаточно уметь получать единицу с помощью линейных горизонтальных шаблонов в любой клетке строки, чтобы построить любой образ на линейном поле.

Определение 1.3. Наименьший набор шаблонов, который позволяет представить единицу в любой клетке строки, называется базисом линейной мозаики.

Самым тривиальным базисом является один шаблон $S = \{1\}$. Для двух шаблонов длиной s_1 и s_2 , как было указано, базис может составлять набор $S = \{d, d+1\}$ ($d > 1$). При наложении двух таких шаблонов можно получить единицу либо справа, либо слева от меньшего шаблона. Если один из шаблонов по длине больше, чем $\left\lfloor \frac{n}{2} \right\rfloor + 1$, то появляются ограничения на передвижение этого шаблона вдоль строки, и базис может не существовать для некоторых единиц.

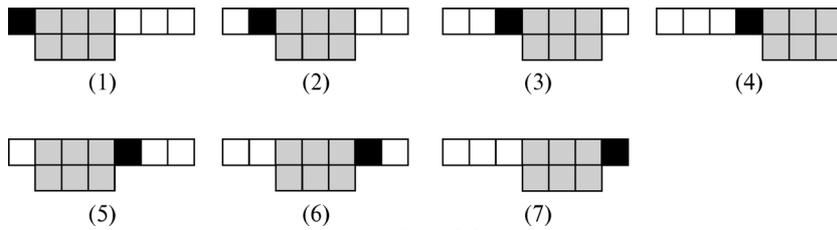


Рис. 1.3

Поэтому для такого базиса необходимо выполнение условия

$$2 < s_1 < s_2 < \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

Пример 1.1. На рис. 1.3 показан базис для шаблонов $S = \{4, 3\}$ и $n = 7$.

На этом примере продемонстрировано построение единицы, когда каждый шаблон берется ровно по одному экземпляру. В общем виде это не всегда возможно, поэтому в дальнейшем будем предполагать, что, если не оговорено противное, каждый шаблон представлен в необходимом количестве.

Для $s_1 = 2$ можно в качестве второго шаблона взять $s_2 = 2k + 1$ ($k \geq 1$). В этом случае получить единицу для любого l можно с помощью нескольких шаблонов первого типа с координатами $x_1^{(j)}$ и одного шаблона второго типа с координатой x_2 .

Для $l = 2i + 1$ ($i \geq 0$) это $x_1^{(j)} = 2j + 1$ ($i \leq j \leq k$) и $x_2 = 2l + 2$; для $l = 2i$ — $x_1^{(j)} = 2j$ ($i \leq j \leq k$) и $x_2 = 2l + 1$. Если построены все единицы для $l < \left\lfloor \frac{n}{2} \right\rfloor + 1$, то остальные единицы можно получить зер-

кальным построением относительно центральной оси симметрии. Если $2k + 1 < n$, то, используя сдвиг, можно построить единицы и для остальных клеток. Для произвольных двух типов шаблонов при $s_1 \geq 3$ такие зависимости имеют более сложный вид. Укажем, что для любого n имеется пороговое значение длин двух шаблонов, когда существует ровно один базис, а для других значений базис либо не существует, либо их несколько.

Пример 1.2. Рассмотрим два шаблона $s_1 = 5$, $s_2 = 13$ и $n = 16$. Здесь $s_2 > \left\lfloor \frac{16}{2} \right\rfloor + 1 = 9$. Составим систему уравнений типа (1.1):

$$\left. \begin{array}{l}
 x_1 + \dots + x_{14} = b_1 \\
 x_1 + x_2 + \dots + x_{14} + x_{15} = b_2 \\
 x_1 + x_2 + x_3 + \dots + x_{14} + x_{15} + x_{16} = b_3 \\
 x_1 + x_2 + x_3 + x_4 + \dots + x_{14} + x_{15} + x_{16} + x_{17} = b_4 \\
 x_1 + x_2 + x_3 + x_4 + x_5 + \dots + x_{14} + x_{15} + x_{16} + x_{17} = b_5 \\
 \dots \\
 x_5 + x_6 + x_7 + x_8 + x_9 + \dots + x_{14} + x_{15} + x_{16} + x_{17} = b_9 \\
 x_6 + x_7 + x_8 + \dots + x_{10} + \dots + x_{14} + x_{15} + x_{16} + x_{17} = b_{10} \\
 \dots \\
 x_8 + \dots + x_{12} + x_{14} + x_{15} + x_{16} + x_{17} = b_{12} \\
 x_9 + \dots + x_{12} + x_{14} + x_{15} + x_{16} + x_{17} = b_{13} \\
 x_{10} + \dots + x_{12} + \dots + x_{15} + x_{16} + x_{17} = b_{14} \\
 x_{11} + x_{12} + \dots + x_{16} + x_{17} = b_{15} \\
 x_{12} + \dots + x_{17} = b_{16}
 \end{array} \right\} \text{mod } 2. \quad (1.3)$$

При заданных параметрах координата первого шаблона принимает значение $x_i^{(1)} = 1$ для $i = 1, 2, \dots, 12$, а для второго — $x_i^{(2)} = 1$ для $i = 1, 2, 3, 4$. Чтобы не указывать верхние индексы, обозначим переменные первого шаблона как x_1, x_2, \dots, x_{12} , а переменные второго шаблона — $x_{14}, x_{15}, x_{16}, x_{17}$. Здесь x_{13} пропущено из соображений, которые мы раскроем позднее.

Можно решать систему данных уравнений, исходя из общих позиций, используя известные методы, например, из работы [1]. Однако воспользуемся тем, что мы имеем дело со специфической системой уравнений. Здесь правые части могут быть произвольными. Но нас интересует вопрос о существовании базиса для этих шаблонов. Поэтому будем решать систему, полагая, что в правых частях находятся все нули, кроме одного значения $b_j \equiv 1 \pmod{2}$, $1 \leq j \leq n$. Очевидно, что в этом случае правые части уравнений линейно независимы. Мы имеем систему уравнений с n уравнениями и n неизвестными. Важной особенностью этой системы есть условие $s_1 + s_2 = n + 2$. Так как число переменных для первого шаблона равно $n + 1 - s_1 = s_2 - 1$, то по аналогии число неизвестных для второго шаблона равно $s_1 - 1$. Поэтому в $(s_1 - 1)$ -й и s_1 -й строках система имеет одинаковое количество переменных второго шаблона, а для первого шаблона — разное, отличающееся на одно. Складывая эти уравнения, получаем решение $x_{s_1} \equiv (b_{s_1-1} + b_{s_1}) \pmod{2}$. В нашей системе, складывая четвертое и пятое уравнения, получаем $x_5 \equiv (b_4 + b_5) \pmod{2}$. Если подставить значение x_5 в самое нижнее уравнение (9-е), где присутствует x_5 , то, складывая его с десятым уравнением, получаем $x_{10} = x_5 + b_{10} + b_9 =$

$= (b_4 + b_5 + b_9 + b_{10}) \pmod{2}$. Продолжая этот процесс дальше, определяем решение для x_{15} . Теперь, возвращаясь в самое верхнее уравнение, где присутствует x_{15} (второе уравнение), и складывая его с первым, получаем решение для x_2 . В общем случае, делая k шагов, находим значение

$$x_{ks_1} = \sum_{i=1}^k (b_{ts_1} + b_{ts_1-1}) \pmod{2}, \quad (1.4)$$

где ks_1 — положительный вычет по $\text{mod}(s_1 + s_2)$, $k \geq 1$. Выражение ks_1 должно пробегать все значения индексов переменных от 1 до $n + 1$, если k принимает значения от 1 до $s_1 + s_2 - 1$. Для последнего значения индексов переменных находим $s_1(s_1 + s_2 - 1) = -s_1 \equiv s_2 \pmod{s_1 + s_2}$.

Для этого необходимо, чтобы $\text{НОД}(s_1, s_1 + s_2) = \text{НОД}(s_1, s_2) = 1$. Если это не так, то найдется такое $d > 1$, что $s_1 = \alpha d$ и $s_2 = \beta d$. Тогда для $k = \beta + \alpha + 1$ получаем $x_{s_1} = x_{s_1(\alpha+\beta+1)}$, что приводит к зависимости между значениями правых частей, а это недопустимо, т. е. система не имеет решения. Тем самым доказана следующая теорема.

Теорема 1.1. Два разных числа s_1 и s_2 с условием $s_1 + s_2 = n + 2$ ($n > 3$) образуют базис, если $\text{НОД}(s_1, s_2) = 1$.

Пусть в правой части $b_j = 1$ ($b_i = 0, i \neq j$). Обозначим t_1 (соответственно t_2) — наименьшее (соответственно наибольшее) решение из двух уравнений в положительных вычетах $xs_1 = j \pmod{s_1 + s_2}$ или $xs_1 = (j + 1) \pmod{s_1 + s_2}$. Тогда получаем решение

$$x_k = \begin{cases} 1, & \text{если } t_1 \leq t < t_2; \\ 0, & \text{в остальных случаях,} \end{cases} \quad (1.5)$$

где $ts_1 = k \pmod{s_1 + s_2}$.

В нашем примере пусть $b_3 = 1$. Тогда результаты записываем в виде табл. 1.1.

Т а б л и ц а 1.1

ts_1	= 5, 10, 15, 2, 7, 12, 17, 4, 9, 14, 1, 6, 11, 16, 3, 8, 13.
t	= 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17.
x	= 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0.

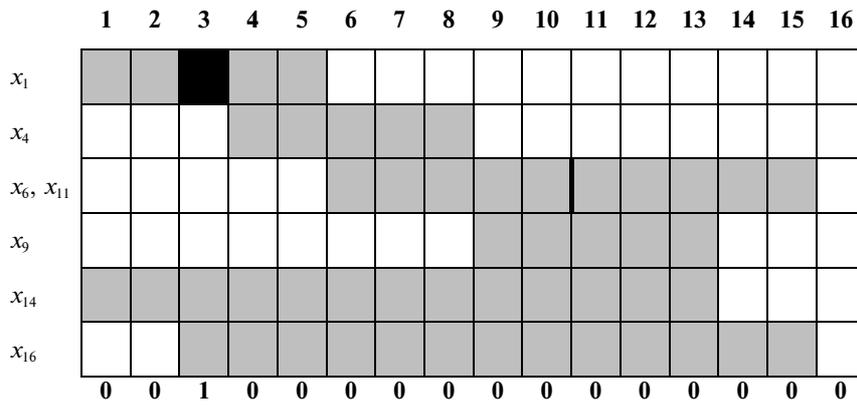


Рис. 1.4

Здесь $t_1 = 8$, $t_2 = 15$. Отсюда, в соответствии с табл. 1.1, для $8 \leq t < 15$ получаем $x_4 = x_9 = x_{14} = x_1 = x_6 = x_{11} = x_{16} = 1$. Остальные $x_i = 0$. Решение системы для $b_3 = 1$ показано на рис. 1.4. При этом предполагалось, что для всех переменных, начиная с x_{14} , место положения левой клетки на 13 значений переменных меньше их индекса.

Если $s_1 + s_2 > n + 2$, то число уравнений будет больше числа переменных и система не всегда имеет решения. Если $s_1 + s_2 < n + 2$, то число переменных будет больше числа уравнений и система может иметь много решений. В этом случае уменьшаем n до необходимого, чтобы применять условие теоремы 1.1, а решения для новых правых клеток поля получаем путем сдвига решений, найденных для левой части поля.

Если в правой части системы (1.2) стоят произвольные значения b_j , то решение получают, складывая решения для каждого

Таблица 1.2

t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
ts_1	5	10	15	2	7	12	17	4	9	14	1	6	11	16	3	8	13
b_2	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0
b_5	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
b_{11}	0	0	0	0	0	1	1	1	1	1	1	1	0	0	0	0	0
b_{13}	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	0
Σ	1	1	1	0	0	1	1	1	1	0	0	1	0	0	1	1	0

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1			■	■	■	■	■									
2				■	■	■	■	■								
3					■	■	■	■	■							
4						■	■	■	■	■						
5								■	■	■	■	■				
6									■	■	■	■	■			
7										■	■	■	■	■		
8											■	■	■	■	■	
9		■	■	■	■	■	■	■	■	■	■	■	■	■		
10			■	■	■	■	■	■	■	■	■	■	■	■	■	
Σ		■			■						■		■			

Рис. 1.5

$b_j = 1$. После этого удаляют из решения лишние значения, чтобы $x_i = 0 \vee 1$. То же самое можно выполнить, используя общую табл. 1.1 для всех значений $b_j = 1$.

Пусть при тех же условиях для нашего примера необходимо построить образ $b_2 = b_5 = b_{11} = b_{13} = 1$, а все остальные $b_j = 0$. Составляем таблицу типа табл. 1.1, т. е. имеем табл. 1.2.

В результате получаем: $x_3 = x_4 = x_5 = x_6 = x_8 = x_9 = x_{10} = x_{12} = x_{15} = x_{17} = 1$, остальные переменные равны 0. Это решение (построение образа $b_2 = b_5 = b_{11} = b_{13} = 1$) показано на рис. 1.5, при этом x_{15} и x_{17} — переменные, обозначающие второй шаблон, с координатами 2 и 4.

1.3. РЕШЕНИЕ ЗАДАЧИ ДЛЯ ЛИНЕЙНОЙ ДВУХЦВЕТНОЙ МОЗАИКИ

Зная алгоритм построения любой единицы, покажем, как при этом получить решение для произвольной правой части системы (1.2).

Пример 1.3. Для удобства изложения рассмотрим систему с параметрами $S = \{5, 8\}, n = 11, B = \{b_1, b_2, \dots, b_n\}$.

Обозначим переменные для первого шаблона как x_i ($i = 1, 2, \dots, n + 1 - s_1$), для второго шаблона — x_{s_2+j} ($j = 1, 2, \dots, n + 1 - s_2$),

где i и j — координаты в строке меток соответствующих шаблонов. Тогда система (1.2) принимает вид

$$\begin{array}{rcl}
 x_1 + \dots + x_9 & = & b_1 \\
 x_1 + x_2 + \dots + x_9 + x_{10} & = & b_2 \\
 x_1 + x_2 + x_3 + \dots + x_9 + x_{10} + x_{11} & = & b_3 \\
 x_1 + x_2 + x_3 + x_4 + \dots + x_9 + x_{10} + x_{11} + x_{12} & = & b_4 \\
 x_1 + x_2 + x_3 + x_4 + x_5 + \dots + x_9 + x_{10} + x_{11} + x_{12} & = & b_5 \\
 x_2 + x_3 + x_4 + x_5 + x_6 + \dots + x_9 + x_{10} + x_{11} + x_{12} & = & b_6 \\
 x_3 + x_4 + x_5 + x_6 + x_7 + \dots + x_9 + x_{10} + x_{11} + x_{12} & = & b_7 \\
 x_4 + x_5 + x_6 + x_7 + \dots + x_9 + x_{10} + x_{11} + x_{12} & = & b_8 \\
 x_5 + x_6 + x_7 + \dots + x_{10} + x_{11} + x_{12} & = & b_9 \\
 x_6 + x_7 + \dots + x_{11} + x_{12} & = & b_{10} \\
 x_7 + \dots + x_{12} & = & b_{11}
 \end{array} \left. \vphantom{\begin{array}{rcl}} \right\} \text{mod } 2. \quad (1.6)$$

Отметим особенности общей системы для двух шаблонов. Она естественным образом по столбцам делится на две подобные части. Левая часть состоит из $s_2 - 1$ столбцов, в каждом из которых ровно s_1 переменных. Все столбцы одинаковы, но сдвигаются вниз ровно на одну позицию по отношению к предыдущему. Аналогично правая часть состоит из $s_1 - 1$ столбцов, в которых ровно s_2 переменных.

В системе отсутствует переменная x_{s_2} . В строке s_1 переменных первого шаблона на одну больше, а переменных второго шаблона — одинаковое число. То же самое относится к строке $n + 2 - s_1$. Пусть $b_0 \equiv b_{12} \equiv 0 \pmod{2}$. Начиная со второй строки, прибавляем к ней предыдущую по mod 2. В результате получаем новую систему, в которой все строки, за исключением указанных выше, имеют по одной переменной от каждого шаблона, а в строках s_1 и $n + 2 - s_1$ — ровно по одной переменной от первого шаблона. Добавляя в систему последнее уравнение из (1.6), записываем

$$\begin{array}{rcl}
 x_1 + \cdot & +x_9 & \cdot & \cdot & \cdot & = & b_0 + b_1 \\
 \cdot & x_2 + & \cdot & +x_{10} & \cdot & \cdot & = & b_1 + b_2 \\
 \cdot & \cdot & x_3 + & \cdot & +x_{11} & = & b_2 + b_3 \\
 \cdot & \cdot & \cdot & x_4 + & \cdot & +x_{12} & = & b_3 + b_4 \\
 \cdot & \cdot & \cdot & \cdot & \bigcirc x_5 & \cdot & = & b_4 + b_5 \\
 x_1 + & \cdot & \cdot & \cdot & \cdot & x_6 + & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & = & b_5 + b_6 \\
 \cdot & x_7 + & \cdot & = & b_6 + b_7 \\
 \cdot & \cdot & \bigcirc x_8 & \cdot & = & b_7 + b_8 \\
 \cdot & \cdot & \cdot & x_4 + & \cdot & \cdot & \cdot & \cdot & +x_9 & \cdot & \cdot & \cdot & = & b_8 + b_9 \\
 \cdot & \cdot & \cdot & \cdot & x_5 + & \cdot & \cdot & \cdot & \cdot & +x_{10} & \cdot & \cdot & = & b_9 + b_{10} \\
 \cdot & \cdot & \cdot & \cdot & \cdot & x_6 + & \cdot & \cdot & \cdot & +x_{11} & \cdot & \cdot & = & b_{10} + b_{11} \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_7 + & \cdot & \cdot & \cdot & +x_{12} & \cdot & = & b_{11} + b_{12}
 \end{array} \left. \vphantom{\begin{array}{rcl}} \right\} \text{mod } 2. \quad (1.7)$$

Получаем непосредственное решение $x_5 \equiv (b_4 + b_5)(\text{mod } 2)$, а также $x_3 \equiv (b_7 + b_8)(\text{mod } 2)$. Подставляя эти значения в остальные уравнения, находим полное решение системы (1.7).

Теорема 1.2. Решением системы (1.7) есть

$$x_i \equiv \sum_{j=1}^{\lambda} (b_j + b_{j-1})(\text{mod } 2), \quad (1.8)$$

где $\gamma \equiv js_1 \pmod{(s_1 + s_2)}$, а $\lambda = i \cdot s_1^{-1} \pmod{(s_1 + s_2)}$.

Доказательство. Будем рассуждать по индукции. Для x_{s_1} получаем $\lambda = s_1 \cdot s_1^{-1} \pmod{(s_1 + s_2)} = 1$ и $x_{s_1} \equiv (b_{s_1} + b_{s_1-1})(\text{mod } 2)$ или, конкретно, $x_5 \equiv (b_4 + b_5)(\text{mod } 2)$.

Переменная x_5 встречается ниже на 5 позиций. Подставляя значение x_5 , находим решение для x_{10} . Для него $\lambda = 2 \cdot s_1 \cdot s_1^{-1} \pmod{(s_1 + s_2)} = 2$. Получаем $x_{10} \equiv (b_4 + b_5 + b_9 + b_{10})(\text{mod } 2)$. Далее, поднимаясь на 8 позиций вверх и подставляя значение x_{10} , определяем решение для x_2 . Таким образом, получаем последовательное движение либо вниз на s_1 позиций (при этом индексы увеличиваются на s_1), либо вверх на s_2 позиций (при этом индексы уменьшаются на s_2). Однако $-s_2 \equiv s_1 \pmod{(s_1 + s_2)}$, т. е. в классе вычетов каждый раз индекс увеличивается на s_1 .

В результате выражение ts_1 , когда t принимает все значения от 1 до $s_1 + s_2 - 2$, пробегает все индексы переменных, а при $t = s_1 + s_2 - 2$ получаем

$$i = s_1(s_1 + s_2 - 1) \equiv -s_1 \equiv s_2 \pmod{(s_1 + s_2)}.$$

Однако у нас переменная x_{s_2} отсутствует. А предыдущая переменная имела индекс $i = s_1(s_1 + s_2 - 2) \equiv -2s_1 \pmod{(s_1 + s_2)}$. Для нашего примера это составляет $2 \cdot 5 \equiv 3 \pmod{13}$. И для него справедливо выражение

$$x_3 \equiv \sum_{\substack{j=1 \\ j \neq 8}}^{11} (b_j + b_{j-1})(\text{mod } 2) \equiv (b_7 + b_8)(\text{mod } 2),$$

что совпадает с непосредственным равенством в (1.7). Это и завершает доказательство теоремы.

Пример 1.4. Построение для этих решений образа $B = (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$ приведено на рис. 1.6.

Согласно теореме 1.2 имеем

$$\begin{aligned} x_5 &= b_4 + b_5 = 0; & x_9 &= x_4 + b_8 + b_9 = 1; \\ x_{10} &= x_5 + b_9 + b_{10} = 0; & x_1 &= x_9 + b_0 + b_1 = 1; \\ x_2 &= x_{10} + b_1 + b_2 = 1; & x_6 &= x_1 + b_5 + b_6 = 1; \\ x_7 &= x_2 + b_6 + b_7 = 0; & x_{11} &= x_6 + b_{10} + b_{11} = 1; \\ x_{12} &= x_7 + b_{11} + b_{12} = 1; & x_3 &= x_{11} + b_2 + b_3 = 1. \\ x_4 &= x_{12} + b_3 + b_4 = 0; \end{aligned}$$

Напомним, что переменные x_j для $j > 8$ соответствуют второму шаблону с метками $j = 8$.

Так решается проблема для двух шаблонов при заданных двух цветах. Если $s_1 + s_2 > n + 2$, то некоторые образы построить невозможно. В этом случае число уравнений больше числа переменных, что накладывает ограничения на правые части системы уравнений (1.2). Если они не выполняются, то система не имеет решений. Здесь могут быть два принципиально различающихся случая в зависимости от значений s_1 .

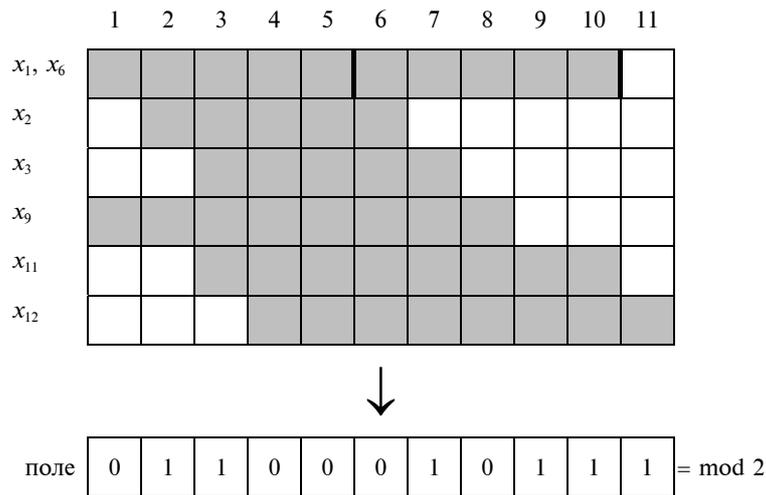


Рис. 1.6

Пример 1.5. Пусть $s_1 = 7$, $s_2 = 8$, $n = 10$.

Число переменных для первого шаблона равно $10 + 1 - 7 = 4$, для второго — $10 + 1 - 8 = 3$. Обозначим их x_i ($i = 1, 2, 3, 4$) и y_j ($j = 1, 2, 3$). Составим для них систему типа (1.2):

$$\left. \begin{array}{rcl} x_1 + & & + y_1 & = b_1 \\ x_1 + x_2 + & & + y_1 + y_2 & = b_2 \\ x_1 + x_2 + x_3 + & & + y_1 + y_2 + y_3 & = b_3 \\ x_1 + x_2 + x_3 + x_4 + & & + y_1 + y_2 + y_3 & = b_4 \\ x_1 + x_2 + x_3 + x_4 + & & + y_1 + y_2 + y_3 & = b_5 \\ x_1 + x_2 + x_3 + x_4 + & & + y_1 + y_2 + y_3 & = b_6 \\ x_1 + x_2 + x_3 + x_4 + & & + y_1 + y_2 + y_3 & = b_7 \\ & x_2 + x_3 + x_4 + & + y_1 + y_2 + y_3 & = b_8 \\ & & x_3 + x_4 & + y_2 + y_3 = b_9 \\ & & & x_4 & + y_3 = b_{10} \end{array} \right\} \text{mod } 2. \quad (1.9)$$

Здесь $s_1 = 7 \geq \lfloor n/2 \rfloor + 1 = 6$. Это приводит к тому, что число переменных для первого шаблона $4 < s_1$. Система имеет матрицу размером 7×10 и ее переменные образуют два касающихся параллелограмма, в каждом из которых левые нижние вершины находятся ниже правых верхних вершин. Если взять в качестве координат вершин номер столбца и номер строки матрицы системы уравнений, то для первого параллелограмма получим такие координаты вершин $(1;1)$, $(n+1-s_1, n+1-s_1)$, $(s_1, 1)$ и $(n, n+1-s_1)$ или $(1,1)$, $(4,4)$, $(7,1)$ и $(10,4)$. Поскольку $n+1-s_1 < s_1$ (то же имеет место и для второго шаблона), то матрица системы содержит одинаковые строки, начиная со строки $n+1-s_1$ и заканчивая строкой s_1 .

Здесь четыре одинаковых строки в матрице системы — 4, 5, 6 и 7 и определитель этой системы равен $0 \pmod{2}$. Поэтому для существования решения системы необходимо, чтобы $b_4 = b_5 = b_6 = b_7$. Если удалить из системы три зависимые строки, то получим систему вида

$$\left. \begin{array}{rcl} x_1 + & & + y_1 & = b_1 \\ x_1 + x_2 + & & + y_1 + y_2 & = b_2 \\ x_1 + x_2 + x_3 + & & + y_1 + y_2 + y_3 & = b_3 \\ x_1 + x_2 + x_3 + x_4 + & & + y_1 + y_2 + y_3 & = b_4 \\ & x_2 + x_3 + x_4 + & + y_1 + y_2 + y_3 & = b_8 \\ & & x_3 + x_4 + & + y_2 + y_3 = b_9 \\ & & & x_4 + & + y_3 = b_{10} \end{array} \right\} \text{mod } 2. \quad (1.10)$$

Эта система имеет размеры 7×7 и решается указанным выше способом для $n = 7$ и $S = \{4, 5\}$. Если условие $s_1 \geq \lfloor n/2 \rfloor + 1$ не выполняется, то определитель этой системы также равен $0 \pmod{2}$, но найти зависимые строки в системе сложнее.

Если $s_1 + s_2 < n + 2$, то возникает множество решений, так как путем сдвига шаблонов, которые являются базисом для $s_1 + s_2 = n + 2$, можно получить базис для больших значений n .

