Квантові алгоритми для розв'язку алгебраїчних задач та можливості їх застосування в криптоаналізі

член-кореспондент НАН України,
доктор фіз.-мат. наук **Савчук М.М.**
кандидат фіз.-мат. наук **Фесенко А.В.**

Навчально-науковий фізико-технічний
інститут КПІ ім. Ігоря Сікорського, м. Київ

Гільбертів простір

Основним поняттям квантової механіки є квантовий стан. Стан квантової системи описується деяким вектором станів, який пов'язаний з поняттям амплітуди ймовірностей, або хвильової функції. Математично цей вектор можна розглядати як вектор в гільбертовому просторі над полем комплексних чисел.

Означення

Гільбертовим простором називають векторний простір H над полем $\mathbb{C}$ (або $\mathbb{R}$) разом з функцією $H \times H \to \mathbb{C}(\mathbb{R})$, яку називають **скалярним добутком**, позначають як (x, y), $x, y \in H$ та яка має властивості:

Гільбертів простір

Означення (Гільбертовий простір)

1. $(x,x) = 0 \Leftrightarrow x = 0,\ x \in H$
2. $(x,x) \geq 0$
3. $(x,y) = \overline{(y,x)}$
4. $\forall \lambda \in \mathbb{C},\ x,y, \in H\ \ (\lambda x, y) = \lambda (x,y)$ і $(x, \lambda y) = \overline{\lambda}(x,y)$
5. $(x+y,z) = (x,z) + (y,z),\ \forall x,y,z \in H$
6. Якщо послідовність $x_n \in H,\ n = 1,2,\ldots,$ фундаментальна, $\lim\limits_{m,n\to\infty} (x_n - x_m, x_n - x_m) = 0$, то існує єдине $x \in H$ таке, що $\lim\limits_{n\to\infty} (x_n - x, x_n - x) = 0$
7. H — нескінченновимірний простір

Позначення Дірака

Для опису стану квантової системи в квантовій фізиці використовують гільбертів простір над полем комплексних чисел в нотації і позначеннях Дірака. Якщо в математиці гільбертів простір вважається нескінченновимірним, то в квантовій механіці векторний простір має скінченну вимірність.

Позначення Дірака

Для опису стану квантової системи в квантовій фізиці використовують гільбертів простір над полем комплексних чисел в нотації і позначеннях Дірака. Якщо в математиці гільбертів простір вважається нескінченновимірним, то в квантовій механіці векторний простір має скінченну вимірність.

Вектори $\varphi \in H$ позначаються як $|\varphi\rangle$ (і в такому позначенні розглядаються як вектори-стовпці, а в позначенні $\langle\varphi|$ розглядаються як вектори-рядки), скалярний добуток векторів φ і ψ позначається $\langle\varphi|\psi\rangle$, $\langle\varphi|$ визначає лінійну функцію, яка задається скалярним добутком $\langle\varphi| : \psi \mapsto \langle\varphi|\psi\rangle$, норма $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$. В якості представника класу векторів, що відрізняються на комплексний скалярний множник вибрано нормований на одиницю вектор, для якого $\langle\varphi|\varphi\rangle = 1$. Вектор може бути представлений як лінійна комбінація базисних векторів $|\varphi\rangle = \sum_{i=1}^{N} \langle e_i|\varphi\rangle \cdot |e_i\rangle = \sum_{i=1}^{N} a_i |e_i\rangle$, де $\{ e_i \}_{i=1,\dots,N}$ — ортонормований базис, $\sum_{i=1}^{N} |a_i|^2 = 1$.

Позначення Дірака

- Процес зміни квантового стану описується як застосування до вектору станів унітарних операторів.

Позначення Дірака

- Процес зміни квантового стану описується як застосування до вектору станів унітарних операторів.
- Процес вимірювання полягає в проектуванні вектора квантового стану на базисні вектори. Ймовірність проектування на базисний стан e_i дорівнює $|a_i|^2$, $i = 1, \ldots, N$.

Позначення Дірака

- Процес зміни квантового стану описується як застосування до вектору станів унітарних операторів.
- Процес вимірювання полягає в проектуванні вектора квантового стану на базисні вектори. Ймовірність проектування на базисний стан e_i дорівнює $|a_i|^2$, $i = 1, \ldots, N$.

Приклад

Нехай кубіт знаходиться в квантовому стані $\frac{4}{5}|0\rangle - \frac{3}{5}|1\rangle$. При вимірюванні отримаємо класичний біт 0 з ймовірністю $\left(\frac{4}{5}\right)^2 = 64\%$, і класичний біт 1 з ймовірністю $\left(\frac{-3}{5}\right)^2 = 36\%$.

Модель обчислень

- **модель квантових схем**
- квантова машина Тюрінга
- квантові обчислення на основі вимірювань
- адіабатичні квантові обчислення (квантовий відпал, quantum annealing)
- топологічні квантові обчислення

Модель обчислень

- **модель квантових схем**
- квантова машина Тюрінга
- квантові обчислення на основі вимірювань
- адіабатичні квантові обчислення (квантовий відпал, quantum annealing)
- топологічні квантові обчислення

Technology	Best Argument For	Best Argument Against	Companies Involved
Majorana	Fundamentally protected from errors	Hard to engineer	Microsoft
Solid-state spins (P:Si, NV centers, etc.)	Small footprint	Heterogeneous, hard to scale	Turing, CQC2T
Quantum dots	Small footprint, scalable fabrication	Connectivity	HRL, Intel
Neutral atoms	Homogeneous, long-range gates	Lack of demonstrated good 2-qubit gates	Atom Computing, Inc.
Linear optics[50]	Scalable fabrication	Lack of key components (single photon sources)	PsiCorp, Xanadu
Superconductors	Demonstrated programmability, lithographically definable	Large footprint, 10 mK	Google, IBM, Rigetti, Intel, QCI
Ions[51]	Demonstrated programmability, long coherence, homogeneous,	Microsecond gate speeds, lasers	IonQ, Honeywell

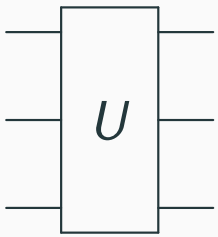
Однокубітні квантові перетворення

- $|0\rangle$ кубіт; $|0\rangle^{\otimes n}$ —/^{n}— регістр кубітів; $I = |0\rangle\langle 0| + |1\rangle\langle 1|$
- —[X]— матриця Паулі $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |1\rangle\langle 0| + |0\rangle\langle 1|$
- —[Y]— матриця Паулі $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i|1\rangle\langle 0| - i|0\rangle\langle 1|$
- —[Z]— матриця Паулі $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |1\rangle\langle 0| - |0\rangle\langle 1|$
- —[H]— Адамара $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle-|1\rangle}{\sqrt{2}}\langle 1|$
- —[$P(\phi)$]— $P(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} = |1\rangle\langle 0| + e^{i\phi}|0\rangle\langle 1|$
- —[S]— фазове $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = |1\rangle\langle 0| + i|0\rangle\langle 1|$
- —[T]— $\frac{\pi}{8}$ перетворення $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix} = |1\rangle\langle 0| + e^{\frac{i\pi}{4}}|0\rangle\langle 1|$

Багатокубітні квантові перетворення

-  вентиль $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$

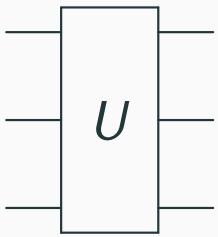
$= |0\rangle |0\rangle \langle 0| \langle 0| + |0\rangle |1\rangle \langle 1| \langle 0| + |1\rangle |1\rangle \langle 0| \langle 1| + |1\rangle |0\rangle \langle 1| \langle 1|$

-  3-кубітний вентиль U (3 регістри)
- — квантовий канал; $=$ класичний канал
-  вимірювання

Багатокубітні квантові перетворення

-  вентиль $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$

$= |0\rangle |0\rangle \langle 0| \langle 0| + |0\rangle |1\rangle \langle 1| \langle 0| + |1\rangle |1\rangle \langle 0| \langle 1| + |1\rangle |0\rangle \langle 1| \langle 1|$

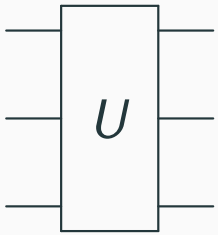
-  3-кубітний вентиль U (3 регістри)
- — квантовий канал; $=$ класичний канал
-  вимірювання

група Кліффорда — породжена вентилями H, S та $CNOT$

Багатокубітні квантові перетворення

-  вентиль $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$

$= |0\rangle |0\rangle \langle 0| \langle 0| + |0\rangle |1\rangle \langle 1| \langle 0| + |1\rangle |1\rangle \langle 0| \langle 1| + |1\rangle |0\rangle \langle 1| \langle 1|$

-  3-кубітний вентиль U (3 регістри)
- — квантовий канал; $=$ класичний канал
-  вимірювання

група Кліффорда — породжена вентилями H, S та $CNOT$

Теорема Готтесмана-Кніла

Будь-які квантові обчислення, які використовують лише вимірювання у стандартному базисі та вентилі групи Кліффорда можуть бути змодельованими ймовірнісними методами на класичному комп'ютері за поліноміальний час.

Модель обчислень

$+$ переплутаність $\Rightarrow$ квантовий паралелізм

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм

? унітарність перетворень $\Rightarrow$ модель обернених обчислень

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм
? унітарність перетворень $\Rightarrow$ модель обернених обчислень
- дослідження функції як оракула $\Rightarrow$ стандартна модель

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм
? унітарність перетворень $\Rightarrow$ модель обернених обчислень
- дослідження функції як оракула $\Rightarrow$ стандартна модель
- схемна складність, кількість запитів до оракулу

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм
? унітарність перетворень $\Rightarrow$ модель обернених обчислень
- дослідження функції як оракула $\Rightarrow$ стандартна модель
- схемна складність, кількість запитів до оракулу
- відсутність клонування та інші no-go теореми

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм
? унітарність перетворень $\Rightarrow$ модель обернених обчислень
- дослідження функції як оракула $\Rightarrow$ стандартна модель
- схемна складність, кількість запитів до оракулу
- відсутність клонування та інші no-go теореми
- декогеренція (більше зв'язків — більше помилок)

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм
? унітарність перетворень $\Rightarrow$ модель обернених обчислень
- дослідження функції як оракула $\Rightarrow$ стандартна модель
- схемна складність, кількість запитів до оракулу
- відсутність клонування та інші no-go теореми
- декогеренція (більше зв'язків — більше помилок)
- помилки реалізації вентилів

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм
? унітарність перетворень $\Rightarrow$ модель обернених обчислень
- дослідження функції як оракула $\Rightarrow$ стандартна модель
- схемна складність, кількість запитів до оракулу
- відсутність клонування та інші no-go теореми
- декогеренція (більше зв'язків — більше помилок)
- помилки реалізації вентилів
- помилки представлення перетворень (теорема Соловея-Кітаєва)

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм
? унітарність перетворень $\Rightarrow$ модель обернених обчислень
- дослідження функції як оракула $\Rightarrow$ стандартна модель
- схемна складність, кількість запитів до оракулу
- відсутність клонування та інші no-go теореми
- декогеренція (більше зв'язків — більше помилок)
- помилки реалізації вентилів
- помилки представлення перетворень (теорема Соловея-Кітаєва)
- помилки вимірювань

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм
? унітарність перетворень $\Rightarrow$ модель обернених обчислень
- дослідження функції як оракула $\Rightarrow$ стандартна модель
- схемна складність, кількість запитів до оракулу
- відсутність клонування та інші no-go теореми
- декогеренція (більше зв'язків — більше помилок)
- помилки реалізації вентилів
- помилки представлення перетворень (теорема Соловея-Кітаєва)
- помилки вимірювань
- коди корекції помилок — щонайменше 5 кубітів (складність відновлення, не повинно вносити більше помилок, ніж виправляє)

Модель обчислень

+ переплутаність $\Rightarrow$ квантовий паралелізм
? унітарність перетворень $\Rightarrow$ модель обернених обчислень
- дослідження функції як оракула $\Rightarrow$ стандартна модель
- схемна складність, кількість запитів до оракулу
- відсутність клонування та інші no-go теореми
- декогеренція (більше зв'язків — більше помилок)
- помилки реалізації вентилів
- помилки представлення перетворень (теорема Соловея-Кітаєва)
- помилки вимірювань
- коди корекції помилок — щонайменше 5 кубітів (складність відновлення, не повинно вносити більше помилок, ніж виправляє)

Квантовий комп'ютер із рівнем фізичних помилок нижче певного порогу може, за допомогою застосування схем квантової корекції помилок, знизити рівень логічних помилок до довільно низьких рівнів.

Модель обчислень

Quantum Supremacy $\Rightarrow$ NISQ пристрої $\Rightarrow$ Quantum Advantage

NISQ — Noisy Intermediate-Scale Quantum

Задача Дойча

Задача (Дойча)

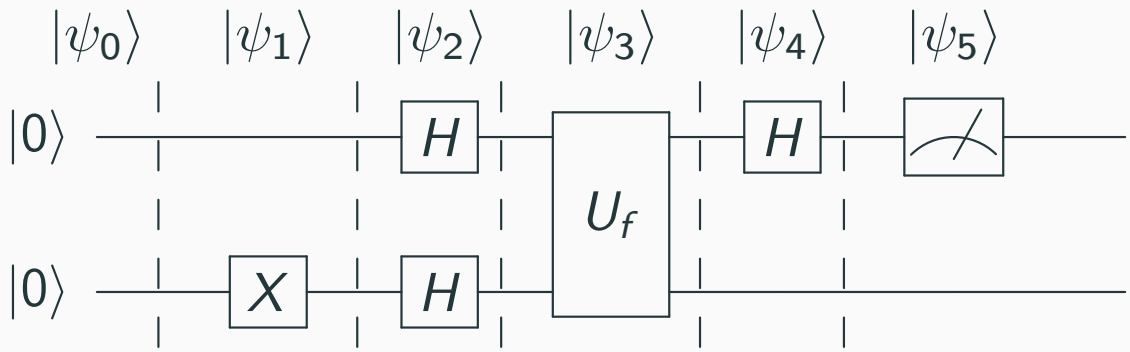
Задана функція $f: \{0,1\} \to \{0,1\}$ за допомогою чорного ящика. З'ясувати, чи є вона сталою.

D. Deutsch "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer" // Proceedings of the Royal Society of London A-400. pp.97-117. 1985. doi:10.1098/rspa.1985.0070

Розв'язок в класичній моделі обчислень

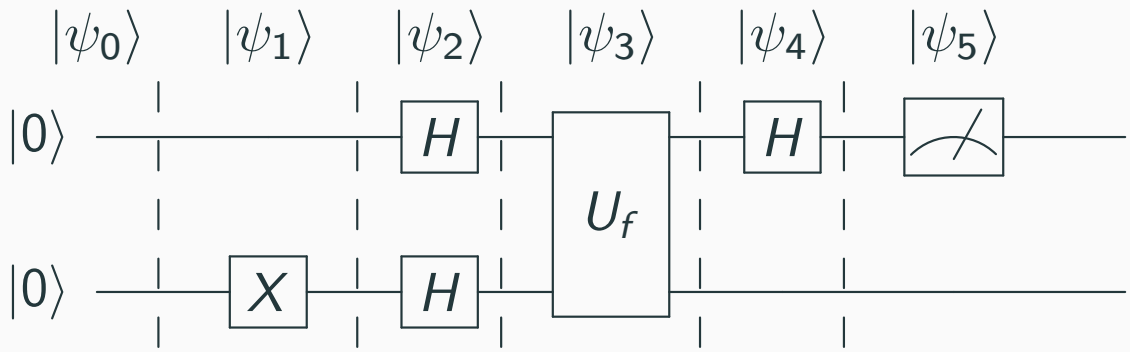
- Будь-який детермінований алгоритм повинен використовувати 2 запити.
- Імовірнісний алгоритм може не використовувати запити до чорного ящика і вгадати правильну відповідь з імовірністю $\frac{1}{2}$ (за рівномірного розподілу при виборі функції).

