Національна академія наук України
Інститут кібернетики ім. В.М. Глушкова

Чжан Бінь

УДК 519.1

РОЗРОБКА МЕТОДІВ ТА АЛГОРИТМІВ РОЗВ'ЯЗУВАННЯ ЗАДАЧ ПРО МАТЕМАТИЧНИЙ СЕЙФ

01.05.01 – теоретичні основи інформатики та кібернетики

Автореферат
дисертації на здобуття наукового ступеня
кандидата фізико-математичних наук

Київ – 2007

Дисертацією є рукопис

Робота виконана в Національному технічному університеті України „КПІ” Міністерства освіти і науки України

Науковий керівник: доктор фізико-математичних наук **Донець Георгій Панасович ,** Інститут кібернетики ім. В.М. Глушкова НАН України, завідувач відділу №110

Офіційні опоненти: доктор фізико-математичних наук **Кривий Сергій Лук’янович**, Інститут кібернетики ім. В.М. Глушкова НАН України, провідний науковий співробітник, професор.

кандидат фізико-математичних наук **Каюров Василь Юрійович,** Міжнародний науковий центр технології програмування „Технософт”, завідувач відділом технології програмування.

Провідна установа: Київський національний університет імені Тараса Шевченка, факультет кібернетики, кафедра математичних методів еколого-економічних досліджень.

Захист відбудеться “ ___” “_____” 2007 р. о _____ годині на засіданні спеціалізованої вченої ради Д 26.194.02 при Інституті кібернетики імені В.М.Глушкова НАН України за адресою:
03680, МСП, Київ-187, проспект Академіка Глушкова , 40

З дисертацією можна ознайомитися в науково-технічному архіві Інституту

Автореферат розісланий “___” _____2007 р.

Учений секретар
спеціалізованої вченої ради СИНЯВСЬКИЙ В.Ф.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Дисертаційна робота присвячена одному із аспектів застосування теорії графів та теорії чисел для розв'язування позиційних ігор, які носять загальну назву як задачі про математичний сейф. Цей аспект стосується питань комбінаторної оптимізації на порівняно нових математичних об'єктах і ще недостатньо висвітлений в науковій літературі.

Актуальність теми. Дослідження задач дискретної оптимізації є передумовою успішного моделювання важливих економічних, природних, соціальних та інших процесів. Наукові публікації протягом минулих двадцяти-тридцяти років в галузі дискретної оптимізації свідчать про необхідність і важливість подібних досліджень. Це пов'язано з тим, що в останній час зросла актуальність розв'язування таких задач при прийнятті рішень в галузі управління та планування виробничих процесів, в задачах геометричного проектування, перспективного планування, теорії розкладів та інших, пов'язаних з вибором одного з можливих варіантів дії. Серед класу комбінаторних оптимізаційних задач особливе місце займають задачі на вершинно розташованих множинах. В Україні серед вчених, роботи яких присвячені різним напрямкам дискретної математики та її застосуванням, в першу чергу слід відзначити Сергієнка І.В., Шора Н.З., Стояна Ю.Г., а також Гуляницького Л.Ф., Донця Г.П., Ємця О.О., Ляшенка І.М., Павлова О.А., Шила В.П., Яковлева С.В. та керовані ними наукові колективи.

Аналіз використання результатів цих досліджень дозволяє зробити висновок про актуальність нових підходів і методів комбінаторної оптимізації, а також про необхідність та своєчасність дослідження властивостей задач оптимізації комбінаторного типу.

У дисертаційній роботі пропонується новий напрямок в цьому питанні, в ній розроблено методи розв'язування дискретних задач, які виникають в теорії

кодування, теорії захисту інформації та інших наукових галузях, і які можна класифікувати як позиційні ігри на графах та матрицях.

Зв'язок роботи з науковими програмами, планами, темами. Основні дослідження за темою дисертації проводились на кафедрі автоматизованих систем обробки інформації та управління Національного технічного університету України "Київський Політехнічний Інститут" згідно з індивідуальним планом підготовки здобувача.

Мета і задачі дослідження. Метою дисертаційного дослідження є вирішення питання про існування розв'язку системи лінійних порівнянь за скінченим модулем, складеної для певного класу графів, або для спеціальних матриць довільного об'єму. При цьому в разі відсутності розв'язку необхідно скоригувати початкові дані таким чином, щоб задача мала розв'язок.

В дисертаційній роботі були поставлені і розв'язані такі задачі:

- знайти достатні умови вирішення задачі про математичний сейф, заданий на орієнтованих графах, з замками, які мають два стани;
- знайти достатні умови вирішення задачі про математичний сейф, заданий на орієнтованих графах, з замками одного типу, які мають довільну кількість станів;
- розробити методи розв'язання загальної задачі на орієнтованих графах, таких як шлях, контур, безконтурна мережа, композиція контурів тощо;
- розробити методи розв'язання загальної задачі на неорієнтованих графах, таких як ланцюг, цикл, зірка, колесо, тривалентний граф тощо;
- знайти необхідні умови існування розв'язку задачі про математичний сейф, заданий на довільних матрицях;
- розробити методи розв'язання задачі про математичний сейф з замками одного типу, заданий на матрицях;
- розробити методи розв'язання задачі про математичний сейф з замками довільного типу, заданий на матрицях.

Об'єкт дослідження. Об'єктом дослідження є комбінаторна позиційна гра на графах та матрицях.

Предмет дослідження. Предметом дослідження є система лінійних порівнянь за скінченим модулем.

Методи дослідження. При розробці алгоритмів та доведенні теоретичних тверджень застосовувалися методи теорії чисел, лінійна алгебра, комбінаторіка та теорія графів.