Вопрос о числе шаблонов больше двух решается аналогично. Пусть задано p шаблонов. Будем считать их упорядоченными по возрастанию. Очевидно, что для них также должно выполняться условие

$$\text{НОД}(s_1, s_2, \dots, s_p) = 1. \quad (1.11)$$

Кроме того, система типа (1.2) должна всегда иметь n переменных, чтобы решение было единственным. Но каждый шаблон может иметь $n + 1 - s_i$ переменных. Поэтому необходимо выполнение условия

$$\sum_{i=1}^p (n + 1 - s_i) = n,$$

откуда

$$\sum_{i=1}^p s_i = (p - 1)n + p. \quad (1.12)$$

Эти условия являются необходимыми. Вопрос о конкретном методе решения задачи для более двух шаблонов остается открытым. Возьмем для начала $p = 3$. Если среди них найдутся два взаимно простых шаблона, то составляем систему типа (1.2) для этих шаблонов и решаем задачу по теореме 1.2. Если из трех шаблонов каждые два имеют общий делитель, а все вместе удовлетворяют условию (1.11), то составляем систему (1.2) для трех шаблонов. Пусть существуют три неравных между собой множителя α_1 , α_2 и α_3 . Тогда $s_1 = \alpha_1\alpha_2$, $s_2 = \alpha_1\alpha_3$ и $s_3 = \alpha_2\alpha_3$ удовлетворяют условию (1.11). Если брать произвольные множители, то не всегда условие (1.12) выполняется, поэтому простейший подходящий пример содержит достаточно большие числа, не дающие возможности наглядно представить систему типа (1.2). Пусть, например, $\alpha_1 = 2$, $\alpha_2 = 3$ и $\alpha_3 = 5$. Тогда $s_1 = 6$, $s_2 = 10$ и $s_3 = 15$. Из (1.10) следует, что

$$n = \frac{\sum_{i=1}^p s_i - p}{p-1} > s_i; \quad i=1, 2, \dots, p. \quad (1.13)$$

Получаем $n = (6 + 10 + 15 - 3)/2 = 14 < s_3$, а это недопустимо. Однако, значения s_i не могут быть произвольными. Возьмем, например, $s_1 = 10$, $s_2 = 15$ и $s_3 = 18$. Эти значения подходят для (1.13), так как при этом $n = 20$. Каждому шаблону соответствует $n + 1 - s_i$ положений на поле или такое же количество переменных. Если подставить значение $p = 3$ в (1.13), то получим

$$s_i + s_j > s_k + 2, \quad (1.14)$$

где $i, j, k \in \{1, 2, 3\}$.

Однако, даже если удовлетворяются все условия (1.12)—(1.14), то не всегда существует решение системы типа (1.2).

Лемма 1.1. Если $s_1 \geq \lfloor n/2 \rfloor + 1$, то система типа (1.2), составленная для p шаблонов, удовлетворяющих условиям (1.12)—(1.14), имеет матрицу A , у которой $\det A \equiv 0 \pmod{2}$.

Доказательство. Система типа (1.8) для p шаблонов будет состоять из p параллелограммов. Так как $s_1 \geq \lfloor n/2 \rfloor + 1$, то в первом параллелограмме левая нижняя вершина будет находиться ниже правой верхней. Поскольку $s_1 < s_i$ для $i > 1$, то изложенное справедливо и для остальных параллелограммов. А это обеспечивает совпадение строк матрицы системы, начиная от строки $n + 1 - s_1$ и заканчивая строкой s_1 , что и дает значение $\det A \equiv 0 \pmod{2}$.

1.4. ЧИСЛОВЫЕ ГРАФЫ И ЛИНЕЙНАЯ МОЗАИКА

Рассмотрим в качестве примера два шаблона: $s_1 = 5$, $s_2 = 8$ и $n = 11$. Составим систему уравнений типа (1.1). При заданных параметрах метка первого шаблона, учитывая размеры поля, может принимать значения $x_i^{(1)} = 1$ для $i = 1, 2, \dots, 7$. Аналогично метка второго шаблона может принимать значения $x_j^{(2)} = 1$ для $j = 1, 2, 3, 4$. Чтобы не иметь дело с верхними индексами, обозначим x_i ($i = 1, 2, \dots, 7$) переменные для первого шаблона, а x_j ($j = 8, 9, 10, 11$) — переменные для второго шаблона. Тогда система (1.2) для нашего примера приобретет конкретный вид:

$$\left. \begin{array}{l}
 x_1 \cdot \cdot \cdot \cdot \cdot \cdot + x_8 \cdot \cdot \cdot \cdot = b_1 \\
 x_1 + x_2 \cdot \cdot \cdot \cdot \cdot \cdot + x_8 + x_9 \cdot \cdot \cdot = b_2 \\
 x_1 + x_2 + x_3 \cdot \cdot \cdot \cdot \cdot \cdot + x_8 + x_9 + x_{10} \cdot \cdot = b_3 \\
 x_1 + x_2 + x_3 + x_4 \cdot \cdot \cdot \cdot \cdot \cdot + x_8 + x_9 + x_{10} + x_{11} = b_4 \\
 x_1 + x_2 + x_3 + x_4 + x_5 \cdot \cdot \cdot \cdot \cdot \cdot + x_8 + x_9 + x_{10} + x_{11} = b_5 \\
 \quad x_2 + x_3 + x_4 + x_5 + x_6 \cdot \cdot \cdot \cdot \cdot \cdot + x_8 + x_9 + x_{10} + x_{11} = b_6 \\
 \quad \quad x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} = b_7 \\
 \quad \quad \quad x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} = b_8 \\
 \quad \quad \quad \quad x_5 + x_6 + x_7 \cdot \cdot \cdot \cdot \cdot \cdot + x_9 + x_{10} + x_{11} = b_9 \\
 \quad \quad \quad \quad \quad x_6 + x_7 \cdot \cdot \cdot \cdot \cdot \cdot + x_{10} + x_{11} = b_{10} \\
 \quad \quad \quad \quad \quad \quad x_7 \cdot \cdot \cdot \cdot \cdot \cdot + x_{11} = b_{11}
 \end{array} \right\} \pmod{2}. \quad (1.15)$$

Если обозначить матрицу этой системы как A , то решение задачи о построении линейной мозаики для двух шаблонов $S = (s_1, s_2)$ сводится к решению системы сравнений с $s_1 + s_2 - 2$ переменными:

$$AX \equiv b \pmod{2}. \quad (1.16)$$

Матрица A имеет специфическую структуру: она состоит из двух массивов единиц (остальные равны нулю), которые напоминают параллелограммы. Относительно строк и столбцов они имеют такие координаты своих вершин: $[(1,1), (s_1,1), (s_2-1, s_2-1), (n, s_2-1)]$ и $[(1, s_2), (s_2, s_2), (s_1-1, n), (n, n)]$. Эту матрицу можно задать и по-другому:

$$a_{ij} = \begin{cases} 1, & \text{если } j \leq i \leq j + s_1 - 1 \text{ и } j \leq s_2 - 1, \\ 1, & \text{если } i \leq j \leq i + s_1 - 1 \text{ и } j \geq s_2, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Если $\det A \not\equiv 0 \pmod{2}$, то решение (1.16) принимает вид $X \equiv A^{-1}b \pmod{2}$, поэтому необходимо найти A^{-1} из условия $A^{-1}A \equiv E \pmod{2}$. Для этого необходимо решить n систем простых уравнений из n неизвестных.

Рассмотрим систему уравнений, где неизвестными являются элементы первой строки матрицы A^{-1} . Обозначим их $y = (y_1, y_2, \dots, y_n)$. Необходимо решить систему

$$A^T y \equiv (1, 0, 0, \dots, 0) \pmod{2}. \quad (1.17)$$

Матрица A^T также имеет два массива единиц (остальные элементы равны 0), которые образуют 2 параллелограмма, но уже в транспонированном виде.

Лемма 1.2. Детерминант матрицы A системы уравнений (1.16) равен $1 \pmod{2}$ тогда и только тогда, когда наибольший общий делитель чисел s_1 и s_2 $\text{НОД}(s_1, s_2) \equiv 1 \pmod{2}$.

Для доказательства рассмотрим матрицу A для двух шаблонов s_1 и s_2 и обозначим ее $A(s_1, s_2)$. В каждом из первых $s_2 - 1$ ее столбцов находится по s_1 единиц, а в каждом из оставшихся $s_1 - 1$ столбцов — по s_2 единиц. Попробуем непосредственно вычислить $\det A = |A|$. Для этого разделим матрицу на ее верхние s_1 строк и нижние $n - s_1$ строк. Затем каждую из этих частей разделим на левые s_1 столбцов и правые $n - s_1$ столбцов. Обозначим полученные подматрицы A_{11} , A_{12} , A_{21} и A_{22} . Подматрица A_{11} является треугольной, у нее наддиагональные элементы равны нулю, а остальные равны 1. В подматрице A_{12} все столбцы с единицами равны первым $s_1 - 1$ столбцам подматрицы A_{11} . Вычтем в матрице A из последних $s_1 - 1$ столбцов первые $s_1 - 1$ столбцы. В результате подматрица A_{12} преобразуется в нулевую подматрицу:

$$|A| = \begin{vmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{vmatrix} = \begin{vmatrix} A_{11} & 0 \\ A_{21} & A'_{22} \end{vmatrix} = |A'_{22}|. \quad (1.18)$$

Выражение (1.18) означает, что $\det A = \det A_{11} \det A'_{22} = \det A'_{22} \pmod{2}$, так как $\det A_{11} \equiv 1 \pmod{2}$. А подматрица A'_{22} имеет размеры $(n - s_1) \times (n - s_1)$. В ней остались $s_2 - 1 - s_1$ столбцов, каждый из которых содержит по s_1 единиц, и $s_1 - 1$ столбцов, каждый из которых содержит по $s_2 - s_1$ единиц. Получаем последовательный переход:

$$\det A(s_1, s_2) = \det A(s'_1, s'_2),$$

где $s'_1 = \min\{s_1, s_2 - s_1\}$; $s'_2 = \max\{s_1, s_2 - s_1\}$; $n' = n - s_1 = s'_1 + s'_2 - 2 = s_2 - 2$.

Вследствие конечности чисел s_1 и s_2 эти действия в итоге приводят к образованию одной из матриц: $A(1, k)$ или $A(0, k)$. Первую матрицу получим, если $\text{НОД}(s_1, s_2) = 1$. Она тождественна E_{k-1} , поэтому $\det A(s_1, s_2) \equiv 1 \pmod{2}$. Вторую матрицу получим, если $\text{НОД}(s_1, s_2) = d > 1$. В ней присутствуют столбцы с нулями, поэтому $\det A(s_1, s_2) \equiv 0 \pmod{2}$, что и требовалось доказать. Покажем это на нашем примере:

$$\begin{aligned}
 A(5,8) &= \left(\begin{array}{ccccc|ccccc}
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
 \hline
 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1
 \end{array} \right) \rightarrow \\
 &\rightarrow \left(\begin{array}{ccccc|ccccc}
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 \hline
 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1
 \end{array} \right) \rightarrow \\
 &\rightarrow \left(\begin{array}{ccccc}
 1 & 0 & 0 & 0 & 1 & 0 \\
 1 & 1 & 0 & 0 & 1 & 1 \\
 1 & 1 & 1 & 0 & 1 & 1 \\
 0 & 1 & 1 & 1 & 1 & 1 \\
 0 & 0 & 1 & 1 & 1 & 1 \\
 0 & 0 & 0 & 1 & 0 & 1
 \end{array} \right) = A(3,5) \rightarrow A(2,3) = \left(\begin{array}{ccc}
 1 & 0 & 1 \\
 1 & 1 & 1 \\
 0 & 1 & 1
 \end{array} \right) \rightarrow \left(\begin{array}{ccc}
 1 & 0 & 0 \\
 1 & 1 & 0 \\
 0 & 0 & 1
 \end{array} \right).
 \end{aligned}$$

(1.19)

Детерминант последней матрицы равен $1 \pmod{2}$, что соответствует соотношению между s_1 и s_2 , а именно $\text{НОД}(5,8)=1$.

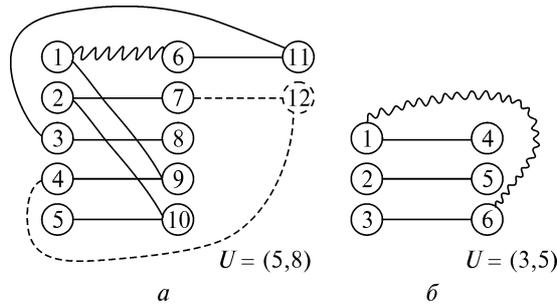


Рис. 1.7

Рассмотрим теперь NM -граф $G = (Y, U)$, где $U = (5, 8)$, а $n = 11$, изображенный на рис. 1.7, а. Граф отображает свойство смежности для двух вершин, соответствующих двум переменным, для которых $y_i \equiv y_j \pmod{2}$ из системы (1.21).

Единственное ребро (волнистое) отображает соотношение $y_1 + y_6 \equiv 1 \pmod{2}$ или $y_1 \neq y_6$. В графе 11 вершин ($n = s_1 + s_2 - 2$). По теореме [6] NM -граф связан, если $u_1 + u_2 \leq n + 1$. Но у нас $5 + 8 = 13 > 11 + 1$. Если добавить вершину 12 и соответствующие ей два ребра (на рис.1.7 они обозначены пунктиром), то получим связный граф. Это означает, что исходный граф несвязный и состоит из двух компонент. Одна компонента содержит вершину $n + 1 - s_1 = s_2 - 1$ (на рис. 1.7 это 7), а вторая — вершину $n + 1 - s_2 = s_1 - 1$ (на рис. 1.7 это 4). Одна из этих компонент разделена волнистым ребром на две части: одна часть соответствует значениям переменных $y_i \equiv 0 \pmod{2}$, а другая часть — переменным $y_j \equiv 1 \pmod{2}$. Определить эти значения можно из первого и s_2 -го уравнений системы (1.21):

$$\sum_{i=1}^{s_1} y_i \equiv 1 \pmod{2}; \quad \sum_{j=1}^{s_2} y_j \equiv 0 \pmod{2}. \quad (1.22)$$

Систему (1.20) можно упростить. Если подставить в нее значения из (1.21), то придем к системе

$$\left. \begin{array}{l} y_1 + y_2 + y_3 + y_4 + y_5 \quad \cdot \equiv 1 \\ \cdot \quad y_2 + y_3 + y_4 + y_5 + y_6 \equiv 0 \\ y_1 + y_2 + y_3 \quad \cdot \quad \cdot \quad \cdot \equiv 0 \\ \cdot \quad y_2 + y_3 + y_4 \quad \cdot \quad \cdot \equiv 0 \\ \cdot \quad \cdot \quad y_3 + y_4 + y_5 \quad \cdot \equiv 0 \\ \cdot \quad \cdot \quad \cdot \quad y_4 + y_5 + y_6 \equiv 0 \end{array} \right\} \pmod{2}. \quad (1.23)$$

Если в системе (1.23) переместить две верхние строки вниз, то получим систему уравнений типа (1.20), но для $s'_1 = 3$ и $s'_2 = 5$. При этом единица в правой части находится в первой строке уравнений для s'_2 . Тем самым доказан следующий результат.

Лемма 1.3. Систему уравнений (1.20) для образующих $S = (s_1, s_2)$ можно свести к системе уравнений для $S' = (s'_1, s'_2)$, где $s'_1 = \min\{s_1, s_2 - s_1\}$, а $s'_2 = \max\{s_1, s_2 - s_1\}$.

Тот факт, что уравнение с единицей в правой части перемещается вниз, отмечаем подчеркиванием второго шаблона, т. е. $S(s_1 s_2) \rightarrow S'(s'_1, \underline{s'_2})$ или $(s_1 s_2) \rightarrow (\underline{s'_1}, s'_2)$. Если единица после ряда таких переходов возвращается в первую строку, то подчеркивание убираем.

Если в системе (1.23) сложить две первые строки, затем к i -й строке добавить $(i + 1)$ -ю ($3 \leq i \leq n - 1$), то получим соотношение: $y_1 \neq y_6; y_1 = y_4; y_2 = y_5; y_3 = y_6$. Этим значениям соответствует MM -граф на рис. 1.7, б. Из первых строк системы (1.23) находим

$$y_1 \neq y_2; y_2 = y_3; y_1 + y_2 + y_3 = 0 \text{ или } y_1 = 0; y_2 = y_3 \equiv 1 \pmod{2}.$$

Подставляя эти данные в исходный граф на рис. 1.7, а, получаем решение $Y = (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$.

Таким образом, с помощью леммы 1.3 можно уменьшить размер исходной системы уравнений до такого уровня, когда решение становится очевидным. Затем это решение подставляем в MM -граф исходной системы и определяем полное решение. Так как количество указанных переходов конечно, то в результате придем к системе уравнений для таких шаблонов $(2, s_2)$ или $(s_1, s_1 + 1)$. Каждый из этих случаев, в свою очередь, распадается на два в зависимости от наличия подчеркивания второго шаблона. Рассмотрим каждый из них.

Пусть $S = (2, s_2)$. Тогда система (1.20) приобретает вид

$$\begin{aligned} y_1 + y_2 &\equiv 1 \pmod{2}; \\ y_i + y_{i+1} &\equiv 0 \pmod{2} \quad (i = 2, 3, \dots, s_2 - 1); \\ \sum_{i=1}^{s_2} y_i &\equiv 0 \pmod{2}. \end{aligned} \quad (1.24)$$

Очевидно, что s_2 — нечетное число, иначе в изначальной системе s_1 и s_2 имели бы общий делитель 2, что невозможно. Поэтому

$y_1 \neq y_2 \pmod{2}$, а остальные $y_i = y_2 \ (i > 2)$. Из последнего уравнения получаем $y_1 = 0$, остальные $y_i = 1 \ (i > 2)$.

Пусть $S = (2, s_2)$. Тогда система (1.20) имеет вид

$$y_i + y_{i+1} \equiv 0 \pmod{2} \quad (i = 1, 2, \dots, s_2 - 1);$$

$$\sum_{i=1}^{s_2} y_i \equiv 1 \pmod{2}. \quad (1.25)$$

Здесь все $y_i = y_1 \ (i = 2, 3, \dots, s_2)$. А из последнего уравнения получаем $y_i \equiv 1 \pmod{2} \quad (1 \leq i \leq s_2)$.

Пусть $S = (s_1, s_1 + 1)$. Тогда система (1.20) имеет вид

$$\sum_{i=1}^{s_1} y_i \equiv 1 \pmod{2}; \quad \sum_{i=j}^{j+s_1-1} y_i \equiv 0 \pmod{2} \quad (j = 2, 3, \dots, s_1);$$

$$\sum_{i=j}^{j+s_1} y_i \equiv 0 \pmod{2}. \quad (1.26)$$

Вычитая из уравнений, входящих в третью сумму, уравнения второй суммы, получаем решение $y_1 = y_2 = \dots = y_{s_1-1} \equiv 0 \pmod{2}$. Из первого уравнения, входящего в первую сумму, находим $y_{s_1} \equiv 1 \pmod{2}$.

Из первого уравнения, входящего во вторую сумму, определяем $y_{s_1+1} \equiv 1 \pmod{2}$. Остальные $y_i \equiv 0 \pmod{2} \quad (i > s_1 + 1)$.

Пусть $S = (s_1, s_1 + 1)$. Тогда система (1.20) приобретает вид

$$\sum_{i=j}^{j+s_1-1} y_i \equiv 0 \pmod{2} \quad (j = 1, 2, \dots, s_1);$$

$$\sum_{i=1}^{s_1+1} y_i \equiv 1 \pmod{2} \quad (j = 2, 3, \dots, s_1);$$

$$\sum_{i=j}^{j+s_1} y_i \equiv 0 \pmod{2} \quad (j = 2, 3, \dots, s_1 - 1). \quad (1.27)$$

Если из уравнений, входящих в третью сумму, вычесть $s_1 - 1$ нижних уравнений, входящих в первую сумму, то получим решение $y_1 = 1; y_2 = y_3 = \dots = y_{s_1-1} \equiv 0 \pmod{2}$. Из первого уравнения следует, что $y_{s_1} = 1$, а из второго — $y_{s_1+1} = 1$. Остальные $y_i \equiv 0 \pmod{2}$.

1.5. МНОГОЦВЕТНЫЕ ДВОЙСТВЕННЫЕ ШАБЛОНЫ

Если цветов более двух, или $K > 2$, то шаблоны могут быть окрашены не единственным цветом. Будем обозначать каждый шаблон последовательностью цветов $s = (q_1, q_2, \dots, q_r)$, где r — длина шаблона.

Определение 1.5. Назовем шаблон двойственным к s , если он имеет обратную последовательность цветов $\bar{s} = (q_r, q_{r-1}, \dots, q_1)$.

Двойственный шаблон можно получить, если его перевернуть в пространстве. Двойственные положения шаблонов могут играть существенную роль в построении образов. Среди них встречаются самодвойственные, когда $s = \bar{s}$.

Поскольку наложение шаблонов предполагает операцию сложения цветов, то в такой записи шаблоны можно умножать на скалярную величину $\lambda \neq 0$, при этом $\lambda s = (\lambda q_1, \lambda q_2, \dots, \lambda q_r) \pmod{K}$.

Прежде всего, возникает вопрос, может ли один шаблон (вместе с двойственным положением) образовывать базис только наложением самого на себя? Очевидно, что такой шаблон не может быть самодвойственным.

Рассмотрим сначала шаблон из двух клеток $s_1 = \{q_1, q_2\}$, где $q_1, q_2 \in Q \setminus \{0\}$. Двойственный шаблон $s_2 = \{q_2, q_1\}$. Для построения образа $b_i \equiv 1 \pmod{K}$, $b_i \equiv 0 \pmod{K}$ ($i > 1$) необходимо решить систему уравнений

$$\left. \begin{aligned} x_1^{(1)}q_1 + x_1^{(2)}q_2 &= 1 \\ x_1^{(1)}q_2 + x_1^{(2)}q_1 &= 0 \end{aligned} \right\} \pmod{K}. \quad (1.28)$$

Здесь $x_1^{(1)}$ и $x_1^{(2)}$ означают количество первых (вторых) шаблонов, метка которых находится в первой клетке строки. Система имеет решение, если детерминант системы

$$\det = q_1^2 - q_2^2 \neq 0 \pmod{K}. \quad (1.29)$$

Таким образом, если $q_1^2 - q_2^2 \neq 0 \pmod{K}$, то существуют такие шаблоны длиной 2 с соответствующей раскраской, которые позволяют наложением на самого себя получать любую клетку строки с окраской 1. Путем сдвига можно получить решение для базиса системы типа (1.2). Легко убедиться, что для $K = 2, 3$ таких шаблонов не существует. Для произвольных простых K множество шаблонов имеет вид (i, j) , где $i = 1, 2, \dots, K - 1$, а $j \neq K - i$. Тогда решение системы (1.28) имеет вид

$$\left. \begin{aligned} x_1^{(1)} &= q_1 (q_1^2 - q_2^2)^{-1} \\ x_1^{(2)} &= -q_2 (q_1^2 - q_2^2)^{-1} \end{aligned} \right\} \text{mod } K. \quad (1.30)$$

Выражение d^{-1} равно решению сравнения $td \equiv 1 \pmod{K}$, если оно существует. Для составных K этого недостаточно, так как возможны случаи, когда условия (1.29) не выполняются.

Пример 1.6. Пусть $K = 5$. Тогда число всех пар шаблонов, которые существуют, равно 6 (белая краска или 0 для шаблона отсутствует): (1,2), (1,3), (1,4), (2,3), (2,4), (3,4). Из них две пары не удовлетворяют условию (1.29), так как $1^2 - 4^2 = -15 \equiv 0 \pmod{5}$ и $2^2 - 3^2 = -5 \equiv 0 \pmod{5}$. Остальные пары образуют базис с помощью наложения на себя, их число равно четыре: $S_1 = (1, 2)$, $S_2 = (1, 3)$, $S_3 = (2, 4)$ и $S_4 = (3, 4)$. В частности:

а) $S_1 = (1, 2)$.

Детерминант системы (1.28) равен $1^2 - 2^2 = -3 \equiv 2 \pmod{5}$.

$$x_1^{(1)} = 1 \cdot (2)^{-1} = 3 \pmod{5}; \quad x_1^{(2)} = -2 \cdot (2)^{-1} = -1 \equiv 4 \pmod{5}.$$

Проверка: $3(1, 2) + 4(2, 1) = (11, 10) \equiv (1, 0) \pmod{5}$.

б) $S_2 = (1, 3)$.

Детерминант системы (1.28) равен $1^2 - 3^2 = -8 \equiv 2 \pmod{5}$.

$$x_1^{(1)} = 1 \cdot (2)^{-1} = 3 \pmod{5}; \quad x_1^{(2)} = -3 \cdot (2)^{-1} \equiv 1 \pmod{5}.$$

Проверка: $3(1, 3) + (3, 1) = (6, 10) \equiv (1, 0) \pmod{5}$.

в) $S_3 = (2, 4)$.

Детерминант системы (1.28) равен $2^2 - 4^2 = -12 \equiv -2 \pmod{5}$.

$$x_1^{(1)} = 2 \cdot (-2)^{-1} = -1 \equiv 4 \pmod{5}; \quad x_1^{(2)} = -4 \cdot (-2)^{-1} \equiv 2 \pmod{5}.$$

Проверка: $4(2, 4) + 2(4, 2) = (16, 20) \equiv (1, 0) \pmod{5}$.

г) $S_4 = (3, 4)$.

Детерминант системы (1.28) равен $3^2 - 4^2 = -7 \equiv +3 \pmod{5}$.

$$x_1^{(1)} = 3 \cdot 3^{-1} \equiv 1 \pmod{5}; \quad x_1^{(2)} = -4 \cdot (-2)^{-1} \equiv 2 \pmod{5}.$$

Проверка: $(3, 4) + 2(4, 3) = (11, 10) \equiv (1, 0) \pmod{5}$.

На рис.1.8 показано наложение двойственных шаблонов S_3 и S_4 самих на себя, подтверждающее приведенные результаты.

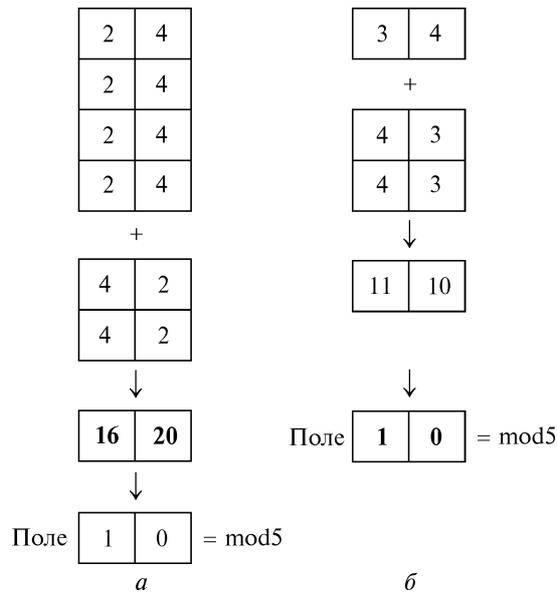


Рис. 1.8

Однако для шаблонов большей длины аналогичный результат не возможен.

Лемма 1.3. Шаблон $s_1 = (q_1, q_2, \dots, q_s)$ для $s > 2$ не может представлять базис наложением на себя.

Для доказательства этого запишем систему (1.28) для искомого базиса:

$$\left. \begin{aligned} x_1^{(1)}q_1 + x_1^{(2)}q_s &\equiv 1 \\ x_1^{(1)}q_2 + x_1^{(2)}q_{s-1} &\equiv 0 \\ \dots\dots\dots & \\ x_1^{(1)}q_{s-1} + x_1^{(2)}q_2 &\equiv 0 \\ x_1^{(1)}q_s + x_1^{(2)}q_1 &\equiv 0 \end{aligned} \right\} \text{mod } K. \quad (1.31)$$

Пусть $s \equiv 1 \pmod{2}$. Рассмотрим уравнение с номером $\lambda = \frac{s+1}{2}$:

$$x_1^{(1)}q_\lambda + x_1^{(2)}q_\lambda \equiv 0 \pmod{K}.$$

Так как $q_\lambda \not\equiv 0 \pmod{K}$, то $x_1^{(1)} + x_1^{(2)} \equiv 0 \pmod{K}$. Подставляя $x_1^{(2)} \equiv -x_1^{(1)} \pmod{K}$ в уравнения (1.30), приходим к равенствам

$$\left. \begin{aligned} x_1^{(1)}(q_1 - q_s) &\equiv 1 \\ x_1^{(1)}(q_1 - q_s) &\equiv 0 \end{aligned} \right\} \pmod{K},$$

что невозможно.