Квантовий алгоритм розв'язку задачі Дойча



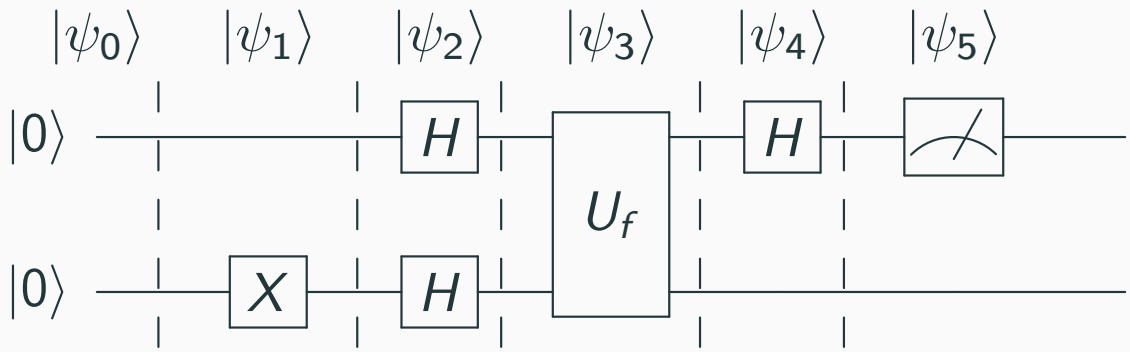
- $|\psi_0\rangle = |0\rangle\,|0\rangle$

Квантовий алгоритм розв'язку задачі Дойча



- $|\psi_0\rangle = |0\rangle\,|0\rangle$
- $|\psi_1\rangle = (I \otimes X)\,(|\psi_0\rangle) = (I \otimes X)\,(|0\rangle\,|0\rangle) = |0\rangle \otimes X\,(|0\rangle) = |0\rangle\,|1\rangle$

Квантовий алгоритм розв'язку задачі Дойча



- $|\psi_0\rangle = |0\rangle\,|0\rangle$
- $|\psi_1\rangle = (I \otimes X)\,(|\psi_0\rangle) = (I \otimes X)\,(|0\rangle\,|0\rangle) = |0\rangle \otimes X\,(|0\rangle) = |0\rangle\,|1\rangle$
- $|\psi_2\rangle = (H \otimes H)\,(|\psi_1\rangle) = (H \otimes H)\,(|0\rangle\,|1\rangle) =$
  $= \frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}\,(|0\rangle - |1\rangle) = \frac{1}{2}\,(|0\rangle\,|0\rangle - |0\rangle\,|1\rangle + |1\rangle\,|0\rangle - |1\rangle\,|1\rangle)$

Квантовий алгоритм розв'язку задачі Дойча

- $|\psi_3\rangle = U_f(|\psi_2\rangle) = U_f(\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)) =$
  $= \frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle) =$
  $= \frac{1}{2}(|0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle) =$
  $= \frac{1}{2}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle) =$
  $= \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle)$

Квантовий алгоритм розв'язку задачі Дойча

- $|\psi_3\rangle = U_f(|\psi_2\rangle) = U_f(\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)) =$
  $= \frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle) =$
  $= \frac{1}{2}(|0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle) =$
  $= \frac{1}{2}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle) =$
  $= \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle)$
- $|\psi_4\rangle = (H \otimes I)(|\psi_3\rangle) =$
  $= (H \otimes I)\left(\frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)(|0\rangle - |1\rangle)\right) =$
  $= \frac{1}{2}H((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle) =$
  $$= \begin{cases} \frac{(-1)^{f(\mathbf{0})}}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle), & f(0) = f(1) \\ \frac{(-1)^{f(\mathbf{0})}}{\sqrt{2}}|1\rangle \otimes (|0\rangle - |1\rangle), & f(0) \neq f(1) \end{cases}$$

Квантовий алгоритм розв'язку задачі Дойча

- $|\psi_3\rangle = U_f(|\psi_2\rangle) = U_f(\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)) =$
  $= \frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle) =$
  $= \frac{1}{2}(|0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle) =$
  $= \frac{1}{2}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle) =$
  $= \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle)$
- $|\psi_4\rangle = (H \otimes I)(|\psi_3\rangle) =$
  $= (H \otimes I)\left(\frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)(|0\rangle - |1\rangle)\right) =$
  $= \frac{1}{2}H((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle) =$
  $= \begin{cases} \frac{(-1)^{f(\mathbf{0})}}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle), & f(0) = f(1) \\ \frac{(-1)^{f(\mathbf{0})}}{\sqrt{2}}|1\rangle \otimes (|0\rangle - |1\rangle), & f(0) \neq f(1) \end{cases}$
- $|\psi_5\rangle = \begin{cases} |0\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}, & f(0) = f(1) \\ |1\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}, & f(0) \neq f(1) \end{cases}$

Задача Дойча-Йожи

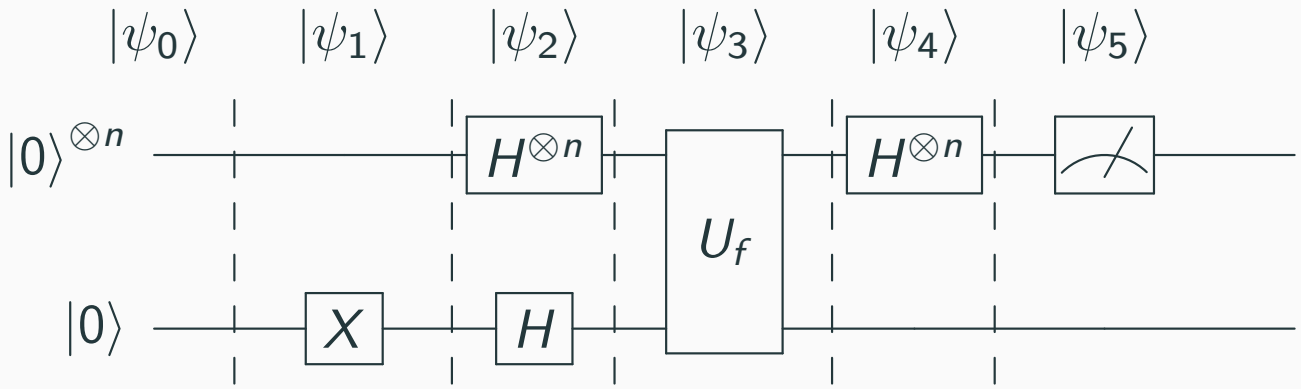
Задача Дойча-Йожи

Задана функція $f\colon \{0,1\}^n \to \{0,1\}$ за допомогою чорного ящика. Відомо апріорі, що функція f є сталою або збалансованою — $\left|f^{-1}(0)\right| = \left|f^{-1}(1)\right| = 2^{n-1}$. З'ясувати, чи є вона сталою.

- *D. Deutsch, R. Jozsa "Rapid solutions of problems by quantum computation" // Proceedings of the Royal Society of London A-439. pp. 553-558. - 1992. doi:10.1098/rspa.1992.0167*
- *R. Cleve, A. Ekert, C. Macchiavello, M. Mosca "Quantum algorithms revisited" // Proceedings of the Royal Society of London A-454. pp. 339-354. - 1998. doi:10.1098/rspa.1998.0164*

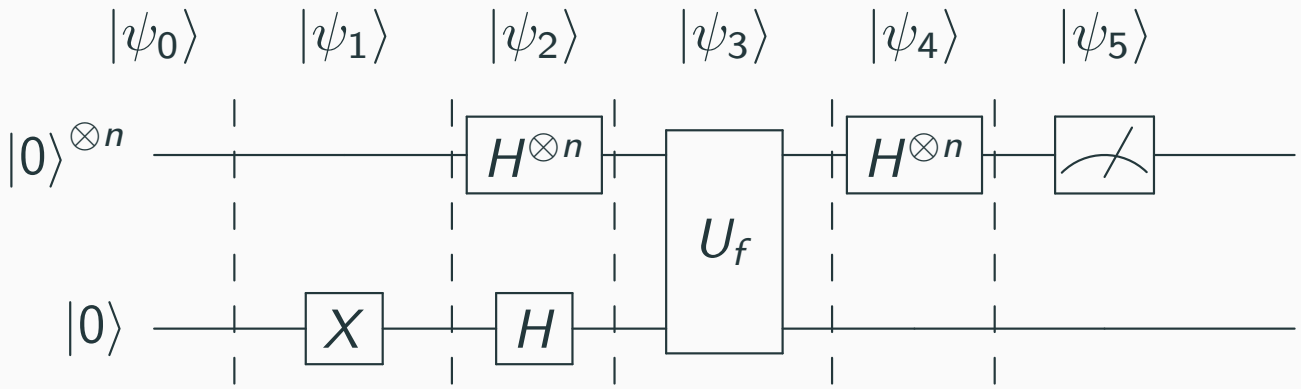
- Тепер будь-який детермінований алгоритм повинен використовувати $2^{n-1}+1$ запитів в найгіршому випадку.
- Імовірнісний алгоритм може вибрати довільні два значення і порівняти результати. Помилка $\frac{1}{2}$ — одностороння.

Квантовий алгоритм розв'язку задачі Дойча-Йожи



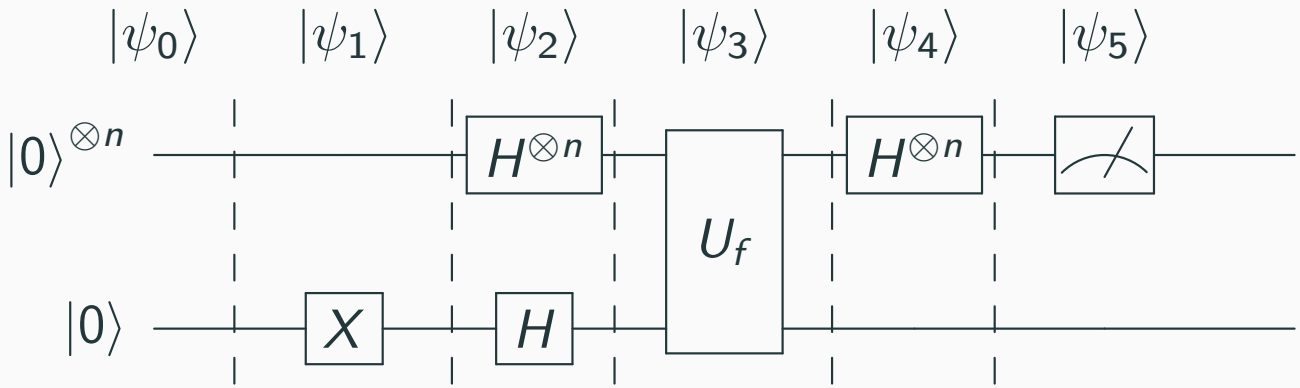
- $|\psi_0\rangle = |0\rangle^{\otimes n} |0\rangle$;

Квантовий алгоритм розв'язку задачі Дойча-Йожи



- $|\psi_0\rangle = |0\rangle^{\otimes n} |0\rangle$;
- $|\psi_1\rangle = (I_n \otimes X)(|\psi_0\rangle) = (I_n \otimes X)(|0\rangle^{\otimes n} |0\rangle) = |0\rangle^{\otimes n} \otimes X(|0\rangle) =$
  $= |0\rangle^{\otimes n} |1\rangle$;

Квантовий алгоритм розв'язку задачі Дойча-Йожи



- $|\psi_0\rangle = |0\rangle^{\otimes n} |0\rangle$;
- $|\psi_1\rangle = (I_n \otimes X)(|\psi_0\rangle) = (I_n \otimes X)(|0\rangle^{\otimes n} |0\rangle) = |0\rangle^{\otimes n} \otimes X(|0\rangle) =$
  $= |0\rangle^{\otimes n} |1\rangle$;
- $|\psi_2\rangle = (H_n \otimes H)(|\psi_1\rangle) = (H_n \otimes H)(|0\rangle^{\otimes n} |1\rangle) =$
  $= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle)$;

Квантовий алгоритм розв'язку задачі Дойча-Йожи

- $|\psi_3\rangle = U_f(|\psi_2\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle \left(|f(x)\rangle - |1 \oplus f(x)\rangle\right) =$
  $= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \left(|0\rangle - |1\rangle\right)$

Квантовий алгоритм розв'язку задачі Дойча-Йожи

- $|\psi_3\rangle = U_f(|\psi_2\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle \left(|f(x)\rangle - |1 \oplus f(x)\rangle\right) =$
  $= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \left(|0\rangle - |1\rangle\right)$
- $|\psi_4\rangle = (H_n \otimes I)(|\psi_3\rangle) =$
  $= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \otimes \left(|0\rangle - |1\rangle\right)$

Квантовий алгоритм розв'язку задачі Дойча-Йожи

- $|\psi_3\rangle = U_f(|\psi_2\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle \left(|f(x)\rangle - |1 \oplus f(x)\rangle\right) =$
  $= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \left(|0\rangle - |1\rangle\right)$
- $|\psi_4\rangle = (H_n \otimes I)(|\psi_3\rangle) =$
  $= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \otimes \left(|0\rangle - |1\rangle\right)$
- $Pr\{|\psi_5\rangle = |0^{\otimes n}\rangle\} = \left| \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} \right|^2 =$
  $= \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2 = \begin{cases} 1, & f - \text{стала} \\ 0, & f - \text{збалансована} \end{cases}$

Розвиток задачі Дойча

- *D. Deutsch "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer" // Proceedings of the Royal Society of London A-400. pp.97-117. - 1985. doi:10.1098/rspa.1985.0070*

  Оригінальний розв'язок не є детермінованим, а має ймовірність успіху $\frac{1}{2}$.

- *D. Deutsch, R. Jozsa "Rapid solutions of problems by quantum computation" // Proceedings of the Royal Society of London A-439. pp. 553-558. - 1992. doi:10.1098/rspa.1992.0167*

  Детермінований розв'язок, але два запити до оракула.

- *R. Cleve, A. Ekert, C. Macchiavello, M. Mosca "Quantum algorithms revisited" // Proceedings of the Royal Society of London A-454. pp. 339-354. - 1998. doi:10.1098/rspa.1998.0164*

  Покращений детермінований розв'язок задачі Дойча-Йожи з одним запитом до оракула.

Задача Бернштейна-Вазірані

Задача Бернштейна-Вазірані

Задана функція $f\colon \{0,1\}^n \to \{0,1\}$ за допомогою чорного ящика. Відомо, що $f(x) = s \cdot x \pmod 2$ для деякого фіксованого невідомого s. Знайти значення s.

E. Bernstein, U. Vazirani "Quantum complexity theory" // SIAM Journal on Computing, 26(5) pp. 1411-1473. 1997

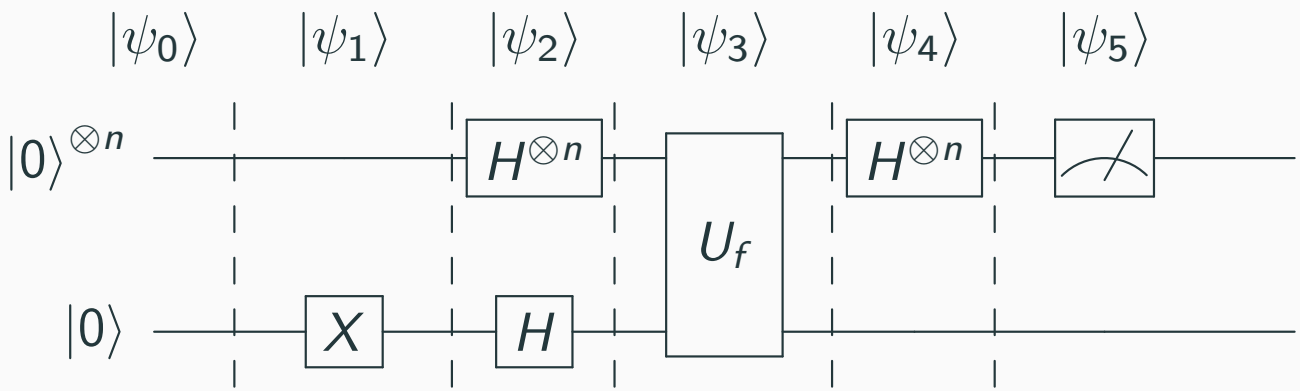
Розв'язок в класичній моделі обчислень

Один запит — один біт інформації.

Зробити n запитів за всіма векторами з вагою 1.