Наукова новизна одержаних результатів:

- в дисертації вперше започатковано нову перспективну тему, яка має пряме відношення до однієї з галузей теорії ігор. Маються на увазі задачі, де необхідно, виходячи з початкового стану об'єкту, за певними правилами досягти іншого, наперед заданого стану. Такі задачі зустрічаються в комп'ютерних іграх, але математична постановка задачі як задачі про математичний сейф і методи її розв'язання подані вперше. Тому всі результати, отримані дисертантом, є новими і не мають аналогу;

- вперше проблема знаходження оптимального шляху до заданого кінцевого стану в подібних іграх зводиться до розв'язання лінійної системи порівнянь у класі лишків за скінченим модулем;

- проблема спочатку розглядається для орієнтованих та неорієнтованих графів. Знаходяться умови, при яких задані стани замків сейфа гарантують існування розв'язку задачі. Доведено ряд тверджень, які дозволяють отримати розв'язок задачі у явному вигляді;

- задача про математичні сейфи, які задані на матрицях, має свою специфіку і де в чому відрізняється від такої задачі на графах. Для неї знаходяться необхідні умови існування розв'язку задачі, які суттєво залежать від розмірів матриці;

- за умови існування розв'язку задачі пропонуються розроблені методи, які дозволяють отримати цей розв'язок у явному вигляді як для математичних

сейфів з замками одного типу, так і для замків різного типу. Якщо задача не має розв'язку, пропонується в початковий стан математичного сейфа внести корективи, після яких задача матиме розв'язок.

Практичне значення одержаних результатів дисертаційної роботи.

Перш за все треба відмітити ті теоретичні результати, які дозволять їх застосовувати для отримання розв'язків багатьох практичних задач, що зводяться до ігор подібного класу.

Отримані результати можна використовувати також в теорії кодування та теорії захисту інформації.

Значна частина результатів дисертації може бути використана в навчальному процесі вузів України, де викладаються такі дисципліни як "Дискретна математика" та "Прикладна математика".

Особистий внесок здобувача. Всі результати в опублікованих роботах за темою дисертації отримані автором самостійно або з його участю.

У працях, що написані в співавторстві, дисертанту належать: в [1] – розробка алгоритму і його теоретичне обгрунтування, а співавтору(керівнику дисертанта) – постановка задачі та ідея обґрунтування деяких тверджень; в [2] – співавтору належить постановка задачі, а дисертант розробив алгоритм, здійснив його програмну реалізацію та тестування; у роботі [3] автор особисто продовжив дослідження робіт [1] та [2] і розпочав дослідження нового підкласу математичних сейфів; в [4] – автор особисто одержав нові результати про математичні сейфи з довільними замками, серед яких дві теореми про знаходження розв'язку задачі у явному вигляді.

Апробація результатів роботи. Основні результати роботи доповідалися та обговорювалися на наукових семінарах, конференціях, зокрема на наукових семінарах в Інституті кібернетики імені В.М.Глушкова НАН України (2004 – 2005 рр.), Дніпропетровському національному університеті (2004 р.), Київському національному університеті імені Тараса Шевченка (2005 р.) та на

другому Міжвузівському науково-практичному семінарі „Комбінаторні конфігурації та їх застосування” – 19-20 жовтня 2006 року, Кіровоград.

Публікації. Основні результати дослідження опубліковано в 4 друкованих роботах, з них 3 статті – у наукових фахових журналах, рекомендованих ВАК України, а одна робота - в працях міжнародної наукової конференції.

Структура дисертації. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел з 62 найменувань. Обсяг дисертації – 117 сторінок, яка викладена російською мовою.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовується актуальність вибраної теми, формулюється мета дослідження, зазначається наукова новизна отриманих результатів та висвітлюється їх теоретична і практична цінність.

У першому розділі подано огляд наукових досліджень, які близькі за тематикою до теми дисертаційної роботи, і які послужили відправною точкою для вибору напрямку досліджень. Показано, що багато задач на графах, серед яких такі відомі як пошук оптимальних релейних схем, пошук хроматичного числа планарних графів, пошук товщини та профілю графа, розв’язання різних проблем оптимального кодування графів та інші можна формулювати за допомогою теорії чисел, які, як правило, зводяться до пошуку розв’язку системи лінійних порівнянь в класі лишків за скінченим модулем. Задача про математичний сейф належить до такого типу задач, вона налічує не більше десятка публікацій і ще не має серйозних результатів. Ця обставина і є причиною привабливості даної проблеми. В своїй постановці вона розглядалася як чисто комбінаторна задача, але ще ніхто не пов’язував її з графами. В дисертації показана складність цієї наукової проблеми та обґрунтовується доцільність її постановки.

У **другому розділі** дається загальна постановка задачі про математичний сейф та наводяться результати розв'язання цієї задачі для деяких графів.

Загальна постановка задачі про математичний сейф була запропонована у роботах Донця Г.П. в 2002 році.

Задача. Математичним сейфом називається система S**(Z, b,**$\langle \mathbf{Z} \rangle$**)**, яка складається з множини замків **Z** = {z_1, z_2, . . . , z_N}, вектора початкового стану сейфа $\mathbf{b} = (b_1, b_2, \ldots, b_N)$, де $b_i \in \{0,1,\ldots,k_i - 1\}$ – стан i - го замка, та множини $\langle \mathbf{Z} \rangle = \{Z_1, Z_2, \ldots, Z_N\}$, $z_l \notin Z_l$, $Z_l \in 2^Z (1 \le i, l \le N)$. В результаті одного повороту ключем в замку z_l за годинниковою стрілкою всі замки $z_j \in Z_l$ переходять зі стану b_j в стан $(b_j + 1) (\mathrm{mod}\, k_j)$. Сейф вважається відкритим, якщо він знаходиться в стані $b = (0,0,\ldots,0) = b_{fin}$. Необхідно знайти для кожного замка z_i таку кількість поворотів x_i ключем, щоб відкрити сейф.