Пусть теперь $s \equiv 0 \pmod{2}$. Сложим в (1.30) первое и второе уравнения:

$$(x_1^{(1)} + x_1^{(2)})(q_1 + q_s) \equiv 1 \pmod{K}.$$

Отсюда вытекает, что $x_1^{(1)} + x_1^{(2)} \not\equiv 0 \pmod{K}$. Рассмотрим теперь уравнения с номерами $\lambda = \frac{s}{2}$ и $\lambda + 1$:

$$\left. \begin{aligned} x_1^{(1)}q_\lambda + x_1^{(2)}q_{\lambda+1} &\equiv 0 \\ x_1^{(1)}q_{\lambda+1} + x_1^{(2)}q_\lambda &\equiv 0 \end{aligned} \right\} \pmod{K}. \quad (1.32)$$

Если сложить эти равенства, то получим

$$(x_1^{(1)} + x_1^{(2)})(q_\lambda + q_{\lambda+1}) \equiv 0 \pmod{K}.$$

Учитывая предыдущий вывод, имеем $q_{\lambda+1} = -q_\lambda \pmod{K}$. Подставляя это выражение в любое уравнение (1.32), получаем $x_1^{(1)} = x_1^{(2)} \pmod{K}$.

Подставим теперь эти значения в первое и последнее уравнения системы (1.31):

$$\left. \begin{aligned} x_1^{(1)}(q_1 + q_s) &\equiv 1 \\ x_1^{(1)}(q_1 + q_s) &\equiv 0 \end{aligned} \right\} \pmod{K}.$$

Опять пришли к абсурду, что подтверждает справедливость леммы 1.3.

Очевидно, что лемма 1.3 справедлива и для других единиц в правой части системы (1.31), за исключением одного случая, когда решение этой системы существует.

Лемма 1.4. Пусть $s \equiv K \equiv 1 \pmod{2}$ и задан шаблон $s_1 = (q_1, q_2, \dots, q_s)$. Обозначим $\lambda = \frac{s+1}{2}$. Система (1.31) имеет решение для $b_\lambda \equiv 1 \pmod{K}$, $b_i \equiv 0 \pmod{K}$ ($i \neq \lambda$), если:

- а) $q_i + q_{s+1-i} \equiv 0 \pmod{K}$ ($i = 1, 2, \dots, \lambda - 1$);
- б) $\text{НОД}(q_\lambda, K) = 1$.

Действительно, если совместим шаблон и его двойственный, то получим в s позициях строки $(0, 0, \dots, 2q_\lambda, 0, \dots, 0)$. Будем считать это новым шаблоном. Необходимо сложить несколько таких шаблонов, чтобы получить единицу в позиции под номером λ , т. е. решить уравнение

$$2q_\lambda \cdot x \equiv 1 \pmod{K}.$$

В силу условия б) и нечетности K существует элемент, обратный к $2q_\lambda$, и тогда $x \equiv (2q_\lambda)^{-1} \pmod{K}$.

Рассмотрим теперь другой вопрос: может ли существовать один шаблон, который вместе с двойственным образует базис при произвольном наложении на поле?

Для шаблонов длиной 2 ответ на этот вопрос положительный, так как это выполнимо даже с помощью наложения такого шаблона на себя.

Пусть $s > 2$. Рассмотрим произвольный шаблон $s_1 = (q_1, q_2, \dots, q_{s-1}, q_s)$ и ему двойственный $s_2 = (q_s, q_{s-1}, \dots, q_2, q_1)$.

Число положений в строке длиной n для каждого шаблона равно $n + 1 - s$. Так как число уравнений равно числу клеток строки, то для однозначности решения системы (1.2) число переменных должно быть равным числу уравнений, т. е. $2(n + 1 - s) = n$. Отсюда

$$s = \frac{n}{2} + 1. \tag{1.33}$$

Таким образом, для любого шаблона единственный базис может существовать только при условии (1.33), при этом строка поля должна содержать четное число клеток.

Составим соответствующую систему уравнений для определения базиса. При этом переменные для шаблона s_1 обозначим x_i , а двойственные переменные — y_i ($i \geq 1$):

Доказательство. Запишем матрицу (1.35) для $s = 3$, размерность которой равна 4:

$$A = \begin{vmatrix} q_1 & 0 & q_3 & 0 \\ q_2 & q_1 & q_2 & q_3 \\ q_3 & q_2 & q_1 & q_2 \\ 0 & q_3 & 0 & q_1 \end{vmatrix}. \quad (1.37)$$

Вычтем из первого столбца третий, затем добавим к третьей строке первую:

$$\det A = \begin{vmatrix} q_1 - q_3 & 0 & q_3 & 0 \\ 0 & q_1 & q_2 & q_3 \\ q_3 - q_1 & q_2 & q_1 & q_2 \\ 0 & q_3 & 0 & q_1 \end{vmatrix} = \begin{vmatrix} q_1 - q_3 & 0 & q_3 & 0 \\ 0 & q_1 & q_2 & q_3 \\ 0 & q_2 & q_1 + q_3 & q_2 \\ 0 & q_3 & 0 & q_1 \end{vmatrix},$$

$$\det A = (q_1 - q_3) \begin{vmatrix} q_1 & q_2 & q_3 \\ q_2 & q_1 + q_3 & q_2 \\ q_3 & 0 & q_1 \end{vmatrix}.$$

Вычтем из первого столбца третий и добавим первую строку к третьей:

$$\det A = (q_1 - q_3) \begin{vmatrix} q_1 - q_3 & q_2 & q_3 \\ 0 & q_1 + q_3 & q_2 \\ q_3 - q_1 & 0 & q_1 \end{vmatrix} = (q_1 - q_3) \begin{vmatrix} q_1 - q_3 & q_2 & q_3 \\ 0 & q_1 + q_3 & q_2 \\ 0 & q_2 & q_1 + q_3 \end{vmatrix}.$$

Окончательно, $\det A \equiv (q_1 - q_3)^2 [(q_1 + q_3)^2 - q_2^2] \pmod{K}$. Если $\det A \not\equiv 0 \pmod{K}$, то должны выполняться условия а), б) теоремы 1.3.

Зная значения $\det A$, можно найти значения x_i и y_i ($i = 1, 2$) системы (1.34):

$$x_1 = \frac{q_1(q_1 + q_3) - q_2^2}{(q_1 - q_3)[(q_1 + q_3)^2 - q_2^2]} \pmod{K};$$

$$x_2 = -\frac{q_1 q_2}{(q_1 - q_3)[(q_1 + q_3)^2 - q_2^2]} \pmod{K};$$

$$y_1 = \frac{q_2^2 - q_3(q_1 + q_3)}{(q_1 - q_3)[(q_1 + q_3)^2 - q_2^2]} \pmod{K};$$

$$y_2 = \frac{q_2 q_3}{(q_1 - q_3)[(q_1 + q_3)^2 - q_2^2]} \pmod{K}. \quad (1.38)$$

Условия теоремы 1.3 могут не выполняться для составного K . Если для $K = 5$ существует 16 допустимых раскрасок шаблонов, которые образуют базис, то для $K = 4$ таких шаблонов только 2: $s_1 = (1, 2, 2)$ и $s_2 = (2, 2, 3)$.

Пример 1.7 (рис. 1.9):

а) рассмотрим шаблон $s_1 = (1, 2, 2)$ для $K = 4$. Вычислим знаменатель для (1.38):

$$(q_1 - q_3)[(q_1 + q_3)^2 - q_2^2] \pmod{4} =$$

$$= -1 \cdot [3^2 - 2^2] \equiv -1 \pmod{4} \equiv 3 \pmod{4}.$$

Тогда

$$x_1 = [1 \cdot (1+2) - 2^2] \cdot 3^{-1} \equiv 1 \pmod{4}; \quad x_2 \equiv -\frac{2}{3} \pmod{4} \equiv 2 \pmod{4};$$

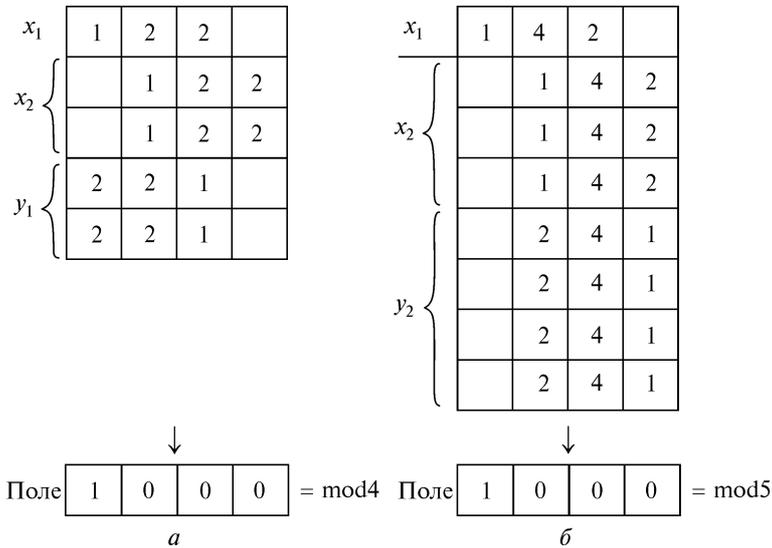


Рис. 1.9

$$y_1 = [2^2 - 2 \cdot (1+2)]3^{-1} \equiv 2 \pmod{4}; \quad y_2 = -2 \cdot \frac{2}{3} \equiv 0 \pmod{4};$$

б) пусть $s_1 = (1, 4, 2)$ и $K = 5$. Определим знаменатель для (1.38):

$$-1 \cdot [(1+2)^2 - 4^2] \equiv 2 \pmod{5}.$$

Тогда

$$x_1 = \frac{1 \cdot (1+2) - 4^2}{2} \equiv \frac{-3}{2} \pmod{5} \equiv 1 \pmod{5}; \quad x_2 \equiv \frac{-4}{2} \equiv 3 \pmod{5};$$

$$y_1 = \frac{4^2 - 2 \cdot (1+2)}{2} = \frac{10}{2} \equiv 0 \pmod{5}; \quad y_2 = \frac{4 \cdot 2}{2} \equiv 4 \pmod{5}.$$

1.6. ЛИНЕЙНАЯ СИСТЕМА ДЛЯ ПРОИЗВОЛЬНЫХ ЦВЕТНЫХ ШАБЛОНОВ

Использование шаблонов в количестве более одного приводит к новым осложнениям при решении поставленной задачи. Если раньше использовался один шаблон, то его двойственное положение расценивалось как второй шаблон, если только он не был самодвойственным. Если взять больше шаблонов, то теперь каждый самодвойственный шаблон выступает как один шаблон, а остальные — как два. Это приводит к образованию принципиально разных систем уравнений, а следовательно, к различным способам их решения.

Определение 1.6. Два шаблона s_1 и s_2 называются кратными, если существует некоторое целое число λ такое, что $s_1 = \lambda s_2$.

Очевидно, что кратные шаблоны могут заменять друг друга при наложении на поле, т. е. оба шаблона равносильны одному.

Рассмотрим два некратных шаблона $s_1 = (\beta_1, \beta_2, \dots, \beta_k)$ и $s_2 = (\gamma_1, \gamma_2, \dots, \gamma_l)$, где $\beta_i, \gamma_j \in \mathcal{Q} \setminus \{0\}$ ($1 \leq i \leq k; 1 \leq j \leq l; k \leq l$). Возможны четыре случая.

Случай 1. Оба шаблона самодвойственные. Тогда систему уравнений составляют как для двух разных шаблонов. Чтобы решение системы уравнений было единственным, для них должно выполняться условие

$$n + 2 = k + l. \tag{1.39}$$

Рассмотрим всевозможные значения k и l , для которых существует единственное решение системы уравнений. Если $k = l = 2$,

то $n = 2$ и определитель системы равен $\begin{vmatrix} \beta_1 & \gamma_1 \\ \beta_1 & \gamma_1 \end{vmatrix} = 0$, так как обе строки совпадают.

Теорема 1.4. Определитель системы уравнений типа (1.2) для двух самодвойственных шаблонов, удовлетворяющих условию (1.39), с параметрами $k = 2$ и с произвольным $l \geq 3$ равен

$$\beta^{l-1} \sum_{i=1}^l (-1)^{i+1} \gamma_{l+1-i}, \text{ если } l \equiv 1(\text{mod } 2)$$

и 0, если $l \equiv 0(\text{mod } 2)$. (1.40)

Доказательство. Так как при таких параметрах $n = l$, то определитель соответствующей системы будет иметь $l - 1$ столбцов для первого шаблона и один столбец для второго шаблона. Первый шаблон равен $s_1 = (\beta_1, \beta_1)$, поэтому определитель имеет вид

$$\begin{vmatrix} \beta_1 & 0 & \dots & \gamma_1 \\ \beta_1 & \beta_1 & \dots & \gamma_2 \\ 0 & \beta_1 & \dots & \gamma_3 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \beta_1 & \beta_1 & \gamma_2 \\ 0 & 0 & \dots & \beta_1 & \gamma_1 \end{vmatrix}. \quad (1.41)$$

Вычтем из второй строки в (1.41) первую и раскроем определитель по первому столбцу. Получаем исходный определитель размера $l - 1$, а в последнем столбце — элемент $\gamma_2 - \gamma_1$. Продолжая эти операции, получаем в итоге выражение (1.40). Но так как $\gamma_i = \gamma_{l+1-i}$ ($i > 0$), то для l четного получим симметричные элементы с противоположными знаками, что приведет к их взаимному уничтожению.

Таким образом, для четных значений l система имеет зависимые уравнения, и поскольку n уменьшать нельзя (второй шаблон не помещается на поле), то задача неразрешима.

Пример 1.8. Рассмотрим шаблоны $s_1 = (2, 2)$, $s_2 = (1, 3, 2, 3, 1)$ для $K = n = 5$ (рис. 1.10).

Составляем соответствующую систему уравнений для определения базиса, т. е. с правыми частями $b_1 = 1$, а $b_i = 0$ ($i = 2, 3, 4, 5$). Поскольку размерность второго шаблона равна n , его переменным соответствует один столбец. При этом переменные для первого шаблона обозначаем x_i ($i = 1, 2, 3, 4$), а для второго — x_5 :

$$\left. \begin{array}{l} 2x_1 + + + + x_5 = 1 \\ 2x_1 + 2x_2 + + + 3x_5 = 0 \\ + 2x_2 + 2x_3 + + 2x_5 = 0 \\ + + 2x_3 + 2x_4 + 3x_5 = 0 \\ + + + 2x_4 + x_5 = 0 \end{array} \right\} \pmod{5}. \quad (1.42)$$

Обозначаем матрицу системы (1.42) как A , а матрицы для переменных — A_i ($1 \leq i \leq 5$). Тогда

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 2 & 2 & 0 & 0 & 3 \\ 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 & 3 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 3 \\ 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 & 3 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 2 & 1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 3 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 & 3 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 2 & 0 & 1 & 0 & 1 \\ 2 & 2 & 0 & 0 & 3 \\ 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 2 & 0 & 0 & 1 & 1 \\ 2 & 2 & 0 & 0 & 3 \\ 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$A_5 = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 2 & 2 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 \end{pmatrix}.$$

x_1 {

2	2			
2	2			
		2	2	
		2	2	
		2	2	
			2	2
			2	2
			2	2
			2	2
1	3	2	3	1
1	3	2	3	1

↓

1	0	0	0	0
---	---	---	---	---

mod 5

При вычислении определителей этих матриц последовательно вычитаем верхние строки из

Рис. 1.10

нижних. В результате получаем следующие значения:

$$\det A = 2^4 (1 - 3 + 2 - 3 + 1) = -2 \pmod{5},$$

$$\det A_1 = 2^3 (1 - 3 + 2 - 3) = -24 = 1 \pmod{5},$$

$$\det A_2 = 2^3 (1 - 3 + 2) = 0 \pmod{5}, \det A_3 = 2^3 (1 - 3) = 4 \pmod{5},$$

$$\det A_4 = -2^3 (1) = 2 \pmod{5}, \det A_5 = 2^4 = 1 \pmod{5}.$$

Соответствующие значения переменных равны

$$x_i = \frac{\det A_i}{\det A} \text{ или } x_1 = 2, x_2 = 0, x_3 = 3, x_4 = 4, x_5 = 2.$$

Проверяем это решение на шаблонах.

Аналогично строится базис для других единиц в правой части системы (1.42).

Рассмотрим, как строить базис для $b_3 = 0$. Матрица A будет такая же, а матрицы A_i ($i = 1, 2, 3, 4, 5$) имеют следующий вид:

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 3 \\ 1 & 2 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 & 3 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 3 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 & 3 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix}, A_3 = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 2 & 2 & 0 & 0 & 3 \\ 0 & 2 & 1 & 0 & 2 \\ 0 & 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 2 & 2 & 0 & 0 & 3 \\ 0 & 2 & 2 & 1 & 2 \\ 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, A_5 = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 \end{pmatrix}.$$

Отсюда

$$\det A_1 = -8 = 2 \pmod{5}, \det A_2 = -16 = -1 \pmod{5}, \det A_3 = -1 \pmod{5},$$

$$\det A_4 = -2^3 = 2 \pmod{5}, \det A_5 = 2^4 = 1 \pmod{5}$$

$$\text{или } x_1 = 4, x_2 = 3, x_3 = 3, x_4 = 4, x_5 = 2.$$

Проверяем полученный результат на шаблонах (рис. 1.11).

Случай 2. Из двух шаблонов только первый самодвойственный. Тогда систему уравнений составляют как для трех разных шаблонов. Чтобы решение системы уравнений было единственным, для них согласно (1.12) должно выполняться условие

$$2n + 3 = k + 2l. \quad (1.43)$$

Рассмотрим всевозможные значения k и l , для которых существует единственное решение системы уравнений (1.43). Очевидно, что $k \equiv 1 \pmod{2}$. Из условия $n \geq l$ следует, что $n = (k + 2l - 3)/2 \geq l$ или $k \geq 3$. Если $k < 3$, то число уравнений всегда больше числа переменных, и решения системы уравнений не существует. Для $k = 3$ следует $n = l$, поэтому два последних столбца в матрице отведены параметрам второго шаблона. Например, для $k = 3$ (а $n = l = 4$) получаем систему с матрицей четвертого порядка, где первые два столбца занимают параметры первого самодвойственного шаблона, а последние столбцы — параметры второго шаблона и двойственного ему, т. е.

2	2			
2	2			
2	2			
2	2			
	2	2		
	2	2		
	2	2		
		2	2	
		2	2	
		2	2	
			2	2
			2	2
			2	2
1	3	2	3	1
1	3	2	3	1

$$\downarrow$$

0	0	1	0	0
---	---	---	---	---

mod 5

Рис. 1.11

$$A = \begin{pmatrix} \beta_1 & 0 & \gamma_1 & \gamma_4 \\ \beta_2 & \beta_1 & \gamma_2 & \gamma_3 \\ \beta_1 & \beta_2 & \gamma_3 & \gamma_2 \\ 0 & \beta_1 & \gamma_4 & \gamma_1 \end{pmatrix}.$$

Чтобы вычислить определитель этой матрицы, вычтем первую строку из третьей, а четвертую из второй. В результате получаем

$$A = \begin{pmatrix} \beta_1 & 0 & \gamma_1 & \gamma_4 \\ \beta_2 & 0 & \gamma_2 - \gamma_4 & \gamma_3 - \gamma_1 \\ 0 & \beta_2 & \gamma_3 - \gamma_1 & \gamma_2 - \gamma_4 \\ 0 & \beta_1 & \gamma_4 & \gamma_1 \end{pmatrix}.$$

Отсюда

$$\det A = \beta_1^2 [(\gamma_2 - \gamma_4)^2 - (\gamma_3 - \gamma_1)^2] + \beta_2^2 (\gamma_1^2 - \gamma_4^2) + 2\beta_1\beta_2 (\gamma_3\gamma_4 - \gamma_1\gamma_2).$$

Существуют параметры для двух шаблонов, при которых этот определитель отличен от нуля, тогда система имеет решение.

Пример 1.9. Рассмотрим шаблоны $s_1 = (1, 2, 1)$, $s_2 = (1, 3, 4, 4)$ для $K = 5$ и $n = 4$. Для первого шаблона имеем 2 переменные, а для второго (так как он не является самодвойственным) — тоже две переменные. Строим соответствующую систему уравнений для базиса решений, т. е. с правыми частями $b_i = 1$, а $b_i = 0$ ($i = 2, 3, 4, 5$):

$$\left. \begin{aligned} x_1 + x_3 + 4x_4 &= 1 \\ 2x_1 + x_2 + 3x_3 + 4x_4 &= 0 \\ x_1 + 2x_2 + 4x_3 + 3x_4 &= 0 \\ x_2 + 4x_3 + x_4 &= 0 \end{aligned} \right\} \text{mod } 5. \quad (1.44)$$

Матрица A системы (1.44) и матрицы A_i для переменных имеют вид

1	2	1	
1	2	1	
1	2	1	
1	2	1	
	1	2	1
	1	2	1
1	3	4	4
1	3	4	4
1	3	4	4
1	3	4	4
4	4	3	1
4	4	3	1
			↓
1	0	0	0

mod 5

$$A = \begin{pmatrix} 1 & 0 & 1 & 4 \\ 2 & 1 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 0 & 1 & 4 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 1 & 4 \\ 0 & 1 & 3 & 4 \\ 0 & 2 & 4 & 3 \\ 0 & 1 & 4 & 1 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} 1 & 1 & 1 & 4 \\ 2 & 0 & 3 & 4 \\ 1 & 0 & 4 & 3 \\ 0 & 0 & 4 & 1 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 1 & 0 & 1 & 4 \\ 2 & 1 & 0 & 4 \\ 1 & 2 & 0 & 3 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & 3 & 0 \\ 1 & 2 & 4 & 0 \\ 0 & 1 & 4 & 0 \end{pmatrix}.$$

В результате получаем значения
 $\det A = -1(\text{mod } 5)$, $\det A_1 = 1(\text{mod } 5)$,
 $\det A_2 = -2(\text{mod } 5)$,

$\det A_3 = 1(\text{mod } 5)$, $\det A_4 = -2(\text{mod } 5)$

или $x_1 = 4$, $x_2 = 2$, $x_3 = 4$, $x_4 = 2$.

Проверяем найденные значения на шаблонах (рис. 1.12).

Рис. 1.12

Случай 3. Из двух шаблонов второй самодвойственный. Тогда систему уравнений, как и в случае 2, составляют для трех разных шаблонов. Чтобы решение системы уравнений было единственным, для них согласно (1.12) должно выполняться условие

$$2n + 3 = 2k + l. \quad (1.45)$$

Очевидно, что $l \equiv 1 \pmod{2}$. Из условия $n \geq l$ вытекает, что $2k - 3 \geq n$. Отсюда имеем $k \geq 4$, $l \geq 5$, а $n \geq 5$. Вычислять определители таких размеров вследствие этого достаточно сложно, поэтому достаточно данных, чтобы исследовать их структуру. Для конкретных данных делаем те же вычисления, что и в случае 2 и строим соответствующие образы по шаблонам.

Случай 4. Оба шаблона не являются самодвойственными. Тогда систему уравнений составляют как для четырех разных шаблонов. Чтобы решение системы уравнений было единственным, для них согласно (1.12) должно выполняться условие

$$3n + 4 = 2k + 2l. \quad (1.46)$$

В этом случае $n \equiv 0 \pmod{2}$. Непосредственно можно убедиться, что $n \geq 6$. При этом возможные значения $k = 5$, $n = l = 6$. Вычисляя определитель системы уравнений для заданных параметров шаблонов, находим значения переменных для каждого шаблона и строим соответствующий образ.

Пример 1.10. Пусть $s_1 = (1, 3, 4, 4, 2)$, $s_2 = (2, 3, 4, 4, 1, 3)$ для $K = 5$, $k = 5$ и $n = l = 6$.

Строим соответствующую систему уравнений для базиса решений, т. е. с правыми частями $b_1 = 1$, а $b_i = 0$ ($i = 2, 3, 4, 5, 6$). При этом первые четыре переменных отводятся первому шаблону, остальные две — второму:

$$\left. \begin{array}{l} x_1 + \quad \quad 2x_3 + \quad \quad 2x_5 + 3x_6 = 1 \\ 3x_1 + \quad x_2 + 4x_3 + 2x_4 + 3x_5 + \quad x_6 = 0 \\ 4x_1 + 3x_2 + 4x_3 + 4x_4 + 4x_5 + 4x_6 = 0 \\ 4x_1 + 4x_2 + 3x_3 + 4x_4 + 4x_5 + 4x_6 = 0 \\ 2x_1 + 4x_2 + \quad x_3 + 3x_4 + \quad x_5 + 3x_6 = 0 \\ \quad \quad 2x_2 + \quad \quad x_4 + 3x_5 + 2x_6 = 0 \end{array} \right\} \pmod{5}. \quad (1.47)$$

Матрица A системы (1.47) и матрицы A_i для переменных имеют вид

$$A = \begin{pmatrix} 1 & 0 & 2 & 0 & 2 & 3 \\ 3 & 1 & 4 & 2 & 3 & 1 \\ 4 & 3 & 4 & 4 & 4 & 4 \\ 4 & 4 & 3 & 4 & 4 & 4 \\ 2 & 4 & 1 & 3 & 1 & 3 \\ 0 & 2 & 0 & 1 & 3 & 2 \end{pmatrix}, A_1 = \begin{pmatrix} 1 & 0 & 2 & 0 & 2 & 3 \\ 0 & 1 & 4 & 2 & 3 & 1 \\ 0 & 3 & 4 & 4 & 4 & 4 \\ 0 & 4 & 3 & 4 & 4 & 4 \\ 0 & 4 & 1 & 3 & 1 & 3 \\ 0 & 2 & 0 & 1 & 3 & 2 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} 1 & 1 & 2 & 0 & 2 & 3 \\ 3 & 0 & 4 & 2 & 3 & 1 \\ 4 & 0 & 4 & 4 & 4 & 4 \\ 4 & 0 & 3 & 4 & 4 & 4 \\ 2 & 0 & 1 & 3 & 1 & 3 \\ 0 & 0 & 0 & 1 & 3 & 2 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 2 & 3 \\ 3 & 1 & 0 & 2 & 3 & 1 \\ 4 & 3 & 0 & 4 & 4 & 4 \\ 4 & 4 & 0 & 4 & 4 & 4 \\ 2 & 4 & 0 & 3 & 1 & 3 \\ 0 & 2 & 0 & 1 & 3 & 2 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 1 & 0 & 2 & 1 & 2 & 3 \\ 3 & 1 & 4 & 0 & 3 & 1 \\ 4 & 3 & 4 & 0 & 4 & 4 \\ 4 & 4 & 3 & 0 & 4 & 4 \\ 2 & 4 & 1 & 0 & 1 & 3 \\ 0 & 2 & 0 & 0 & 3 & 2 \end{pmatrix}, A_5 = \begin{pmatrix} 1 & 0 & 2 & 0 & 1 & 3 \\ 3 & 1 & 4 & 2 & 0 & 1 \\ 4 & 3 & 4 & 4 & 0 & 4 \\ 4 & 4 & 3 & 4 & 0 & 4 \\ 2 & 4 & 1 & 3 & 0 & 3 \\ 0 & 2 & 0 & 1 & 0 & 2 \end{pmatrix},$$

$$A_6 = \begin{pmatrix} 1 & 0 & 2 & 0 & 2 & 1 \\ 3 & 1 & 4 & 2 & 3 & 0 \\ 4 & 3 & 4 & 4 & 4 & 0 \\ 4 & 4 & 3 & 4 & 4 & 0 \\ 2 & 4 & 1 & 3 & 1 & 0 \\ 0 & 2 & 0 & 1 & 3 & 0 \end{pmatrix}.$$

В результате находим значения

$$\det A = -87 = 3(\text{mod } 5), \det A_1 = -11 = 4(\text{mod } 5),$$

$$\det A_2 = -12 = 3(\text{mod } 5), \det A_3 = -12 = 3(\text{mod } 5),$$

$$\det A_4 = 47 = 2(\text{mod } 5), \det A_5 = 7 = 2(\text{mod } 5), \det A_6 = -22 = 3(\text{mod } 5),$$

$$\text{или } x_1 = 3, x_2 = x_3 = 1, x_4 = x_5 = 4, x_6 = 1.$$

Проверим полученный результат на шаблонах (рис. 1.13).