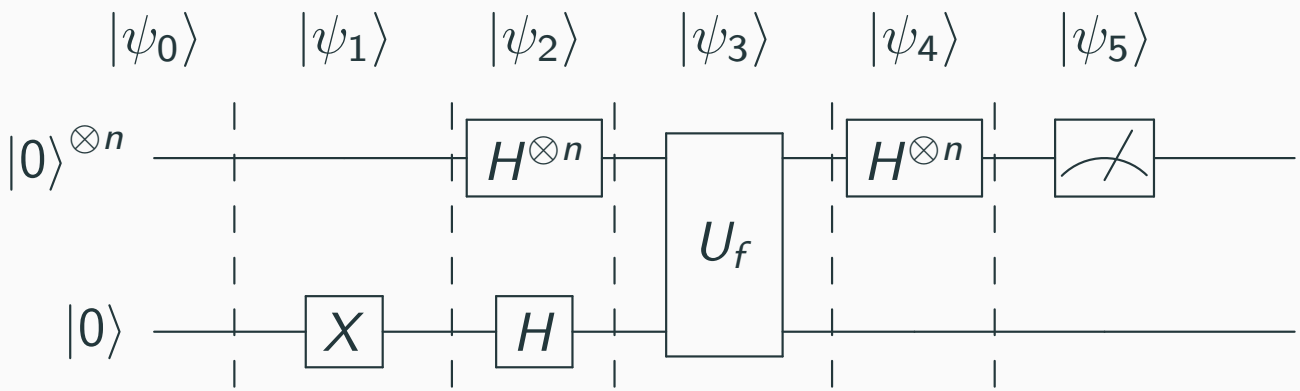
(навіть в межах BPP)

Квантовий алгоритм розв'язку задачі Бернштейна-Вазірані



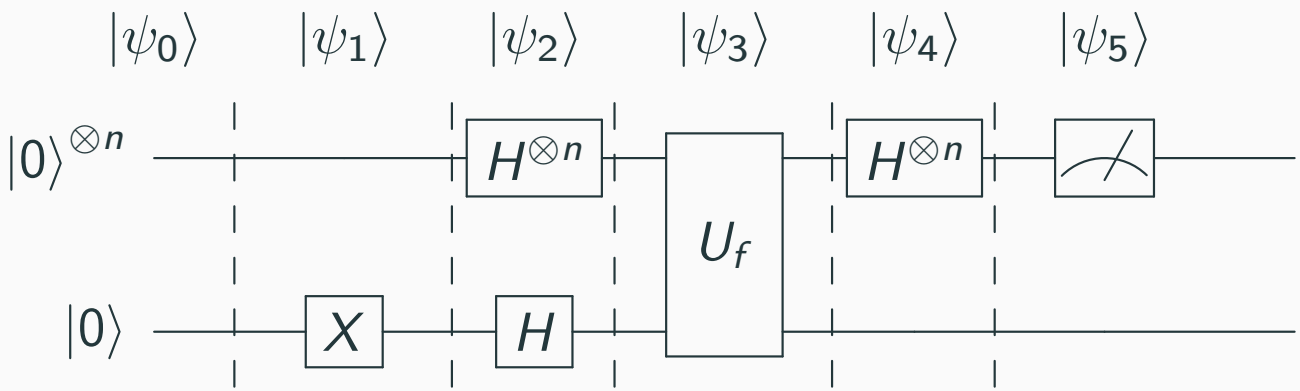
- $|\psi_1\rangle = |0\rangle^{\otimes n} |1\rangle$

Квантовий алгоритм розв'язку задачі Бернштейна-Вазірані



- $|\psi_1\rangle = |0\rangle^{\otimes n} |1\rangle$
- $|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle)$

Квантовий алгоритм розв'язку задачі Бернштейна-Вазірані



- $|\psi_1\rangle = |0\rangle^{\otimes n} |1\rangle$
- $|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle)$
- $|\psi_4\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{f(x)+x\cdot y} |y\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} = |s\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$

Задача Саймона

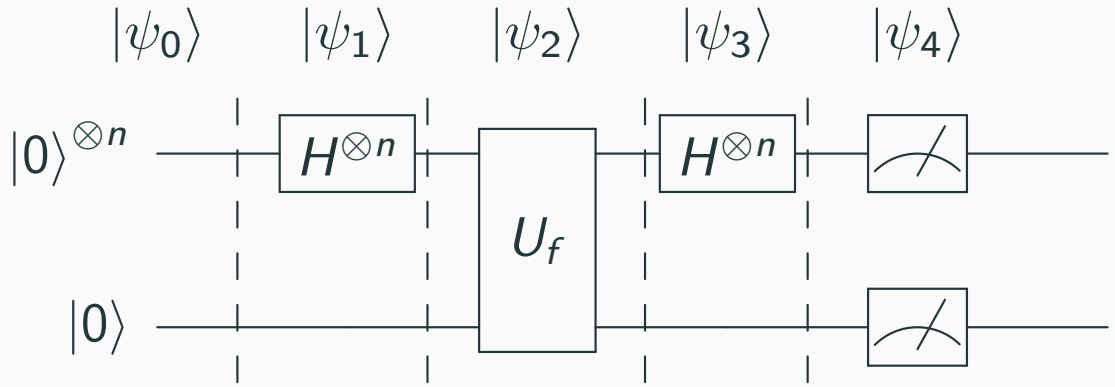
Задана функція $f : \{0,1\}^n \to \{0,1\}^n$ за допомогою чорного ящика. Відомо, що $f(x) = f(y) \Leftrightarrow x \oplus y \in \{0, s\}$ для деякого фіксованого невідомого s. Якщо $s = 0(0..0)$, то має місце варіант '1-1', інакше – варіант '2-1'. Визначити до якого варіанту належить задана функція. (Знайти значення s.)

Simon, D.R. "On the power of quantum computation" // Foundations of Computer Science, Proceedings of 35th Annual Symposium pp. 116-123. - 1994

Розв'язок в класичній моделі обчислень

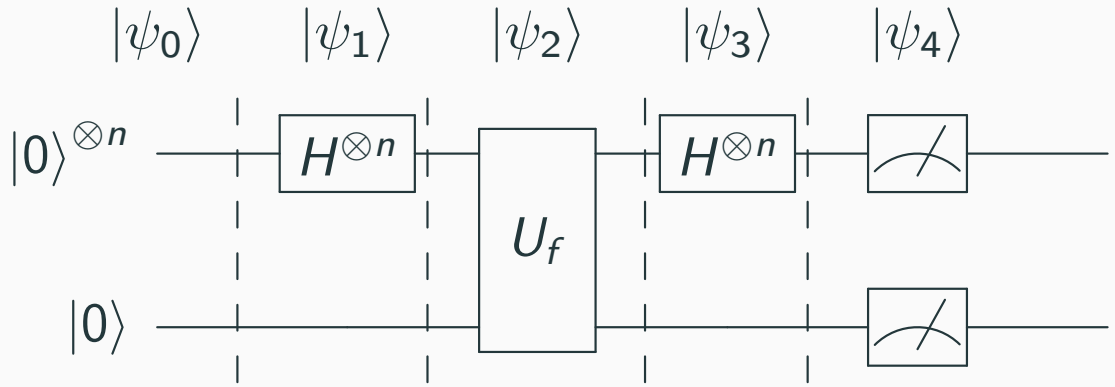
Навіть з імовірнісним алгоритмом — $\mathcal{O}(\sqrt{2^n})$ запитів.

Квантовий алгоритм розв'язку задачі Саймона



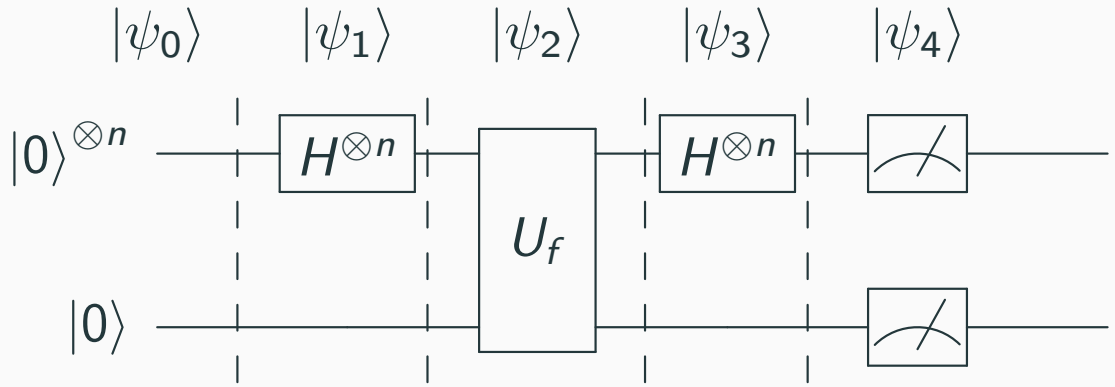
- $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\,|f(x)\rangle$

Квантовий алгоритм розв'язку задачі Саймона



- $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$
- $|\psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} |y\rangle \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle$

Квантовий алгоритм розв'язку задачі Саймона



- $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\, |f(x)\rangle$
- $|\psi_3\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} |y\rangle \sum_{x=0}^{2^n-1} (-1)^{x \cdot y}\, |f(x)\rangle$
- 1-1 $Pr\{\, y = k \,\} = \frac{1}{2^n}$
- 2-1 $Pr\{\, y = k \,\} = \begin{cases} \frac{1}{2^{n-1}}, & k \cdot s - \text{парне} \\ 0, & k \cdot s - \text{непарне} \end{cases}$,

  $y_1, \ldots, y_{n-1}$ — лін. незалежні з імовірністю 0.289

Алгоритм Шора факторизації цілих чисел

Зведення задачі факторизації до пошуку періоду

Задача факторизації цілих чисел

Для заданого складеного числа n знайти один з його нетривіальних дільників (знайти таке натуральне число d, $1 < d < n$, що $d|n$).

- n – парне число $=> d = 2$
- n – просте число більше 2
  Перевіряється окремо за допомогою алгоритму AKS (детермінований) або Міллера-Рабіна (ймовірнісний).
- n – степінь простого числа більше 2
  $n = p^k$, $p \geq 2$, $k \leq log_2 n$.
  Обчислюються всі $m = \left\lceil n^{\frac{1}{k}} \right\rceil$ і перевіряється тотожність $m^k = n$.

  D. Bernstein "Detecting perfect powers in essentially linear time" // Mathematics of Computation 67. - 1998. pp.1253-1283

Далі вважаємо, що n — непарне і має не менше двох різних простих дільників.

Зведення задачі факторизації до пошуку періоду

Твердження

Для складеного числа n за значенням нетривіального квадратного кореня з 1 за модулем n (не +1, і не -1) обчислюється значення нетривіального дільника числа n.

Доведення.

$x^2 = 1 \pmod{n} => (x-1)(x+1) = 0 \pmod{n} =>$
НСД $(n, x+1) = d > 1$. $\square$

Зведення задачі факторизації до пошуку періоду

Твердження

Для складеного числа n за значенням нетривіального квадратного кореня з 1 за модулем n (не +1, і не -1) обчислюється значення нетривіального дільника числа n.

Доведення.

$x^2 = 1 \pmod{n} => (x-1)(x+1) = 0 \pmod{n} =>$
НСД $(n, x+1) = d > 1$. □

Твердження

Якщо n — непарне число, то, щонайменше, половина елементів мультиплікативної групи Z_n^* належить парному показнику.

Доведення.

Для кожного $x \in Z_n^*$ з непарним показником $ord(x) = r$
елемент $(-x) \in Z_n^*$ має парний порядок.
$(-x)^r = (-1)^r x^r = -1 \pmod{n}$ □

Зведення задачі факторизації до пошуку періоду

Теорема

Нехай $n = p_1^{\alpha_1} p_2^{\alpha_2} .. p_k^{\alpha_k}$ – канонічний розклад непарного числа. Тоді ймовірність того, що (рівномірно) випадково обраний елемент $x \in \mathbb{Z}_n^*$ належить парному показнику r і $x^{\frac{r}{2}} \neq -1 \pmod{n}$, більша або дорівнює величині $1 - \frac{1}{2}^{k-1}$.

Доведення.

Китайська теорема про залишки – $x_i \in Z^*_{p_i^{\alpha_i}}$ з порядками r_i, $i = \overline{1,k}$.
$r = \text{НСК}\ (r_1, \ldots, r_k)$.
r — непарне, коли всі $(r_1, \ldots, r_k)$ — непарні.
Якщо r — парне, то $x^{\frac{r}{2}} = \pm 1 \pmod{n} \Leftrightarrow x^{\frac{r}{2}} = \pm 1 \pmod{p_i^{\alpha_i}}$ для кожного p_i. Імовірність цього 2^{-k}. Загальна ймовірність вдалого вибору $(1 - 2^{-k})(1 - 2^{-k}) \geq 1 - 2^{-k+1}$. □

Якщо $n = pq$, то ймовірність вдалої факторизації не менша за $\frac{1}{2}$.

Дискретне перетворення Фур'є

Нехай $x = (x_0, x_1, \ldots, x_N)$, $\hat{x} = (\hat{x}_0, \ldots, \hat{x}_N) \in \mathbb{C}^N$.

Означення

(Прямим) дискретним перетворенням Фур'є (DFT) називають відображення $x \mapsto \hat{x}$, де $\hat{x}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{-2\pi ijk/N}$.

Зворотним дискретним перетворенням Фур'є (IDFT) називають відображення $\hat{x} \mapsto x$, де $x_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \hat{x}_j e^{2\pi ijk/N}$.

Складність $\mathcal{O}(N^2)$ або апроксимаційні алгоритми, як Кулі-Тьюкі мають оцінку складності $\mathcal{O}(N \log N)$

Дискретне перетворення Фур'є

Нехай $\omega_N = e^{-2\pi i/N}$, $\omega_N^N = 1$.

Матриця перетворення DFT має вигляд

$$\frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_N & \omega_N^2 & \dots & \omega_N^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \dots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$ — лінійний оператор

Приклад $N = 2$

$DFT_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ — перетворення Уолша-Адамара

Дискретне перетворення Фур'є

Приклад $N = 4$

$$DFT_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & 1 \end{pmatrix}$$

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & 1 \end{pmatrix}\left[\frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}\right] = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Квантове перетворення Фур'є

Нехай $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$ — ортонормований базис квантової системи і вектор стану $|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$

Означення

Квантовим перетворенням Фур'є (QFT) називають відображення $|\psi\rangle \mapsto |\hat{\psi}\rangle$, де $|\hat{\psi}\rangle = \sum_{k=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{-jk} |k\rangle$.

$$|j\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{-jk} |k\rangle$$

$$QFT_N = \frac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} \omega^{-jk} |k\rangle \langle j|$$

Властивості квантового перетворення Фур'є

Теорема

Квантове перетворення Фур'є є унітарним.

Доведення.

$\omega_N^* = \omega_N^{-1}$.

$$\sum_{k=0}^{N-1} \omega_N^{ks} = \frac{\omega_N^{Ns-1}}{\omega_N^s - 1} = 0$$

$$QFT_N^+ = \frac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} \omega^{jk} |k\rangle \langle j|.$$

$$QFT_N QFT_N^+ = \frac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} \omega^{-jk} |k\rangle \langle j| \frac{1}{\sqrt{N}} \sum_{r,s=0}^{N-1} \omega^{rs} |r\rangle \langle s| =$$

$$= \frac{1}{N} \sum_{j,k,r,s=0}^{N-1} \omega^{rs-jk} |k\rangle \langle j| |r\rangle \langle s| = \frac{1}{N} \sum_{j,k,r,s=0}^{N-1} \omega^{rs-jk} \delta_{jr} |k\rangle \langle s| =$$

$$= \frac{1}{N} \sum_{j,k,s=0}^{N-1} \omega^{j(s-k)} |k\rangle \langle s| = \sum_{k,s=0}^{N-1} \delta_{ks} |k\rangle \langle s| = \sum_{k=0}^{N-1} |k\rangle \langle k| = I \qquad \square$$

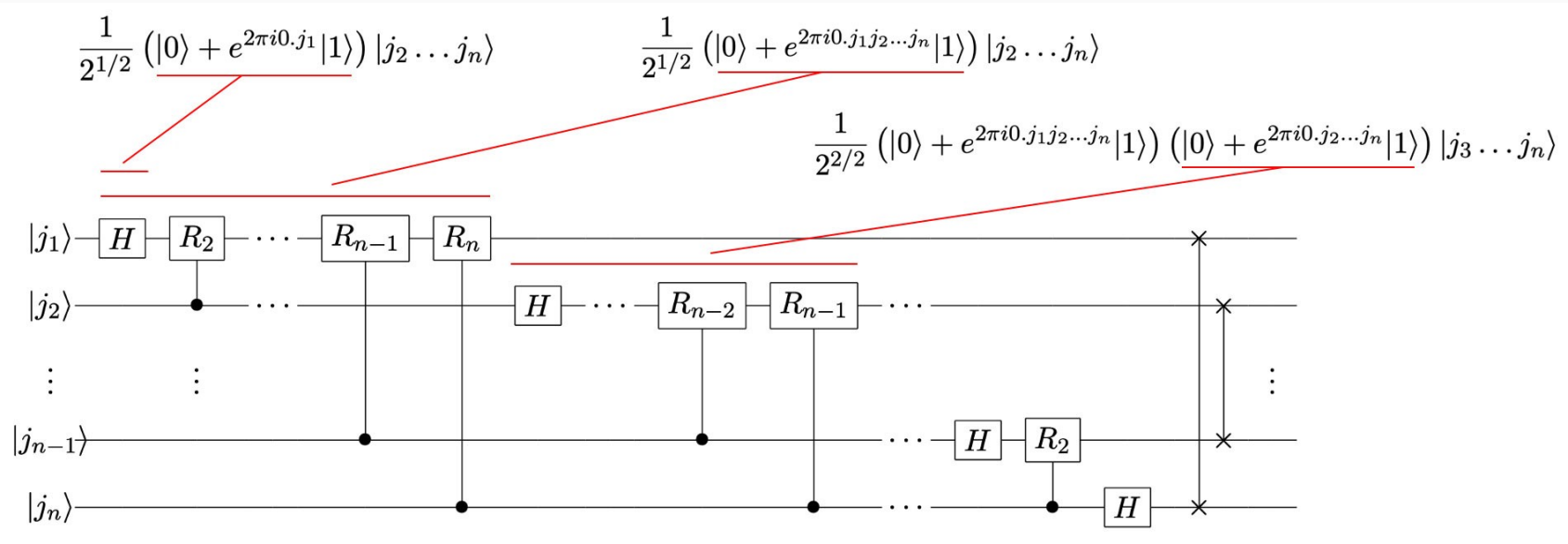
Властивості квантового перетворення Фур'є

D. Coppersmith "An approximate Fourier transform useful in quantum factoring" //

Technical Report RC19642, IBM. 1994

$$j = j_1 j_2 \dots j_n = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n$$
$$0.j_l j_{l+1} \dots j_m = j_l/2 + j_{l+1}/4 + \dots + j_m/2^{m-l+1}$$

