КВАНТОВА ИНФОРМАТИКА, ЛЕКЦИЯ 11 / 22.12.2021

КОРЕКЦИИТЕ И ДОПЪЛНЕНИЯТА СПРЯМО ПРЕДХОДНАТА ВЕРСИЯ СА ПОСТАВЕНИ В ЛИЛАВ ЦВЯТ - ТЕ СА НА СТР. 2, 3 и 4

Алгоритъм за търсене на Grover

(ВИЖ СЪЩО: http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/NC2010.pdf
***Nielsen M.A., Chuang_I.L., Quantum Computation and Quantum Information, 10th Anniversary Edition*т. 6.1 / СТР. 248-256)**

Вход на алгоритъма: функция $f:\{0,\dots,N-1\}\to\{0,1\}$ $(N=2^n)$
Изход на алгоритъма: решение $l\in\{0,\dots,N-1\}$ на условието $f(l)=1$

В случаи когато сложността на f ("изчислителното време") има асимптотичен ръст на порядъка от $n=\log N$, тогава намирането на решение на $f(l)=1$ може да изисква до $N=2^n$ - проверки. Квантовия алгоритъм ускорява това до изчислително време $\sim\sqrt{N}=2^{n/2}$.

Например, нека L е n-битово двоично число, т.е., $\frac{N}{2}<L<N$ и

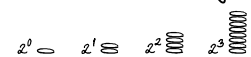
$$f(l)\,(:=f_L(l))=\begin{cases}1 & \text{ако } l \text{ дели } L\\ 0 & \text{ако } l \text{ не дели } L\end{cases}$$

Тогава намирането на решение l на $f(l)=1$ е $\Longleftrightarrow$ намиране на делител l на L.

За делене на n-битови числа сложността ("изчислителното време") варира при известните алгоритми между между $O(n\log n)$ и $O(n^2)$

Последователното тестване изисква $\sim N=2^n$ проби (за проблема за факторизация има и по-бързи класически алгоритми, но осново с експоненциален ръст).

Илюстрация на бързия ръст на експонентата: редене на оризови зърна върху шахматна дъска с удвояване на всяка стъпка: 2^n зърна на n-то поле.



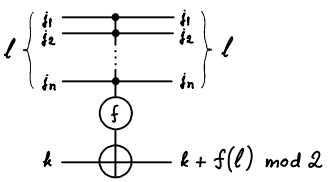
Ако приемем, че всяко зърно е ~ 1мм широко, то колоната на n-тото поле ще бъде

n	дължина
10	2^{10} мм $>$ 1м.
20	2^{20} мм $>$ 1км.
36	2^{36} мм $>$ обиколката на Земята
64	2^{64} мм $>$ 1 светлинна година
+40	2^{104} мм $>$ размера на видимата вселена

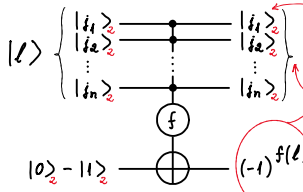
Изпсквания за постигане на по-добра ефикасност

ако $M:=\#\{l\mid f(l)=1\}$, то трябва $M\ll N$.

Функцията f е вградена в класическия гейт:



Приложен върху кубити :



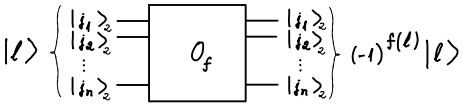
$|i_j\rangle_2 \in \mathbb{C}^2$, $j \in \{0,1\}$

$|l\rangle \in \mathbb{C}^N$, $l \in \{0, \dots, N-1\}$

понеже е в тензорно произведение

$$|l\rangle \otimes (-1)^{f(l)} (|0\rangle_2 - |1\rangle_2) = (-1)^{f(l)} |l\rangle \otimes (|0\rangle_2 - |1\rangle_2)$$