Для количества шаблонов больше двух можно также успешно строить линейную мозаику, однако наличие несамодвойственных шаблонов требует для них отдельной переменной в соответствующей системе уравнений, т. е. общее число шаблонов увеличивается.

Пример 1.11. Пусть $K=7$, $k = 10$, $l = 11$, $m = n = 12$ и заданы три несамодвойственных шаблона: $s_1 = (2, 5, 1, 2, 6, 3, 2, 1, 4, 5)$, $s_2 = (3, 4, 2, 1, 4, 5, 6, 5, 5, 3, 6)$, $s_3 = (5, 2, 1, 4, 4, 3, 2, 2, 1, 3, 3, 6)$.

Строим соответствующую систему уравнений для базиса решений с правыми частями $b_1 = 1$, а $b_i = 0$ ($i = 2, 3, 4, 5, 6$). При этом первые шесть переменных отводятся первому шаблону, четыре — второму и два — третьему:

1	3	4	4	2	
1	3	4	4	2	
1	3	4	4	2	
	1	3	4	4	2
2	4	4	3	1	
	2	4	4	3	1
	2	4	4	3	1
	2	4	4	3	1
	2	4	4	3	1
2	3	4	4	1	3
2	3	4	4	1	3
2	3	4	4	1	3
2	3	4	4	1	3
3	1	4	4	3	2

↓

16	35	55	55	30	20
1	0	0	0	0	0

mod 5

Рис. 1.13

$$\left. \begin{aligned}
 2x_1 &+ 5x_4 &+ 3x_7 &+ 6x_9 &+ 5x_{11} + 6x_{12} &= 1 \\
 5x_1 &+ 2x_2 &+ 4x_4 + 5x_5 &+ 4x_7 + 3x_8 + 3x_9 + 6x_{10} + 2x_{11} + 3x_{12} &= 0 \\
 x_1 &+ 5x_2 + 2x_3 + x_4 + 4x_5 + 5x_6 + 2x_7 + 4x_8 + 5x_9 + 3x_{10} + x_{11} + 3x_{12} &= 0 \\
 2x_1 &+ x_2 + 5x_3 + 2x_4 + x_5 + 4x_6 + x_7 + 2x_8 + 5x_9 + 5x_{10} + 4x_{11} + x_{12} &= 0 \\
 6x_1 &+ 2x_2 + x_3 + 3x_4 + 2x_5 + x_6 + 4x_7 + x_8 + 6x_9 + 5x_{10} + 4x_{11} + 2x_{12} &= 0 \\
 3x_1 &+ 6x_2 + 2x_3 + 6x_4 + 3x_5 + 2x_6 + 5x_7 + 4x_8 + 5x_9 + 6x_{10} + 3x_{11} + 2x_{12} &= 0 \\
 2x_1 &+ 3x_2 + 6x_3 + 2x_4 + 6x_5 + 3x_6 + 6x_7 + 5x_8 + 4x_9 + 5x_{10} + 2x_{11} + 3x_{12} &= 0 \\
 x_1 &+ 2x_2 + 3x_3 + x_4 + 2x_5 + 6x_6 + 5x_7 + 6x_8 + x_9 + 4x_{10} + 2x_{11} + 4x_{12} &= 0 \\
 4x_1 &+ x_2 + 2x_3 + 5x_4 + x_5 + 2x_6 + 5x_7 + 5x_8 + 2x_9 + x_{10} + x_{11} + 4x_{12} &= 0 \\
 5x_1 &+ 4x_2 + x_3 + 2x_4 + 5x_5 + x_6 + 3x_7 + 5x_8 + 4x_9 + 2x_{10} + 3x_{11} + x_{12} &= 0 \\
 &+ 5x_2 + 4x_3 &+ 2x_5 + 5x_6 + 6x_7 + 3x_8 + 3x_9 + 4x_{10} + 3x_{11} + 2x_{12} &= 0 \\
 &+ 5x_3 &+ 2x_6 &+ 6x_8 &+ 3x_{10} + 6x_{11} + 5x_{12} &= 0
 \end{aligned} \right\} \text{mod } 7. \tag{1.48}$$

Матрица A системы (1.48) и матрицы A_i ($i = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$) для переменных имеют вид

$$A_{12} = \begin{pmatrix} 2 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 6 & 0 & 5 & 1 \\ 5 & 2 & 0 & 4 & 5 & 0 & 4 & 3 & 3 & 6 & 2 & 0 \\ 1 & 5 & 2 & 1 & 4 & 5 & 2 & 4 & 5 & 3 & 1 & 0 \\ 2 & 1 & 5 & 2 & 1 & 4 & 1 & 2 & 5 & 5 & 4 & 0 \\ 6 & 2 & 1 & 3 & 2 & 1 & 4 & 1 & 6 & 5 & 4 & 0 \\ 3 & 6 & 2 & 6 & 3 & 2 & 5 & 4 & 5 & 6 & 3 & 0 \\ 2 & 3 & 6 & 2 & 6 & 3 & 6 & 5 & 4 & 5 & 2 & 0 \\ 1 & 2 & 3 & 1 & 2 & 6 & 5 & 6 & 1 & 4 & 2 & 0 \\ 4 & 1 & 2 & 5 & 1 & 2 & 5 & 5 & 2 & 1 & 1 & 0 \\ 5 & 4 & 1 & 2 & 5 & 1 & 3 & 5 & 4 & 2 & 3 & 0 \\ 0 & 5 & 4 & 0 & 2 & 5 & 6 & 3 & 3 & 4 & 3 & 0 \\ 0 & 0 & 5 & 0 & 0 & 2 & 0 & 6 & 0 & 3 & 6 & 0 \end{pmatrix}.$$

Чтобы решение системы уравнений было единственным, для них согласно (1.12) должно выполняться условие

$$5n + 6 = 2k + 2l + 2m. \quad (1.49)$$

Так как длина первого шаблона $k = 10$, второго $l = 11$, а третьего $m = 12$, то это условие выполняется.

Вычисляем определители, а затем значения неизвестных по формуле: $x_i = \frac{\det A_i}{\det A}$ ($1 \leq i \leq 12$). Итак,

$$\det A = -134360512 = 1(\text{mod } 7), \det A_1 = 15447968 = 4(\text{mod } 7),$$

$$\det A_2 = 11582834 = 4(\text{mod } 7), \det A_3 = 10599574 = 6(\text{mod } 7),$$

$$\det A_4 = -8637306 = 1(\text{mod } 7), \det A_5 = -10961246 = 5(\text{mod } 7),$$

$$\det A_6 = 2527520 = 3(\text{mod } 7), \det A_7 = -5879492 = 4(\text{mod } 7),$$

$$\det A_8 = 2384680 = 4(\text{mod } 7), \det A_9 = -6236088 = 2(\text{mod } 7),$$

$$\det A_{10} = 8341468 = 2(\text{mod } 7), \det A_{11} = -14961574 = 2(\text{mod } 7),$$

$$\det A_{12} = 1298826 = 4(\text{mod } 7).$$

Определяем решение системы

$$x_1 = x_2 = 4, x_3 = 6, x_4 = 1, x_5 = 5, x_6 = 3, x_7 = 4,$$

$$x_8 = 4, x_9 = x_{10} = x_{11} = 2, x_{12} = 4.$$

ЗАДАЧА ПОСТРОЕНИЯ ДВУМЕРНОЙ ОДНОЦВЕТНОЙ МОЗАИКИ

2.1. ПОСТАНОВКА ЗАДАЧИ

Перейдем к двумерному полю и рассмотрим построение на нем дискретных образов. Как и ранее, будем полагать, что поле $\Pi = (\pi_{ij})_{m,n}$ задано в виде прямоугольника, разбитого на $N = mn$ клеток, где m — число последовательных горизонтальных клеток (строк), а n — число последовательных вертикальных клеток (столбцов). По умолчанию будем считать два поля с $N = mn$ клетками идентичными. Множеству K цветов поставим в соответствие множество чисел $Q = \{0, 1, 2, \dots, K - 1\}$.

Пусть имеется набор связанных фигур, состоящих из клеток определенного цвета (не равных 0) и называемых *блоками* или *шаблонами* $S = \{s_1, s_2, \dots, s_p\}$. Здесь под связанной фигурой подразумевается множество клеток, каждая из которых имеет общую сторону хотя бы с одной клеткой из этого множества. Предполагается, что количество каждого типа шаблонов ограничено числом $r(t)$, где $t = 1, 2, \dots, p$. Построение произвольных изображений осуществляется с помощью наложения на поле разных шаблонов, которые имеют небольшие размеры и определенную раскраску. При этом операция наложения на одну клетку различных цветов задается как бинарная операция на множестве Q .

Необходимо решить задачу, существует ли такой набор из наличного запаса шаблонов, который при определенном наложении на поле Π составил бы заданное изображение.

Если в поле Π $m=1$, а $n>1$, то оно является строкой, и соответствующая задача называется *задачей о построении линейной мозаики*. Ее решению посвящена глава 1.

Если $m, n>1$, то соответствующая задача называется *задачей о двумерной мозаике*. В данной главе вводятся необходимые определения, понятия и заложены основы решения такой задачи.

Прежде всего, необходимо точно определить операцию наложения цветов. В зависимости от конкретной задачи под операцией наложения (сложения) подразумевают различные действия. В общем виде операцию наложения можно задавать бинарной таблицей. Решить задачу о мозаике означает найти, как при заданном способе накладывания раскрашенных шаблонов построить заданный образ на плоскости Π .

Операция наложения цветов может задаваться произвольным способом в виде цветовой таблицы, бинарной таблицы и таблицы сложения в классе вычетов по определенному модулю. Ниже приведен пример цветовой таблицы (табл. 2.1), где в первом столбце и первой строке указаны цвета, а на пересечении соответствующей строки и соответствующего столбца — цвет как результат наложения (сложения). Первым указан белый цвет, который при сложении играет роль «нуля», так как он при сложении (обозначено символом \oplus) не изменяет другой цвет.

Очевидно, что выполнение операции сложения должно соответствовать некоторым правилам. Например, она должна быть коммутативной. В нашем примере это требование выполняется, поскольку таблица симметрична.

Если перенумеровать цвета с условием, что белый цвет = 0, голубой = 1, желтый = 2, красный = 3 и синий = 4, то сложение цветов можно записать в виде бинарной таблицы (табл. 2.2).

Главный недостаток этой таблицы состоит в том, что сложение не удовлетворяет аксиоме ассоциативности. Например, $(1 \oplus 2) \oplus 3 = 3 \oplus 3 = 2$. Однако $1 \oplus (2 \oplus 3) = 1 \oplus 0 = 1 \neq 2$. Поэтому операция сложения должна быть симметричной и ассоциативной. Таким свойством обладает групповая операция сложения, в качестве которой может выступать сложение в классе вычетов по конечному модулю K .

Т а б л и ц а 2.1

\oplus	Белый	Голубой	Желтый	Красный	Синий
Белый	Белый	Голубой	Желтый	Красный	Синий
Голубой	Голубой	Синий	Красный	Синий	Красный
Желтый	Желтый	Красный	Голубой	Белый	Голубой
Красный	Красный	Синий	Белый	Желтый	Белый
Синий	Синий	Красный	Голубой	Белый	Красный

Т а б л и ц а 2.2

\oplus	0	1	2	3	4
0	0	1	2	3	4
1	1	4	3	4	3
2	2	3	1	0	1
3	3	4	0	2	0
4	4	3	1	0	3

Если переменные принимают два значения 0 или 1, то как операцию сложения можно выбрать логическую операцию дизъюнкции, когда $x \oplus y = x + y - xy$. Однако при этом происходит накопление единиц на клетках поля, которые в дальнейшем нельзя устранить. В практическом смысле эта операция не целесообразна.

Поэтому из всех возможных определений выберем наиболее существенное, когда операция сложения идентична сложению двух чисел по $\text{mod } K$. Рассмотрим

самый простой случай $K = 2$. Тогда все шаблоны будут одноцветными, так как число 0, естественно, означает отсутствие какого-либо цвета (белый цвет). Поскольку шаблон можно накладывать любой стороной (внешней и обратной), а также поворачивать в плоскости на любой угол, кратный 90° , проще считать, что мы имеем дело с разными шаблонами, которые всегда располагаются фиксированным образом в пространстве.

Определение 2.1. Назовем меткой шаблона самую левую среди самых верхних клеток шаблона.

Заполним все поле всеми возможными способами множеством различных шаблонов. Каждому шаблону (точнее, его месту на плоскости Π) поставим в соответствие переменную x_i ($i = 1, 2, \dots, r$), равную 0 или 1. Тогда задача о возможности построения необходимой мозаики на поле Π при заданном множестве шаблонов $S = \{s_1, s_2, \dots, s_p\}$ сводится к решению системы линейных уравнений:

$$\sum_{i=1}^r x_i = b_j, \quad j=1, 2, \dots, N. \quad (2.1)$$

Здесь сложение для каждой клетки происходит по заданной операции сложения, а i -й шаблон учитывается только тогда, когда его пересечение с j -й клеткой не пусто.

В зависимости от видов и количества шаблонов возникает задача с огромным количеством переменных, число которых в большинстве случаев намного превышает число равенств. Решение задачи зависит от искусства определения ранга этой системы.

2.2. ДОПУСТИМОЕ ПОЛЕ ДВУМЕРНЫХ ШАБЛОНОВ И ИХ УРАВНЕНИЯ

Поскольку шаблоны на плоском двумерном поле могут размещаться разными способами, для каждого из них необходимо ввести такое обозначение, чтобы однозначно определять на поле его каждую клетку, если известна координата его метки.

Пусть задан образ, представленный на поле Π с размерами $N = 42$, где $m = 7$ и $n = 6$ (рис. 2.1). Несложно убедиться, что этот образ составлен с помощью 3-х типов шаблонов (на рис. 2.1 справа). В этом образе задействовано три шаблона первого типа, два из которых расположены так, как показано справа на рисунке, а один — в перевернутом виде. Остальные два типа представлены в единственном экземпляре, при этом второй — в перевернутом виде.

Будем считать два типа положений шаблона разными, если их нельзя совместить параллельным переносом. Очевидно, что таких типов не больше 8. Пронумеруем клетки поля от 1 до N сначала по первой строке, затем по второй и так до конца. Зная

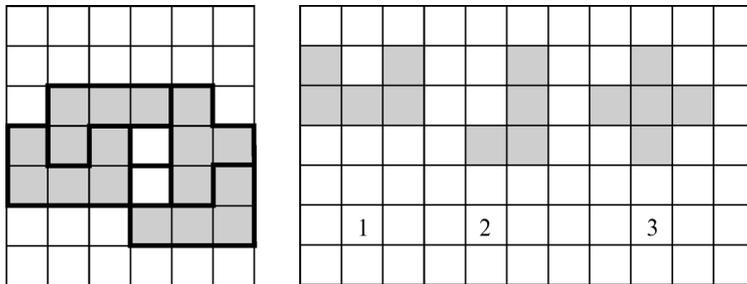


Рис. 2.1

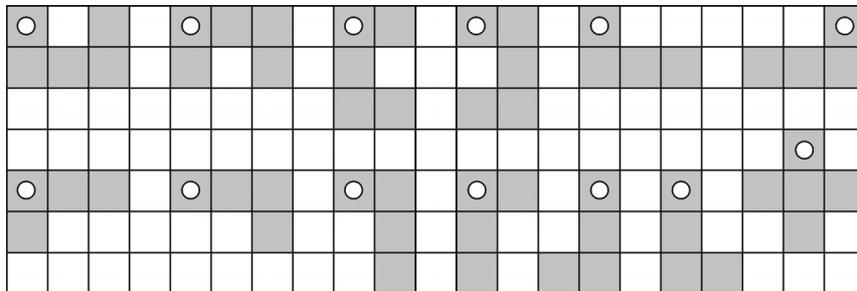


Рис. 2.2

координату метки шаблона, можно однозначно расположить его на поле. Рассмотрим всевозможные положения указанных на рис. 2.1 шаблонов (рис.2.2) (метка обозначена белым кружком).

В нашем примере шаблон s_1 имеет четыре типа положений, шаблон s_2 — восемь типов, а s_3 — только один тип. Для простоты обозначений полагаем все типы положений новыми шаблонами. Таким образом, с учетом всех положений имеем три разных шаблона, которые преобразуются в 13 шаблонов, т. е. $S = \{s_i\}, 1 \leq i \leq 13$.

Рассмотрим подробнее шаблон 1 на рис. 2.1, который на рис. 2.3 изображен в четырех возможных позициях. Обозначим их s_1, s_2, s_3 и s_4 . Зная координату метки шаблона, можно однозначно расположить его на поле. Если координату произвольного шаблона обозначить α , то любой шаблон можно задать его уравнением, которое в общем виде будет выражаться через эту координату. Для этого каждую клетку шаблона в порядке их следования на поле выразим через координату метки и параметры поля m и n :

$$\begin{aligned} s_1(\alpha) &= (\alpha, \alpha + 1, \alpha + n + 1, \alpha + 2n, \alpha + 2n + 1); \\ s_2(\alpha) &= (\alpha, \alpha + 1, \alpha + n, \alpha + 2n, \alpha + 2n + 1); \\ s_3(\alpha) &= (\alpha, \alpha + 2, \alpha + n, \alpha + n + 1, \alpha + n + 2); \\ s_4(\alpha) &= (\alpha, \alpha + 1, \alpha + 2, \alpha + n, \alpha + n + 2). \end{aligned} \quad (2.2)$$

Для линейного поля, рассмотренного в гл. 1, также можно составить уравнение шаблона, которое не зависит от параметра n :

$$s_i(\alpha) = (\alpha, \alpha + 1, \dots, \alpha + s_i - 1).$$

В общем случае в зависимости от вида шаблона и величины поля координата α может принимать только ограниченные значения. Множество допустимых значений α определяет множество

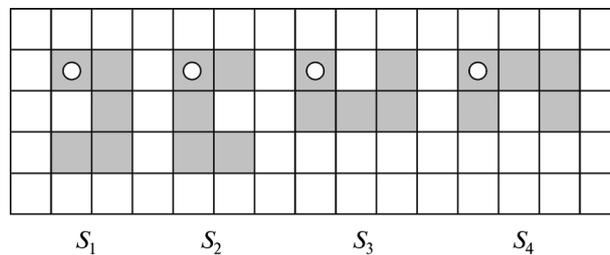


Рис. 2.3

допустимых положений шаблона (или, точнее, его метки) на заданном поле. На рис. 2.4 приведены допустимые значения координаты α для каждого шаблона из рис. 2.3 на поле α размерности $N = 4 \times 3 = 12$. В сумме число положений шаблонов равно 14.

Обозначим изображение, которое необходимо построить с помощью шаблонов, вектором $b = \{b_1, b_2, \dots, b_N\}$, где $b_i \in \{0, 1\}$ ($1 \leq i \leq N$). Каждому допустимому положению шаблона поставим в соответствие переменную x_j ($j = 1, 2, \dots, 14$), которая принимает значение 0 или 1 в зависимости от того, принимает ли данный шаблон участие в построении изображения. Если вместо координаты α для каждого шаблона подставить значения из рис. 2.4, то для каждой переменной будет составлен кортеж, определяющий номера клеток, на которые накладывается соответствующий шаблон:

$$\begin{aligned} c_1 &= (1, 2, 5, 7, 8), c_2 = (2, 3, 6, 8, 9), c_3 = (4, 5, 8, 10, 11), \\ c_4 &= (5, 6, 9, 11, 12), c_5 = (1, 2, 4, 7, 8), c_6 = (2, 3, 5, 8, 9), \\ c_7 &= (4, 5, 7, 10, 11), c_8 = (5, 6, 8, 11, 12), c_9 = (1, 3, 4, 5, 6), \\ c_{10} &= (4, 6, 7, 8, 9), c_{11} = (7, 9, 10, 11, 12), c_{12} = (1, 2, 3, 4, 6), \\ c_{13} &= (4, 5, 6, 7, 9), c_{14} = (7, 8, 9, 10, 12). \end{aligned}$$

Суммируя для каждой клетки поля переменные, в кортежи которых входит номер этой клетки, получаем систему уравнений:

$$\sum_{c_i \cap j \neq \emptyset} x_i \equiv b_j \pmod{2}, \quad j=1, 2, \dots, N. \quad (2.3)$$

На рис. 2.5 показаны допустимые положения всех четырех шаблонов и указаны обозначающие их переменные. Внутри шаблона попадают номера клеток, которые определяют каждый кортеж c_i ($1 \leq i \leq N$). Заметим, что система (2.3) для произвольного

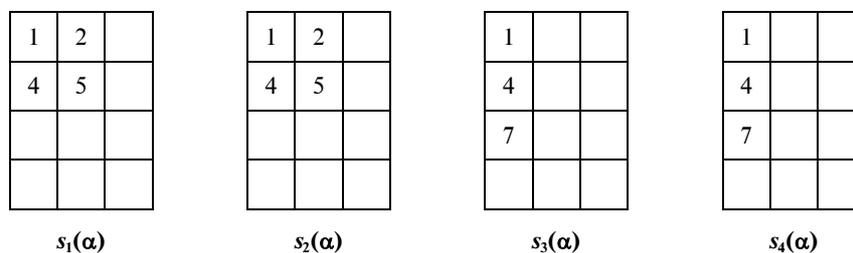


Рис. 2.4

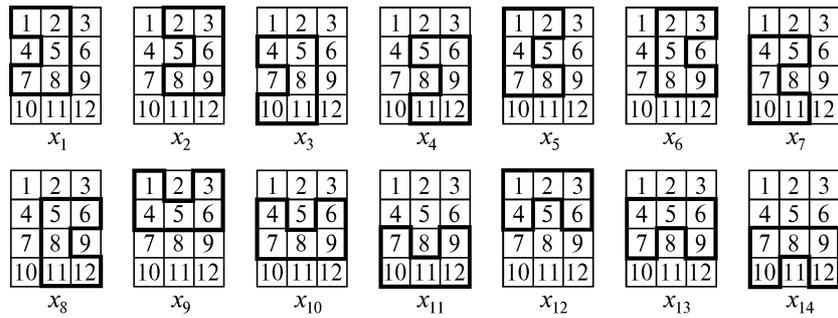


Рис. 2.5

множества шаблонов содержит N уравнений, а число переменных может быть произвольным в зависимости от количества допустимых положений меток шаблонов. Для единственности решения системы уравнений это обстоятельство иногда играет существенную роль.

Теперь, учитывая рис. 2.5, можно легко составить систему уравнений для наших шаблонов. В i -й строке суммируются переменные, кортежи которых содержат i -ю клетку, а в правой части стоят b_i ($1 \leq i \leq N$):

$$\left. \begin{aligned}
 x_1 \cdot \cdot \cdot + x_5 \cdot \cdot \cdot + x_9 \cdot \cdot \cdot + x_{12} \cdot \cdot \cdot &\equiv b_1 \\
 x_1 + x_2 \cdot \cdot \cdot + x_5 + x_6 \cdot \cdot \cdot + x_{12} \cdot \cdot \cdot &\equiv b_2 \\
 \cdot x_2 \cdot \cdot \cdot + x_6 \cdot \cdot \cdot + x_9 \cdot \cdot \cdot + x_{12} \cdot \cdot \cdot &\equiv b_3 \\
 \cdot \cdot x_3 \cdot \cdot + x_5 \cdot \cdot + x_7 \cdot \cdot + x_9 + x_{10} \cdot \cdot + x_{12} + x_{13} \cdot &\equiv b_4 \\
 x_1 \cdot \cdot + x_3 + x_4 \cdot \cdot + x_6 + x_7 + x_8 + x_9 \cdot \cdot \cdot + x_{13} \cdot &\equiv b_5 \\
 \cdot x_2 \cdot \cdot + x_4 \cdot \cdot \cdot + x_8 + x_9 + x_{10} \cdot \cdot + x_{12} + x_{13} \cdot &\equiv b_6 \\
 x_1 \cdot \cdot \cdot + x_5 \cdot \cdot + x_7 \cdot \cdot + x_{10} + x_{11} \cdot \cdot + x_{13} + x_{14} &\equiv b_7 \\
 x_1 + x_2 + x_3 \cdot \cdot + x_5 + x_6 \cdot \cdot + x_8 \cdot \cdot + x_{10} \cdot \cdot \cdot + x_{14} &\equiv b_8 \\
 \cdot x_2 \cdot \cdot + x_4 \cdot \cdot + x_6 \cdot \cdot \cdot + x_{10} + x_{11} \cdot \cdot + x_{13} + x_{14} &\equiv b_9 \\
 \cdot \cdot x_3 \cdot \cdot \cdot + x_7 \cdot \cdot \cdot + x_{11} \cdot \cdot \cdot + x_{14} &\equiv b_{10} \\
 \cdot \cdot x_3 + x_4 \cdot \cdot \cdot + x_7 + x_8 \cdot \cdot \cdot + x_{11} \cdot \cdot \cdot &\equiv b_{11} \\
 \cdot \cdot \cdot x_4 \cdot \cdot \cdot + x_8 \cdot \cdot \cdot + x_{11} \cdot \cdot \cdot + x_{14} &\equiv b_{12}
 \end{aligned} \right\} \text{mod } 2. \quad (2.4)$$

Вопрос о существовании решения данной системы уравнений представляет самостоятельный интерес. Как правило, число переменных в ней больше количества уравнений, что позволяет найти хотя бы одно решение.

2.3. ПОСТРОЕНИЕ БАЗИСА РЕШЕНИЯ ДЛЯ ОДНОГО ШАБЛОНА

Если система (2.4) не имеет специфической структуры, то решать ее в общем случае, когда используется много шаблонов (а переменных тогда во много раз больше), практически невозможно. Необходимо придумать способ, чтобы отсеять зависимые переменные. Один из возможных способов следующий.