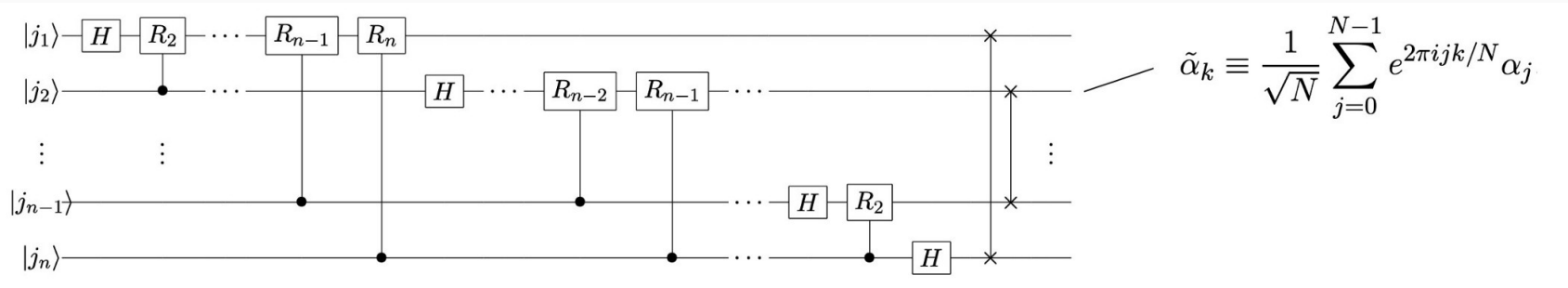
$$QFT(|j_1 j_2 \dots j_n\rangle) = \frac{(|0\rangle + e^{2\pi \mathbf{0}.j_n}|1\rangle)(|0\rangle + e^{2\pi \mathbf{0}.j_{n-1}j_n}|1\rangle)..(|0\rangle + e^{2\pi \mathbf{0}.j_1 j_2 \dots j_n}|1\rangle)}{2^{n/2}}$$



Властивості квантового перетворення Фур'є

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

$\mathcal{O}(n^2)$ квантових вентилів



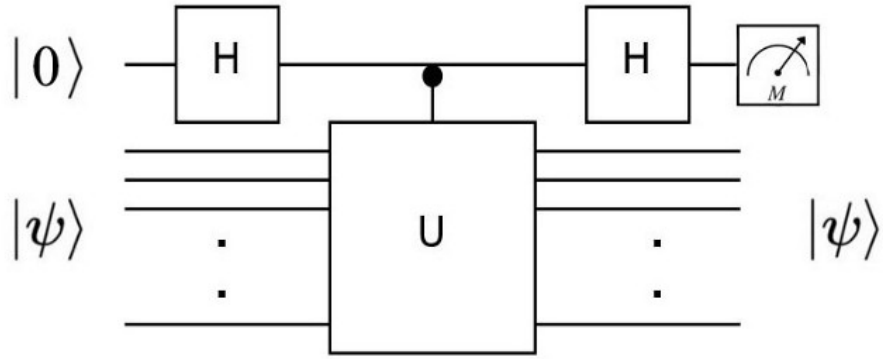
Оцінка фази

eigenvector

$$U|\psi\rangle = e^{2\pi i\phi}|\psi\rangle, 0 \leq \phi < 1$$

complex eigenvalue

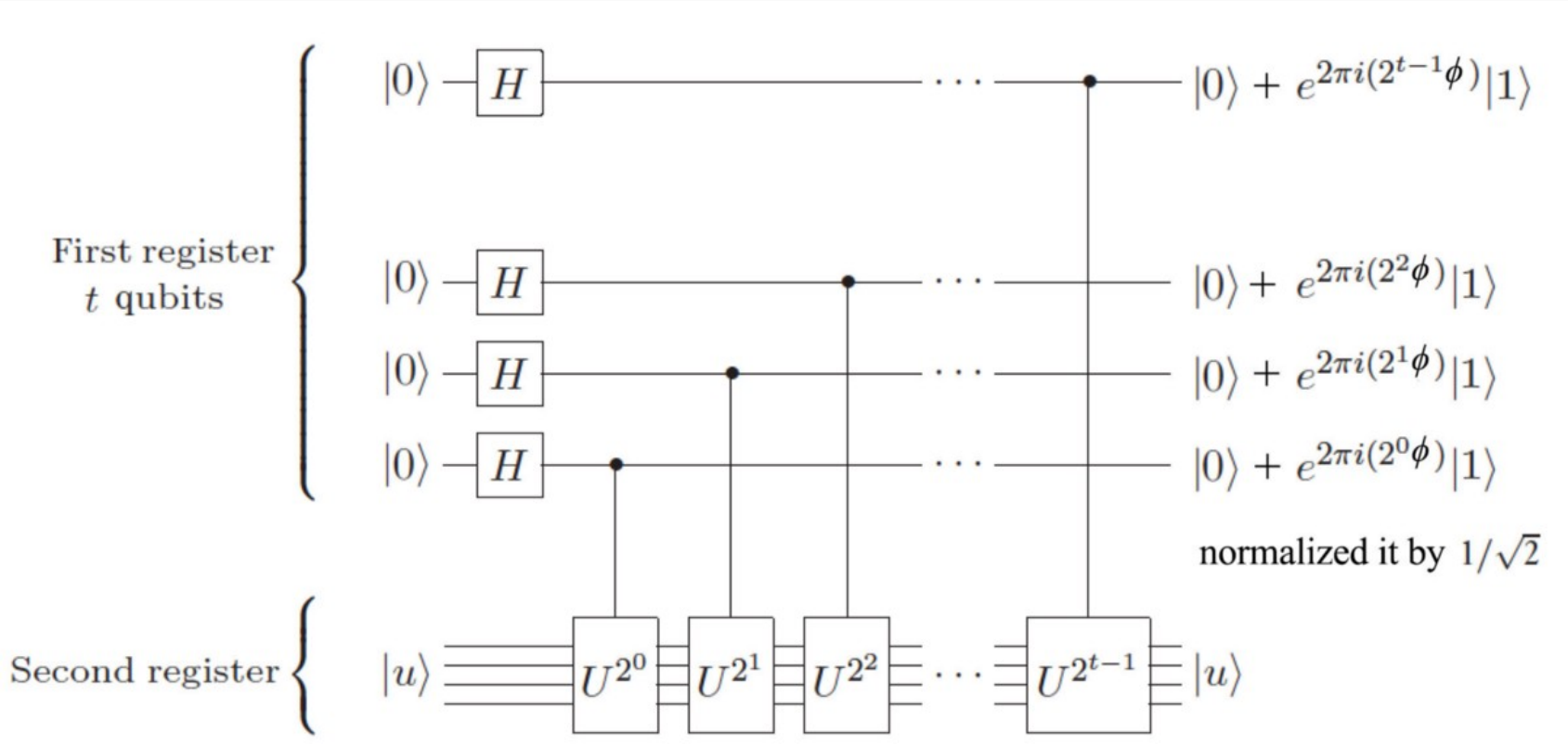
За відомими значеннями оператора U і власного вектора $|\psi\rangle$ можна оцінити значення ϕ за допомогою такої квантової схеми



$$\langle\psi|U + U^{+}|\psi\rangle/2 = \frac{1}{2}(e^{2\pi i\phi} + e^{-2\pi i\phi}) = cos(2\pi\phi)$$

Оцінка фази

A.Yu. Kitaev "Quantum measurements and the Abelian Stabilizer Problem", 1995



$2^1\phi = \phi_1.\phi_2 \dots \phi_t$

$e^{2\pi i \phi_1.\phi_2 \dots \phi_t} = e^{2\pi i 0.\phi_2 \dots \phi_t} => QFT^{-1}$

Алгоритм Шора

P.W. Shor "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" // SIAM Journal on Computing. Vol. 26. Iss.5. 1997. pp. 1484-1509

Функція $f(x) = a^x \pmod N$ — періодична.

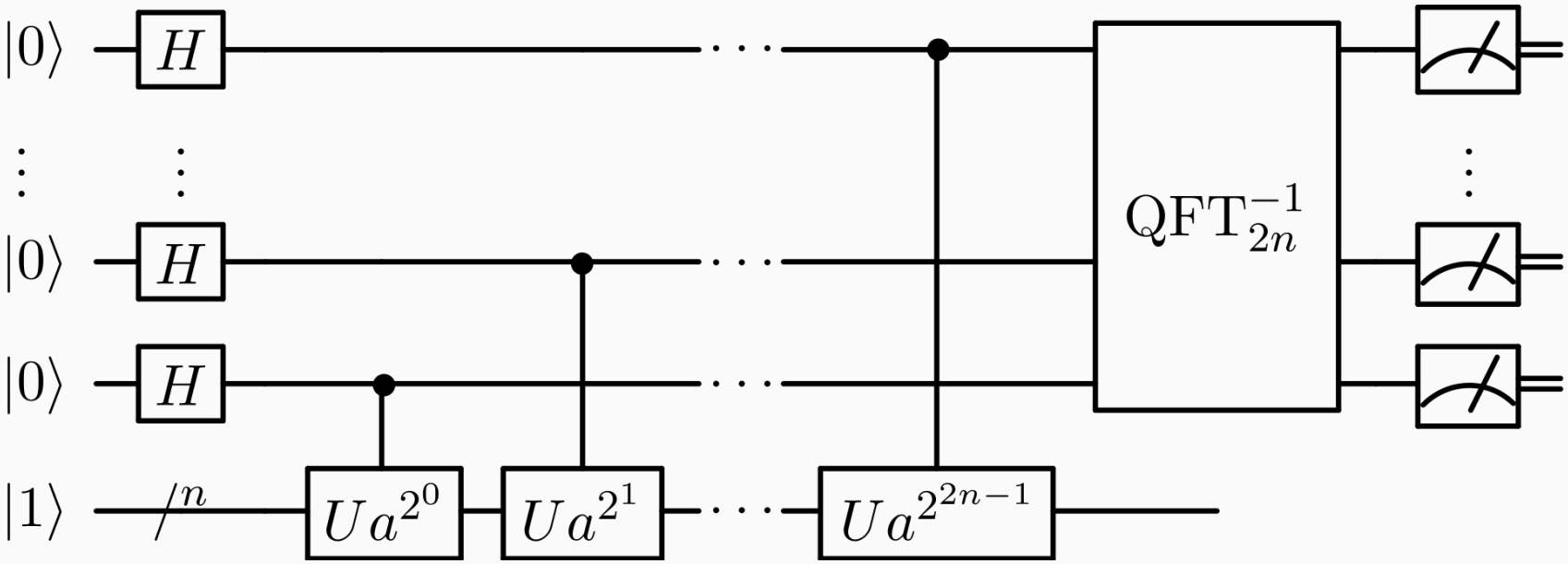
$U|y\rangle = |xy \pmod N\rangle$

$U|u_s\rangle = e^{\frac{2\pi i s}{r}}|u_s\rangle$

Власний вектор $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi i s k}{r}} |x^k \pmod N\rangle$ (r – період)

Власний вектор є невідомим, але $\sum_x |x\rangle |f(x)\rangle$

Алгоритм Шора



Алгоритм Шора

$f(x) = a^x \pmod N$, $(a, N) = 1$, $Q = 2^q$, $N^2 \leq Q < 2N^2$, $\omega = e^{\frac{2\pi i}{Q}}$, $a^r = 1 \pmod N$, $(\frac{Q}{r} > N)$

1. $\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |f(x)\rangle$;
2. $\frac{1}{Q} \sum_{x=0}^{Q-1} \sum_{y=0}^{Q-1} \omega^{xy} |y\rangle |f(x)\rangle = \frac{1}{Q} \sum_{z=0}^{N-1} \sum_{y=0}^{Q-1} \sum_{x \in \{0,..,Q-1\}; f(x)=z} \omega^{xy} |y\rangle |z\rangle$;
3. $\sum_{x \in \{0,..,Q-1\}; f(x)=z} \omega^{xy} = \omega^{x_0 y} \sum_{t=0}^{\lfloor (Q-x_0-1)/r \rfloor} \omega^{rty}$, $f(x_0 = z)$;
4. Імовірність істотно більша для цілих значень близьких до $\frac{yr}{Q}$. Існує ціле значення d таке, що для результату вимірювання y $-\frac{r}{2} \leq ry - dQ \leq \frac{r}{2}$ або $\left|\frac{y}{Q} - \frac{d}{r}\right| \leq \frac{1}{2Q}$.

Приклад алгоритму Шора. Факторизація числа 21

Обираємо "випадково" число $a = 4$ і будемо використовувати функцію $f : \mathbb{Z}_{21} \to \mathbb{Z}_{21}$. Нехай $\omega = e^{\frac{2\pi i}{21}}$.

- $|\psi_0\rangle = |0\rangle\,|0\rangle$;
- $|\psi_1\rangle = (H \otimes I)\,|\psi_0\rangle = \frac{1}{\sqrt{21}} \sum_{j=0}^{20} |j\rangle\,|0\rangle$;
- $|\psi_2\rangle = (U_f)\,|\psi_1\rangle = \frac{1}{\sqrt{21}} \sum_{j=0}^{20} |j\rangle\,|4^j \pmod{21}\rangle =$
  $\frac{1}{\sqrt{21}}((|0\rangle + |3\rangle + |6\rangle + |9\rangle + |12\rangle + |15\rangle + |18\rangle)\,|1\rangle +$
  $(|1\rangle + |4\rangle + |7\rangle + |10\rangle + |13\rangle + |16\rangle + |19\rangle)\,|4\rangle +$
  $(|2\rangle + |5\rangle + |8\rangle + |11\rangle + |14\rangle + |17\rangle + |20\rangle)\,|16\rangle)$;

Приклад алгоритму Шора. Факторизація числа 21

- $|\psi_{3s}\rangle = \frac{1}{\sqrt{7}} \sum_{k=0}^{6} |s+3k\rangle$ з ймовірністю $\frac{1}{3}$, $s \in \{0,1,2\}$;
- $|\psi_{4s}\rangle = (QFT)\,|\psi_{3s}\rangle = \frac{1}{\sqrt{21 \cdot 7}} \sum_{j=0}^{20} \sum_{k=0}^{6} \omega^{j\cdot(s+3k)} |j\rangle =$
  $\frac{1}{\sqrt{3}}(|0\rangle + \omega_3^s |7\rangle + \omega_3^{2s} |14\rangle)$, где $\omega_3 = e^{\frac{2\pi i}{3}}$;

$$\frac{1}{\sqrt{21 \cdot 7}} \sum_{j=0}^{20} |j\rangle \sum_{k=0}^{6} \omega^{j\cdot(s+3k)} = \frac{1}{\sqrt{21 \cdot 7}} \sum_{j=0}^{20} |j\rangle\, \omega^{js} \sum_{k=0}^{6} (\omega^{3j})^k =$$

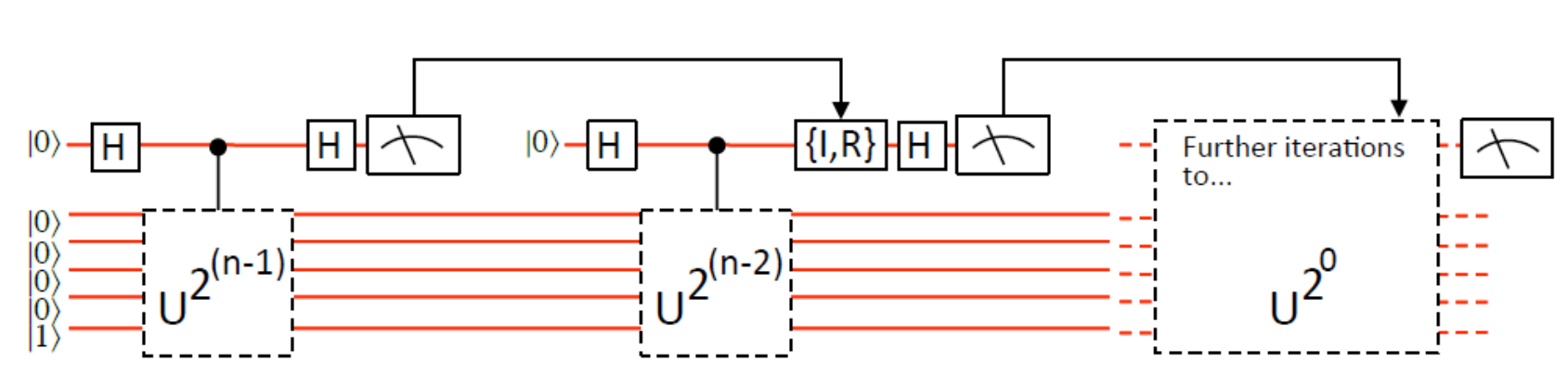
$$\frac{1}{\sqrt{21 \cdot 7}} \sum_{j=0}^{20} |j\rangle\, \omega^{js\,\frac{(\omega^{3j})^7 - 1}{\omega^{3j} - 1}} = \begin{cases} 0, (j,21) = 1 \\ \frac{1}{\sqrt{3}}(|0\rangle + \omega_3^s |7\rangle + \omega_3^{2s} |14\rangle), (j,21) \neq 1 \end{cases}$$

Алгоритм Шора з оцінкою фази

1. $|0\rangle\,|0\rangle$;
2. $\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\,|0\rangle$;
3. $\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\,|a^x \pmod N\rangle \approx \frac{1}{\sqrt{rQ}}\sum_{s=0}^{r-1}\sum_{x=0}^{Q-1} e^{2\pi i s x/r}\,|x\rangle\,|u_s\rangle$;
4. $\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|s/r\rangle\,|u_s\rangle$;
5. $\frac{s}{r}$.