Вектор $\vec{x} = (x_1, x_2, \ldots, x_N)$ будемо називати розв'язком задачі про сейф. Множина $\langle \mathrm{Z} \rangle$ називається множиною інцидентності. Її можна записати у вигляді матриці інцидентності $\mathrm{A}_0 = a_{ij}^0$ розміром $N \times N$, де на головній діагоналі стоять нулі, а $a_{ij}^0 = 1$, якщо z_j належить множині $Z_i (1 \le i, j \le N)$, і нулю в протилежному випадку. Матриці A_0 можна поставити у відповідність орієнтований граф $\mathrm{G}(\mathrm{Z})$, в якому від вершини z_i в вершину z_j заходить дуга, якщо $a_{ij}^0 = 1$. В залежності від складності цієї матриці виникають різні задачі про математичний сейф. Позначимо $\mathrm{A} = \mathrm{A}_0 + \mathrm{E}_N$, де E_N – одинична матриця. В стовпці цієї матриці, який відповідає *j*-у замку, стоять одиниці навпроти тих замків, які впливають на стан *j*-го замка. Враховуючи кількість всіх поворотів у цих замках та кількість поворотів x_j в даному замку, отримаємо сумарну кількість поворотів ключем, яка виконувалася в *j*-му замку. В сумі з початковим станом *j*-го замка це повинно дорівнювати $0 (\mathrm{mod}\, k_j)$. Тоді загальна

задача про математичний сейф зводиться до розв'язання лінійної системи порівнянь: $\vec{x}\vec{a}_i + b_i \equiv 0(\mathrm{mod}\, k_i), (1 \le i \le N),$ (1)

де $\vec{a}_i$ – i - й стовпчик матриці A.

Якщо $k_i = K = const$ для всіх $1 \le i \le N$, то такі замки називаються однотиповими. В цьому розділі розглянуто задачі з однотиповими замками для $K = 2$, тобто $b_i \in \{0,1\}, (1 \le i \le N)$. Нехай граф утворює шлях (рис. 1).

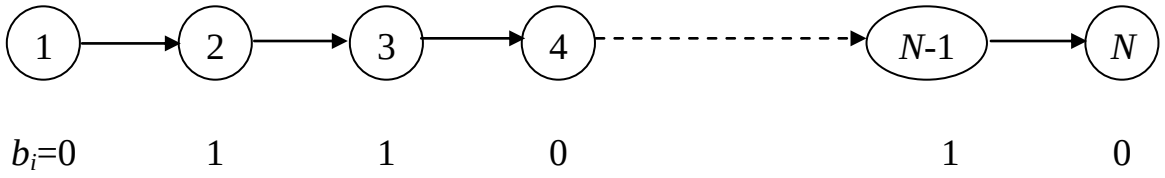

Рис.1. Компонента – шлях з N вершин

Алгоритм розв'язання задачі: покладемо i = 1. Якщо $b_i = 0$, то переходимо до вершини $i+1$. Якщо $b_i = 1$, то робимо поворот в замку z_i, переводячи його стан в 0, а b_{i+1} переходить в стан $(b_{i+1}+1)(\mathrm{mod}\, 2)$. Теперь переходимо до вершини $i+1$. В решті решт приходимо до вершини N, стан якої переводимо в $b_N = 0$. В результаті для всієї компоненти отримаємо стани $b_i = 0\,(1 \le i \le N)$.

Розглянемо цикл з односторонньою орієнтацією – контур (рис. 2).

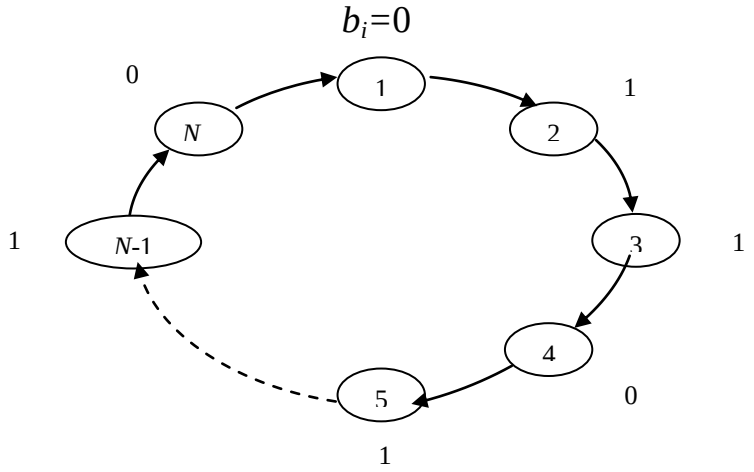

Рис.2. Контур з N вершин

Лемма 2.1. Для того, щоб задача про математичний сейф для контура довжиною N мала розв'язок, необхідно і достатньо, щоб

$$\sum_{i-1}^{N} b_i \equiv 0 (\mathrm{mod}\ 2). \qquad (2)$$

Такий же алгоритм, як і для шляху, застосовується і для циклу, у якого орієнтація неоднозначна, тому що він розпадається на декілька незалежних шляхів.

Для складніших орієнтованих графів доведені такі твердження:

Теорема 2.1. Задача про сейф, заданий на транспортній мережі, завжди має розв'язок для довільного початкового стану.

Теорема 2.2. Задача про сейф, заданий на орієнтованому графі з незалежними контурами, має розв'язок для довільного початкового стану, якщо канонічний стан кожного контура задовольняє умову (2).

Лемма 2. 2. Задача про сейф, заданий на двох зв'язних контурах, має розв'язок для довільних початкових станів.