Представим, что изображение, которое необходимо построить, есть вектор b такой, что $b_\alpha = 1$ ($1 \leq \alpha \leq n$), а остальные $b = 0$ ($i \neq \alpha$). Если существует решение системы уравнений (2.3), то назовем такое решение единицей и обозначим его $I(\alpha)$. Чтобы число переменных в системе уравнений (2.4) сравнялось с числом уравнений, положим $x_{13} = x_{14} = 0$. Решая систему уравнений (2.4) для правой части $b_1 \equiv 1 \pmod{2}$ и $b_j \equiv 0 \pmod{2}$ ($j > 1$), получаем $x_1 = x_3 = x_7 = x_9 = x_{12} = 1$, а все остальные x_i равны нулю. Это означает, что если вместо переменных подставить координаты соответствующих шаблонов из рис. 2.5, то наложением их на поле получим в первой клетке черный цвет, а в остальных клетках — цвет 0 (отсутствие цвета). Имеем уравнение

$$I(1) \equiv [s_1(1) + s_1(4) + s_2(4) + s_3(1) + s_4(1)] \pmod{2}. \quad (2.5)$$

Для проверки суммируем множества соответствующих кортежей, при этом одноименные элементы складываются по mod 2:

$$(1) = (1, 2, 5, 7, 8) + (4, 5, 8, 10, 11) + (4, 5, 7, 10, 11) + \\ + (1, 3, 4, 5, 6) + (1, 2, 3, 4, 6) \pmod{2}.$$

Может получиться, что для других клеток поля не существует решения в виде (2.5), что возможно при ограничении поля или по другим причинам.

Рассмотрим еще два решения для правых частей: 1) $b_3 \equiv 1 \pmod{2}$, остальные $b_i = 0$; 2) $b_4 \equiv 1 \pmod{2}$, остальные $b_i = 0$. В первом случае получаем решение $x_4 = x_6 = x_8 = x_9 = x_{12} = 1$, остальные x_i равны нулю; во втором — $x_1 = x_2 = x_3 = x_4 = x_7 = x_8 = x_9 = 1$, остальные x_i равны нулю.

Таким образом, можно найти решение для любой единицы в правой части, тогда решение для произвольных правых частей будет состоять из суммы решений для отдельных единиц. Например, если взять равные правые части: $b_1 = b_3 = b_4 \equiv 1 \pmod{2}$,

остальные $b_i = 0$, то решением будет сумма полученных ранее решений по mod 2, а именно: $x_2 = x_6 = x_9 = 1$, остальные = 0. Это можно проверить, если сложить кортежи соответствующих шаблонов из рис. 2.5:

$$(2, 3, 6, 8, 9) + (2, 3, 5, 8, 9) + (1, 3, 4, 5, 6) = (1, 3, 4).$$

Определение 2.2. Подмножество шаблонов $S_0 \subset S$ образует базис решения системы уравнений (2.3), если с его помощью можно построить любую единицу $I(\alpha)$ ($1 \leq \alpha \leq N$).

Самым элементарным базисом есть шаблон, состоящий из одной клетки.

Определение 2.3. Шаблон s обладает свойством гомоморфности, если с помощью наложения его на самого себя в разных положениях можно получить связный фрагмент, имеющий меньшее количество клеток.

Например, если сложить шаблоны на рис. 2.5, соответствующие переменным x_1 и x_5 на том же поле, то в результате получим образ, состоящий из двух клеток 4 и 5. Найденный результат можно записать в виде уравнения

$$s_1(1) + s_2(1) = (1, 2, 5, 7, 8) + (1, 2, 4, 7, 8) = (4, 5)(\text{mod } 2).$$

Определение 2.4. Назовем шаблон s гомоморфным единице $I(\alpha)$, если существует решение уравнения

$$I(\alpha) = \sum_i s(i) \pmod{2},$$

где i — некоторое значение метки допустимых положений шаблона и всех его преобразований.

Как видим, шаблон на рис. 2.3 гомоморфен единице.

Шаблон s называется *самодостаточным для базиса*, если он гомоморфен любой единице поля.

Лемма 2.1. Если число клеток шаблона четно, то он не гомоморфен ни одной единице.

Это утверждение вытекает из того, что наложение любого количества таких шаблонов и их допустимых преобразований дает в пересечении четное число. Иными словами, правая часть системы уравнений (2.4) будет иметь число клеток цвета 1, равное $0 \pmod{2}$, а в левой части не должна появиться единица.

Теорема 2.1. Линейный шаблон $s = 2l + 1$ ($l \geq 1$) не гомоморфен ни одной единице.

Доказательство. Построим для шаблона s систему уравнений (2.3) на поле размером $N = m \times n$. Число горизонтальных шаблонов, расположенных в каждой строке, равно $n - s + 1$, а всех — $m(n - s + 1)$. Обозначим соответствующие переменные x_k , где $k = j + (i - 1)(n - s + 1)$ ($1 \leq i \leq m$; $1 \leq j \leq n - s + 1$). Число всех вертикальных шаблонов будет равно $n(m - s + 1)$. Обозначим соответствующие переменные y_v , где $v = j + n(i - 1)$ ($1 \leq i \leq m - s + 1$; $1 \leq j \leq n$).

Рассмотрим матрицу $A(m_1, m_2)$ специального вида, которая обладает следующими свойствами:

- а) число столбцов равно m_2 ;
- б) в i -м столбце ($1 \leq j \leq m_2$) первые $i - 1$ элементов равны 0, затем следует m_1 единиц, а дальше до конца опять нули.

Пусть $m_1 = 5$, $m_2 = 4$. Тогда матрица $A(5, 4)$ имеет вид

$$A(5, 4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (2.6)$$

Число строк в такой матрице равно $m_1 + m_2 - 1$, поэтому в ней всегда $m_1 - 1$ строк зависимы. Если $m_2 < m_1$, то строки от m_2 до m_1 состоят из одних единиц.

Лемма 2.2. Путем сложения нескольких строк всегда можно добиться, чтобы первые m_1 строк состояли из одних единиц.

Это легко достигнуть, если заметить, что начиная с $(m_1 + 1)$ -й строки слева появляются нули. Поэтому, если к i -й строке ($1 \leq i \leq m_1$), в которой справа есть нули, добавить все строки с номером $i \pmod{m_1}$, то получим необходимое заполнение единицами.

В нашем примере строки 4 и 5 (от m_2 до m_1) уже состоят из единиц. Если к первой строке добавить строку $6 \equiv 1 \pmod{5}$, то получим все единицы, и так до 3-й строки.

Если рассматривать систему уравнений $A(m_2, m_1) \bar{X} = \bar{C}$, где \bar{X} и \bar{C} — векторы размерности $(m_2 + m_1 - 1)$, то после образования единиц в первых m_1 строках, получаем разбиение правых частей на m_1 классов:

$$\left[\sum_{i=1(\bmod m_1)} C_i \equiv \sum_{i=2(\bmod m_1)} C_i \equiv \dots \equiv \sum_{i=0(\bmod m_1)} C_i \right] (\bmod 2). \quad (2.7)$$

Введем понятие индексной функции от двух аргументов:

$$\varphi(n_1, n_2) = (n_1 - 1)(n_2 - s + 1),$$

где s — длина шаблона.

Обозначим

$$\lambda_i = (x_{\beta+1}, x_{\beta+2}, \dots, x_{\beta+n-s+1}) \quad (1 \leq i \leq m);$$

$$\sigma_j = (y_{\gamma+1}, y_{\gamma+2}, \dots, y_{\gamma+n-s+1}) \quad (1 \leq j \leq n),$$

где $\beta = \varphi(i, m)$, $\gamma = \varphi(j, n)$.

Запишем уравнение (2.3) для первой строки поля. В наших обозначениях оно имеет вид

$$A(s, n)\lambda_1^T + E_n\sigma_1^T \equiv \tilde{b}; \quad \tilde{b} = (b_1, b_2, \dots, b_n). \quad (2.8)$$

Введем для удобства символические вектор-столбцы:

$$\Lambda = [A(s, n)\lambda_1^T, A(s, n)\lambda_2^T, \dots, A(s, n)\lambda_m^T]^T;$$

$$\Sigma = [E_n\sigma_1^T, E_n\sigma_2^T, \dots, E_n\sigma_n^T]^T.$$

Тогда систему (2.3) можно записать в клеточном виде:

$$E_m\Lambda + A(s, m-s+1)\Sigma = B.$$

Используем лемму 3.2 о свойствах матриц $A(m_1, m_2)$ для получения одинаковых элементов σ_i^T в первой и второй клеточных строках. Для этого в первой клеточной строке сложим все клеточные строки матрицы $A(s, m-s+1)$ с номером $1(\bmod s)$, а во второй — все строки с номером $2(\bmod s)$. Здесь сложение подразумевается как сложение соответствующих матриц. После этого в первых двух клеточных строках получаем

$$s \times \sum_{i=1}^{n(m+s-1)} y_i = R.$$

При всех этих преобразованиях в векторе Λ будут складываться переменные x_i , но матрицы $A(s, n)$ в первых двух клеточных строках не изменяются.

В общем виде находим

$$\begin{aligned} A(s, n) Z_1^T + RE_n &= \bar{C}_1; \\ A(s, n) Z_2^T + RE_n &= \bar{C}_2. \end{aligned} \quad (2.9)$$

Здесь Z_1, Z_2 — векторы, полученные сложением переменных x_i во время предыдущих операций. Аналогично \bar{C}_1 и \bar{C}_2 получены от сложения элементов правых частей, при этом ни один элемент не принадлежит обоим этим векторам. Если применить равенство (2.7), то получим разбиение элементов вектора b на s равных по сумме частей. Если бы линейный шаблон был гомоморфен единице, то какое-нибудь b_r было бы равно единице, а все остальные — нулю. Но тогда равенство (2.7) никогда бы не выполнялось. Это противоречие и подтверждает справедливость теоремы.

Можно показать, что такие шаблоны не гомоморфны ни одной связной фигуре. Для того чтобы шаблон обладал указанным свойством, необходимо иметь определенную структуру, которая в некотором смысле идентична выпуклости. Такую структуру имеет первый шаблон на рис. 2.1 (или 2.3), и не имеют два остальных шаблона. Характеристика второго шаблона приведена в лемме 2.1.

Теорема 2.2. Шаблон s на рис. 2.3 является самодостаточным для базиса в любом поле размерности не меньше, чем $N = 4 \times 3$.

Для доказательства теоремы необходимо непосредственно найти уравнение каждой единицы $I(\alpha)$ ($1 \leq \alpha \leq N$). Однако это не рациональный путь. Для такого поля уже найдено уравнение единицы $I(1)$. Если воспользоваться свойством симметрии шаблонов, то легко найти уравнение для $I(3)$. Относительно вертикальной оси симметрии поле в соответствующих определенных позициях s_1 симметрично s_2 , а s_3 и s_4 симметричны сами себе. Поэтому

$$I(3) \equiv [s_2(2) + s_2(5) + s_1(5) + s_3(1) + s_4(1)] \pmod{2}. \quad (2.10)$$

Уравнению (2.10) соответствуют переменные на рис. 2.5: x_4, x_6, x_8, x_9 и x_{12} . Это можно проверить так же, как и уравнение (2.5):

$$(2, 3, 5, 8, 9) + (5, 6, 8, 11, 12) + (5, 6, 9, 11, 12) + (1, 3, 4, 5, 6) + (1, 3, 4, 5, 6) \equiv (3).$$

Если использовать свойство симметрии шаблонов относительно вертикальной оси симметрии поля, то получим следующее соответствие:

$$x_1 \leftrightarrow x_6, x_2 \leftrightarrow x_5, x_3 \leftrightarrow x_8, x_4 \leftrightarrow x_7,$$

остальные симметричны сами себе.

Если использовать свойство симметрии шаблонов относительно горизонтальной оси симметрии поля, то получим иное соответствие:

$$x_1 \leftrightarrow x_3, x_2 \leftrightarrow x_4, x_5 \leftrightarrow x_7, x_6 \leftrightarrow x_8, x_9 \leftrightarrow x_{14}, x_{10} \leftrightarrow x_{13}, x_{11} \leftrightarrow x_{12}.$$

Теперь легко перейти от $I(1)$ к $I(3)$, заменив последовательность переменных $x_1, x_3, x_7, x_9, x_{12}$ на симметричную относительно вертикальной оси симметрии последовательность переменных $x_4, x_6, x_8, x_9, x_{12}$. $I(10)$ легко получить из $I(1)$, если поменять последовательность переменных $x_1, x_3, x_7, x_9, x_{12}$ на симметричную относительно горизонтальной оси симметрии последовательность переменных $x_1, x_3, x_5, x_{11}, x_{14}$. Аналогично можно получить $I(12)$ из $I(3)$. Если найдено уравнение для $I(2)$, то все единицы поля легко получить с помощью добавления одного из двух уравнений, определяющих две последовательные клетки (горизонтальные или вертикальные), которые назовем *димерами*. Горизонтальный димер имеет уравнение $(\beta, \beta+1)$, а вертикальный — $(\beta, \beta+n)$. Приведем уравнение горизонтального димера:

$$s_1(\alpha) + s_2(\alpha) = (\alpha, \alpha+1, \alpha+n+1, \alpha+2n, \alpha+2n+1) + (\alpha, \alpha+1, \alpha+n, \alpha+2n, \alpha+2n+1) \equiv (\alpha+n, \alpha+n+1) \pmod{2}. \quad (2.11)$$

Очевидно, что горизонтальные димеры можно образовать только во второй и третьей строках, а их всего 4 (4, 5), (5, 6), (7, 8) и (8, 9).

Приведем уравнение вертикального димера:

$$s_3(\alpha) + s_4(\alpha) = (\alpha, \alpha+2, \alpha+n, \alpha+n+1, \alpha+n+2) + (\alpha, \alpha+1, \alpha+2, \alpha+n, \alpha+n+2) \equiv (\alpha+1, \alpha+n+1) \pmod{2}. \quad (2.12)$$

Вертикальные димеры можно образовать только во втором столбце и их всего 3: (2, 5), (8, 9) и (8, 11).

Добавляя к $I(2)$ вертикальный димер $(2, 5)$, получаем $I(5)$ и т. д. Если в уравнения (2.9)—(2.11) вместо шаблонов подставить кортежи, то запись уравнений единиц будет выглядеть компактно. $I(2)$ можно найти перебором либо решая систему уравнений (2.4) с правой частью $b_2 \equiv 1 \pmod{2}$, остальные $b_i = 0$. Окончательная запись всех единиц имеет вид (вместо x , записываем i):

$$\begin{aligned} I(1) &= (1, 3, 7, 9, 12); & I(2) &= (2, 3, 4, 5, 7, 8, 12); \\ I(3) &= (6, 7, 8, 9, 12); & I(4) &= (1, 2, 3, 4, 7, 8, 9); \\ I(5) &= (2, 3, 4, 5, 7, 8, 9); & I(6) &= (3, 4, 5, 6, 7, 8, 9); \\ I(7) &= (1, 2, 3, 4, 5, 6, 14); & I(8) &= (1, 2, 3, 4, 5, 6, 7, 8, 10); \\ I(9) &= (1, 2, 3, 5, 6, 7, 10); & I(10) &= (1, 3, 5, 11, 14); \\ I(11) &= (1, 2, 4, 5, 6, 7, 11); & I(12) &= (2, 6, 8, 11, 14). \end{aligned} \quad (2.13)$$

Этим и завершается доказательство теоремы. Применяемый способ доказательства можно назвать конструктивным.

Докажем еще одну теорему о самодостаточности шаблона иным способом.

Теорема 2.3. Шаблон, уравнение которого имеет вид $s_1 = (\alpha, \alpha + 1, \alpha + 2, \alpha + 3, \alpha + n)$, является самодостаточным для базиса в любом поле размерности не меньше, чем $N = 5 \times 4$.

Доказательство. Записываем уравнения других положений указанного шаблона, считая заданное уравнение первым:

$$\begin{aligned} s_2 &= (\alpha, \alpha + n, \alpha + n + 1, \alpha + n + 2, \alpha + n + 3); \\ s_3 &= (\alpha, \alpha + 1, \alpha + n + 1, \alpha + 2n + 1, \alpha + 3n + 1); \\ s_4 &= (\alpha, \alpha + 1, \alpha + n, \alpha + 2n, \alpha + 3n); \\ s_5 &= (\alpha, \alpha + n - 3, \alpha + n - 2, \alpha + n - 1, \alpha + n); \\ s_6 &= (\alpha, \alpha + 1, \alpha + 2, \alpha + 3, \alpha + 3 + n); \\ s_7 &= (\alpha, \alpha + n, \alpha + 2n, \alpha + 3n - 1, \alpha + 3n); \\ s_8 &= (\alpha, \alpha + n, \alpha + 2n, \alpha + 3n, \alpha + 3n + 1). \end{aligned}$$

Изобразим все восемь положений самодостаточного шаблона на поле (рис. 2.6). Убедимся в гомоморфности этого шаблона, складывая $s_3(5)$ и $s_4(6)$:

$$(5, 6, 10, 14, 18) + (6, 7, 10, 14, 18) = (5, 7).$$

Складывая те же шаблоны с координатами 6 и 7, т. е. $s_3(6)$ и $s_4(7)$, в результате получаем $(6, 8)$. В сумме это дает окрашенную вторую строку поля, т. е. $(5, 6, 7, 8)$. Прибавляя теперь к этим четы-

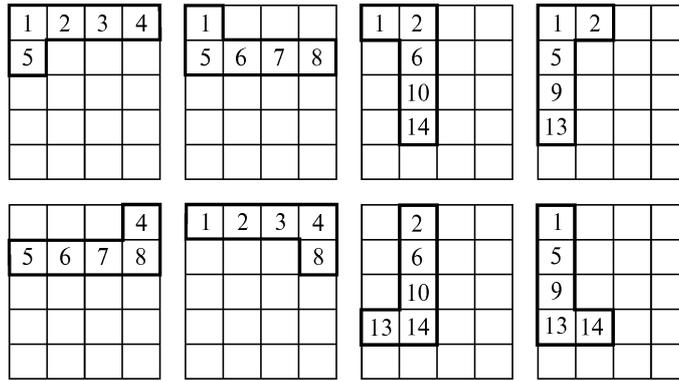


Рис. 2.6

рем клеткам $s_2(1)$, $s_5(4)$, $s_1(5)$ и $s_6(5)$, получаем четыре единицы $I(1)$, $I(4)$, $I(9)$ и $I(12)$.

Таким образом, получено уравнение четырех единиц, которые удобно записать через уравнения шаблонов:

$$\begin{aligned}
 I(1) &\equiv [s_3(5) + s_4(6) + s_3(6) + s_4(7) + s_2(1)] \pmod{2}; \\
 I(4) &\equiv [s_3(5) + s_4(6) + s_3(6) + s_4(7) + s_5(5)] \pmod{2}; \\
 I(9) &\equiv [s_3(5) + s_4(6) + s_3(6) + s_4(7) + s_1(5)] \pmod{2}; \\
 I(12) &\equiv [s_3(5) + s_4(6) + s_3(6) + s_4(7) + s_6(5)] \pmod{2}.
 \end{aligned}
 \tag{2.13}$$

Здесь приведены уравнения клеток 1, 4, 9, 12. Если в этих уравнениях все координаты увеличить на n , то получим уравнения клеток с координатами больше на n , а именно: 5, 8, 13 и 16. Это две последовательности из четырех клеток, касающиеся левой и правой частей поля.

Складывая единицы в клетках 1, 5, 9 и 13 с шаблоном $s_4(1)$, получаем единицу в клетке 2. Складывая те же единицы с шаблоном $s_8(1)$, получаем единицу в клетке 14; складывая единицы в клетках 1, 2, 4 и 5 с шаблоном $s_1(1)$, — единицу в клетке 3. Теперь введем новые координаты шаблонов для системы уравнений (2.13): $\alpha' = 21 - \alpha$. Так как число клеток поля равно 20, то это равносильно тому, что поле повернули в плоскости на 180° . Это приведет к построению всех единиц поля, кроме 10 и 11. Однако, имея уравнения единиц в остальных клетках, легко построить единицы в клетках 10 и 11. Тем самым доказана справедливость теоремы 2.3.

2.4. ПОСТРОЕНИЕ БАЗИСА РЕШЕНИЯ ДЛЯ НЕСКОЛЬКИХ ШАБЛОНОВ

Если из множества заданных шаблонов не удастся найти самодостаточный, то необходимо поискать такой, который был бы гомоморфен какой-либо единице. Тогда в сочетании с другими шаблонами можно построить единицы для всех клеток поля. Кроме того, складывая два шаблона, получим либо самодостаточный шаблон, либо шаблон меньшего размера, который позволит с заданными шаблонами построить единицы во всех клетках поля.

Рассмотрим различные комбинации из двух шаблонов, учитывая лемму 2.1 и не комбинируя два шаблона, если каждый имеет четное количество клеток. Обозначим количество клеток первого шаблона k , а второго — l .

1. Пусть $k = 2$, а $l = 3$. В этом случае задача решается легко. Первый шаблон является линейным, а второй шаблон — либо линейный, и тогда можно построить единицу в любой клетке (это показано в первой главе), либо представляет «уголок», который является самодостаточным шаблоном. Построение единицы для первой клетки показано на рис. 2.7.

Кроме того, приставляя к уголку первый шаблон, получаем единицу в любой из четырех клеток уголка.

2. Пусть $k = 2$, а $l = 5$. Из пяти клеток можно образовать шаблоны, показанные на рис. 2.8. Нетрудно убедиться, что для каждого из типов шаблона из пяти клеток благодаря первому шаблону можно построить единицу в любой клетке поля.

Кроме того, второй и шестой типы самодостаточны, как доказано выше. Третий тип самодостаточен, так как из него легко образовать димер, исходя из уравнения $(\alpha, \alpha+1, \alpha+2, \alpha+3, \alpha+l+2)$. Складываем это уравнение с ему

$$\begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array} + \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array} + \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array} = \begin{array}{|c|} \hline 1 \\ \hline \end{array}$$

Рис. 2.7

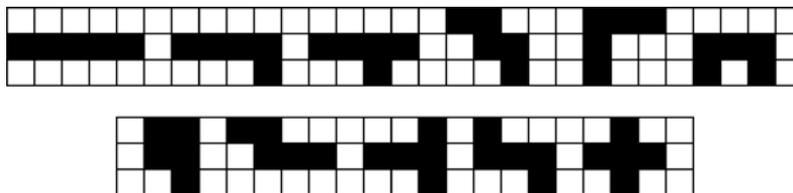


Рис. 2.8

подобным $(\alpha, \alpha + 1, \alpha + 2, \alpha + 3, \alpha + n + 1)$ и получаем димер $(\alpha + n + 1, \alpha + n + 2)$. Учитывая тот факт, что димер необходимо двигать вправо и влево, а также ставить вертикально, то поле должно иметь размеры не меньше, чем 5×4 . Покажем, что в этом поле можно построить все единицы непосредственно. Перенумеруем клетки поля от 1 до 20 и сложим два шаблона $(12, 13, 14, 15, 19) + (12, 13, 14, 15, 9) = (9, 19)$. Если сделать сдвиг координат на одну горизонталь вверх, то получим пару $(4, 14)$. Теперь приложим к этим клеткам вертикальный шаблон $(4, 9, 14, 19, 10)$, получим единицу $I(10)$. Делая в координатах сдвиг на одну вертикаль влево, получаем последовательно единицы $I(7)$, $I(8)$, $I(9)$. Затем зеркальным отображением относительно вертикальной оси симметрии получаем $I(6)$. В результате имеем все единицы во второй строке. Проводя зеркальное отображение относительно горизонтальной оси симметрии, таким же образом получаем все единицы третьей строки. Теперь, размещая шаблоны основным телом во второй строке, а пятой клеткой — в первой строке, строим единицы в клетках 2, 3, 4. Симметричным построением получаем единицы в клетках 17, 18, 19. Осталось построить единицы по углам поля в клетках 1, 5, 16 и 20. Это сделать легко, например, располагая шаблон по координатам $(2, 3, 4, 5, 9)$. Складывая его с единицами $I(2)$, $I(3)$, $I(4)$, $I(9)$, получаем желаемую $I(5)$. Аналогично находим остальные угловые единицы.

Лемма 2.3. Четвертый шаблон самодостаточен на поле размером не меньше, чем $N = 7 \times 4$.

Перенумеруем клетки поля от 1 до 28 и к уравнению шаблона $(13, 14, 19, 20, 26)$ прибавим шаблон $(6, 12, 13, 18, 19)$, в результате получим $(6, 12, 14, 18, 20, 26)$. Прибавим сюда еще два шаблона $(13, 19, 20, 25, 26)$ и $(12, 13, 18, 19, 25)$. В итоге имеем $(6, 14)$. Выполним такую же операцию с шаблонами, у которых координаты на единицу меньше. В результате получим $(5, 13)$. Теперь сложим с этими парами шаблон $(5, 6, 13, 14, 21)$ и получим $I(21)$. Образует единицу $I(20)$, уменьшая на единицу координаты шаблонов, которые использовались для построения $I(21)$. Поскольку при этом наименьшей координатой в третьей строке была 17, то здесь будет 16, и остается построить еще $I(19)$.

Аналогичными действиями относительно вертикальной оси симметрии можно построить единицы $I(15)$, $I(16)$ и $I(17)$. То же самое, только относительно горизонтальной оси симметрии, относится к построению всех единиц, кроме $I(11)$, во второй стро-

ке. Имея блоки единиц массивом 3×2 , можно строить единицы в первой и последней строках, что и требовалось доказать.

Седьмой тип тоже самодостаточен, что нетрудно доказать, учитывая тот факт, что концевая клетка шаблона может находиться на любой клетке поля. С учетом этого можно построить димер в необходимом месте, затем удалить с шаблона четное число клеток и получить единицу в любом месте поля.

Лемма 2.4. Восьмой шаблон самодостаточен на поле размером не меньше, чем $N = 7 \times 4$.

Складываем два шаблона с такими координатами (20, 21, 25, 26, 27) и (19, 20, 21, 25, 26). В результате получим пару (19, 27). Образует еще одну пару (18, 26), складывая шаблоны (19, 20, 24, 25, 26) и (18, 19, 20, 24, 25). Теперь к двум парам прибавим шаблон (18, 19, 26, 27, 28) и получим $I(28)$. Выполняя такую же операцию с шаблонами, координаты которых на единицу и на двойку меньше прежних, получаем последовательно $I(27)$ и $I(26)$. Проводя зеркальное отображение относительно вертикальной оси симметрии, получаем $I(22)$, $I(23)$, $I(24)$, а относительно горизонтальной оси симметрии — все единицы поля, кроме четвертого столбца. Однако, имея массив единиц в три столбца, легко получить единицы в остальных клетках, что и подтверждает справедливость леммы 2.4.

3. Пусть $k = 3$, а $l = 4$. Из трех клеток можно создать два шаблона — один линейный и «уголок», который является самодостаточным и его можно не учитывать. Все линейные шаблоны длиной k будем обозначать d_k . Из четырех клеток можно образовать шаблоны, показанные на рис. 2.9.

Накладывая на первые два и четвертый шаблоны исходный шаблон d_3 , получаем единицы. Накладывая вертикально d_3 на первый столбец третьего шаблона, получаем «уголок», и это решает проблему. Накладывая в последнем шаблоне на две строчки d_3 , получаем шаблон длиной два, что сводится к случаю 2.

4. Пусть $k = 3$, а $l = 5$. Рассмотрим последовательно шаблоны на рис. 2.8. Накладывая на первый шаблон последовательно дважды d_3 , получаем единицу. То же применимо и для второго шаблона, только второй раз d_3 накладываем вертикально. Третий шаблон зеркально накладываем на себя, чтобы длинная часть совпала. Получаем две изолированные клетки, ко-

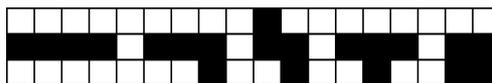


Рис. 2.9

торые накрываем d_3 и получаем единицу. К четвертому шаблону прикладываем d_3 в третьем столбце и первой строке, получаем единицу. К пятому, девятому и одиннадцатому шаблонам прикладываем d_3 по вертикали и по горизонтали, получаем единицу. К шестому и восьмому шаблонам прикладываем d_3 по первой и второй горизонталям, получая единицу. Также получаем единицы, прикладывая d_3 вертикально в первом и во втором столбцах седьмого шаблона, а также по двум горизонталям и в третьем столбце вертикально десятого шаблона.