Складність — $3\log N$ кубітів, $72(\log N)^3$ вентилів
з довжиною 4096 – необхідно $12\cdot 10^3$ кубітів, $5\cdot 10^{12}$ вентилів

Повторне використання кубітів



- *C. Zalka "Shor's algorithm with fewer (pure) qubits" // arXiv, Quantum Physics Archive, preprint arXiv:quant-ph/0601097. 2006*

  Кількість кубітів з $3 \log N$ до $2 + \frac{3}{2} \log N$

- *R. Griffiths "Semiclassical fourier transform for quantum computation" // Physical Review Letters. 1996. Vol. 76. pp. 3228-3231*

  Напівкласичне перетворення Фур'є

  скомпільована (англ. compiled) версія алгоритму Шора

Рекорди розкладу цілих чисел

Geller M., Zhou M. Factoring 51 and 85 with 8 qubits // Scientific Reports 3. - Article number: 3023. - 2013.

51 і 85, використовуючи 8 кубітів (два простих числа Ферма $2^{2^k}+1$)

Dattani N.S. Bryans N. Quantum factorization of 56153 with only 4 qubits arXiv, Quantum Physics Archive, preprint arXiv:1411.6758

Розклад 3599, 13081 і 44929 за допомогою 4 кубітів (11663, 56153).

Smolin J., Smith G., Vargo A. Oversimplifying quantum factoring // Nature. - Vol. 499. - 2013. - pp. 163-165.

$N = pq \Rightarrow a = \pm pu \pm qv \pmod N$

Нехай лінійна комбінація двох різних простих чисел $p, q > 2$ має вигляд $pu + qv = 1$. Тоді числа $a_1 = p|u| + q|v| \pmod{pq}$ та $a_2 = -p|u| - q|v| \pmod{pq}$ задовольняють умовам алгоритму Шора для розкладу числа pq.

Рекорди розкладу цілих чисел

2916711827974296680312388524755228716883139473760487809056920297187614868524482179340027267139111663717978230371533096070383443864665046308620098850958353740633886815387408545737569847633656759610631072945412618068295192122520736252529037291648269392299372683581403592027608398784492836198250894098306632017902318060791198979254423887016354246768344544491695574093822544480479694112108432408360032429499567251557665315913973256341025110821895980343239063853117646889543922629177406663229044132495936519347117992454977360394817501014332754665920912752404715625740126393252744079373599395659976447448886268793523386277509273708176862717156082508484611729101925001249179130430847237602003369622545447364499769348262804510940337291735608840581880620237472430582144458020444777844681739901154946610653493348042926670336117030953062998874078868121741781428213891506942270143248275093366627964651405225454583983871565575264362070619245995253404335408406274094251541507930489962223602030929303691712004615864747144692211143061105117331141055062323357324460102868892844639853717969528879351032463576007666327939656407836743524210349898144569255819880974190189305810145241824888176440377351421523315104316733335908319061929445055729133925865146591071591421679131991197036305913625909498340745837550238328616326523389612310879552063687648891986904369780354725953974787385107223223832114017138513220531177078928032986060859457771425731786827039909622718285516730355393505286899545948163961825009753295588976152109191688116010897357674168750650492870848101577102451310605267976075295333529213407219664870902388850239990718626327039893057964446352732915530241645516773560132623203458636259796368356550333043110173026786958537035214345542077336150264816717981513016247954721580427073825997541840931859808164635011594724330939913007650568245502383870368041453459263754759406353853687477455823233420901890015100878056397859474610773041517410611808209219346654805199431181155631624419569373925024519740402548661122395732351117884868480173303232957645005239714108606271082064663555971798635477976910425470036884927832372789952924790282755970761560810409635372472166986402891610926666549336312846892273308382987189287185455951612156540657170365064603107793784152103879665519702057160295355048164858113325456806649781899152536807443293486165899770616835010455656569158700587446952602783601617752265792077476085428630992896082724075633093545036431337255099844273247050208842591556573993998880726490232292711942576145836505462461414999055539863396140960056130387255948701297203961099403416057823462615316595448422457386338203243582737274645497316596508416755679786238338349177340910373760981581439915740362476111629626645054391847771221190549981322755239542781839338054517185352342865146072342422069856036865359906907111113263583138392558645866964113159659295459041701754819537614773383671211193327938398490691341078157491279981631613006621789579449868546084565609653393713164497140184704421865461123131795498894932527378272085659816826730421859492184433810357750641658322748591197196075240799638039461339269358657947904299989047952337704316850808375247137807390381938390314930710568529707955099544849757967368961276782183642516799426087633143418807980654131554358585961242226044865977529815340188981828067362153114896493542741979174524060365061826514406268397341325934797427101118300

Задача про приховану підгрупу

Задача про приховану підгрупу (HSP)

Задача про приховану підгрупу, The Hidden Subgroup Problem, HSP

Нехай задано множину твірних елементів групи G, деяку скінченну множину S і відображення $f : G \to S$ (задане за допомогою оракула — чорного ящика) з додатковою умовою, що існує така підгрупа $H \subseteq G$, що $\forall g_1, g_2 \in G$ виконується тотожність $f(g_1) = f(g_2) \Leftrightarrow g_1^{-1} g_2 \in H$ (будемо говорити, що функція f **приховує** підгрупу H). Необхідно знайти множину твірних елементів підгрупи H, використовуючи запити до оракула обчислення функції f.

Властивості

- H відновлюється за таблицею значень функції f – $f(e) = f(h) \Leftrightarrow h \in H$;
- $\forall h_1, h_2 \in H$: $f(h_1) = f(h_2)$;
- $g \in G$, $g \notin H$: $f(g) = f(x) \Leftrightarrow x \in gH$ (класи суміжності);

Задача про приховану підгрупу (HSP)

Ефективний розв'язок

Розв'язок задачі HSP будемо називати **ефективним**, якщо його складність обмежена зверху деяким поліномом від величини $\lceil \log |G| \rceil$

Теорема

Нехай у групі G є клас W з N підгруп, загальним елементом яких є тільки нейтральний елемент. У класичній моделі, в загальному випадку, необхідно $O(\sqrt{N})$ запитів до оракула для розв'язку задачі HSP.

Доведення.

l-ий запит у вигляді g_l. Якщо існує підгрупа $H \in W$: $\forall j, k, 1 \leq j < k \leq l : g_k \notin g_j H$, то видати значення l. Необхідно близько t запитів, щоб отримати близько C_t^2 елементів виду $g_k g_j^{-1}$. Щоб гарантувати потрібно $C_t^2 > N$. □

Задача про приховану підгрупу (HSP)

Зауваження

У класичній моделі обчислень існують часткові випадки з поліном. кількістю запитів. Наприклад, можна ефективно перевірити чи є підгрупа прихованої => мала кількість запитів для
$\mathbb{Z}_p$, p — просте, (2 підгрупи);
$\mathbb{Z}_{2^n}$ ($n+1$ підгрупа).

Якщо в умовах задачі HSP група G —

- абелева, то будемо говорити **абелева задача про приховану підгрупу** або AHSP (операція '+');
- діедральна, то будемо говорити **діедральна задача про приховану підгрупу** або DHSP;

Задача Дойча як AHSP

Задача Дойча

Задана функція $\varphi : \{0,1\} \to \{0,1\}$ за допомогою чорного ящика. З'ясувати, чи є вона сталою.

- $G = \mathbb{Z}_2 = (\{0,1\}, \oplus)$
- $S = \{0,1\}$
- $f : \{0,1\} \to \{0,1\}$, $f = \varphi$, задана як оракул
- якщо φ – стала, $H = \mathbb{Z}_2$
- якщо φ – не є сталою, $H = (0, \oplus)$

$x^{-1}y = x \oplus y$

Задача Дойча-Йожи як AHSP

Задача Дойча-Йожи

Задана функція $\varphi : \{0,1\}^n \to \{0,1\}$ за допомогою чорного ящика. Відомо апріорі, що функція f є сталою або збалансованою – $\left|\varphi^{-1}(0)\right| = \left|\varphi^{-1}(1)\right| = 2^{n-1}$. З'ясувати, вона є сталою чи збалансованою.

- $G = \mathbb{Z}_2^n = (\{0,1\}^n, \oplus)$
- $S = \{0,1\}$
- $f : \{0,1\} \to \{0,1\}$, $f = \varphi$, задана як оракул
- якщо φ — стала, $|H| = |G|$
- якщо φ — збалансована, $|H| = \frac{|G|}{2}$

$x^{-1}y = x \oplus y$

Задача Бернштейна-Вазірані як AHSP

Задача Бернштейна-Вазірані

Задана функція $\varphi : \{0,1\}^n \to \{0,1\}$ за допомогою чорного ящика. Відомо, що $\varphi(x) = s \cdot x = (s_{n-1}x_{n-1} \oplus s_{n-1}x_{n-1} \oplus ..)$ для деякого фіксованого невідомого значення s. Знайти значення s.

- $G = \mathbb{Z}_2^n = (\{0,1\}^n, \oplus)$
- $S = \{0,1\}$
- $f : \{0,1\}^n \to \{0,1\}$, $f = \varphi$, задана як оракул
- $H = \{y \in \mathbb{Z}_2^n | s \cdot y = 0\}$

$\varphi(g_1) = \varphi(g_2) => s \cdot g_1 = s \cdot g_2$

Задача Саймона як AHSP

Задача Саймона

Задана функція $\varphi : \{0,1\}^n \to \{0,1\}^n$ за допомогою чорного ящика. Відомо, що $\varphi(x) = \varphi(y)$ тйттк $x \oplus y \in \{0^n, s\}$ для деякого фіксованого невідомого s. Якщо $s = 0^n$, то має місце варіант '1-1', інакше – варіант '2-1'. Визначити до якого варіанту належить задана функція. (Знайти значення s.)

- $G = \mathbb{Z}_2^n = (\{0,1\}^n, \oplus)$
- $S = \{0,1\}^n$
- $f : \{0,1\}^n \to \{0,1\}$, $f = \varphi$, задана як оракул
- $H = \{0^n, s\}$

$\varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$ або $g_1 = g_2 \oplus s$

Пошук періоду (факторизація) як AHSP

Задача пошуку періоду

Задана функція $\varphi\colon \mathbb{Z}_Q \to \mathbb{Z}_N$ за допомогою чорного ящика. Відомо, що $\varphi(x) = \varphi(x + r)$ для деякого невідомого мінімального значення r, $r|Q$. Знайти значення r.

- $G = \mathbb{Z}_Q$
- $S = \mathbb{Z}_N$
- $f\colon \mathbb{Z}_Q \to \mathbb{Z}_N$, $f = \varphi$, задана як оракул
- $H = r\mathbb{Z}_Q$
- ідеально, коли $Q >> N$, навіть $\mathbb{Z}_Q = \mathbb{Z}$

$\varphi(g_1) = \varphi(g_2) => r|(g_1 - g_2)$

Задача дискретного логарифмування як AHSP

Задача дискретного логарифмування

Задані просте число p і примітивний елемент g за модулем p. Також відомо значення $y = g^x \pmod p$ для деякого невідомого значення $x \in \mathbb{Z}_p$. Знайти значення x.

- $G = (\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}, +)$
- $S = \mathbb{Z}_p$
- $f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p$, $f(a, b) = g^a y^{-b} \pmod p$ задана як оракул
- f – гомоморфізм $f(a_1 + a_2, b_1 + b_2) = f(a_1, b_1) f(a_2, b_2) \pmod p$
- ядро відображення $Ker(f) = \{(0, 0), (r, 1)\}$
- $H = \{(a, b)\} | a = rb \pmod{p - 1}\}$
- справедливо для ел. кривих, включаючи алгоритм Кедлая для підрахунку точок

  K.S. Kedlaya "Quantum computation of zeta functions of curves" // Computational Complexity, 15, 2006, № 1, p.1-19, doi:math.NT/0411623

Умови для ефективного розв'язку задачі HSP

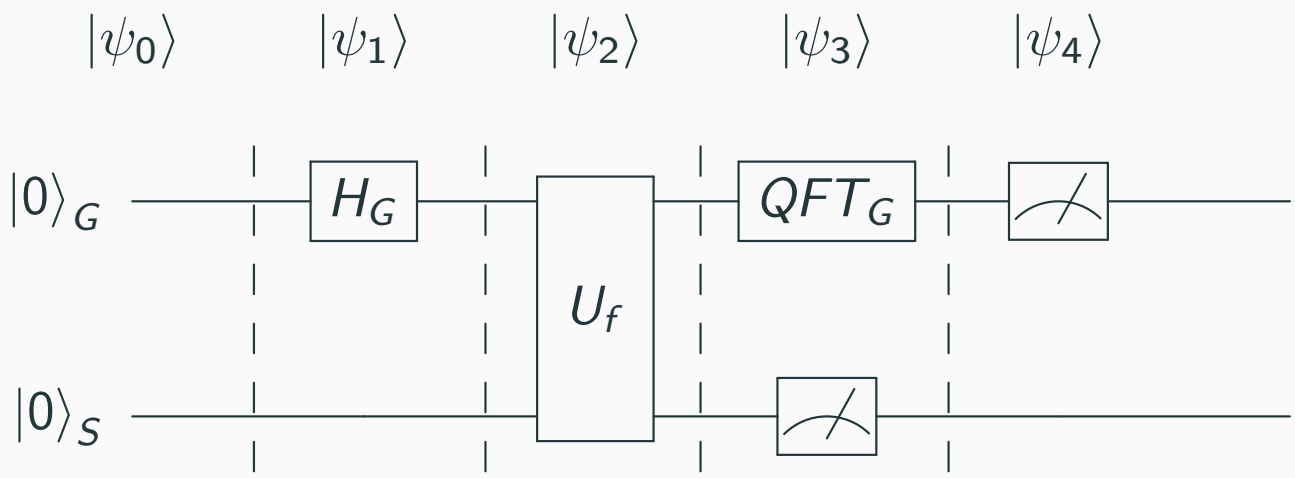
Для ефективного розв'язку задачі HSP необхідно:

1. функція f повинна мати ефективний алгоритм обчислення;
2. має бути достатнім поліноміально обмеженої кількості запитів до оракула обчислення функції f;
3. потужність множини твірних елементів підгрупи H має бути поліноміально обмеженою.

1. загальна кількість функцій $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ дорівнює $(2^n)^{2^n}$ – всі не можуть обчислюватися ефективно;
2. для групи G і довільної підгрупи $H \subseteq G$ необхідна лише поліноміальна кількість запитів до оракула (навіть $O(\log |G|)$) *M.Ettinger, P.Høyer, E.Knill Hidden Subgroup States are Almost Orthogonal. - 1999*
3. достатньо $\log |H| < \log |G|$ елементів.

Квантовий стандартний підхід до розв'язку задачі HSP

H_G, H_S — гільбертові простори з ортонормованими базисами $\{|g\rangle : g \in G\}$, $\{|x\rangle : x \in S\}$.



- $|\psi_2\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle\,|f(g)\rangle$;
- $|\psi_3\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |r+h\rangle\,|f(r)\rangle$; G – абелева

Задача про приховану підгрупу (HSP)

Ефективність перетворення QFT

- $QFT_{Z_2^n} = H^{\otimes n}$;
- $QFT_{Z_{2^n}}$ — алгоритм Шора;
- QFT_{Z_N} — апроксимація за допомогою $QFT_{Z_{2^n}}$;
- для будь-якої абелевої групи — $G \cong Z_{p_1^{\alpha_1}} \times \ldots \times Z_{p_n^{\alpha_n}}$

  K.H. Cheung, M. Mosca "Decomposing Finite Abelian Group" 2001
- $QFT_{\mathbb{Z}}$ і $QFT_{\mathbb{R}}$

  S. Hallgren "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem" // Journal of the ACM (JACM), 54(1):4. 2007

Теорема

Задача AHSP має ефективний (поліноміальний) розв'язок в квантовій моделі обчислень. *A. Yu. Kitaev "Quantum measurements and the Abelian Stabilizer Problem" 1995*

Загальний розв'язок задачі про приховану підгрупу (HSP)

- коеф. в розкладі Фур'є — матриці комплексних чисел (розширення базису, істотне збільшення часової складності перетворення)
  - для більшості класів груп QFT можна реалізувати ефективно

    C. Moore, D. Rockmore, A. Russell, L.J. Schulman "The Power of Strong Fourier Sampling: Quantum Algorithms for Affine Groups and Hidden Shifts" 2005
  - weak Fourier sampling (DHSP, S_n) — тільки представлення
  - strong Fourier sampling — представлення з координатами
- обробка результатів по відновленню прихованої групи повинні виконуватися за поліноміальний час в класичній моделі обчислень

Наявні розв'язки неабелевої задачі про приховану підгрупу (HSP)

- розв'язні групи з обмеженим рядом комутантів та експоненти
  K.Friedl, G.Ivanyos, F.Magniez, M.Santha, P.Sen Hidden translation and orbit coset in quantum computing - 2003. - pp. 1-9.
- екстраспеціальні групи
  G.Ivanyos, L.Sanselme, M.Santha An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups // Proc. 24th STACS, LNCS. - 2007. - Vol. 4393. - pp. 586-597.
- групи Гейзенберга
  D.Bacon, A.Childs, W. van Dam From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups // In Proc. 46th IEEE FOCS. - 2005. - pp. 469-478.