Теорема 2.3. Система рівнянь (1), записана для регулярного орієнтованого графа степеня 3, який складається з гамільтонового контура з діагоналями, є залежною тоді і тільки тоді, коли знайдеться такий підконтур, куди заходить парна кількість дуг, які можна розбити на спряжені пари.

Це самий останній результат для орієнтованих графів. Для неорієнтованих графів кількість залежних замків збільшується. Система порівнянь для ланцюга довжиною N, має вигляд:

$$\left.\begin{array}{lllllll} x_1 + x_2 & \cdot & \cdot & \cdot & & \equiv b_1 \\ x_1 + x_2 + x_3 & \cdot & \cdot & \cdot & \equiv b_2 \\ \cdot & x_2 + x_3 + x_4 & \cdot & \cdot & \equiv b_3 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot & + x_{N-1} + x_N & \equiv b_N \end{array}\right\} \mathrm{mod}\ 2 \qquad (3)$$

Лема 2.3. Система порівнянь (3) лінійно залежна тільки для $N \equiv -1 (\mathrm{mod}\ 3)$.

В цьому випадку система має розв'язок тільки при умові:

$$\sum_{i=1}^{l}\left(b_{3i-2}+b_{3i-1}\right)\equiv 0(\mathrm{mod}\,2), \qquad \text{де } l=\frac{N+1}{3}. \tag{4}$$

В загальному випадку справедлива

Теорема 2.4. Якщо $N \neq -1(\mathrm{mod}\,3)$, то розв'язком задачі про сейф, заданий на неорієнтованому ланцюгу, є

$$x_\alpha \equiv \sum_{i=1}^{l}\left(b_{3i-2}+b_{3i-1}\right)(\mathrm{mod}\,2),\ \alpha\equiv 0(\mathrm{mod}\,3);\ l=\frac{\alpha}{3};$$

$$x_\alpha \equiv \sum_{i=0}^{l}\left(b_{\alpha+3i+1}+b_{\alpha+3i+2}\right)(\mathrm{mod}\,2),\ \alpha\equiv (N-2)(\mathrm{mod}\,3);\ l=\frac{N-2-\alpha}{3}; \tag{5}$$

$$x_\alpha \equiv \left(x_{\alpha-1}+b_\alpha+x_{\alpha+1}\right)(\mathrm{mod}\,2),\ \left(x_0=x_{n+1}=0\right).,\ \alpha\equiv(N-1)(\mathrm{mod}\ 3).$$

Подібні результати отримані для циклу, для якого система порівнянь визначається як система (3) з додачею в перше порівняння змінної x_N а в останнє – змінної x_1.

Лема 2.4. Якщо цикл має довжину $N\equiv 0(\mathrm{mod}\,3)$, то ранг системи порівнянь для нього дорівнює $N-2$.

Це витікає з таких рівностей, які можна отримати безпосередньо

$$\sum_{i=1}^{l}\left(b_{3i-1}+b_{3i-2}\right)=\sum_{i=1}^{l}\left(b_{3i}+b_{3i-1}\right)\equiv 0(\mathrm{mod}\,2),\ \text{де } l=N/3. \tag{6}$$

З них випливають такі залежності

$$b_{N-1}\equiv\left(\sum_{i=1}^{N-2}b_i+\sum_{i=1}^{l-1}b_{3i}\right)(\mathrm{mod}\,2), \tag{7}$$

$$b_N\equiv\left(\sum_{i=1}^{N-2}b_i+\sum_{i=1}^{l-1}b_{3i-1}\right)(\mathrm{mod}\,2).$$

Якщо ці умови не виконуються, відповідна система порівнянь і сама задача не мають розв'язків.

Позначимо $R(i)$ множину індексів $\{i,\ i+1,\ i+3,\ i+4,\ldots,\ i+3j,\ i+3j+1\}$,

де $1\le i\le N$ $j=\left\lfloor\frac{N}{3}\right\rfloor$, і суми індексів обчислюються по $\mathrm{mod}\,N$.

Теорема 2.5. Якщо $N \neq 0 \pmod 3$, то задача про сейф, записана для циклу довжиною N, має розв'язок

$$x_\alpha \equiv \left(\sum_{i \in R(\alpha-\delta)} b_i + b_{\alpha-\delta} \right) (\mathrm{mod}\, 2), 1 \le \alpha \le N, \qquad (8)$$

де $\delta \equiv (N^2 + N + 1) (\mathrm{mod}\, 3)$.

Аналогічні результати одержані для складніших графів типу зірки, або колеса. Відповідні системи порівнянь, складені для них, мають подібну структуру, яка дозволяє обчислити визначники матриць. Наводяться формули розв'язків задач для цих графів.

В третьому розділі продовжуються вивчатися математичні сейфи на графах, але при цьому сейфи мають різні типи замків. Це означає, що типи замків описуються вектором $\mathbf{K} = \{k_1, k_2, \ldots, k_N\}$, де деякі компоненти можуть співпадати. Позначимо вектор $\mathbf{b}(\mathbf{mod\ K}) = (b_1 (\mathrm{mod}\ k_1), b_2 (\mathrm{mod}\ k_2), \ldots, b_N (\mathrm{mod}\ k_N))$. Тоді загальна задача про сейф на графах зводиться до розв'язування системи лінійних порівнянь

$$A\vec{x} \equiv -\mathbf{b}(\mathbf{mod\ K}). \qquad (9)$$

Якщо існує обернена матриця A^{-1}, то звідси $\vec{x} \equiv -A^{-1}\mathbf{b}(\mathbf{mod\ K.}$

Для сейфа, заданого на графах у вигляді шляху, алгоритм розв'язання задачі майже аналогічний описаному у розділі 2.