5. Пусть $k = 4$, а $l = 5$. Все такие шаблоны представлены на рис. 2.8 и 2.9.

Рассмотрим среди шаблонов пятого порядка только несамодостаточные, т. е. первый — d_5 , пятый, девятый, десятый и одиннадцатый. Указываем в переборе вариантов первым номер шаблонов на рис. 2.9, а вторым — на рис. 2.8.

(1—1). Оба линейные, вопрос очевиден.

(1—5). Если на концы угла наложить d_4 , то получим «уголок», и проблема решена.

(1—9). Построение предполагает размеры поля как минимум 6×6 , поэтому занумеруем клетки от 1 до 36. Сложим два шаблона (16, 17, 18, 23, 29) и (5, 11, 16, 17, 18), а затем приложим d_4 (5, 11, 17, 23). Получим пару (17, 29). То же самое выполним с шаблонами (10, 14, 15, 16, 22) и (10, 16, 17, 18, 22), прибавив к ним d_4 (14, 15, 16, 17). Получим еще пару (16, 18). Теперь приложим шаблон (16, 17, 18, 23, 29) и получим $I(23)$. Аналогично можно найти $I(29)$, $I(11)$, $I(17)$. Проведя зеркальные отражения относительно горизонтальной и вертикальной осей симметрии, найдем единицы на всех клетках поля, кроме первых и шестых строк и столбцов. Однако массив единиц достаточен для получения единиц и в этих клетках.

(1—10). Выберем поле размером 5×6 , нумеруя клетки от 1 до 30. Сложим шаблоны (16, 22, 23, 24, 30) и (16, 17, 23, 29, 30), затем еще два (9, 15, 16, 17, 23) и (9, 10, 16, 22, 23). В результате получим две пары (10, 15) и (24, 29). Прибавим шаблон (24, 18, 17, 16, 10) и $d_4 = (15, 16, 17, 18)$, в результате получим $I(29)$. Сдвинув на единицу и двойку координаты шаблонов, получим единицы $I(28)$ и $I(27)$. Проводя различные зеркальные отображения, найдем последовательно все единицы для всех клеток поля.

(1—11). Для построения единицы достаточные размеры поля составляют 6×6 . Сложим шаблоны (9, 14, 15, 16, 21) и (11, 16, 17, 18, 23), затем еще четыре: $d_4 = (15, 16, 17, 18)$, $d_4 = (14, 15,$

16, 17), $d_4 = (9, 15, 21, 27)$ и $d_4 = (11, 17, 23, 29)$. В результате получим пару (27, 29). Добавим к ней шаблон (22, 27, 28, 29, 34) и $d_4 = (16, 22, 28, 34)$, получим $I(16)$.

(2—1). Непосредственно получим единицу $I(4)$ в поле размером 6×6 , сложив два первых шаблона (1, 2, 3, 9), (3, 4, 5, 9) и $d_5 = (1, 2, 3, 4, 5)$.

(2—5, 9, 10). Непосредственно приложим шаблоны и получим единицу.

(2—11). Приложив первый шаблон по столбцу и по строке второго шаблона, получим единицу.

(3—1). Рассмотрим поле размером 6×4 . Сложив в нем два первых шаблона (4, 5, 9, 10), (2, 3, 9, 10) и $d_5 = (1, 2, 3, 4, 5)$, получим $I(4)$.

(3—5). В поле размером 6×4 сложим три первых шаблона (1, 2, 8, 9), (1, 7, 8, 14), (8, 13, 14, 19) и один второй (7, 8, 9, 13, 19), получим $I(2)$.

(3—9). В том же поле размером 6×4 сложим два первых шаблона (2, 3, 7, 8), (2, 8, 9, 15) и один второй (3, 7, 8, 9, 15), получим $I(8)$.

(3—10). Сложим шаблоны (1, 7, 8, 9, 15) и (2, 8, 9, 15), получим «уголок» (1, 2, 7), что решило проблему.

(3—11). Сложим два первых шаблона (1, 2, 8, 9), (1, 7, 8, 14) и один второй (2, 7, 8, 9, 14), получим $I(8)$.

(4—1). Сложим четыре первых шаблона (3, 8, 9, 15), (3, 9, 10, 15), (4, 9, 10, 16), (4, 10, 11, 16) и один второй (7, 8, 9, 10, 11), получим $I(7)$.

(4—5). Приложим в первом столбце первый шаблон и получим «уголок», что решило проблему.

(4—9). Непосредственно получим единицу, поставив первый шаблон в третий столбец второго.

(4—10). Сложим три первых шаблона (1, 7, 8, 13), (7, 13, 14, 19), (9, 14, 15, 21) и три вторых (1, 7, 8, 9, 15), (7, 13, 14, 15, 21), (9, 13, 14, 15, 19), получим $I(17)$.

(4—11). Непосредственно получим единицу, поставив первый шаблон во второй столбец второго шаблона.

(5—1). Суммируем четыре первых шаблона (8, 9, 14, 15), (20, 21, 26, 27), (10, 11, 16, 17), (22, 23, 28, 29) и пять вторых (2, 8, 14, 20, 26), (3, 9, 15, 21, 27), (4, 10, 16, 22, 28), (5, 11, 17, 23, 29), (1, 2, 3, 4, 5), получая $I(1)$.

(5—5, 9, 11). Эти сочетания не являются базисом решения системы.

(5—10). Сложив первые четыре шаблона (2, 3, 8, 9), (13, 14, 19, 20), (10, 11, 16, 17), (21, 22, 27, 28) и пять других (2, 3, 8, 13, 14), (8, 9, 14, 19, 20), (10, 11, 16, 21, 22), (16, 17, 22, 27, 28), (8, 14, 15, 16, 22), получим $I(15)$.

В поле размером 7×6 с помощью зеркальных отображений находим еще единицы $I(16)$, $I(21)$, $I(22)$, $I(27)$, $I(28)$, что составляет достаточный базис для получения остальных единиц на любой клетке поля.

6. Пусть $k = l = 5$. Не учитывая самодостаточные шаблоны, берем пары из первого, пятого, девятого, десятого и одиннадцатого шаблонов.

(1—5). Для построения единицы достаточно в поле размером 7×6 взять один первый и два пятых шаблона, а именно: (1, 2, 3, 4, 5), (1, 2, 3, 9, 15) и (3, 4, 5, 9, 15). В результате получаем $I(3)$.

(1—9). Суммируем шаблоны в поле той же размерности (3, 7, 8, 9, 15), (3, 9, 10, 11, 15) и (7, 8, 9, 10, 11), получаем $I(9)$.

(1—10). Суммируем пять первых шаблонов (1, 7, 13, 19, 25), (7, 8, 9, 10, 11), (14, 14, 15, 16, 17), (19, 20, 21, 22, 23), (25, 26, 27, 28, 29) и восемь десятых (8, 14, 15, 16, 22), (9, 15, 16, 17, 23), (10, 14, 15, 16, 20), (11, 15, 16, 17, 21), (14, 20, 21, 22, 28), (15, 21, 22, 23, 29), (16, 20, 21, 22, 26), (17, 21, 22, 23, 27), получаем $I(1)$.

(1—11). Для такого сочетания базис найти невозможно.

(5—9). Для такого сочетания базис найти невозможно.

(5—10). Если мы сложим один пятый шаблон (9, 15, 19, 20, 21) и два десятых (7, 13, 14, 15, 21), (8, 9, 14, 19, 20), то получим «уголок» (7, 8, 13), который является самодостаточным шаблоном. Однако проще добавить к первому «уголку» второй «уголок» (3, 8, 9) и десятый шаблон (3, 7, 8, 9, 13), чтобы получить $I(9)$.

(5—11). Для такого сочетания базис не существует.

(9—10). Суммируем три девятых (2, 8, 13, 14, 15), (3, 7, 8, 9, 15), (9, 13, 14, 15, 21) и два десятых (2, 3, 8, 13, 14), (7, 13, 14, 15, 21) шаблона, получаем $I(8)$.

(9—11). Для такого сочетания базис не существует.

(10—11). Образует сумму из двух десятых шаблонов (1, 7, 8, 9, 15), (1, 2, 8, 14, 15) и одного одиннадцатого (2, 7, 8, 9, 14). В результате получаем единицу $I(8)$.

Подобные вычисления можно продолжить и для более объемных шаблонов, сводя их к построению либо единицы, либо к шаблону с меньшим числом клеток, либо к самодостаточному шаблону.

ПОСТРОЕНИЕ ДВУМЕРНОЙ МНОГОЦВЕТНОЙ МОЗАИКИ

3.1. ПОСТРОЕНИЕ ПЛОСКИХ ИЗОБРАЖЕНИЙ ДЛЯ $K > 2$

Очевидно, что все теоретические выводы относительно линейного поля и линейных шаблонов при использовании произвольного количества цветов переносятся и на двумерное поле. Поэтому все определения, если они не противоречат основной задаче в новых условиях, будут полностью перенесены на двумерное поле. Будем считать, что число красок также обозначается числом K , а множеству цветов поставлено в соответствие множество чисел $Q = \{0, 1, 2, \dots, K - 1\}$.

В отличие от одноцветных шаблонов, которые соответствовали $K = 2$, для многоцветных уравнение шаблона должно включать распределение цветов по его составляющим клеткам. Поэтому его записывают в виде

$$s(\alpha) = \{(\alpha, q_1), (\alpha + i_1, q_2), \dots, (\alpha + i_{r-1}, q_r)\}, \quad (3.1)$$

где $0 < i_1 < i_2 < \dots < i_{r-1} \leq N - \alpha$; $q_j \in Q \setminus \{0\}$ ($1 \leq j \leq r$), а r равно числу клеток шаблона. При этом, как и прежде, предполагается соседство всех клеток шаблона только через общие стороны, а не вершины клеток.

Для каждого шаблона определяется его допустимое положение на поле, как и в главе 2 (см. рис. 2.4). Пусть, например, первый шаблон (см. рис. 2.3) окрашен в цвета в порядке нумерации его клеток как (3, 8, 2, 2, 3) для $K = 10$ (рис.3.1). Тогда его уравнение имеет вид

$$s(\alpha) = \{(\alpha, 3), (\alpha + 1, 8), (\alpha + n + 1, 2), (\alpha + 2n, 3), (\alpha + 2n + 1, 2)\}. \quad (3.2)$$

Для нескольких шаблонов цвета в одинаковых клетках накладываются по $\text{mod } K$. Например, наложение шаблона (3.2) самого на себя приводит к новой раскраске шаблона:

$$\begin{aligned} 2s(\alpha) &= s(\alpha) + s(\alpha) = \\ &= \{(\alpha, 6), (\alpha + 1, 16), (\alpha + n + 1, 4), (\alpha + 2n, 6), (\alpha + 2n + 1, 4)\} \pmod{10}. \end{aligned} \quad (3.3)$$

3	8	
	2	
3	2	

Рис. 3.1

Количество переменных не зависит от K и по-прежнему равно сумме всех возможных положений на поле каждого шаблона вместе с его преобразованными копиями. То же касается и кортежей соответствующих переменных. При этом $x_i \in Z, i = 1, 2, \dots, N$.

Пусть задан вектор изображения $b_j = (b_1, b_2, \dots, b_n)$, где $b_j \in Q (1 \leq j \leq N)$. Для каждой клетки поля можно записать уравнение, куда будут входить вместе с цветом переменные, кортежи которых содержат номер этой клетки. Получаем следующую систему уравнений типа (3.2):

$$\sum_{c_i \cap j \neq \emptyset} x_i q_j^{(i)} \equiv b_j \pmod{K}, \quad j=1,2, \dots, N, \quad (3.4)$$

где $q_j^{(i)}$ — цвет клетки соответствующего i -го шаблона, наложенной на клетку j .

В отличие от шаблона для линейного поля двумерные шаблоны могут иметь две оси геометрической симметрии. Поэтому в уравнении (3.4) в зависимости от вида шаблона может участвовать до восьми соответствующих ему переменных. В зависимости от раскраски эта симметричность может нарушаться. Очевидно, что число осей симметрий раскрасок не может быть больше числа геометрических осей симметрий. Общее число переменных в зависимости от наличия осей симметрии для положений шаблона и числа осей симметрий красок указано в табл. 3.1.

Таким образом, если шаблон имеет 8 положений, то каждая его раскраска уникальная и при фиксированной метке соответствует восьми переменным, что и отражено в табл. 3.1. Если же шаблон имеет геометрическую ось симметрии, то появляется возможность совпадения раскрасок шаблона после поворота его вокруг оси симметрии.

Определение 3.1. Назовем раскраску шаблона, полученную после его поворота в пространстве вокруг вертикальной (горизонтальной) оси симметрии, горизонтально (вертикально) двойственной.

Т а б л и ц а 3.1

Число геометрических осей симметрий	0	1	1	2	2	2	4	4	4	4
Число положений шаблона	8	4	4	2	2	2	1	1	1	1
Число осей симметрии красок	0	0	1	0	1	2	0	1	2	4
Число переменных	8	8	4	8	4	2	8	4	2	1

Если шаблон имеет две оси симметрии, то раскраску перевернутого шаблона назовем просто двойственной.

Определение 3.2. Назовем горизонтально (вертикально) двойственную раскраску шаблона вертикально (горизонтально) самодвойственной, если она совпадает с основной. Аналогично, если двойственная и основная раскраски совпадают, назовем их самодвойственными.

Понятно, что самодвойственные (горизонтально или вертикально) шаблоны при фиксированной метке соответствуют четырем переменным, а просто самодвойственные — двум переменным.

Рассмотрим опять шаблоны на рис. 2.1 (правая часть) и зафиксируем их метки. Первый шаблон имеет вертикальную ось симметрии, поэтому число его переменных равно 4 или 8, второй шаблон не имеет осей симметрии, поэтому количество его переменных равно 8, третий шаблон имеет 4 оси симметрии, поэтому в зависимости от раскрасок он может иметь число переменных 8, 4, 2 или 1.

Теперь, после введения необходимых определений и терминов, рассмотрим составление основной системы линейных сравнений.

3.2. ПОСТРОЕНИЕ БАЗИСА РЕШЕНИЙ ДЛЯ ОДНОГО ШАБЛОНА

Если система (3.4) имеет хотя бы одно решение, то заданное изображение можно построить с помощью наличных шаблонов. Однако решение системы уравнений (3.4) стандартными методами в общем виде искать очень сложно, поэтому действуем аналогично случаю $K = 2$.

Представим, что правые части (3.4) не заданы.

Определение 3.3. Если с помощью подбора значений переменных получим в правой части системы уравнений (3.4) для какого-либо одного $b_\alpha \neq 0 \pmod{K}$, а для всех остальных $b_j \equiv 0 \pmod{K} (j \neq \alpha)$, то назовем такое решение одноклеточным.

Этому решению соответствует уравнение типа (3.4):

$$(\alpha, q) = \sum_{s_j(\alpha_j) \cap \alpha \neq \emptyset} y_j s_j(\alpha_j) \pmod{K}, \quad q \in \mathcal{Q} \setminus \{0\}, y_j \in \mathbb{Z}, \quad (3.5)$$

где α_j — метка соответствующих шаблонов и сложение проводится по правилу (3.4).

Если для каждого K существует обратный элемент q^{-1} , то, обозначая $z_j = y_j q^{-1}$ и имея решение уравнения (3.5), получаем решение для построения единицы в клетке α .

Определение 3.4. Назовем шаблон s гомоморфным одной клетке α , если существует решение уравнения (3.5) только для этого типа шаблона и его различных положений в пространстве.

Определение 3.5. Подмножество шаблонов $S_0 \subset S$ образует базис для решения системы уравнений (3.3), если:

а) с его помощью в каждой клетке поля можно построить раскраску $q \in Q \setminus \{0\}$;

б) q имеет для данного K обратный элемент.

Шаблон s называется самодостаточным для решения системы (3.3), если он совместно со своими преобразованиями образует базис.

Очевидно, что всякий самодостаточный шаблон является гомоморфным каждой клетке поля. Но обратное утверждение неверно, так как если шаблон гомоморфен каждой клетке поля, то для некоторых клеток значения цвета не удовлетворяют условию б).

Из всех самодостаточных шаблонов иногда можно выделить такие, которые образуют одноклеточное решение кратным наложением шаблона на себя. Это рассмотрено в [3] для линейного поля, а все изложенное выше о линейных шаблонах остается справедливым для двумерного поля.

Лемма 3.1. Шаблон s , у которого раскраска клеток удовлетворяет условию

$$\text{НОД}\{q_1, q_2, \dots, q_r, K\} = \lambda > 1, r = |s|, \quad (3.6)$$

не может быть самодостаточным для решения системы уравнений (3.3).

Действительно, при сложении такого шаблона и всех его преобразований сумма цветов всегда дает цвет $q = 0 \pmod{\lambda}$, $q \in Q \setminus \{0\}$.

Представим, что q^{-1} существует, что должно быть обязательным для самодостаточности шаблона. Это означает, что существует такое $t \neq 0 \pmod{K}$, для которого $tq = 1 \pmod{K}$ или то же самое $tq = Kl + 1$ для некоторого целого l . Но $K \equiv 0 \pmod{\lambda}$, поэтому $tq \equiv 1 \pmod{\lambda}$. Отсюда вытекает, что $q \neq 0 \pmod{\lambda}$, а это противоречит начальным условиям.

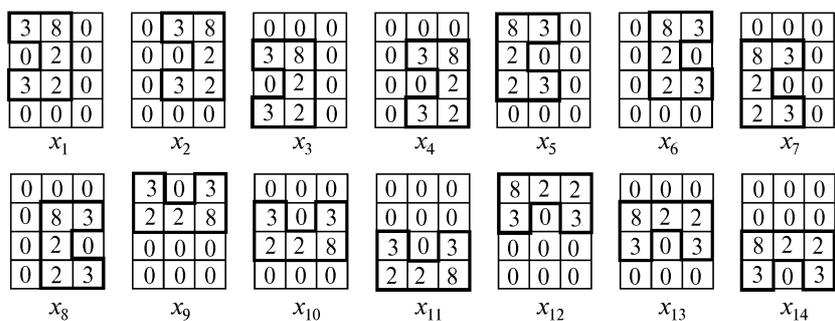


Рис. 3.2

Рассмотрим шаблон на рис.3.1 и покажем, что он является гомоморфным для клетки α , принадлежащей множеству допустимых положений, число которых, согласно рис. 2.5, равно 14. Переменные для всех положений раскрашенного шаблона показаны на рис. 3.2.

Составим систему уравнений, где для каждой клетки поля отводится одно уравнение. В каждое уравнение входят те и только те переменные, изображения которых на рис. 3.2 пересекаются с данной клеткой. Определим базовое решение для $b_1 = 1$, а $b_i = 0$ ($i > 1$) и для $K = 11$:

$$\left. \begin{aligned}
 3x_1 \cdot \cdot \cdot + 8x_5 \cdot \cdot \cdot + 3x_9 \cdot \cdot \cdot + 8x_{12} \cdot \cdot \cdot &\equiv 1 \\
 8x_1 + 3x_2 \cdot \cdot \cdot + 3x_5 + 8x_6 \cdot \cdot \cdot \cdot \cdot \cdot + 2x_{12} \cdot \cdot \cdot &\equiv 0 \\
 8x_2 \cdot \cdot \cdot + 3x_6 \cdot \cdot \cdot + 3x_9 \cdot \cdot \cdot + 2x_{12} \cdot \cdot \cdot &\equiv 0 \\
 3x_3 \cdot \cdot \cdot + 2x_5 \cdot \cdot \cdot + 8x_7 \cdot \cdot \cdot + 2x_9 + 3x_{10} \cdot \cdot \cdot + 3x_{12} + 8x_{13} \cdot \cdot &\equiv 0 \\
 2x_1 \cdot \cdot \cdot + 8x_3 + 3x_4 \cdot \cdot \cdot + 2x_6 + 3x_7 + 8x_8 + 2x_9 \cdot \cdot \cdot \cdot \cdot \cdot + 2x_{13} \cdot \cdot &\equiv 0 \\
 + 2x_2 \cdot \cdot \cdot + 8x_4 \cdot \cdot \cdot \cdot \cdot \cdot + 3x_8 + 8x_9 + 3x_{10} \cdot \cdot \cdot + 3x_{12} + 2x_{13} \cdot \cdot &\equiv 0 \\
 3x_1 \cdot \cdot \cdot + 2x_5 \cdot \cdot \cdot + 2x_7 \cdot \cdot \cdot + 2x_{10} + 3x_{11} \cdot \cdot \cdot + 3x_{13} + 8x_{14} &\equiv 0 \\
 2x_1 + 3x_2 + 2x_3 \cdot \cdot \cdot + 3x_5 + 2x_6 \cdot \cdot \cdot + 2x_8 \cdot \cdot \cdot + 2x_{10} \cdot \cdot \cdot \cdot \cdot \cdot + 2x_{14} &\equiv 0 \\
 2x_2 \cdot \cdot \cdot + 2x_4 \cdot \cdot \cdot + 3x_6 \cdot \cdot \cdot \cdot \cdot \cdot + 8x_{10} + 3x_{11} \cdot \cdot \cdot + 3x_{13} + 2x_{14} &\equiv 0 \\
 3x_3 \cdot \cdot \cdot \cdot \cdot \cdot + 2x_7 \cdot \cdot \cdot \cdot \cdot \cdot + 2x_{11} \cdot \cdot \cdot \cdot \cdot \cdot + 3x_{14} &\equiv 0 \\
 2x_3 + 3x_4 \cdot \cdot \cdot \cdot \cdot \cdot + 3x_7 + 2x_8 \cdot \cdot \cdot \cdot \cdot \cdot + 2x_{11} \cdot \cdot \cdot \cdot \cdot \cdot &\equiv 0 \\
 2x_4 \cdot \cdot \cdot \cdot \cdot \cdot + 3x_8 \cdot \cdot \cdot \cdot \cdot \cdot + 3x_{11} \cdot \cdot \cdot \cdot \cdot \cdot + 3x_{14} &\equiv 0
 \end{aligned} \right\} \pmod{11}. \quad (3.7)$$

В этой системе 12 уравнений и 14 неизвестных. Положим $x_{13} = x_{14} = 0$. Решая оставшуюся систему, получаем решение

$$\begin{aligned}
 x_1 &\equiv 3 \pmod{11}, \quad x_2 \equiv 5 \pmod{11}, \quad x_3 \equiv 1 \pmod{11}, \quad x_4 \equiv 6 \pmod{11}, \\
 x_5 &\equiv 7 \pmod{11}, \quad x_6 \equiv 4 \pmod{11}, \quad x_7 \equiv 6 \pmod{11}, \quad x_8 \equiv 5 \pmod{11},
 \end{aligned}$$

$$x_9 \equiv 6 \pmod{11}, x_{10} \equiv 2 \pmod{11}, x_{11} \equiv 9 \pmod{11}, x_{12} \equiv 9 \pmod{11}.$$

Рассмотрим последовательно варианты построения базиса решения системы для одного шаблона, удовлетворяющего системе (3.5).

1. Пусть $r = 2$. Тогда $s(\alpha) = \{(\alpha, q_1), (\alpha + 1, q_2)\}$. Известно, что если $q_1 = q_2$, то шаблон не является самодостаточным. Поэтому положим $q_1 \neq q_2$.

Двойственный к нему будет шаблон $s(\alpha) = \{(\alpha, q_2), (\alpha + 1, q_1)\}$. Записываем систему уравнений для построения единицы в точке α :

$$\begin{aligned} x q_1 + y q_2 &= 1 \pmod{K}; \\ x q_2 + y q_1 &= 0 \pmod{K}. \end{aligned} \quad (3.8)$$

Определитель системы равен $q_1^2 - q_2^2 \neq 0 \pmod{K}$, поэтому решение существует всегда, если $K > 3$:

$$x = \frac{q_1}{q_1^2 - q_2^2}; \quad y = \frac{-q_2}{q_1^2 - q_2^2}.$$

Так же можно получить единицу для произвольной клетки поля.

2. Пусть $r = 3$. Тогда существует только два типа шаблонов: один линейный $s(\alpha) = \{(\alpha, q_1), (\alpha + 1, q_2), (\alpha + 2, q_3)\}$, а другой в виде «уголка»: $s(\alpha) = \{(\alpha, q_1), (\alpha + 1, q_2), (\alpha + n, q_3)\}$. Для линейного шаблона, учитывая двойственный шаблон, получаем уравнения

$$\begin{aligned} x q_1 + y q_2 + z q_3 &= 1 \pmod{K}; \\ x q_3 + y q_2 + z q_1 &= 0 \pmod{K}. \end{aligned}$$

Если $q_1 = q_2 = q_3$, то шаблон не может образовать единицу, поэтому найдутся два разных цвета, например $q_1 \neq q_2$. Тогда задача сводится к предыдущему случаю 1. В общем случае линейный шаблон произвольной длины сводится к случаю 1.

Для второго типа шаблона решение существует. Зафиксируем положение шаблона на поле размером 2×2 (рис. 3.3). Запишем соответствующую систему для образования базиса $b_1 = 1, b_2 = b_3 = b_4 = 0$.

$$\begin{aligned} x_1 q_1 + \quad + x_3 q_3 + x_4 q_2 &\equiv 1 \pmod{K}; \\ x_1 q_2 + x_2 q_1 + \quad + x_4 q_3 &\equiv 0 \pmod{K}; \\ \quad x_2 q_3 + x_3 q_2 + x_4 q_1 &\equiv 0 \pmod{K}; \\ x_1 q_3 + x_2 q_2 + x_3 q_1 &\equiv 0 \pmod{K}. \end{aligned} \quad (3.9)$$

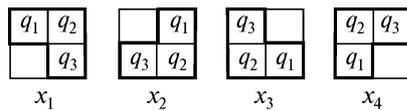


Рис. 3.3

Определитель системы равен

$$\det A = q_2^4 - 4q_1 q_2^2 q_3 - (q_1^2 - q_3^2)^2.$$

Решение системы имеет вид

$$x_i = A_i/A,$$

где

$$A_1 = q_1q_3^2 - q_3q_2^2 - q_1^3, A_2 = q_2q_3^2 + q_1^2q_2, A_3 = q_1^2q_3 - q_3^3 - q_1q_2^2, \\ A_4 = -2q_1q_2q_3 + q_2^3.$$

Для произвольных значений цветов всегда можно подобрать подходящие шаблоны, чтобы построить единицу в первой клетке поля. Задавая единицу в других клетках, получаем соответствующее решение.

3. Пусть $r = 4$. Тогда существует пять типов шаблонов с уравнениями

$$\{(\alpha, q_1), (\alpha + 1, q_2), (\alpha + 2, q_3), (\alpha + 4, q_4)\}, \{(\alpha, q_1), (\alpha + 1, q_2), \\ (\alpha + 2, q_3), (\alpha + n + 2, q_4)\}, \{(\alpha, q_1), (\alpha + 1, q_2), (\alpha + 2, q_3), \\ (\alpha + n + 1, q_4)\}, \{(\alpha, q_1), (\alpha + 1, q_2), (\alpha + n + 1, q_3), \\ (\alpha + n + 1, q_4)\}, \{(\alpha, q_1), (\alpha + 1, q_2), (\alpha + n, q_3), (\alpha + n + 1, q_4)\}.$$

Эти типы шаблонов из четырех клеток показаны на рис. 3.4.