Наявні розв'язки неабелевої задачі про приховану підгрупу (HSP)

- нільпотентні групи класу не більше 2
  G.Ivanyos, L.Sanselme, M.Santha An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups - 2008.
- Групи виду $G = Z_{p^r} \rtimes_\varphi Z_q$, де p, q — прості числа, $r \geq 1$
  Y. Inui, F. Le Gall Efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups // Quantum Inf. Comput. -2007. - Vol. 7. - pp. 559-570.
- певний вид метациклічних груп
  D.N. Goncalves, R. Portugal, C.M.M. Cosme Solutions to the hidden subgroup problem on some metacyclic groups - 2009.
- сплетіння груп Z_2^k та Z_2
  M. Roetteler, T. Beth Polynomial-time solution to the Hidden Subgroup Problem for a class of non-abelian groups - 1998.

Задача про прихований зсув

Задача про прихований зсув, DHSP

Задача про прихований зсув, Hidden Shift Problem, Hidden Translation Problem, DHSP

Нехай задані множина твірних елементів скінченної групи G, $(G, \circ, ^{-1}, e)$, і дві ін'єктивні функції — f_0 і f_1, які відображають групу G в деяку скінченну множину S з додатковою умовою, що існує такий елемент $u \in G$, який називають **зсувом**, що для будь-якого значення $g \in G$ виконується співвідношення $f_0(g) = f_1(g \circ u)$. Необхідно знайти невідоме значення зсуву u, використовуючи обчислення значень функцій f_0 і f_1.

W. van Dam, S. Hallgren, L. Ip "Quantum algorithms for some hidden shift problems" // SIAM Journal on Computing. 2006. № 36. pp. 763-778

Зауваження

Якщо G — абелева, то говоримо про **абелеву задачу про прихований зсув** $(G, +, -, 0)$.

Часткові випадки задачі про прихований зсув

van Dam, S. Hallgren, L. Ip. Quantum algorithms for some hidden shift problems.SIAM Journal on Computing, 36:763-778, 2006.
пошук символу Лежандра зі зсувом

A. Childs, L.J. Schulman, U. Vazirani Quantum algorithms forhidden nonlinear structures. (FOCS'07), pp. 395-404, 2007.
геометрична задача пошуку центра сфери зі зсувом

O.Regev Quantum computation and lattice problems // SIAM Journal on Computing, 33(2):738-760, 2004.
задачі на решітках зі зсувом

A.Childs, P.Wocjan On the quantum hardness of solving isomorphism problems as nonabelian hidden shift problems // Quantum Information and Computation, 7(5-6):504-521, 2007.
ізоморфізм графів

Наявні ефективні розв'язки задачі DHSP

- $G = Z_2^n$
- $G = Z_p^n$, $p > 2$

W. van Dam, S. Hallgren, L. Ip Quantum algorithms for some hidden shift problems// SIAM Journal on Computing. - 2006. - №36. - pp. 763-778.

G. Ivanyos, F. Magniez, M. Santha Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem // International Journal of Foundations of Computer Science. - 2003. - Vol. 14. - №5. - pp. 723-739.

S. Fenner, Y. Zhang On the complexity of the hidden subgroup problem // Proceedings of the 5th international conference on Theory and applications of models of computation. Xi'an, China, April 25-29. - 2008.

Задача DHSP

Діедральна група

$D_n = (r, s | r^n = 1, s^2 = 1, srs = r^{-1})$
$(a, 0)(b, i) = (a + b, i)$ і $(a, 1)(b, i) = (a - b, i + 1 \pmod 2)$

Твердження

Абелева задача про прихованний зсув для циклічної групи $\mathbb{Z}_N$ еквівалентна задачі про приховану підгрупу для діедральної групи D_N.

M. Ettinger, P. Hoyer On quantum algorithms for noncommutative hidden subgroups // Advances in Applied Mathematics. - 2000. - Vol. 25. - №3. - pp. 239-251.

Алгоритм Куперберга

В класичній моделі — близько N запитів для розв'язку задачі DHSP.

$N = 2^n$

$|\psi_b\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \omega_N^{bu} |1\rangle)$

$|\psi_c\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \omega_N^{cu} |1\rangle)$

$|\psi_b\rangle |\psi_c\rangle = \frac{1}{2}(|0\rangle |0\rangle + \omega_N^{bu} |1\rangle |0\rangle + \omega_N^{cu} |0\rangle |1\rangle + \omega_N^{u(b+c)} |1\rangle |1\rangle) \longmapsto^{CNOT}$

$\frac{1}{\sqrt{2}}(|\psi_{b+c}\rangle |0\rangle + \omega_N^{cu} |\psi_{b-c}\rangle |1\rangle)$ (декомпозиція Клебша-Гордона)

Необхідною є дуже велика кількість станів такого виду

Алгоритм Куперберга

G. Kuperberg G. Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem // Proceedings of the 8th Conference on the Theory of Quantum Computation, Communication and Cryptography. - 2013. - Vol. 22. - pp. 20-34.

$O(16^{\sqrt{n}})$ – станів при $N = 2^n$, відкидаємо з $+$

O. Regev A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space // e-Print archive. - 2004.

O. Regev On the complexity of lattice problems with polynomial approximation factors // The LLL Algorithm, Information Security and Cryptography. - 2010. - pp. 475-496

Використання NP-повної задачі про суму підмножини для поліноміальної оцінки пам'яті

Зв'язок з пошуком найкоротшого вектора решітки

M-узагальнена задача про прихований зсув

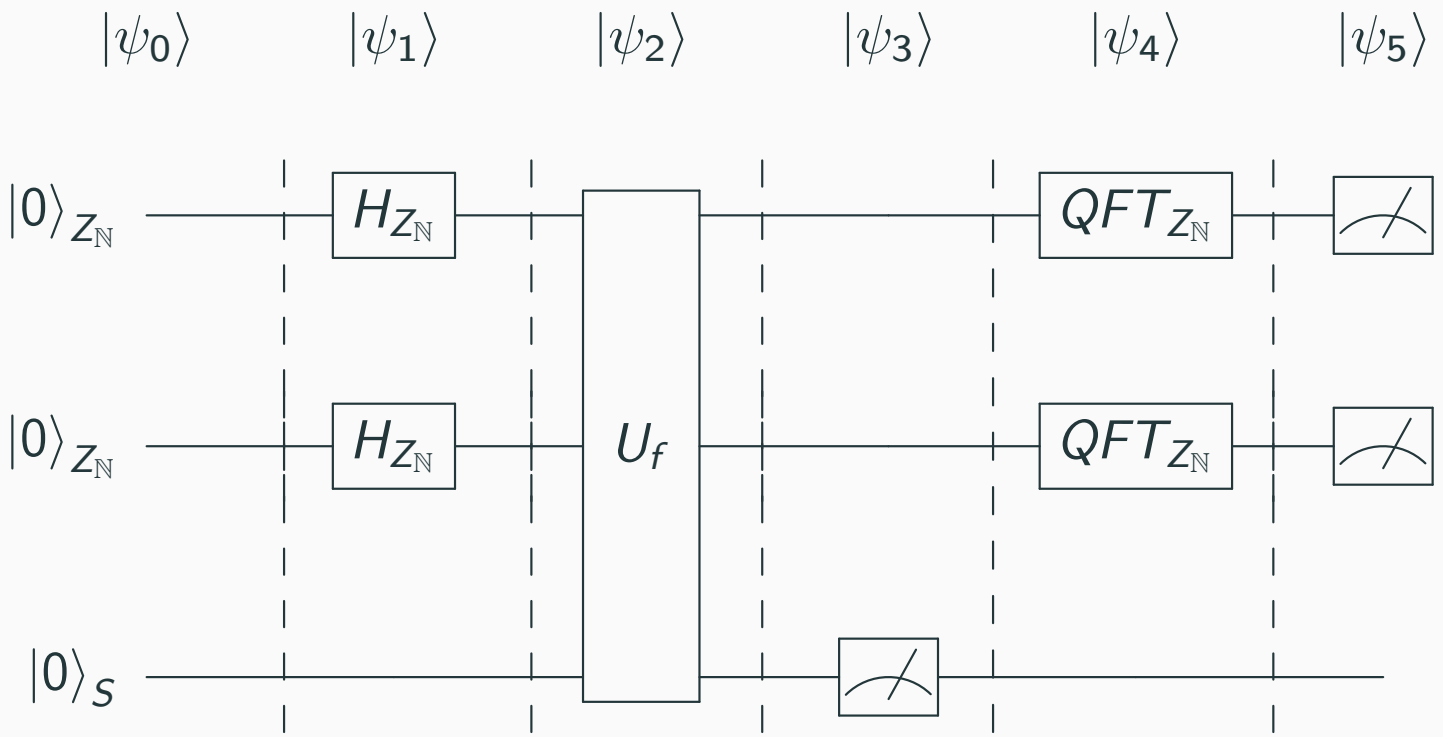
A. Childs, W. van Dam Quantum algorithm for a generalized hidden shift problem // Proc. 18th ACM-SIAM Symposium on Discrete Algorithms (SOD'2007). 2007. pp. 1225-1232.

M-узагальнена задача про прихований зсув, M-generalized hidden shift problem

Нехай задано множину твірних елементів скінченної групи G, $(G, \circ, ^{-1}, e)$, і відображення $f\colon \{0, \ldots, M-1\} \times G \to S$ таке, що для будь-якого фіксованого значення b відображення $f(b, \cdot) : G \to S$ є ін'єктивним, а також, для всіх значень b, $0 \leq b < M-1$, $f(b, g) = f(b+1, g \circ u)$ для довільного значення $g \in G$ і невідомого значення зсуву $u \in G$. Необхідно знайти невідоме значення зсуву u, використовуючи обчислення значень функції f.

При $M = 2$ — задача про прихований зсув, але при досить великих значеннях M узагальнена задача стає набагато простішою.

Розв'язок M-узагальненої задачі про прихований зсув



$$U_f(|b\rangle\,|x\rangle\,|0\rangle) = |b\rangle\,|x\rangle\,|f(b,x)\rangle$$

Розв'язок M-узагальненої задачі про прихований зсув

- $|\psi_2\rangle = \frac{1}{N} \sum_{b=0}^{M-1} \sum_{x=0}^{N-1} |b\rangle |x\rangle |f(b,x)\rangle$
- $|\psi_3\rangle = \frac{1}{\sqrt{N}} \sum_{b=0, f(0,x)=t}^{M-1} |b\rangle |x+bu\rangle |t\rangle$
- $|\psi_4\rangle = (QFT_{Z_{\mathbb{N}}} \otimes QFT_{Z_{\mathbb{N}}}) |\psi_3\rangle =$
  $\frac{1}{N\sqrt{N}} \sum_{y,z \in Z_N} \omega^{xz} \sum_{b=0, f(0,x)=t}^{M-1} \omega^{b(y+uz)} |y\rangle |z\rangle$, $\omega = e^{2\pi i/N}$
- якщо $M = N$, то $|\psi_4\rangle = \frac{1}{\sqrt{N}} \sum_{z \in Z_N} \omega^{xz} |-uz\rangle |z\rangle$

[CvD07] – $M \geq \frac{N}{poly(\log N)}$, використовуючи PGM та цілочисельне програмування

Узагальнення задачі про прихований зсув

- *W. van Dam, S. Hallgren, L. Ip "Quantum algorithms for some hidden shift problems" // SIAM Journal on Computing. 2006. № 36. pp. 763-778*

  Задача про прихований клас суміжності (*Hidden Coset Problem*). Нехай задано множину твірних елементів скінченної групи G, $(G, \circ, ^{-1}, e)$, і два відображення – $f_0 : G \to S$ та $f_1 : G \to S$, де S – деяка скінченна множина, така, що для певних значень зсуву $u \in G$ виконується співвідношення $f_0(g) = f_1(g \circ u)$ для всіх елементів $g \in G$. Необхідно знайти всі невідомі значення зсуву u, використовуючи обчислення значень функцій f_0 і f_1.

Узагальнення задачі про прихований зсув

- *D.N. Goncalves, R. Portugal, C.M.M. Cosme "Solutions to the hidden subgroup problem on some metacyclic groups" // In: Proc. TQC2009, Lect. Notes Comput. Sci. Berlin: Springer-Verlag. 2009. Vol. 5906. pp. 1-9*

  Задача про орбіту класу суміжності,(*Orbit Coset Problem*, OCP). Нехай задано множину твірних елементів скінченної групи G, $(G, \circ, ^{-1}, e)$, і деяку множину попарно ортогональних квантових станів Γ, а також два стани $|\phi_0\rangle, |\phi_1\rangle \in \Gamma$. Необхідно визначити чи виконується $G(|\phi_0\rangle) \cap G(|\phi_1\rangle) = \varnothing$, і знайти $u \in G$ $|u \cdot \phi_0\rangle = |\phi_1\rangle$

Узагальнення задачі про прихований зсув

- *T. Decker, G. Ivanyos, M. Santha, P. Wocjan "Hidden Symmetry Subgroup Problems" // SIAM J. Comput. 2013. Vol. 42(5). pp. 1987-2007*

  Задача про приховану симетрію підгрупи (*Hidden Symmetry Subgroup Problem*, HSSP). Нехай задані множина твірних елементів скінченної групи G, яка діє на множині M, операція $\circ\colon G \times M \to M$, скінченна множина S і деяка функція $f\colon M \to S$ з додатковою умовою, що існує підгрупа $H \subset G$ така, що $\forall m_1, m_2 \in M$ виконується співвідношення $f(m_1) = f(m_1) \Leftrightarrow H \circ m_1 = H \circ m_2$. Необхідно знайти множину твірних елементів підгрупи H.

Узагальнена задача дискретного логарифмування

Задача (узагальненого дискретного логарифмування)

Нехай заданий елемент $A \in G$ з відомим порядком a і є відомим такий елемент $B \in G$, що $A^n B \neq BA^n$ для будь-якого значення $n \in Z_a$, $n \neq 0$. За заданим значенням $K = A^x Z$, де $x \in Z_a$ – невідоме значення, а Z – невідомий елемент з перетину $Z_G(A) \cap Z_G(B)$, знайти значення x та елемент Z.

Розв'язок узагальненої задачі дискретного логарифмування

$f : Z_a \times Z_a \to G$, Z_a — адитивна група кільця лишків

$f(m,n) = A^m K^{-n} B K^n A^{-m} = A^{m-xn} B A^{-m+xn}$

$H = \{(tx, t) | t \in Z_a\} \subseteq Z_a \times Z_a$

якщо $f(m_1, n_1) = f(m_2, n_2)$, то $A^{m_1 - m_2 - xn_1 + xn_2} B = B A^{m_1 - m_2 - xn_1 + xn_2}$