Алгоритм розв'язання задачі: покладемо $i = 1$. Якщо $b_i \equiv 0 (\mathrm{mod}\ k_i)$ $(1 \le i \le N)$, то кладемо $i = i + 1$. Інакше покладемо $b_i' \equiv (k_i - b_i) (\mathrm{mod}\, k_i)$, $b_{i+1}' \equiv (b_{i+1} + k_i - b_i) (\mathrm{mod}\, k_{i+1})$ і переходимо до наступного замка. В результаті N кроків всі замки перейдуть в нульовий стан.

Можна побудувати інший, загальний алгоритм розв'язання цієї задачі. Він ґрунтується на локальному перемиканню одного замка, при цьому стан залежного сусіднього замка не змінюється. Це зводиться до розв'язання системи з двох порівнянь:

$$x \equiv a (\mathrm{mod}\ k_1),\ x \equiv 0 (\mathrm{mod}\ k_2), \qquad (10)$$

де $k_1 \neq k_2$. Якщо найбільший спільний дільник (НСД) $(k_1,k_2) = 1$, то спочатку знаходимо $t \equiv k_2^{-1} (\mathrm{mod}\, k_1)$, тоді

$$x \equiv atk_2 (\mathrm{mod}\, k_1 k_2). \tag{11}$$

Якщо НСД$(k_1,k_2) = c > 1$, то при $a \neq 0 (\mathrm{mod}\, c)$ система (10) не має розв'язків. В противному разі

$$x \equiv \left(\frac{a}{c}\right)\left(\frac{k_2}{c}\right) t \left(\mathrm{mod}\, \frac{k_1 k_2}{c}\right), \text{ де } t \equiv \left(\frac{k_2}{c}\right)^{-1} \left(\mathrm{mod}\, \frac{k_1}{c}\right). \tag{12}$$

Поступово застосовуючи цю формулу до вершин шляху в їх послідовності, отримаємо розв'язок задачі.

Розглянемо контур (рис. 2) і запишемо для нього систему (9)

$$\begin{aligned}
x_1 + \cdot \quad \cdot \quad \cdot \quad \cdot \quad + x_N &\equiv -b_1 (\mathrm{mod}\, k_1) \\
x_1 + x_2 + \cdot \quad \cdot \quad \cdot \quad \cdot \quad &\equiv -b_2 (\mathrm{mod}\, k_2) \\
x_2 + x_3 + \cdot \quad \cdot \quad \cdot \quad &\equiv -b_3 (\mathrm{mod}\, k_3) \\
\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \\
x_{N-1} + x_N &\equiv -b_N (\mathrm{mod}\, k_N)
\end{aligned} \tag{13}$$

Визначник цієї системи $\det A = 1 - (-1)^N$. Для $N \equiv 1 (\mathrm{mod}\, 2)$ $\det A = 2$, а для $N \equiv 0 (\mathrm{mod}\, 2)$ $\det A = 0$. В другому випадку один рядок матриці A лінійно залежний від інших, і для того, щоб система (13) мала розв'язок, необхідне виконання умови

$$\sum_{i=1}^{N} (-1)^i b_i \equiv 0 (\mathrm{mod}\, k_1 k_2 \ldots k_N). \tag{14}$$

В цьому випадку, відкидаючи одне залежне порівняння із системи (наприклад, останнє), отримаємо систему для шляху, розв'язок якої відомий.

Якщо не існує двох послідовних замків із взаємно простими числами k_1 і k_2, то задача не завжди має розв'язок.

Лема 3.1. Задача для сейфів на контурі завжди має розв'язок, якщо

$$\sum_{i=1}^{N} b_i \equiv 0 (\mathrm{mod}\, 2). \tag{15}$$

Для неорієнтованих графів задача розв'язується складніше.

Система порівнянь (9) для ланцюга має вигляд

$$\begin{array}{rrrrrrrrrrrrr} x_1 + x_2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \equiv -b_1 \pmod{k_1} \\ x_1 + x_2 + x_3 & \cdot & \cdot & \cdot & \cdot & \cdot & \equiv -b_2 \pmod{k_2} \\ x_2 + x_3 + x_4 + & \cdot & \cdot & \cdot & \cdot & \equiv -b_3 \pmod{k_3} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_{N-2} + x_{N-1} + x_N + & \equiv -b_{N-1} \pmod{k_{N-1}} \\ x_{N-1} + x_N + & \equiv -b_N \pmod{k_N} \end{array} \qquad (16)$$

Теорема 3.2. Визначник системи (16) дорівнює

$$\det A = \boldsymbol{C}_N = -\frac{2}{\sqrt{3}} \sin \frac{\pi(N-2)}{3}. \qquad (17)$$

Якщо N ≡ 2(mod 3), то оберненої матриці не існує. Тоді для існування розв'язку системи (16) необхідно виконання умови

$$b_N - b_{N\text{-}1} + b_{N\text{-}3} - b_{N\text{-}4} + \ldots + b_2 - b_1 \equiv 0 (\text{mod } K). \qquad (18)$$

Тоді N-е порівняння та змінну x_N відкидаємо і переходимо до системи, визначник якої відмінний від нуля. Нема необхідності знаходити повністю обернену матрицю A^{-1}. Достатньо знайти вираз її першого рядка, це дозволить знайти значення x_1. Потім, подставляючи його в систему (16), послідовно знаходимо всі значення вектора $\vec{x}$.

Лема 3.2. Перший рядок матриці A^{-1} має вигляд

$$\frac{1}{C_N}\left(C_{N-1}, -C_{N-2}, C_{N-3}, \ldots, (-1)^N C_1, (-1)^{N+1} C_0\right). \qquad (19)$$

Розглянемо ще два типа сейфів, заданих на зірці та на циклі.

Матриця системи (9) для зірки і відповідний визначник дорівнюють:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}; \quad \det A = -N + 2. \qquad (20)$$

Для розв'язання задачі можна безпосередньо знайти обернену матрицю.