Составим для первого из них и двойственного ему уравнения:

$$x_1q_1 + x_2q_4 \equiv 1 \pmod{K}; \\ x_1q_2 + x_2q_3 \equiv 0 \pmod{K}; \\ x_1q_3 + x_2q_2 \equiv 0 \pmod{K}; \\ x_1q_4 + x_2q_2 \equiv 0 \pmod{K}.$$

Складывая первое с четвертым и второе с третьим уравнения, получаем зависимости:

$$(x_1 + x_2)(q_1 + q_4) \equiv 1 \pmod{K}; \\ (x_1 + x_2)(q_2 + q_3) \equiv 0 \pmod{K}.$$

Так как $(x_1 + x_2) \not\equiv 0 \pmod{K}$, то $(q_1 + q_4) \not\equiv 0 \pmod{K}$, и решение будет иметь место только при условии $(q_2 + q_3) \equiv 0 \pmod{K}$, но не единственное: оно является следствием соотношения $x_1 + x_2 = (q_1 + q_4)^{-1}$.

	q_1	q_2	q_3	q_4		q_1	q_2	q_3		q_1	q_2	q_3		q_1	q_2		q_1	q_2		
							q_4			q_4				q_3	q_4		q_3	q_4		
	1					2				3				4					5	

Рис. 3.4

Второй шаблон имеет восемь типов положений, которые изображены на поле размером 3×3 (рис. 3.5).

Если составить уравнение для единицы в первой клетке, то будут заняты переменные x_1 , x_3 и x_7 с соответствующими коэффициентами. Аналогично строят другие уравнения. Таким образом, число уравнений будет на одно больше числа переменных. Отбросим последнее уравнение, тогда условие разрешимости системы имеет вид

$$\text{Det} = \begin{vmatrix} q_1 & 0 & 0 & 0 & q_4 & 0 & q_3 & 0 \\ q_2 & 0 & q_1 & 0 & 0 & 0 & q_4 & q_3 \\ q_3 & 0 & 0 & q_4 & 0 & 0 & 0 & q_4 \\ 0 & q_1 & 0 & q_3 & 0 & q_4 & q_2 & 0 \\ 0 & q_2 & q_2 & 0 & q_2 & 0 & 0 & q_2 \\ q_4 & q_3 & 0 & q_2 & q_1 & 0 & 0 & 0 \\ 0 & 0 & q_4 & 0 & 0 & q_3 & q_1 & 0 \\ 0 & 0 & q_3 & q_4 & 0 & q_2 & 0 & q_1 \end{vmatrix} \neq 0. \quad (3.10)$$

Третий шаблон при построении единицы требует минимальное поле размером 3×3 и при этом необходимо использовать также 8 переменных, что меньше числа уравнений. Для решения системы необходимо найти подматрицу порядка 8, определитель которой не равен нулю.

Четвертый шаблон, как второй и третий, требует 8 клеток и 8 переменных. Для решения соответствующей системы уравнений необходимо, чтобы определитель типа (3.10) также не был равен нулю.

Пятый шаблон имеет только один тип положения и может иметь в поле (размером 3×3) 4 переменные. Однако, если состав-

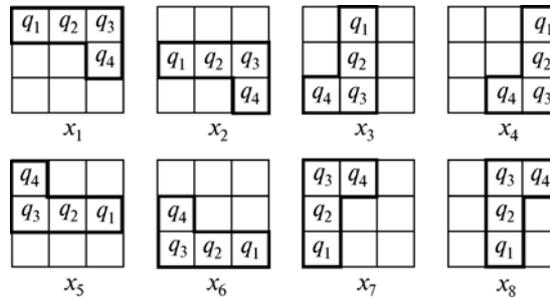


Рис. 3.5

вить систему уравнений только для четырех клеток, которые он занимает, то можно использовать и 4 переменные, переворачивая шаблон в плоскости. Вследствие этого можно получить решение, так как легко найти определитель матрицы, который имеет вид

$$\text{Det} = \begin{vmatrix} q_1 & q_4 & q_3 & q_2 \\ q_2 & q_1 & q_4 & q_3 \\ q_3 & q_2 & q_1 & q_4 \\ q_4 & q_3 & q_2 & q_1 \end{vmatrix} \neq 0 \pmod{K}. \quad (3.11)$$

Определитель равен

$$(q_1^2 - q_3^2)^2 - (q_2^2 - q_4^2)^2 + 4(q_1q_2 - q_3q_4)(q_2q_3 - q_1q_4) \pmod{K}. \quad (3.12)$$

Пусть $q_i = i$. Если $K = 5$, то $\text{Det} = 0 \pmod{K}$, а если $K = 7$, то $\text{Det} = 1 \pmod{7}$ и получаем решение:

$$x_1 = 1, x_2 = 5, x_3 = x_4 = 3.$$

3.3. ПОСТРОЕНИЕ БАЗИСА РЕШЕНИЙ ДЛЯ МНОГИХ ШАБЛОНОВ

Если не удастся построить базис решения для одного шаблона, то при наличии нескольких шаблонов это выполнить легче. При этом поиск можно проводить двумя путями.

1. Находим непосредственно базис решения, если система уравнений позволяет это.

2. Строим из нескольких шаблонов один меньшего размера, который является самодостаточным.

Эти методы мы использовали для построения линейной мозаики, для двумерной мозаики таких возможностей больше. Рассмотрим сначала два шаблона, постепенно увеличивая их объем. Обозначим объем первого шаблона k , а второго — l .

1. Пусть $s_1 = \{(\alpha, q_1), (\alpha + 1, q_2)\}$, $s_2 = \{(\alpha, q_3), (\alpha + 1, q_4)\}$. Из п. 3.2 известно, что если $q_1 \neq q_2$ ($q_3 \neq q_4$), то соответствующий шаблон самодостаточен. Если же $q_1 = q_2$ и $q_3 = q_4$, то два шаблона становятся кратными и их можно заменить одним, о котором нам известно, что он не является самодостаточным. Поэтому в дальнейшем считаем, что используются шаблоны длиной 2 только одноцветные.

2. Пусть $s_1 = \{(\alpha, q_1), (\alpha + 1, q_1)\}$, $s_2 = \{(\alpha, q_2), (\alpha + 1, q_2), (\alpha + 2, q_2), \dots\}$. Здесь второй шаблон — линейный, произвольной длины r . Чтобы получить единицу в клетке α , необходимо наложить первый шаблон на последние две клетки второго шаблона, чтобы в r -й клетке получить 0. Для этого нужно решить уравнение $x_r q_1 + q_r \equiv 0 \pmod{K}$. Отсюда находим решение $x_r = -q_r q_1^{-1} \pmod{K}$. Поступая аналогично, уменьшаем второй шаблон до длины $r - 1$ и т. д., пока не получим двухклеточный шаблон. Если полученные после всех преобразований цвета не совпадают, то единицу строим как обычно. Если цвета совпадают, тогда надо воспользоваться двойственным вторым шаблоном. Если и таким путем не получим единицу, то попытаемся построить ее в другой клетке.

Пример 3.1. Пусть $s_1 = (3, 3)$, $s_2 = \{1, 7, 5, 2\}$, $K = 11$. Для x_4 находим: $x_4 = -2 \cdot 3^{-1} = -2 \cdot 4 = -8 = 3$. После этого второй шаблон перейдет в такой: $s_2 = \{1, 7, 3\}$. Далее, по формуле определяем $x_3 = -3 \cdot 3^{-1} = -3 \cdot 4 = -12 = 10$. После этого второй шаблон перейдет в такой: $s_2 = \{1, 4\}$. Получаем неоднородный шаблон, что гарантирует построение единицы в необходимом месте.

Лемма 3.2. Условие существования решения для двух шаблонов $s_1 = (q, q)$ и $s_2 = (q_1, q_2, \dots, q_r)$ имеет вид

$$\sum_{i=1}^r (-1)^i q_i \neq 0 \pmod{K}. \quad (3.13)$$

Для доказательства вспомним вычисление формул: $x_r = -q_r \times q_1^{-1} \pmod{K}$. После этого предпоследняя клетка (она теперь становится последней) второго шаблона изменится и станет равной $q_{r-1} + x_r q_1 = q_{r-1} - q_r$. Продолжая дальше, получаем в третьей с конца клетке значение $q_{r-2} - q_{r-1} + q_r$. Если сравнить значение во второй клетке, полученное в результате вычислений, со значением в первой клетке, то придем к условию (3.13).

Пусть $s_1 = \{(\alpha, q_1), (\alpha + 1, q_1)\}$, а второй шаблон — произвольный, но не линейный. Тогда, последовательно образовывая нули в клетках (как в случае линейного) второго шаблона, преобразовываем его в двухклеточный.

	8	4			
		3	6	1	
		2		5	

Рис. 3.6

Пример 3.2. Пусть $s_1 = (3, 3)$, а второй шаблон для $K = 11$ вместе с цветами клеток показан на рис. 3.6.

Будем образовывать нули во втором шаблоне, начиная с крайних (висячих) клеток.

8	4				7	3			5	3			5	3	6		9	1		9	1	
	3	6	1	→	3	6	1	→	1	6	1	→	1	6	7	→	1	6	7	→	5	6
	2		5		2		5				5											

Рис. 3.8

Пример 3.4. Возьмем в качестве большого шаблона на рис. 3.7 и покажем на рис. 3.8 соответствующие преобразования наложением трехклеточного шаблона. В результате получили шаблон, который дальше сжать невозможно, но он является самодостаточным, как следует из п. 3.2. Вычисляем по (3.12) определитель системы:

$$\begin{aligned}
 (9^2 - 5^2)^2 - (1^2 - 6^2)^2 + 4(9 \cdot 1 - 5 \cdot 6)(1 \cdot 5 - 9 \cdot 6) &= 1 - 4 + 4 \cdot 1 \cdot 6 \equiv \\
 &\equiv 21 \pmod{11} \equiv 10 \pmod{11}.
 \end{aligned}$$

Очевидно, что такие же операции и преобразования можно выполнять для произвольно раскрашенного трехклеточного шаблона.

ПРИМЕНЕНИЕ ТЕОРИИ ПОСТРОЕНИЯ ДИСКРЕТНЫХ ОБРАЗОВ

4.1. РЕШЕНИЕ СИСТЕМ СРАВНЕНИЙ БОЛЬШИХ РАЗМЕРОВ

Если основная система сравнений, соответствующая построению какого-либо образа, занимает поле достаточно больших размеров, то при ее решении сталкиваются с трудностями принципиального характера. Как правило, в качестве полей во многих практических задачах подразумеваются различного рода экраны мониторов, а элементами поля (клетками) являются пиксели. Даже сравнительно малые размеры экрана, например $N = 500 \times 500$, требуют по меньшей мере 25×10^4 переменных и уравнений. Решение такого размера систем уравнений является предельно возможным даже для самых современных сверхмощных компьютеров. Поэтому теория поиска решения с помощью множества шаблонов, обладающих свойством гомоморфности, — достаточно перспективная. Основные трудности, которые при этом возникают, связаны с поиском самодостаточных шаблонов. Если они имеются в заданном наборе, то с его помощью можно построить произвольную единицу поля (значит, и произвольную раскраску клетки поля), и задача решается просто — путем наложения единиц на клетки, соответствующие клеткам создаваемого образа. Если такого шаблона в наличии нет, то необходимо искать шаблон, который гомоморфен единице на определенной клетке поля. Затем с помощью сдвигов или другого шаблона перенести полученные единицы на другие недоступные клетки. При этом можно использовать различные приемы.

1. *Перемещение единицы*

Рассмотрим этот пример сначала для $K = 2$, т. е. для одноцветных шаблонов. Возьмем два шаблона на рис. 3.8, первый и пятый. Как известно, каждый из них не гомоморфен единице, однако с помощью их двоих можно построить единицу, как показано на рис. 4.1. Это минимальное поле размером $N = 5 \times 3$ (или $N = 3 \times 5$), где можно построить единицу в клетке 3 и за счет симметричного отражения — в клетке 13.

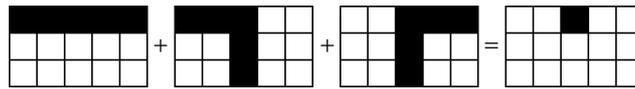


Рис. 4.1

Для полей большего размера таким же способом можно построить единицы во всех клетках, кроме тех, которые находятся в углах поля, с номерами

$$1, 2, n - 1, n, n + 1, n + 2, (m - 2)n + 1, (m - 2)n + 2, (m - 2)n - 1, (m - 2)n, (m - 1)n + 1, (m - 1)n + 2, mn - 1, mn. \quad (4.1)$$

Уже в поле размером не меньше, чем $N = 6 \times 4$, можно построить все единицы. Чтобы создать единицу в клетке 2, надо к единицам 3, 4, $n + 4$, $2n + 4$ добавить второй шаблон на рис. 4.1. Затем можно построить единицу в первой клетке, если добавить второй шаблон к единицам 2, 3, $n + 3$, $2n + 3$. Далее, по аналогии или зеркальным отражением можно получить все единицы.

Более сложный прием перемещения единицы применяют для многоцветных шаблонов. Иногда из двух заданных шаблонов один имеет простую структуру (типа одноцветного линейного), а другой гомоморфен единице, которая находится далеко от края поля. А необходимо построить единицу в первой клетке. Вернемся к примеру 3.4 из главы 3 (см. рис. 3.5). Здесь уравнение первого шаблона имеет вид: $s_1(\alpha) = \{(\alpha, 3), (\alpha + 1, 3), (\alpha + 2, 3)\}$. Второй шаблон имеет сложную структуру, он постепенно приводится к виду самодостаточного шаблона с уравнением

$$s_2(\alpha) = \{(\alpha, 9), (\alpha + 1, 1), (\alpha + n, 5), (\alpha + n + 1, 6)\}. \quad (4.2)$$

Рассмотрим последовательность преобразований (т. е. сведения шаблона к самодостаточному) на рис. 4.2, полагая, что первоначальный шаблон имеет координату метки $3n + 3$. На рис. 4.2 над шаблонами указана кратность, с которой эти шаблоны участвуют в преобразованиях, а внизу — координаты меток соответствующих шаблонов. Строим сначала единицу в клетке $3n + 4$, используя результаты главы 3. Для основной системы сравнений получаем определитель:

$$\text{Det} = \begin{vmatrix} 9 & 6 & 5 & 1 \\ 1 & 9 & 6 & 5 \\ 5 & 1 & 9 & 6 \\ 6 & 5 & 1 & 9 \end{vmatrix} = 6(\text{mod } 11). \quad (4.3)$$

раскрашенного шаблона эта задача иногда решается проще. Для раскрашенного шаблона длиной 2 эта задача решена в главе 3.

Пусть задан линейный шаблон $s_1(\alpha) = \{(\alpha, q_1), (\alpha + 1, q_2), (\alpha + 2, q_3)\}$ и его двойственный $s_2(\alpha) = \{(\alpha, q_3), (\alpha + 1, q_2), (\alpha + 2, q_1)\}$. Решим такую задачу: путем наложения этих шаблонов на себя образовать нулевой цвет в клетке $\alpha + 2$. Составим соответствующую систему сравнений для клеток $\alpha + 1$ и $\alpha + 2$:

$$\begin{aligned} x q_3 + y q_1 &= c \pmod{K}; \\ x q_2 + y q_2 &= 0 \pmod{K}, \end{aligned} \quad (4.5)$$

где $c \neq 0 \pmod{K}$. Определитель системы равен $q_2 (q_3 - q_1)$. Таким образом, если $q_3 \neq q_1$, то решение существует и имеет вид

$$x = -c q_1 [q_2 (q_3 - q_1)]^{-1}; \quad y = c q_3 [q_2 (q_3 - q_1)]^{-1}. \quad (4.6)$$

В результате наложения двух шаблонов в количестве $x s_1(\alpha) + y s_2(\alpha)$ получаем один шаблон с цветами $q_3 = x q_1 + y q_3 = c(q_1 + q_3)/q_2$ и $q_4 = c$. Для этого шаблона, чтобы получить единицу, необходимо выполнение условия $q_3 \neq q_4$, что равносильно $q_2 \neq q_1 + q_3$.

Пример 4.1. Пусть задан шаблон $s_1(\alpha) = \{(\alpha, 2), (\alpha + 1, 7), (\alpha + 2, 3)\}$ и $K = 11$. Определитель системы равен $7 \cdot (3 - 2) = 7$, $7^{-1} = 8 \pmod{11}$. По формулам (4.6) получаем: $x = -2 \cdot 8 c = -5 c$; $y = 3 \cdot 8 c$. Если взять $c = 6$, то получим $x = 3 \pmod{11}$, $y = 1 \pmod{11}$. А новый шаблон длиной 2 примет вид: $s_3(\alpha) = \{(\alpha, 9), (\alpha + 1, 6)\}$. Поскольку $9 \neq 6$, то с помощью нового шаблона и двойственного ему можно построить единицу, однако не в клетке $\alpha = 1$, поскольку для получения двойственного к $s_3(\alpha)$ шаблона необходимо получить в клетке $\alpha - 1$ нулевой цвет, складывая два первых шаблона.

Такой прием можно использовать и для линейных раскрашенных шаблонов большего объема. Если длина шаблона равна d , то при подходящих значениях цветов его клеток и порядке следования можно построить единицу в клетке с номером не меньше, чем $d - 1$. Теперь можно использовать прием, описанный в пункте 1, т. е. перемещать единицу.

Отметим, что в отличие от решения систем сравнений обычными методами, где трудоемкость решения оценивается полиномом четвертой степени, здесь трудоемкость касается только нахождения из данного множества гомоморфных шаблонов, которая выражается полиномом четвертой степени от константы, равной объему найденного шаблона.

4.2. ПРОБЛЕМЫ СОЗДАНИЯ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ

Как известно, проблемой обеспечения секретности передаваемой информации занимается криптология. Криптология разделяется на два направления: криптографию и криптоанализ. Цели этих направлений противоположны. Криптография занимается поиском и исследованием математических методов преобразования информации с целью ее засекречивания. А сфера интересов криптоанализа — исследовать возможности расшифровки зашифрованной информации. Напомним несколько определений, необходимых для дальнейшего изложения материала.

Шифрование — преобразовательный процесс, при котором исходный текст, называемый *открытым текстом*, заменяется *шифрованным текстом*.

Дешифрование — процесс, обратный шифрованию, при котором на основе ключа дешифрованный текст преобразуется в исходный.

Ключ — информация, необходимая для беспрепятственного шифрования или дешифрования текстов. Обычно ключ представляет собой последовательный ряд символов того же алфавита, в котором набрано информационное сообщение.

Пространство ключей — набор возможных значений ключа.

Криптостойкость — характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа, т. е. к криптоанализу.

Эффективность криптоалгоритма — отношение временных затрат криптоаналитика на вскрытие шифровки к временным затратам криптографа на создание шифровки.

Существует много криптографических систем, доступных и удобных для широкого круга пользователей. Среди них отметим *систему шифровки Вижинера*. В отличие от многоалфавитной подстановки, в алгоритме шифрования Вижинера ключ имеет конечную длину. Таким образом, здесь отсутствует требование шифровать каждую букву исходного текста отдельным значением ключа.

Подстановка Вижинера определяется как VIG: $(x_0, x_1, \dots, x_{n-1}) \rightarrow (y_0, y_1, \dots, y_{n-1}) = [(x_0 + k_0) \bmod N, (x_1 + k_1) \bmod N, \dots, (x_{n-1} + k_{n-1}) \times \times \bmod N]$, где N — количество символов в алфавите, а n — длина ключа Вижинера с компонентами k_i ($i = 0, 1, \dots, n$). Таким образом, на исходный текст X накладывается периодическая ключевая последовательность равной длины, и в результате сложения по модулю N соответствующих элементов последовательностей на выходе получают шифрованный текст Y .

В данной работе для шифрования текстов предлагается следующее.

Подстановка M , которая определяется как $M: (x_0, x_1, \dots, x_{n-1}) \rightarrow (y_0, y_1, \dots, y_{n-1}) = [(x_0 + s_1(1)) \bmod K, \dots, (x_i + s_{i+1}(i + 1)) \bmod K, \dots, (x_{n-1} + s_n(n)) \bmod K]$, где сложение набора шаблонов $S = [s_1(\alpha), s_2(\alpha), \dots, s_r(\alpha)]$ ведется по всему полю, а нижние индексы шаблонов вычисляются по правилу $r + 1 = 1$.

Открытый текст составляется в порядке нумерации клеток поля, т. е. представляет собой последовательность раскрашенных клеток в порядке их нумерации.

Пример 4.2. Пусть задано множество $S = [s_1(\alpha) = (\alpha, 1), (\alpha + 1, 1), \dots, (\alpha + d, 1)]$ и $K = 2$. Множество S состоит из одного шаблона длиной d и окрашенного одной краской. Шифрование состоит в наложении этого шаблона в горизонтальном положении для меток с координатами $\alpha = 1, 2, 3, \dots, N$. На рис. 4.3 слева показан открытый текст, а справа — зашифрованный с помощью линейного шаблона текст при $d = 3$.

Нетрудно заметить, что при использовании линейного шаблона шифрование строки состоит в следующем: от первой до $(d - 1)$ -й клетки проводится наложение $1, 0, 1, 0, \dots$, затем идет $d \pmod{2}$ и последние $d - 1$ клетки зеркально отражаются. Для криптоаналитика нужно перебрать числа от 2 до $n - 1$ и для каждого числа проверить n клеток, чтобы расшифровать текст. Трудоемкость расшифрования равна $n(n - 1)$. Поэтому такой набор шаблонов неэффективен.

На первый взгляд более сложная задача возникает, если чередовать попеременно горизонтальное наложение линейного шаблона с его вертикальным положением. Однако в этом случае картина наложений также тривиальная, хотя сложность расшифровки возрастает до четвертого порядка.

Рассмотрим нелинейные шаблоны. Если использовать только одно положение такого шаблона и перемещать только с учетом допустимых положений его метки, то в первой строке зашифрованного текста получим аналогию с линейным шаблоном. В этом случае можно расшифровать первую строку так, как и строку выше. Чтобы этого избежать, можно представить поле как цилиндричес-

0	1	1	0	0	1	1	1	0	1	1	0	1	1	0	0	1	1
1	1	0	0	0	0	1	0	1	0	1	1	1	1	1	0	0	0

Рис. 4.3

кое, склеенное по горизонтальным и вертикальным краям. В этом случае все строки и столбцы будут иметь одинаковую уязвимость.

Пусть шаблон находится в границах прямоугольника размером $p \times q$. Тогда число всяких шаблонов, которые можно на нем построить, равно $L = 2^{pq} / 2^c$, где $c \leq 0,5pq$. Если брать два шаблона и каждый вращать на плоскости, то для определения типа этого шаблона надо перебрать $0,5L(L - 1)$ вариантов, что составляет величину порядка 2^{pq} . Это число еще можно преодолеть для сравнительно небольших p и q при расшифровке криптосистем, в которых используется одноцветные шаблоны.

Если перейти к раскрашенным шаблонам, то можно применить те же рассуждения, но в основу оценок положить число K . Здесь можно достичь определенной гарантии, даже если использовать сравнительно небольшие по размерам шаблоны.

Заметим, что предложенный метод шифрования рассчитан на информацию, которая теряет свою ценность за короткое время после передачи. Например, информация, которая передается по мобильным телефонам. Имея небольшое программирующее устройство для шифрования и дешифрования, которое компактно подключается к мобильному телефону, можно надежно защитить необходимую информацию от несанкционированного ее изъятия.

4.3. ИСПОЛЬЗОВАНИЕ ШАБЛОНОВ ДЛЯ РЕШЕНИЯ НЕКОТОРЫХ СИСТЕМ СРАВНЕНИЙ

Иногда метод решения задач построения дискретных образов с помощью шаблонов можно применять для произвольной системы сравнений, если матрицы этих систем очень близки по структуре. Это относится к разреженным матрицам или теплицевым, которые легко достроить до вида матриц систем, где используются различные шаблоны. Указанная проблема мало исследована, поэтому ограничимся небольшим примером.

Пусть необходимо решить следующую систему линейных сравнений по модулю 2:

$$\left. \begin{array}{rcl} x_1 & & +x_6 & = b_1 \\ x_1 & +x_2 & & +x_6 & +x_7 & = b_2 \\ x_1 & & +x_3 & & +x_6 & +x_7 & = b_3 \\ & +x_2 & +x_3 & +x_4 & +x_6 & +x_7 & = b_4 \\ & & +x_3 & +x_4 & +x_6 & +x_7 & = b_5 \\ & & & x_4 & & +x_7 & = b_6 \end{array} \right\} \text{ mod } 2.$$

Эта система похожа на систему сравнений, составленную для двух линейных шаблонов $S = \{3, 5\}$ и линейного поля длиной $n = 8$. Однако она отличается тем, что в третьем уравнении отсутствует переменная x_2 . Добавим в левую и правую части этого уравнения переменную x_2 . Теперь вместо правой части b_3 всюду записываем $b_3 + x_2$. Согласно теории, разработанной в главе 2, получаем решение приведенной системы:

$$\begin{aligned}
 x_1 &= b_1 + b_2 + (b_3 + x_2) + b_5 + b_6; \\
 x_2 &= b_4 + b_5 + b_6; \\
 x_3 &= b_2 + (b_3 + x_2); \\
 x_4 &= b_1 + b_2 + b_4 + b_5 + b_6; \\
 x_6 &= b_2 + (b_3 + x_2) + b_5 + b_6; \\
 x_7 &= b_1 + b_2 + b_4 + b_5 + b_6.
 \end{aligned}
 \tag{4.7}$$

Если добавленная переменная при решении не попадает в свое решение (как в данном случае), то решение (4.7) существует всегда для произвольных правых частей. Если же переменная попадает в свое решение, то, сокращая эту переменную в обеих частях, получаем зависимость между значениями в правой части. И если она не выполняется, то система не имеет решений.

Описанный прием можно применять и для раскрашенных шаблонов, однако обнаруживать сходство систем при этом труднее.

СПИСОК ЛИТЕРАТУРЫ

К части I

1. *Алгебраические* исследования в комбинаторике / Под редакцией И.А. Фараджева. — М.: Наука, 1978. — 187 с.
2. *Асельдерова И.М.* Об оптимальном кодировании некоторых арифметических графов // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова АН УССР, 1987. — С. 47—54.
3. *Асельдеров З.М., Донец Г.А.* Представление и восстановление графов. — К.: Наук. думка, 1991. — 178 с.
4. *Асельдерова И.М., Донец Г.А.* Об оптимальном кодировании циклов и однородных деревьев // Теория и практика разработки и внедрения интегрированных АСУ. — К., 1988. — С. 56—62.
5. *Асельдерова И.М., Донец Г.А.* Об оптимальном кодировании однородных деревьев // Математические методы дискретной оптимизации. — К.: Изд. КГУ им. Т.Г. Шевченка, 1986. — С. 33—37.
6. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979. — 270 с.
7. *Баннаи Э., Ито Т.* Алгебраическая комбинаторика. Схемы отношений. — М.: Мир, 1987. — 373 с.
8. *Белага Э.Г.* К раскраске плоских графов // УМЖ. — 1972. — № 3. — С. 125—128.
9. *Белага Э.Г.* Мини-геометрии (четыре фрагмента математики XX века). — М.: Знание, 1977. — С. 22.
10. *Белага Э.Г.* Об одной интерпретации 4-раскраски плоского графа // Успехи мат. наук. — 1972. — 27, вып. 3. — С. 191.
11. *Берж К.* Теория графов и ее применение. — М.: Изд-во иностр. л-ры, 1962. — 319 с.
12. *Ван дер Варден Б.Л.* Алгебра. — М.: Наука, 1979. — 624 с.
13. *Бончев Д.Г.* Характеризация химических структур с помощью теории информации и теории графов: Автореф. дис... д.ф.-м. наук: 01.01.09. — М.: МГУ, 1984. — 28 с.
14. *Боревич З.И., Шафаревич И.Р.* Теория чисел. — М.: Наука, 1985. — 503 с.
15. *Бусленко Н.П.* Автоматизация имитационного моделирования сложных систем. — М.: Наука, 1977. — 288 с.
16. *Винцюк Т.К.* Анализ, распознавание и интерпретация речевых сигналов. — К.: Наук. думка, 1987. — 264 с.
17. *Воеводин В.В.* Математические модели и методы в параллельных процессах. — М.: Наука, 1986. — 295 с.