$(m_1 - m_2 - xn_1 + xn_2) \vdots a$

$\forall t_1 \in Z_a \exists t_2 \in Z_a \, t_2 = n_1 + t_1 - n_2$

$(m_1 + t_1 x, n_1 + t_1) = (m_2 + t_2 x, n_2 + t_2)$

$(m_1, n_1)H = (m_2, n_2)H$, тобто f приховує підгрупу H

$Z_a \times Z_a$ — абелева група

за твірними елементами знаходиться значення x, а потім $Z = A^{-x} K$

Задачі комбінаторної теорії груп

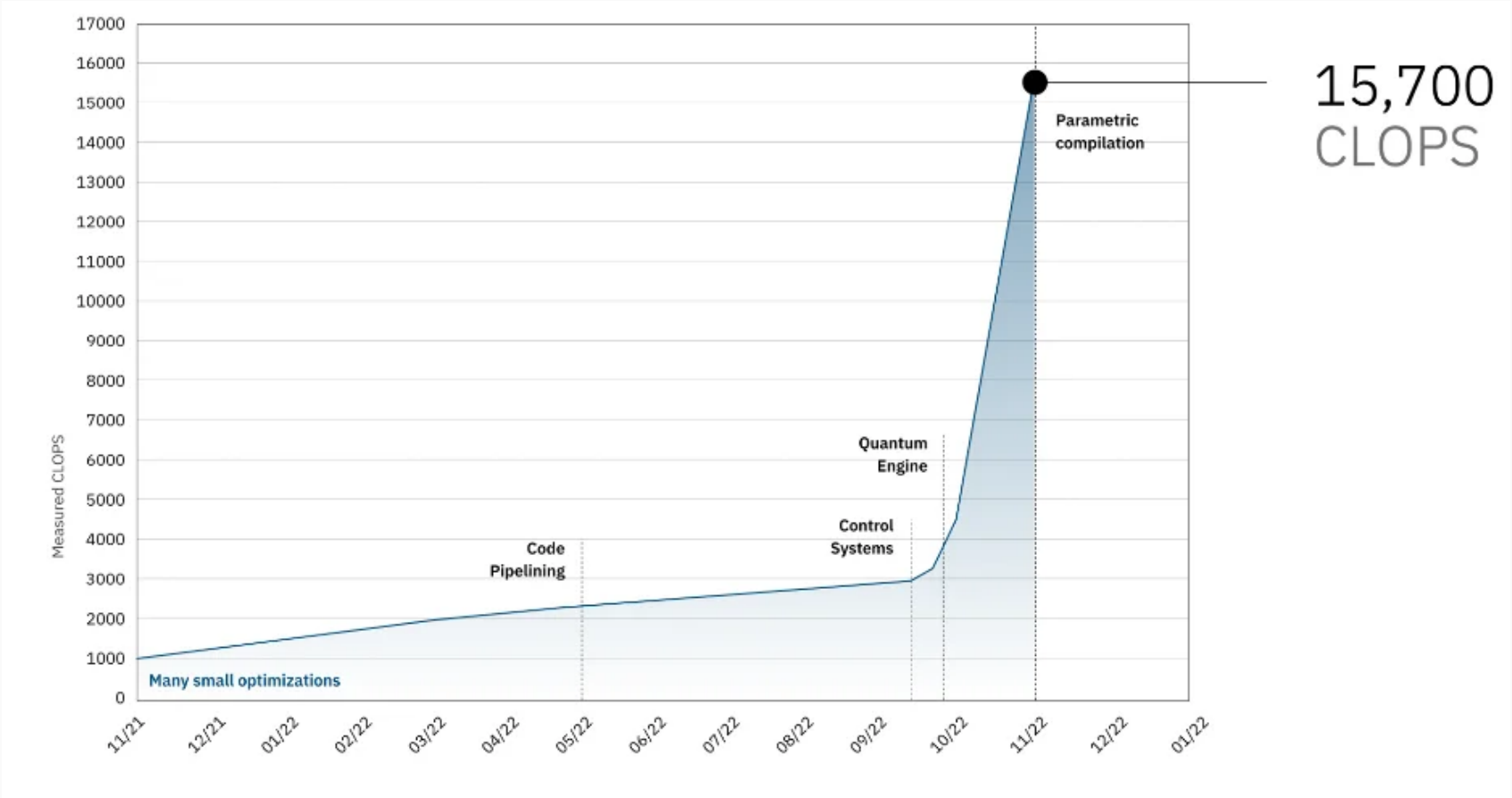
- задача рівності слів (*Word Problem*) — чи правильно, що $g = h$
- задача спряженого елементу (*Conjugacy Problem*) — за заданими словами $g, h \in G$ визначити чи є вони спряженими, тобто $g = vhv^{-1}$
- задача ізоморфізму скінченно визначених груп за їхніми представленнями(*Isomorphism Problem*)
- задача пошуку спряженого елементу (*Conjugacy Search Problem*, CSP): Аншель-Аншель-Голдфельд, група кіс Артіна B_n на n нитках
- задача пошуку спряженого елементу та степеню (*Power Conjugacy Search Problem*, PCSP) : $g = vh^k v^{-1}$, **матричні групи**, **група оборотних елементів узагальненої алгебри кватерніонів над полем** $GF(p)$

Метрики квантових обчислювальних пристроїв

Метрики квантових обчислювальних пристроїв

Класичний комп'ютер — кількість транзисторів

- розмір (кубіти)
- якість
- швидкість (кількість обробки рівнів вентилів в секунду)



Метрика якості

- кількість кубітів

Метрика якості

- кількість кубітів
- точність вентилів

Метрика якості

- кількість кубітів
- точність вентилів
- паралелізм вентилів

Метрика якості

- кількість кубітів
- точність вентилів
- паралелізм вентилів
- оптимізація схеми

Метрика якості

- кількість кубітів
- точність вентилів
- паралелізм вентилів
- оптимізація схеми
- узгодженість (когеренція)

Метрика якості

- кількість кубітів
- точність вентилів
- паралелізм вентилів
- оптимізація схеми
- узгодженість (когеренція)
- точність вимірювання

Метрика якості

- кількість кубітів
- точність вентилів
- паралелізм вентилів
- оптимізація схеми
- узгодженість (когеренція)
- точність вимірювання
- перехресні перешкоди

Метрика якості

- кількість кубітів
- точність вентилів
- паралелізм вентилів
- оптимізація схеми
- узгодженість (когеренція)
- точність вимірювання
- перехресні перешкоди
- точність ініціалізації

Метрика якості

- кількість кубітів
- точність вентилів
- паралелізм вентилів
- оптимізація схеми
- узгодженість (когеренція)
- точність вимірювання
- перехресні перешкоди
- точність ініціалізації
- помилки калібрування

Метрика якості

- кількість кубітів
- точність вентилів
- паралелізм вентилів
- оптимізація схеми
- узгодженість (когеренція)
- точність вимірювання
- перехресні перешкоди
- точність ініціалізації
- помилки калібрування
- помилки спостереження

Метрика якості

- кількість кубітів
- точність вентилів
- паралелізм вентилів
- оптимізація схеми
- узгодженість (когеренція)
- точність вимірювання
- перехресні перешкоди
- точність ініціалізації
- помилки калібрування
- помилки спостереження
- структура стикування

Квантовий об'єм

- кількість кубітів
- кількість елементарних вентилів (глибина)
- характеристики алгоритмів

Nikolaj Moll та ін. Quantum optimization using variational algorithms on near-term quantum devices - 2018

$V_Q = \min N, d(N)$, N — кількість кубітів, d глибина схеми, $d \approx \frac{1}{N\epsilon_{eff}}$, ϵ_{eff} — помилка в середньому двокубитного вентиля.

Квантовий об'єм

$$V_Q = \max_{n \leq N} \min n, \frac{1}{n\epsilon_{eff}}$$

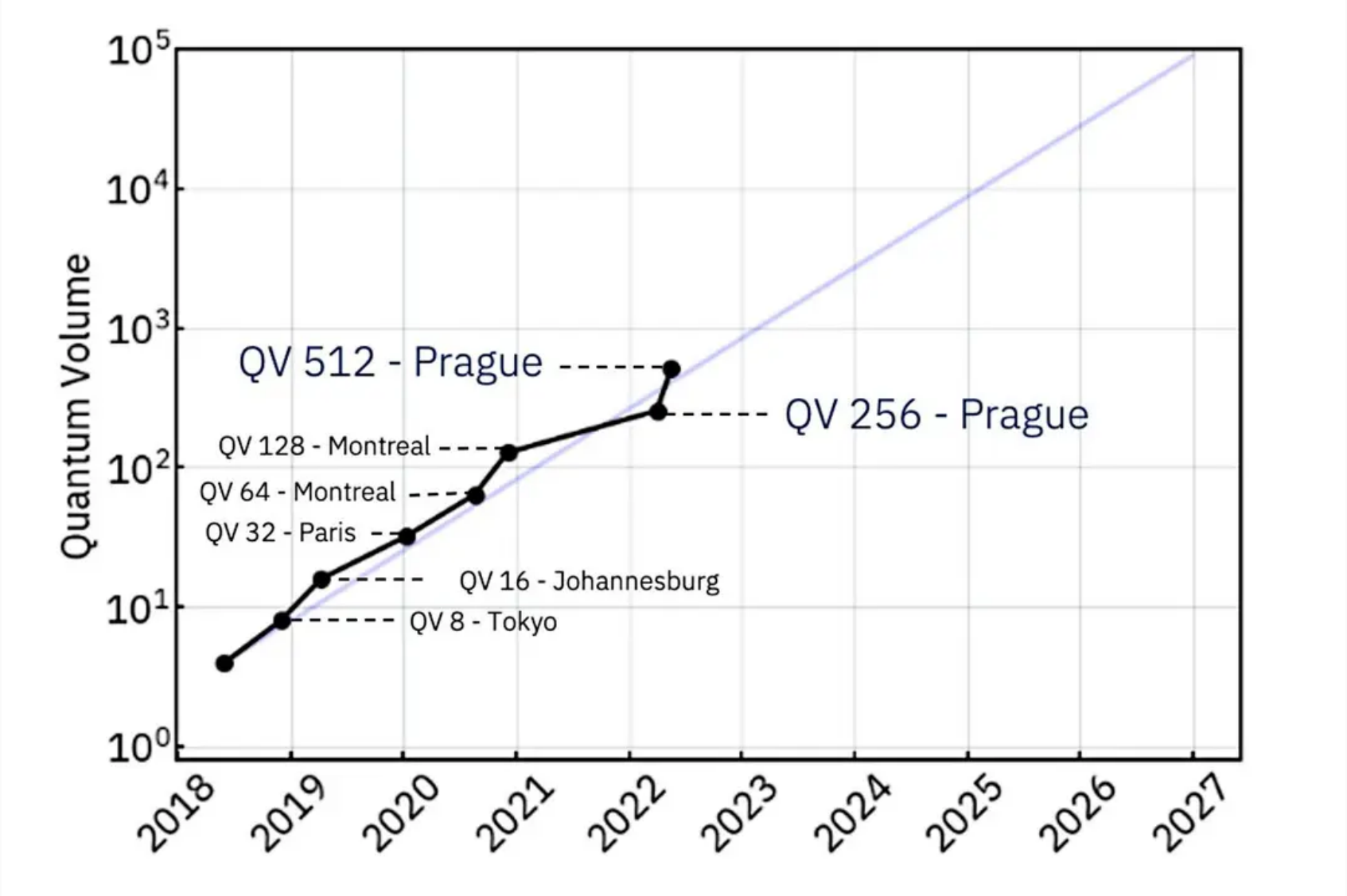
Зауваження

IBM: $\log_2 V_Q = arg \max_{n \leq N} \min n, \frac{1}{n\epsilon_{eff}}$

Квантовий об'єм

Дата	Квантовий об'єм	Виробник	Модель
01.2020	32 (5×5)	IBM	28 кубітів
06.2020	64 (6×6)	Honeywell	6 кубітів
08.2020	64 (6×6)	IBM	27 кубітів
11.2020	128 (7×7)	Honeywell	10 кубітів
12.2020	128 (7×7)	IBM	27 кубітів
03.2021	512 (9×9)	Honeywell	10 кубітів
07.2021	1024 (10x10)	Honeywell	10 кубітів
12.2021	2048 (11x11)	Quantinuum	12 кубітів
04.2022	256 (8×8)	IBM	27 кубітів
04.2022	4096 (12x12)	Quantinuum	12 кубітів
05.2022	512 (9×9)	IBM	27 кубітів
09.2022	8192 (13x13)	Quantinuum	20 кубітів
12.2022	1024 (13x13)	Quantinuum	20 кубітів

Квантовий об'єм



Квантові реалізації

Квантова реалізація шифру AES

M. Grassl, B. Langenberg, M. Roetteler, R. Steinwandt "Applying Grover's Algorithm to AES: Quantum Resource Estimates" // Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016. pp. 29-43. 2016

AES-128

	T-вентилі	Clifford	T вклад.	вклад.	кубіти
KeyGen	143 360	185 464	5 760	12 626	320
10 раундів	917 504	1 194 956	44 928	98 173	536
Всього	1 060 864	1 380 420	50 688	110 799	856+128

Квантова реалізація шифру AES

M. Grassl, B. Langenberg, M. Roetteler, R. Steinwandt "Applying Grover's Algorithm to AES: Quantum Resource Estimates" // Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016. pp. 29-43. 2016

AES-128

	T-вентилі	Clifford	T вклад.	вклад.	кубіти
KeyGen	143 360	185 464	5 760	12 626	320
10 раундів	917 504	1 194 956	44 928	98 173	536
Всього	1 060 864	1 380 420	50 688	110 799	856+128

AES-192

	T-вентилі	Clifford	T вклад.	вклад.	кубіти
KeyGen	114 688	148 776	4 608	10 107	256
12 раундів	1 089 536	1 418 520	39 744	86 849	664
Всього	1 204 224	1 567 296	44 352	96 956	920+192

Квантова реалізація шифру AES

AES-256

	T-вентилі	Clifford	T вклад.	вклад.	кубіти
KeyGen	186 368	240 699	7 488	16 408	416
14 раундів	1 318 912	1 715 400	52 416	114 521	664
Всього	1 505 280	1 956 099	59 904	130 929	1080+256

Квантова реалізація шифру AES

AES-256

	T-вентилі	Clifford	T вклад.	вклад.	кубіти
KeyGen	186 368	240 699	7 488	16 408	416
14 раундів	1 318 912	1 715 400	52 416	114 521	664
Всього	1 505 280	1 956 099	59 904	130 929	1080+256

Атака Гровера на шифр AES-k

k	T-вентилі	Clifford	T вклад.	вклад.	кубіти
128	$1.19 \cdot 2^{86}$	$1.55 \cdot 2^{86}$	$1.06 \cdot 2^{80}$	$1.16 \cdot 2^{81}$	2 953
192	$1.81 \cdot 2^{118}$	$1.17 \cdot 2^{119}$	$1.21 \cdot 2^{112}$	$1.33 \cdot 2^{113}$	4 449
256	$1.41 \cdot 2^{151}$	$1.83 \cdot 2^{151}$	$1.44 \cdot 2^{144}$	$1.57 \cdot 2^{145}$	6 681

Квантовий криптоаналіз

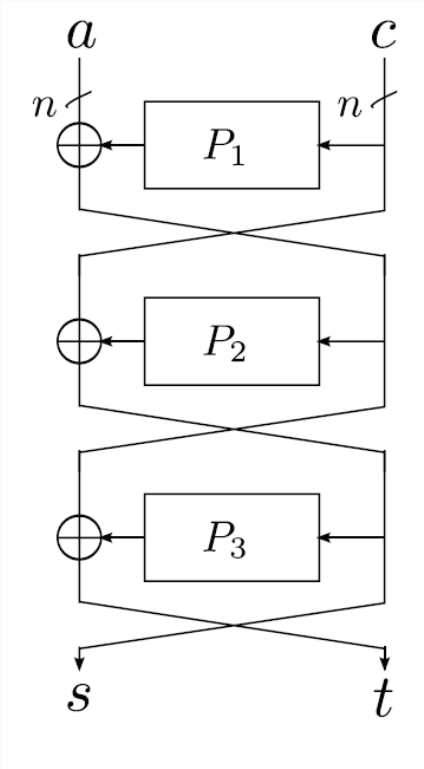
Квантовий аналіз шифру AES

X. Bonnetain, M. Naya-Plasencia, A. Schrottenloher "Quantum Security Analysis of AES" // Cryptology ePrint Archive, Report 2019/272

- побудована атака "Квадрат" з відновленням ключа на 6-раундовий шифр AES-128 та 7-раундові шифри AES-192 та AES-256
- побудована квантова атака Demirci-Selçuk MITM з відновленням ключа на 8-раундовий шифр AES-256

Аналіз 3-раундової схеми Фейстеля

H. Kuwakado, M. Morii "Quantum distinguisher between the 3-round Feistel cipher and the random permutation" // In Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on. pp. 2682-2685. - 2010



$a, c, s, t \in \{0,1\}^n$

$x = a||c$

$FP(x) = FP(a||c) =$

$c \oplus P_2(a \oplus P_1(c))||(a \oplus P_1(c)) \oplus$

$P_3(c \oplus P_2(a \oplus P_1(c))) = s||t$

RP — випадкова підстановка на $\{0,1\}^{2n}$

Необхідно розрізнити FP та RP без використання обернення

Аналіз 3-раундової схеми Фейстеля

Нехай $W\colon \{0,1\}^{2n} \to \{0,1\}^n$
$W(x) = W(a||c) = c \oplus P_2(a \oplus P_1(c))$

Аналіз 3-раундової схеми Фейстеля

Нехай $W\colon \{0,1\}^{2n} \to \{0,1\}^n$
$W(x) = W(a||c) = c \oplus P_2(a \oplus P_1(c))$

Нехай $f : \{0,1\}^{n+1} \to \{0,1\}^n$

$$f(b||a) = \begin{cases} W(a||\alpha) \oplus \beta & b = 0 \\ W(a||\beta) \oplus \alpha & b = 1 \end{cases}, \; b \in \{0,1\}, \; a, \alpha, \beta \in \{0,1\}^n$$

Твердження

$f(b||a) = f(b'||a') \Leftrightarrow b' = b \oplus 1$ і $a' = a \oplus z$, де $z = P_1(\alpha) \oplus P_1(\beta)$

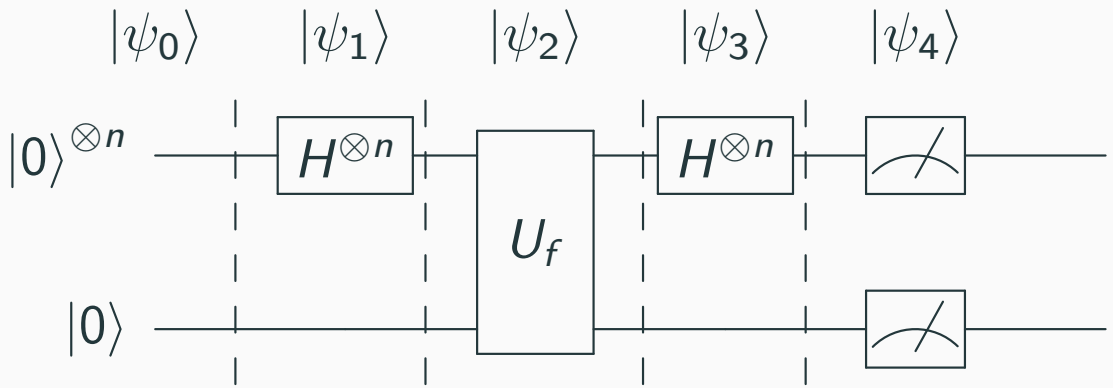
Наслідок

$f(b||a) = f((b||a) \oplus (1||z))$.
Функція f є періодичною

Алгоритм Саймона

Задача Саймона

Задана функція $f\colon \{0,1\}^n \to \{0,1\}^n$ за допомогою чорного ящика. Відомо, що $f(x) = f(y) \Leftrightarrow x \oplus y \in \{0, s\}$ для деякого фіксованого невідомого s. Знайти значення s.