Теорема 3.3. Для сейфа, заданого на зірці, для $N > 2$

$$A^{-1} = \frac{1}{N-2}\begin{pmatrix} -1 & 1 & 1 & \cdot\cdot\cdot & 1 \\ 1 & N-3 & -1 & \cdot\cdot\cdot & -1 \\ 1 & -1 & N-3 & \cdot\cdot\cdot & -1 \\ \cdot & \cdot & \cdot & \cdot\cdot\cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot\cdot\cdot & \cdot \\ 1 & -1 & -1 & \cdot\cdot\cdot & N-3 \end{pmatrix}. \qquad (21)$$

Звідси знаходимо $x_1 \equiv \frac{1}{N-2}\left(+b_1 - b_2 - \ldots - b_N\right)(\mathrm{mod}\, M),$ (22)

де M – найбільше спільне кратне НСК(k_1, k_2,..., k_N). Якщо $M \equiv 0[\mathrm{mod}(N-2)]$, то задача має розв'язок тільки при умові

$$\sum_{i=2}^{N} b_i - b_1 \equiv 0\left[\mathrm{mod}\left(N-2\right)\right]. \qquad (23)$$

Знаючи значення x_1 і підставляючи його в інші порівняння з матрицею **A** (20), отримаємо значення для $x_N, x_{N-1}, \ldots, x_2$.

Для циклу система порівнянь відрізняється від системи для ланцюга наявністю в першому рядку змінної x_N, а в останньому рядку – змінної x_1.

Теорема 3.4. Для сейфа, заданого на циклі, при $N \geq 3$ справедливо

$$A^{-1} = (-1)^{N+1} 4\sin^2\frac{\pi N}{3}. \qquad (24)$$

Для різних значень N можна отримати формули, які визначають всі невідомі системи порівнянь. Та краще застосувати алгоритм, який дозволяє послідовно розв'язати задачу, тобто перевести всі замки в нульовий стан.

Алгоритм: *Починаючи з першого замка, робимо в кожному наступному повороти ключем в напрямку, протилежному знаку стану лівого замка, доти, поки останній не перейде в нульовий стан.*

Особливість цього алгоритма полягає в тому, що в ньому не треба робити ніяких обчислень, пов'язаних з модулями.

В четвертому розділі вивчаються математичні сейфи, які задані на матрицях. В цьому разі один поворот ключем за годинниковою стрілкою в будь-якому замку приводить до ідентичного повороту в усіх замках, які знаходяться в цьому рядку і в цьому стовпчику. Треба досягти фінального стану сейфа, коли всі елементи матриці стануть рівними нулю.

Позначимо $\mathfrak{I}_n$ - квадратну матрицю порядку n, яка складається з одиниць, а E_n – **о**диничну матрицю того ж порядку. Тоді система порівнянь (9) запишеться з матрицею A порядку $m \times n$, яка складається з m^2 підматриць

$$A = \begin{pmatrix} \mathfrak{I}_n & E_n & E_n & \dots & E_n \\ E_n & \mathfrak{I}_n & E_n & \dots & E_n \\ E_n & E_n & \mathfrak{I}_n & \dots & E_n \\ \dots & \dots & \dots & \dots & \dots \\ E_n & E_n & E_n & \dots & \mathfrak{I}_n \end{pmatrix}. \qquad (25)$$

Нехай всі замки сейфа одного типу і $K = 2$. Тоді можливі три випадки.

1. Нехай $m = n = 0 \pmod 2$.

Теорема 4.1. Для матрицы A с параметрами $m = n = 0 \pmod 2$ \справедливо

$$A^{-1} \equiv A \pmod 2 \qquad (26)$$

Із теоремы 4.1 випливає, що $\det A = 1 \pmod 2$, тоді отримуємо роз'язок системи

$$\vec{x} \equiv A\vec{b} \pmod 2 \qquad (27)$$

2. Нехай $m \equiv 0 \pmod 2$, $n \equiv 1 \pmod 2$. Сюди можна віднести випадок, коли $n \equiv 0 \pmod 2$, $m \equiv 1 \pmod 2$. Це досягається транспортуванням матриці A.

Теорема 4.2. Ранг матриці A для $m = 0 \pmod 2$ та $n \equiv 1 \pmod 2$ дорівнює $mn - m + 1$.

Тоді матриця A є виродженою, тому $\det A \equiv 0 \pmod 2$ і розв'язок системы (9) не завжди існує. Після вилучення рядків і стовпчиків з номерами $2n, 3n, \dots, mn$ отримаємо невироджену матрицю C, у якої $\det C \equiv 1 \pmod 2$, а обернена матриця має вигляд

$$C^{-1}=\left(\begin{array}{c|c|cccccc} \mathfrak{I}_{n-1} & 1 & E_{n-1} & E_{n-1} & \cdot\cdot & \cdot\cdot & E_{n-1} \\ \hline 111\ldots & 1 & 00\ldots & 00\ldots & \cdot\cdot & \cdot\cdot & 00\ldots \\ \hline E_{n-1} & 0 & \mathbf{O} & F_{n-1} & \cdot\cdot & \cdot\cdot & \cdot\cdot \\ E_{n-1} & 0 & F_{n-1} & \mathbf{O} & \cdot\cdot & \cdot\cdot & F_{n-1} \\ E_{n-1} & 0 & F_{n-1} & F_{n-1} & \cdot\cdot & \cdot\cdot & F_{n-1} \\ \vdots & 0 & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & 0 & \vdots & \vdots & \vdots & \vdots & \vdots \\ E_{n-1} & 0 & F_{n-1} & F_{n-1} & \cdot\cdot & \mathbf{O} & F_{n-1} \\ E_{n-1} & 0 & F_{n-1} & F_{n-1} & \cdot\cdot & F_{n-1} & \mathbf{O} \end{array}\right). \qquad (28)$$

Тут присутні матриці розміром $(n-1)\times(n-1)$, які містять тільки нулі, а $F_{n-1} = \mathfrak{I}_{n-1} - E_{n-1}$. В цьому випадку система матиме розв'язок, якщо виконуються умови

$$b_{in}=\left(\sum_{j=1}^{n} b_{1j}+\sum_{j=1}^{n-1} b_{2j}\right)(\mathrm{mod}\,2), 2\le i\le m \qquad (29)$$

3. Нехай $m\equiv n\equiv 1(\mathrm{mod}\ 2)$.