18. Глушков В.М. О кибернетике как науке / Вып. Кибернетика, мышление, жизнь. — М.: Мысль, 1964. — С. 53—61.
19. Глушков В.М., Капитонова Ю.В., Лetichevский Л.А. Теоретические основы проектирования дискретных систем // Кибернетика. — 1977. — № 6. — С. 5—20.
20. Глушков В.М., Стогний А.А. и др. Системы автоматизации творческих процессов в научных исследованиях, проектировании и задачах управления роботами // Кибернетика. — 1981. — № 6. — С. 110—115.
21. Горбатов В.А. Основы дискретной математики. — М.: Высш. школа, 1986. — 311 с.
22. Григорьян Ю.Г. Использование вычислительных машин для синтеза цифровых автоматов // Изв. АН АрмССР. Серия тех. науки. 1963. — XVI, № 6. — С. 41—47.
23. Григорьян Ю.Г. Арифметический метод минимизации булевских функций // Материалы научных семинаров по теоретическим и прикладным вопросам кибернетики / Теория автоматов. — К.: Ин-т кибернетики, 1964. — С. 3—24.
24. Григорьян Ю.Г. Вариационная задача функций алгебры логики и метод ее реализации на ЭВМ // Кибернетика. — 1967. — № 1. — С. 26—30.
25. Григорьян Ю.Г., Маноян Г.К. Некоторые вопросы арифметической интерпретации неориентированных графов // Кибернетика. — 1977. — № 3. — С. 129—131.
26. Григорьян Ю.Г. Отображение сокращенных дизъюнктивных нормальных форм на графы // Кибернетика. — 1979. — № 3. — С. 105—107.
27. Григорьян Ю.Г. Классификация и статистические свойства арифметических графов // Кибернетика. — 1979. — № 6. — С. 9—12.
28. Григорьян Ю.Г. Геометрия арифметических графов // Кибернетика. — 1982. — № 4. — С. 1—4.
29. Григорьян Ю.Г. Задача существования и вопросы представления натуральных арифметических графов // Журнал выч. матем. и матем. физики АН СССР. — 1984. — № 11. — С. 1751—1756.
30. Григорьян Ю.Г. Группы автоморфизмов булевских графов // II Всесоюзная конференция «Математические методы распознавания образов» (тезисы докладов). — Дилижан (АрмССР), 1985. — С. 47—48.
31. Григорьян Ю.Г., Адоц А.М. Группы автоморфизмов арифметических графов // Труды ВЦ АН АрмССР и ЕГУ / Математические вопросы кибернетики и вычислительной техники. — 1988. — 15. — С. 174—179.
32. Григорьян Ю.Г., Адоц А.М. Свойства регулярных натуральных арифметических графов // Кибернетика. — 1990. — № 5. — С. 112—113.
33. Григорьян Ю.Г. Группы арифметических автоморфизмов простых циклов // Кибернетика. — 1990. — № 4. — С. 9—16.
34. Григорьян Ю.Г. Группы, индуцируемые булевскими графами // Кибернетика. — 1990. — № 6. — С. 111—113.
35. Григорьян Ю.Г. Информационные методы оценки сложности дискретных объектов в стандартных представлениях // II Всесоюзная конференция по актуальным проблемам информатики и вычислительной техники «Информатика-87» (тезисы докладов). — Ереван, 1987. — С. 69—70.
36. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982. — 416 с.

37. *Дмитриев А.Н., Журавлев Ю.И., Кренделев Ф.П.* О математических принципах классификации предметов и явлений // Дискретный анализ. — Новосибирск: ИМ СО АН СССР, 1966. — Вып. 7. — С. 3—11.
38. *Донец Г.А.* О графах, задаваемых аналитическим способом // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова АН УССР, 1987. — С. 20—27.
39. *Донец Г.А.* Об оптимальном кодировании однородных деревьев в арифметических графах // Методы решения экстремальных задач и смежные вопросы. — К.: Ин-т кибернетики им. В.М. Глушкова АН УССР, 1987. — С. 72—77.
40. *Донец Г.О., Неженцев Ю.И.* Арифметичні графи та їх представлення // Доп. АН УРСР. Сер. А. — 1990. — № 11. — С. 5—8.
41. *Донец Г.А., Неженцев Ю.И.* Об оптимальном кодировании циклов и наборов цепей в арифметических графах // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова АН УССР, 1990. — С. 73—80.
42. *Донец Г.А., Неженцев Ю.И.* Об оценке сложности алгоритмов в арифметических графах // Методы решения задач нелинейного и дискретного программирования. — К.: Ин-т кибернетики им. В.М. Глушкова АН УССР, 1991. — С. 79—88.
43. *Донец Г.А.* Необходимые и достаточные условия связности арифметических графов // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 1992. — С. 69—74.
44. *Донец Г.А., Асельдерова И.М.* Условия однородности арифметических графов // Оптимизация и ее приложения. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 1993. — С. 23—30.
45. *Донец Г.А.* О зависимости связности арифметических графов от числа образующих // Методы исследования экстремальных задач. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 1994. — С. 47—52.
46. *Донец Г.А., Шулинок И.Э.* Однородные натуральные арифметические графы // Препр. 98-7. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 1998. — С. 18.
47. *Донец Г.А., Шулинок И.Э.* Об оценке сложности алгоритмов для натуральных модульных графов // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 2001. — С. 61—68.
48. *Донец Г.А., Шулинок И.Э.* Оптимальное представление однородных деревьев первого ранга в классе А-графов // Комп'ютерна математика. Оптимізація обчислень. — К.: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2001. — С. 127—134.
49. *Донец Г.А., Шулинок И.Э.* Об изоморфизме натуральных арифметических графов // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 2003. — С. 3—10.
50. *Донец Г.А., Шулинок И.Э.* Об оценке сложности алгоритмов для натуральных модульных графов // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 2001. — С. 61—68.
51. *Донец Г.А., Шулинок И.Э.* Об общем представлении числовых графов // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 2004. — С.11—18.

52. *Елфимова Л.Д., Капитонова Ю.В.* Быстрый алгоритм для умножения матриц и его эффективная реализация на систолических массивах // Кибернетика и системный анализ. — 2001. — № 1. — С. 135—150.
53. *Елфимова Л.Д., Капитонова Ю.В.* Интегрированный подход к проектированию процессорных массивов с систолической организацией вычислений // Кибернетика и системный анализ. — 2002. — № 6. — С. 3—15.
54. *Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И.* Лекции по теории графов. — М.: Наука, 1990. — 384 с.
55. *Журавлев Ю.И.* Теоретико-множественные методы в алгебре логики // Проблемы кибернетики. — 1962. — Вып. 8. — С. 5—44.
56. *Журавлев Ю.И.* Об алгебраическом подходе к решению задач распознавания и классификации // Проблемы кибернетики. — 1978. — Вып. 3. — С. 5—68.
57. *Гупал А.М., Сергиенко И.В.* Оптимальные процедуры распознавания. — К.: Наук. думка, 2008. — 232 с.
58. *Зыков А.А.* Теория конечных графов. — Новосибирск: Наука, 1969. — 543 с.
59. *Зыков А.А.* Основы теории графов. — М.: Наука, 1987. — 384 с.
60. *Каюров В.Ю., Шулинок Г.А.* Полиномиальный алгоритм проверки изоморфизма деревьев // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 2002. — С. 92—97.
61. *Кострикин А.И.* Введение в алгебру. — М.: Наука, 1977. — 495 с.
62. *Кэртис Ч., Райнер И.* Теория представлений конечных групп и ассоциативных алгебр. — М.: Наука, 1969. — 668 с.
63. *Курош А.Г.* Теория групп. — М.: Наука, 1967. — 648 с.
64. *Михелович Ш.Х.* Теория чисел. — М.: Высш. школа, 1962. — 260 с.
65. *Неженцев Ю.И.* Об оценке сложности алгоритмов поиска в арифметических графах // Математические методы и программное обеспечение в системах принятия решения и проектирования. — К.: Ин-т кибернетики им. В.М. Глушкова АН УССР, 1990. — С. 14—24.
66. *Пападимитриу Х., Стайглиц К.* Комбинаторная оптимизация / Алгоритмы и сложность. — М.: Мир, 1985. — 512 с.
67. *Оре О.* Теория графов. — М.: Наука, 1980. — 336 с.
68. *Поваров Г.И.* Математическая теория синтеза контактных (1,К)-полусюнктов // ДАН СССР. — 1955. — **100**, № 5. — С. 909—912.
69. *Розенфельд Б.А.* История неевклидовой геометрии. — М.: Наука, 1976. — 413 с.
70. *Сапоженко А.А., Асатрян А.С., Кузюкин Н.Н.* Обзор некоторых результатов по задачам о покрытии // Дискретный анализ. — 1977. — Вып. 30. — С. 46—75.
71. *Свами М., Тхуласираман К.* Графы, сети и алгоритмы. — М.: Мир, 1984. — 455 с.
72. *Серр Ж.-П.* Линейные представления конечных групп. — М.: Мир, 1970. — 131 с.
73. *Теория и методы автоматизации проектирования вычислительных систем* / Под ред. М. Брейера. — М.: Мир, 1977. — 283 с.
74. *Ульман Д.* Вычислительные аспекты СБИС. — М.: Радио и связь, 1990. — 480 с.
75. *Хамермеш М.* Теория групп и ее применение к физическим проблемам. — М.: Мир, 1969. — 587 с.

76. Хан Г., Шапиро С. Статистические модели в инженерных задачах. — М.: Мир, 1969. — 281 с.
77. Харари Ф. Теория графов. — М.: Мир, 1973. — 301 с.
78. Хассе Г. Лекции по теории чисел. — М.: ИЛ, 1953. — 527 с.
79. Чегис И.А., Яблонский С.В. Логические способы контроля электрических схем // Тр. Матем. ин-та им. В.А. Стеклова АН СССР. — 1958. — **51**. — С. 270—360.
80. Шулінок Г.О. Про ізоморфізм натуральних модульних графів // Теорія оптимальних рішень. — К.: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2004. — С.69—73.
81. Шулінок Г.О. Про ізоморфізм одного підкласу числових графів // Праці Міжн. конф. «Питання оптимізації обчислень (ПОО-XXXIII)», присвяченої пам'яті академіка В.С. Михалевича (Крим, Велика Ялта, смт. Кацивелі, 19—23 вересня 2005 р.) — К.: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2005. — С. 216.
82. Шулинок Г.А. Об изоморфизме регулярных NM-графов // Теория оптимальных решений. — К.: Ин-т кибернетики НАН Украины, 2005. — С. 100—106.
83. Шулинок Г.А. Об одном методе раскраски натуральных модульных графов // Компьютерная математика. — 2006. — № 1. — С. 78—89.
84. Шулинок И.Э. Структура натуральных арифметических графов с нечетным числом вершин // Оптимизация и ее приложения. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 1997. — С. 54—60.
85. Шулинок И.Э. Об одном классе числовых графов // Теория и приложения методов оптимизации. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 1998. — С. 24—29.
86. Шулинок И.Э. О связности натуральных модульных графов // Кибернетика и системный анализ. — 1998. — № 5. — С. 50—53.
87. Шулинок И.Э. О связности и цикломатическом числе натуральных модульных графов // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 1999. — С. 51—57.
88. Шулинок И.Э. Полное описание структуры одного подкласса NM-графов // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 1999. — С. 75—81.
89. Шулинок И.Э. О сложности алгоритмов на числовых графах // Прикладная математика: Тез. докл. Междунар. конф., посвященной 65-летию со дня рождения Б.Н.Пшеничного (25—28 июня, 2002). — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, НТУУ «КПИ», ИПСА, 2002. — С. 110—111.
90. Яблонский С.В. Функциональные построения в k -значной логике // Тр. Матем. ин-та им. В.А. Стеклова АН СССР. — 1958. — **51**. — С. 5—143.
91. Kantz W.H. Optimized data encoding for digital computers // IRE Conv. Rec. — 1954. — **4**. — P. 47—56.
92. Kung H.T., Leiserson C.E. Systolic arrays for VLSI // Sparse Matrix Symp., 1978. — Philadelphia: SIAM, 1979. — P. 252 — 282.
93. Kung H.T. Why systolic architectures? // Computer. — 1982. — **15**, N 1. — P. 37—46.

94. *Monien B.* The bandwidth minimization problems for caterpillars with hair length 3 is NP-complete // *SIAM J. Alg. Disc. Meth.* — 1986. — 7, N 4. — P. 505—512.

95. *Papadimitrion C.H.* The NP-completeness of the bandwidth minimization problem // *Computing.* — 1976. — 16. — P. 263—270.

К части II

1. *Айзерман М.А., Браверман Э.М., Розоноер Л.И.* Теоретические основы метода потенциальных функций в задаче обучения автоматов разделению входных ситуаций на классы // *Автоматика и телемеханика.* — 1964. — 25, № 6. — С. 42—47.

2. *Айзерман М.А.* Опыты по обучению машин распознаванию зрительных образов // *Биологические аспекты кибернетики.* — М., 1962. — С. 174—183.

3. *Айзерман М.А., Браверман Э.М., Розоноер Л.И.* Методы потенциальных функций в теории обучения машин. — М.: Наука, 1970. — 384 с.

4. *Аркадьев А.Г., Браверман Э.М.* Опыты по обучению машины распознаванию образов. — М.: Наука, 1964. — 113 с.

5. *Асельдеров З.М., Донец Г.А., Самер И.М. Альшаламе.* Решение задачи о построении линейных образов // *Сб. тр. V Международной конф. «Интеллектуальный анализ информации (ИАИ)».* — К.: Просвіта, 2005. — С. 31—40.

6. *Асельдеров З.М., Самер И.М. Альшаламе.* Построение цветowych дискретных изображений на плоскости // *Математические машины и системы.* — 2006. — № 1. — С. 113—120.

7. *Барабанюк Т.Н. и др.* Система автоматического кодирования изображений печатных плат // *Автоматизированные системы обработки изображений (АСОИЗ-81): Тез. докл. I Всесоюз. конф. (9—11 июня 1981 г.).* — М., 1981. — С. 109.

8. *Башкиров О.А., Браверман Э.М., Мучник И.Б.* Алгоритмы обучения машин распознавания зрительных образов, основанные на использовании потенциальных функций // *Автоматика и телемеханика.* — 1964. — 25, № 5. — С. 11—19.

9. *Бонгард М.М.* Проблема узнавания. — М.: Наука, 1967. — 320 с.

10. *Бонгард М.М.* Моделирование процесса узнавания на цифровой счетной машине // *Биофизика.* — 1961. — 4, вып. 2.

11. *Боревич З.И., Шафаревич И.Р.* Теория чисел. — М.: Наука, 1985. — 504 с.

12. *Браверман Э.М.* Некоторые вопросы построения машин, классифицирующих объекты по не заданному заранее признаку // *Автоматика и телемеханика.* — 1960. — 21, № 10. — С. 21—26.

13. *Браверман Э.М.* Метод потенциальных функций в задаче обучения машины распознаванию образов без учителя // *Автоматика и телемеханика.* — 1966. — № 10. — С. 8—15.

14. *Браверман Э.М., Дорофеев А.А.* Эксперименты по обучению машин распознаванию образов без поощрения // *Самообучающиеся автоматические системы.* — М.: Наука, 1966. — С. 11—16.

15. *Вапник В.А., Лернер А.Я., Червоненкис А.Я.* Системы обучения распознаванию образов при помощи обобщенных портретов // *Изв. АН СССР. Техническая кибернетика.* — 1965. — № 1. — С. 67—71.

16. Вапник В.А., Червоненкис А.Я. Теория распознавания образов. — М.: Наука, 1974. — 415 с.
17. Васильев В.И. Распознающие системы: Справочник. — К.: Наук. думка, 1983. — 422 с.
18. Верхаген К. и др. Распознавание образов: состояние и перспективы. — М.: Радио и связь, 1985. — 104 с.
19. Воеводин В.В. Линейная алгебра. — М.: Наука, 1980. — 400 с.
20. Горелик А.Л. Современное состояние проблемы распознавания. — М.: Радио и связь, 1985. — 274 с.
21. Гренандер У. Лекции по теории образов. Т. 1. Синтез образов / Пер. с англ. — М.: Мир, 1979. — 384 с.
22. Гренандер У. Лекции по теории образов. Т. 2. Анализ образов / Пер. с англ. — М.: Мир, 1981. — 448 с.
23. Дейнека В.С., Сергиенко И.В. Модели и методы решения задач в неоднородных средах. — К.: Наук. думка, 2001. — 606 с.
24. Донец Г.А., Самер И.М. Альшаламе. Задача о дискретном построении образов // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 2004. — С. 117—122.
25. Донец Г.А., Самер И.М. Альшаламе. Решение задачи о построении линейной мозаики // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 2005. — С. 15—24.
26. Дорофеев А.А. Обучение машины распознаванию образов без поощрения // Техническая кибернетика. — М.: Наука, 1966. — Т. 2. — С. 23—30.
27. Елисеев В.К., Ковалевский В.А. Исследование алгоритма распознавания машинописных цифр // Журн. вычислит. матем. и матем. физики. — 1962. — 2, № 5. — С. 165—177.
28. Журавлев Ю.И. Экстремальные задачи, возникающие при обосновании эвристических процедур // Проблемы прикладной математики и механики. — М., 1971. — С. 67—74.
29. Журавлев Ю.И., Никифоров В.В. Алгоритмы распознавания, основанные на вычислении оценок // Кибернетика. — 1971. — № 3. — С. 1—11.
30. Журавлев Ю.И. Непараметрические задачи распознавания образов // Кибернетика. — 1976. — № 6. — С. 93—103.
31. Журавлев Ю.И. Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики. — 1978. — Вып. 33. — С. 5—68.
32. Загоруйко Н.Г. Методы распознавания и их применение. — М.: Сов. радио, 1972. — 208 с.
33. Загоруйко Н.Г. Эмпирическое предсказание и распознавание образов. — Новосибирск: Наука, Сиб. отделение, 1980. — 137 с.
34. Загоруйко Н.Г. Классификация задач прогнозирования на таблицах «объект — свойство» // Машинные методы обнаружения закономерностей: Вычисл. системы. — 1981. — Вып. 88. — С. 3—7.
35. Ивахненко А.Г. Самообучающиеся системы распознавания и автоматического управления. — К.: Техніка, 1969. — 512 с.
36. Карапетян Г.К., Мацелло В.В. Структурный алгоритм распознавания графических изображений // Распознавание образов и автоматизация проектирования робототехнических зрительных систем. — К., 1982. — С. 44—54.

37. Кийко В.М., Шлезингер М.И. Анализ изображений, порождаемых блочными двумерными грамматиками // Обработка и распознавание сигналов. — К., 1975. — С.19—37.
38. Кийко В.М. Алгоритм распознавания изображений, порождаемых блочными двумерными грамматиками // Распознавание образов. — К., 1977. — С. 3—23.
39. Сергиенко И.В. Математические модели и методы решения задач дискретной оптимизации. — К.: Наук. думка, 1988. — 472 с.
40. Ковалевский В.А. Статистический подход к проблеме обучения распознавания образов / Тр. III Всесоюзной конф. по автоматическому управлению (Одесса, сентябрь 1965). — М.: Мир, 1967.
41. Ковалевский В.А. О корреляционном методе распознавания образов // Читающие автоматы. — К.: Наук. думка, 1965. — С.22—32.
42. Ковалевский В.А. Оптимальный алгоритм распознавания некоторых последовательностей изображений // Кибернетика. — 1967. — № 4. — С. 25—31.
43. Ковалевский В.А. Методы оптимальных решений в распознавании изображений. — М.: Наука, 1976. — 328 с.
44. Ковалевский В.А. Локальные и глобальные решения в распознавании изображений // ТИИЭР. — 1979. — № 5. — С. 50—58.
45. Коваль В.К. Распознавание по частям // Распознавание образов. — К., 1977. — С. 41—53.
46. Кривый С.Л. О некоторых методах решения и критериях совместности систем линейных диофантовых уравнений в области натуральных чисел // Кибернетика и системный анализ. — 1999. — № 4. — С.12—36.
47. Нарасимхан Р. Метод маркировки и синтаксическое описание изображений // Автоматический анализ сложных изображений. Сб. научн. тр. — М.: Мир, 1969. — С.87—110.
48. Нарасимхан Р. Синтаксическая интерпретация классов изображений // Автоматический анализ сложных изображений. — М.: Мир, 1969. — С. 111—129.
49. Патрик Э. Основы теории распознавания образов / Пер. с англ. — М.: Сов. радио, 1980. — 408 с.
50. Раудис Ш.Ю. О количестве априорной информации для построения алгоритма классификации // Изв. АН СССР. Техн. кибернетика. — 1972. — № 4. — С. 168—174.
51. Раудис Ш.Ю. Ограниченность выборок в задачах классификации // Статист. пробл. упр. — 1973. — Вып. 18. — С. 1—180.
52. Розенблатт Ф. Принципы нейродинамики. — М.: Мир, 1965. — 480 с.
53. Самер И.М. Альшаламе. Задача о построении образов двумерной мозаики // Математические машины и системы. — 2006. — № 3. — С. 135—142.
54. Ткачев И.И. Об эквивалентности некоторых моделей для распознавания образов // Кибернетика. — 1980. — № 3. — С. 147.
55. Ту Дж., Гансалес Р. Принципы распознавания образов. — М.: Мир, 1978. — 411 с.
56. Фу К.С. Последовательные методы в распознавании образов и обучении машин. — М.: Наука, 1971. — 256 с.

Список литературы

57. Фу К.С. Структурные методы в распознавании образов. — М.: Мир, 1977. — 320 с.
58. Фукунага К. Введение в статистическую теорию распознавания образов. — М.: Наука, 1979. — 368 с.
59. Хомский Н. Формальные свойства грамматик // Кибернетический сб. Новая серия, вып.2. — М.: Мир, 1966.
60. Шлезингер М.И. О самопроизвольном различении образов // Читающие автоматы. — К.: Наук. думка, 1965. — С. 36—39.
61. Шлезингер М.И. Взаимосвязь обучения и самообучения в распознавании образов // Кибернетика. — 1968. — № 2. — С.13—17.
62. Якубович В.А. О некоторых общих принципах построения обучающих опознающих систем // Самообучающиеся автоматические системы. — М.: Наука, 1966. — С.41—47.

ОГЛАВЛЕНИЕ

ЧАСТЬ I. ЧИСЛОВЫЕ ГРАФЫ	3
Введение	3
Глава 1. Основные понятия теории числовых графов	7
1.1. Нумерация графов	7
1.2. Графы, задаваемые аналитическим способом	14
1.3. Числовые графы	25
Глава 2. Арифметические графы (<i>A</i>-графы) и их свойства	32
2.1. Об оптимальном кодировании цепей в классе <i>NA</i> -графов	32
2.2. О перечислении способов кодирования набора цепей	39
2.3. Матрица образующих <i>NA</i> -графов и циклы	45
2.4. Представление фактороидов	48
2.5. Представление набора цепей	57
2.6. Однородные натуральные арифметические графы	65
2.7. Необходимые и достаточные условия связности <i>NA</i> -графов	83
2.8. Представление однородных деревьев первого ранга	96
2.9. Оптимальная кодировка однородных деревьев второго ранга	103
2.10. О гамильтоновости арифметических графов	107
2.11. Об изоморфизме <i>NA</i> -графов	112
Глава 3. Модульные графы (<i>M</i>-графы) и их свойства	120
3.1. Представление модульных графов	120
3.2. О связности натуральных модульных графов (<i>NM</i> -графов)	125
3.3. О цикломатическом числе <i>NM</i> -графов	129
3.4. Структура множества <i>NM</i> -графов с двумя образующими	135
3.5. Изоморфизм натуральных модульных графов	141
Глава 4. Проблемы построения эффективных алгоритмов на числовых графах	163
4.1. Об общем представлении числовых графов	163
4.2. Оценка сложности базового алгоритма поиска в глубину на <i>NM</i> -графах	172
4.3. Оптимальный алгоритм поиска в глубину на <i>NM</i> -графах с двумя образующими	181
4.4. Оптимальный алгоритм поиска в глубину для произвольных <i>NM</i> -графов	187

ЧАСТЬ II. ПОСТРОЕНИЕ ДИСКРЕТНЫХ ОБРАЗОВ	192
Введение	192
Глава 1. Построение линейной мозаики	206
1.1. Задача построения цветной мозаики	206
1.2. Построение базиса решений задачи для двух одноцветных шаблонов ...	209
1.3. Решение задачи для линейной двухцветной мозаики	215
1.4. Числовые графы и линейная мозаика	221
1.5. Многоцветные двойственные шаблоны	229
1.6. Линейная система для произвольных цветных шаблонов	237
Глава 2. Задача построения двумерной одноцветной мозаики	250
2.1. Постановка задачи	250
2.2. Допустимое поле двумерных шаблонов и их уравнения	253
2.3. Построение базиса решения для одного шаблона	257
2.4. Построение базиса решения для нескольких шаблонов	265
Глава 3. Построение двумерной многоцветной мозаики	271
3.1. Построение плоских изображений для $K > 2$	271
3.2. Построение базиса решений для одного шаблона	273
3.3. Построение базиса решений для многих шаблонов	279
Глава 4. Применение теории построения дискретных образов	283
4.1. Решение систем сравнений больших размеров	283
4.2. Проблемы создания криптографической системы	287
4.3. Использование шаблонов для решения некоторых систем сравнений	289
Список литературы	291
К части I	291
К части II	296

Наукове видання
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ КІБЕРНЕТИКИ ім. В.М. ГЛУШКОВА

ДОНЕЦЬ Георгій Панасович
СЕРПІЄНКО Іван Васильович

ЧИСЛОВІ ГРАФИ ТА ПОБУДОВА ДИСКРЕТНИХ ОБРАЗІВ

(російською мовою)

Київ, Науково-виробниче підприємство
«Видавництво “Наукова думка” НАН України», 2014

Художній редактор *І.Р. Сільман*
Технічний редактор *Т.С. Березяк*
Коректор *О.Є. Челок*
Оператор *Л.В. Багненко*
Комп'ютерна верстка *Л.В. Багненко*

Підп. до друку 11.07.2014. Формат 60×90/16. Папір офс. № 1.
Гарн. Таймс. Друк. офс. Ум. друк. арк. 19,0.
Обл.-вид. арк. 16,5. Тираж 150 прим. Зам. № ДФ 224

НВП «Видавництво “Наукова думка” НАН України»
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру ДК № 2440 від 15.03.2006 р.
01601 Київ 1, вул. Терещенківська, 3

ПП «Видавництво “Фенікс”»
03680 Київ 680, вул. Шутова, 13б