T. Santoli, C. Schaffner "Using Simon's algorithm to attack symmetric-key cryptographic primitives" // Quantum Information and Computation. - Vol. 17. - Iss. 1-2. - 2017. - pp. 65-78.

M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia "Breaking symmetric cryptosystems using quantum period finding" // Proceedings (Part II) of CRYPTO 2016 (M. Robshaw, J. Katz, eds.), Springer, Heidelberg, LNCS. - Vol. 9815. - 2016. - pp. 207-237.

Нехай $\epsilon(f,s) = \max_{t \in \{0,1\}^n \setminus \{0,s\}} Pr_x[f(x) = f(x \oplus t)]$

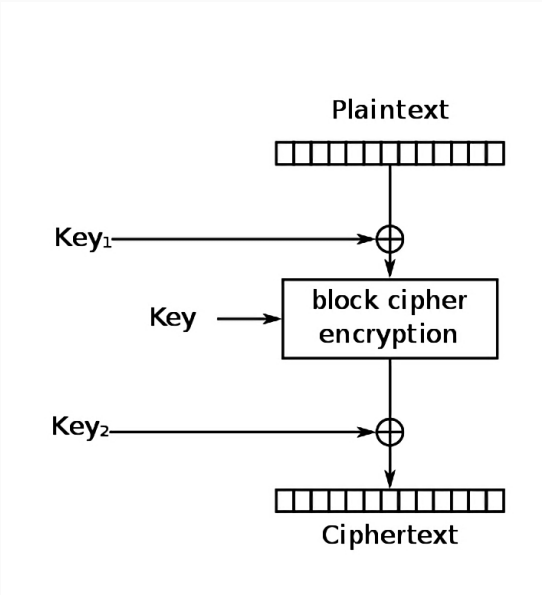
Теорема (Kaplan, Leurent, Leverrier, Naya-Plasencia)

Якщо $\epsilon(f,s) = p < 1$, тоді алгоритм Саймона обчислить значення s за cn стандартних квантових запитів з ймовірністю не менше ніж $1 - (2(\frac{1+p}{2})^c)^n$.

Схема Івена-Мансура

$E(x, k_1, k_2, k_3) = k_1 \oplus S_{k_2}(x \oplus k_3)$

$E(x, k_1, k_2) = k_1 \oplus S(x \oplus k_2)$



$f\colon \{0,1\}^n \to \{0,1\}^n$

$f(x) = E(x, k_1, k_2) \oplus S(x) =$

$= S(x \oplus k_1) \oplus S(x) \oplus k_2$

$f(x) = f(x \oplus k_1)$

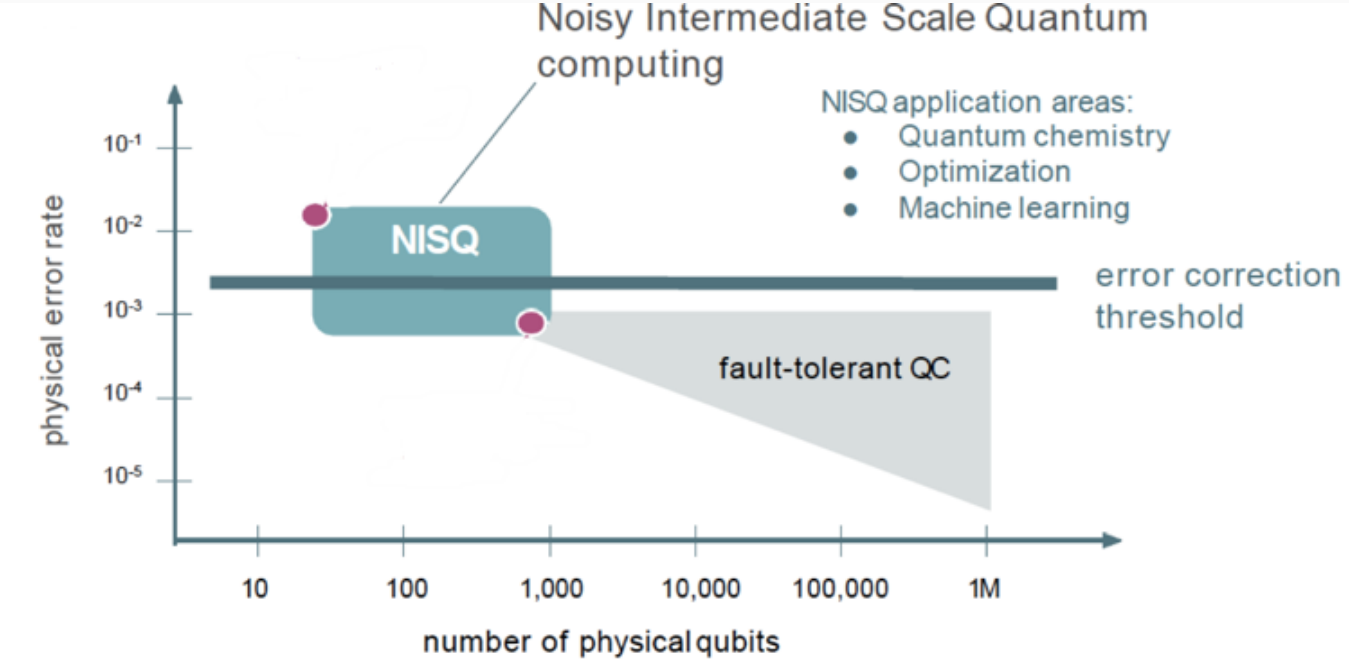
- $\epsilon(f, s) < \frac{1}{2}$ — алгоритм Саймона
- $\epsilon(f, s) \geq \frac{1}{2}$ — атака розрізнення в класичній моделі обчислень

  $t \neq s,\ t \neq 0$

  $Pr[\ S(x) \oplus S(x \oplus s) \oplus$

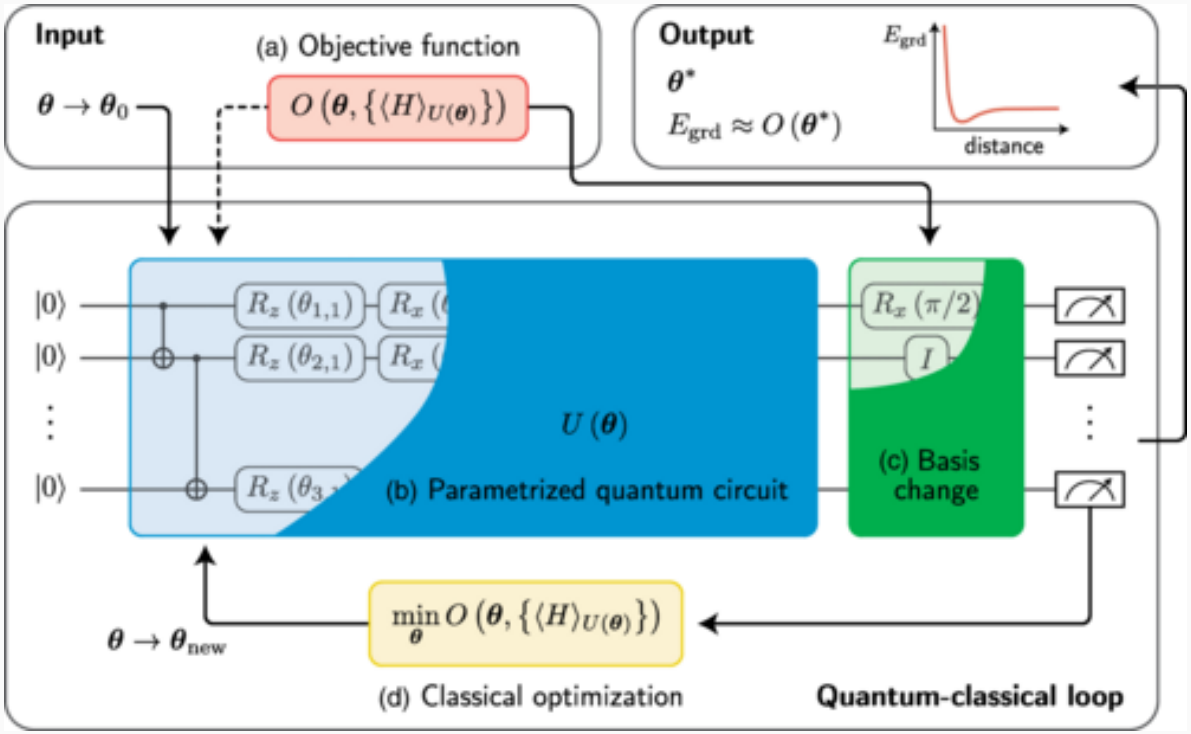
  $\oplus S(x \oplus t) \oplus S(x \oplus s \oplus t) = 0\ ] > \frac{1}{2}$

Епоха NISQ

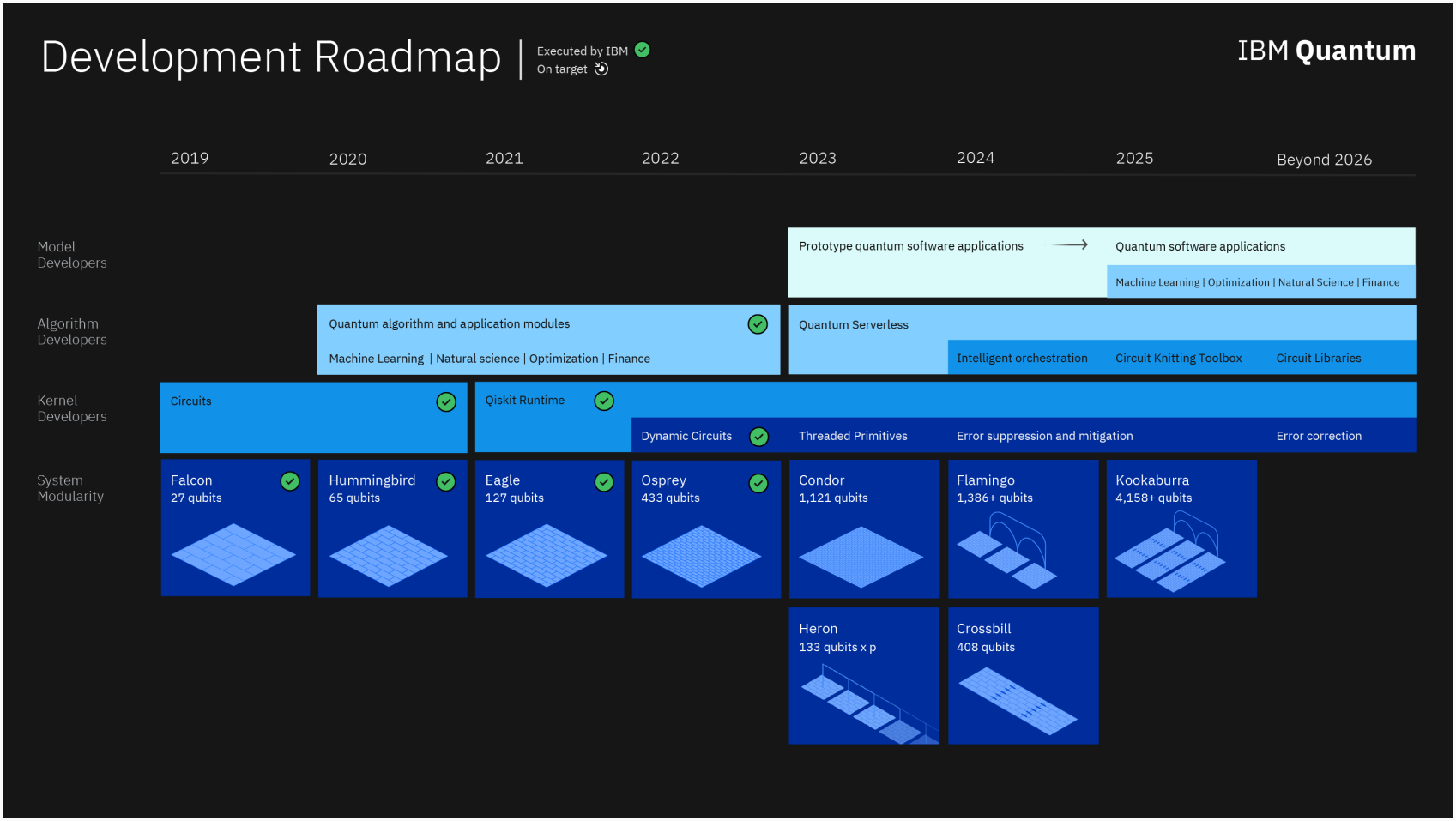

Noisy Intermediate Scale Quantum computing
NISQ application areas:
Quantum chemistry
Optimization
Machine learning
NISQ
error correction threshold
fault-tolerant QC
physical error rate
10-1
10-2
10-3
10-4
10-5
10
100
1,000
10,000
100,000
1M
number of physical qubits

Алгоритми епохи NISQ

- варіаційний квантовий власний розв'язувач (variational quantum eigensolver або VQE)
- алгоритм квантової наближеної оптимізації (quantum approximate optimization algorithm або QAOA)



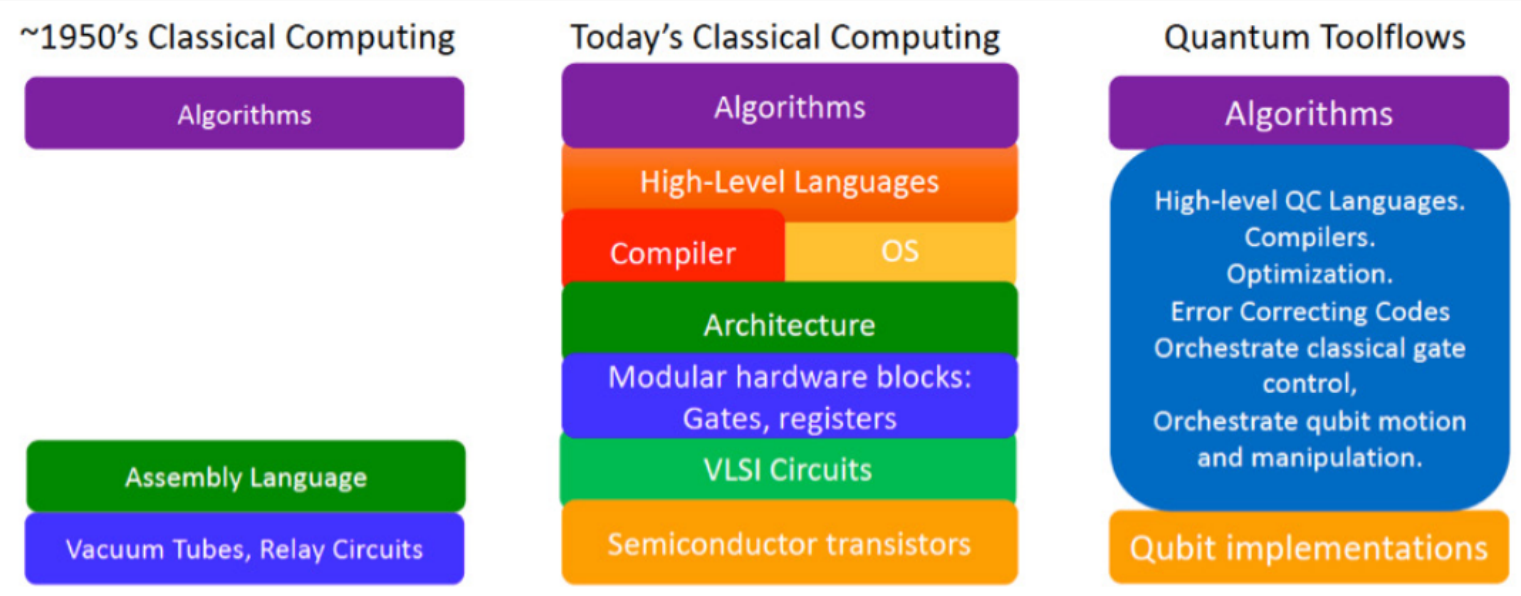
План розвитку IBM



Області досліджень

- оптимізація і реалізація схем
- використання Q#, Qiskit, ...
- алгоритми та протоколи
- схеми корекції помилок
- адаптація алгоритмів
- навчальний процес

- реалізація примітивів
- аналіз стійкості (Гровер-Саймон, Брасар)
- алгебраїчні властивості
- постквантові примітиви і протоколи



Дякую за увагу!