Тоді, як і в випадку 2, рядки матриці A з номерами kn $(2 \le k \le m)$ є залежними. Тому $\det A \equiv 0(\mathrm{mod}\ 2)$ і розв'язок системи (9) не завжди існує.

Теорема 4.3. Ранг матриці A з параметрами $mn \equiv 1(\mathrm{mod}2)$ дорівнює $mn - m - n + 2$.

Після видалення рядків і стовпчиків з номерами $кn$ $(2 \le к \le m-1)$, а також всіх рядків і стовпчиків з номерами, більших $(m-1)n$, отримаємо матрицю типу (28), яка має обернену. Для того щоб задача мала розв'язок, крім умов (29) повинні також виконуватися умови відносно останнього клітинного рядка.

$$b_{mi}=\left(\sum_{j=2}^{n} b_{1j}+\sum_{i=2}^{m-1} b_{i1}\right)(\mathrm{mod}\,2), 1\le i\le n. \qquad (30)$$

Якщо $K > 2$, то проблема знаходження оберненої матриці ускладнюється. Розглянемо симетричну квадратну матрицю порядку n, залежну від двох

параметрів $H_n(\alpha,\beta)=(\alpha-\beta)E_n+\beta\Im_n$. На основі неї побудуємо квадратну матрицю порядку *mn*, залежну від четирьох параметрів і складену з m^2 підматриць $H_n(\alpha,\beta)$.

$$T_{m,n}(\alpha,\beta,\gamma,\delta)=\begin{pmatrix} H_n(\alpha,\beta)\,H_n(\gamma,\delta)\ldots H_n(\gamma,\delta) \\ H_n(\gamma,\delta)\,H_n(\alpha,\beta)\ldots H_n(\gamma,\delta) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ H_n(\gamma,\delta)\,H_n(\gamma,\delta)\ldots H_n(\alpha,\beta) \end{pmatrix}. \qquad (31)$$

Перша необхідна умова розв'язності системи (9):

$$m\neq 1(\mathrm{mod}\,K);\ n\neq 1(\mathrm{mod}\,k);\ m+n\neq 1(\mathrm{mod}\,K). \qquad (33)$$

Лема 4.2. Для системи (9) $A^{-1} = T_{m,n}(\alpha, \beta, \gamma, \delta)$, де

$$\left.\begin{aligned} \alpha &\equiv \frac{1}{m-1}+\frac{1}{n-1}-1+\delta, \\ \beta &\equiv \frac{1}{n-1}+\delta, \\ \gamma &\equiv \frac{1}{m-1}+\delta, \\ \delta &\equiv -\left(\frac{1}{n-1}+\frac{1}{m-1}\right)\frac{1}{m+n-1} \end{aligned}\right\}(\mathrm{mod}\,K).. \qquad (34)$$

<u>Друга умова розв'язності системи (9):</u>

а) для простого числа *K* розв'язок існує завжди;

б) для складеного числа *K* розв'язок існує завжди , якщо

$$НОД(m\text{-}1, K) = НОД(n\text{-}1, K) = НОД(m+n\text{-}1, K) = 1. \qquad (35)$$

Для сейфів з замками одного типу отримані розв'зки у явному вигляді. Для цього використовуються позначення змінних та станів замків у матричному вигляді.

Позначимо $\sum_{\lambda=1}^{m}\sum_{\eta=1}^{n} b_{\lambda\eta}=\sum(b);\ \sum_{\lambda=1}^{m} b_{\lambda j}=\lambda_j;\ \sum_{\eta=1}^{n} b_{i\eta}=\sigma_i$. Тоді

$$x_{ij}\equiv\left[b_{ij}+\frac{1}{m-1}\left(\frac{\sum(b)}{m+n-1}-\lambda_j\right)+\frac{1}{n-1}\left(\frac{\sum b}{m+n-1}-\sigma_i\right)\right](\mathrm{mod\,K}), \qquad (36)$$

де $1 \le i \le m$; $1 \le j \le n$. Для різних співвідношень m і n знайдено конкретні формули.

Якщо в сейфі є замки різних типів, то розв'язок задачі може як ускладнитися, так і спроститися в залежності від різних відношень між кількістю замків та числами, якими описуються стани цих замків.

Позначимо $M = k_1 k_{2\ldots} k_N$, де k_i – прості числа. Для такого сейфа всі теоретичні висновки про розв'язання системи (9) можна отримати по аналогії.

Теорема 4.5. Розв'язок системи (9) для довільної кількості q типов замків зі взаємно простими $k_1, k_2, \cdots, k_q$ задовольняє системі порівнянь

$$A\,\boldsymbol{x} + \mathbf{b} \equiv 0 (\mathrm{mod}\, k_1 k_2 \cdots k_q), \qquad (37)$$

де A – це матриця (25).

Тоді формули (33) і (34) запишуться аналогічно, якщо замість модуля K всюди записати модуль M. Для складених чисел k_i $(1 \le i \le q)$ проблема ускладнюється, але не принципово, а чисто технічно із-за великої кількості частинних випадків.

ВИСНОВКИ

У дисертації одержано нові науково обґрунтовані результати в галузі дискретної математики та її застосувань. В ній вперше започатковано нову перспективну тему, яка має пряме відношення до однієї з галузей теорії позиційних ігор, заданих на графах та матрицях.

Основні результати дисертаційної роботи:

1. Вперше розширено формалізацію позиційної гри, яка отримала назву задачі про математичний сейф, на орієнтовані та неорієнтовані графи, та зведено її до розв'язання системи лінійних порівнянь за скінченим модулем.

2. Для графів повністю розв’язана задача про математичні сейфи, замки яких мають тільки два стани, і отримані відповідні формули у явному вигляді.
3. Розроблені методи розв’язання задачі на графах для математичних сейфів, які мають замки або однакових, або різних типів.
4. Знайдено необхідні умови існування розв’язку задачі про математичний сейф, заданий на матрицях.
5. Для матриць повністю розв’язана задача про математичні сейфи, замки яких мають тільки два стани, і отримані відповідні формули для різних співвідношень розмірів матриць.
6. Повністю розв’язана для матриць задача про математичні сейфи з замками одного типу, кількість станів яких є просте число, і подані відповідні формули.
7. Розроблені методи, які дозволяють розв’язувати загальну задачу на матрицях для сейфів з різними типами замків, і стани яких описуються довільними числами.

ОСНОВНІ ПОЛОЖЕННЯ ДИСЕРТАЦІЇ ОПУБЛІКОВАНІ В ТАКИХ ПРАЦЯХ:

1. Донец Г.А., Чжан Бинь. Постановка и решение некоторых задач о математическом сейфе//Кибернетика и системный анализ.– 2006.- № 3.– С.3-14.

2. Донец Г.А., Чжан Бинь. Задачи о математическом сейфе на графах // Кибернетика и системный анализ. – 2006. - № 5. – С. 84-93.

3. Чжан Бинь. Задачи о математическом сейфе . II Міжвузівський науково-практичний семінар „Комбінаторні конфігурації та їх застосування” – 19-20 жовтня 2006 року, Кіровоград, С. 67-71.

4. Чжань Бинь. Решение матричной задачи о математическом сейфе с различными замками // Математические машины и системы. – 2006. - № 4. – С. 69 – 72.

АНОТАЦІЇ

Чжан Бінь . Розробка методів та алгоритмів розв'язування задач про математичний сейф . – Рукопис.

Дисертація на здобуття наукового ступеня кандидата фізико-математичних наук за спеціальністю 01.05.01 – теоретичні основи інформатики та кібернетики. - Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, 2007.

В дисертації досліджуються питання, пов'язані з розробкою методів розв'язування позиційної гри, яка може задаватися на різних математичних об'єктах таких як матриця, граф тощо, і яка отримала назву задачі про математичний сейф. Показано, що незалежно від об'єкта, на якому розв'язуються задачі, всі вони зводяться до розв'язання системи лінійних порівнянь в класі лишків за скінченим модулем. В залежності від типів замків всі математичні сейфи можна поділити на три групи: з замками, що мають тільки два стани, з замками, що мають однакову кількість станів, та з замками різного типу. Для кожної групи сейфів на графах і матрицях знайдено або явні вирази, які визначають невідомі величини відповідної системи порівнянь, або побудовано алгоритми для їх визначення.

Ключові слова: система порівнянь, класс лишків, скінчений модуль, замки, стан замка, математичний сейф, фінальний стан сейфа, кліткова матриця, корекція початкового стану.

Чжан Бинь. Разработка методов и алгоритмов решения задач о математическом сейфе. – Рукопись.

Диссертация на соискание ученой степени кандидата физико-математических наук по специальности 01.05.01 – теоретические основы информатики и кибернетики. - Институт кибернетики им. В.М. Глушкова НАН Украины, Киев, 2007.

В диссертации исследуются вопросы, связанные с разработкой методов решения позиционной игры, которая может задаваться на таких объектах как

матрица, граф и других, и которая получила название задачи о математическом сейфе. Показано, что независимо от объекта, на котором решаются задачи, все они сводятся к решению системы линейных сравнений в классе вычетов по конечному модулю. В зависимости от типов замков математические сейфы можно разделить на три группы: с замками, которые имеют только два состояния, с замками, которые имеют одинаковое число состояний, и с замками разных типов. Для каждой группы сейфов на графах и матрицах найдены либо явные выражения для определения неизвестных соответствующей системы сравнений, либо разработаны алгоритмы для их определения.

Ключевые слова: система сравнений, класс вычетов, конечный модуль, замки, состояние замка, математический сейф, финальное состояние сейфа, клеточная матрица, коррекция начального состояния.

Zhang Bin. Development of methods and algorithms for solving the mathematical safe problem. – Manuscript.

hesis for a candidate's degree of physics and mathematics by speciality 01.05.01 – theoretical basis of informatics and cybernetics. – V.M.Glushkov institute of cybernetics, National Academy of Science of Ukraine, Kyiv, 2007.

Thesis deals with the development of methods for solving certain positional games which may be defined on various mathematical objects such as matrix, graph etc, and are called by the mathematical safe problem. It is shown that, regardless of mathematical object, such problem can be reduced to solving a system of linear comparisons in a class of residues in a finite modulus. Depending of the lock types, the mathematical safes can be divided into three groups: those having two-state locks, safes with locks of equal quantity of states, and safes with different-type locks. For each group of safes defined on graph or matrix, either explicit expressions for solutions of corresponding system of comparisons are found or algorithms for finding these solutions are derived.

Key words: system of comparisons, residue class, finite modulus, lock, lock state, mathematical safe, final safe state, cell matrix, correction of initial state.