получаване гейт



Геометрична интерпретация : нека въведем векторите $\Psi' := \sum_{l=0}^{N-1} |l\rangle$

$$\Psi'_{(0)} := \sum_{f(l)=0} |l\rangle \,, \quad \Psi'_{(1)} := \sum_{f(l)=1} |l\rangle \,, \quad \Psi' = \Psi'_{(0)} + \Psi'_{(1)} \,, \quad \Psi'_{(0)} \perp \Psi'_{(1)} \,,$$

но тези вектори не са нормирани : $\|\Psi'\|^2 = \sum_{l=0}^{N-1} \underbrace{\||l\rangle\|^2}_{1} = N$ ← ортонормиран базис

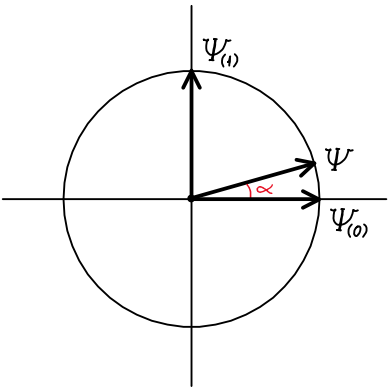
$$\Rightarrow \|\Psi'\| = \sqrt{N} \equiv 2^{\frac{n}{2}} \,. \qquad \Rightarrow \Psi := \frac{1}{\|\Psi'\|} \Psi' = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} |l\rangle \text{ е единичен}$$

Аналогично : $\|\Psi'_{(1)}\| = \sqrt{M}$, $\|\Psi'_{(0)}\| = \sqrt{N-M}$.

$$\Psi_{(0)} := \frac{1}{\sqrt{N-M}} \sum_{f(l)=0} |l\rangle \,, \quad \Psi_{(1)} := \frac{1}{\sqrt{M}} \sum_{f(l)=1} |l\rangle \text{ - единични вектори}$$

$$\Rightarrow \Psi = \underbrace{\frac{\sqrt{N-M}}{\sqrt{N}}}_{=: \cos\alpha} \Psi_{(0)} + \underbrace{\frac{\sqrt{M}}{\sqrt{N}}}_{=: \sin\alpha} \Psi_{(1)}$$

$$\equiv \cos\alpha \, \Psi_{(0)} + \sin\alpha \, \Psi_{(1)}$$



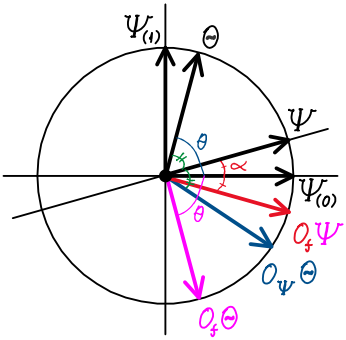
Твърдим, че O_f преобразува векторите $\Theta := \cos\theta\,\Psi_{(0)} + \sin\theta\,\Psi_{(1)}$, като отражение:

$$O_f\Theta = \cos\theta\,\underbrace{O_f\Psi_{(0)}}_{(-1)^0\Psi_{(0)}} + \sin\theta\,\underbrace{O_f\Psi_{(1)}}_{(-1)^1\Psi_{(1)}} = \cos\theta\,\Psi_{(0)} - \sin\theta\,\Psi_{(1)}$$

(отражение спрямо $\Psi_{(1)}$)

Въвеждаме втори гейт: $O_\Psi :=$ отражение спрямо Ψ:

$$O_\Psi\Theta = \cos(2\alpha-\theta)\,\Psi_{(0)} + \sin(2\alpha-\theta)\,\Psi_{(1)}$$



Полагаме: гейт на Гровер:

$$G := O_\Psi O_f = \text{ротация на ъгъл } 2\alpha:$$

$$G\Theta = \cos(\theta+2\alpha)\,\Psi_{(0)} + \sin(\theta+2\alpha)\,\Psi_{(1)}$$

Стратегия: **искаме $G^{N'}\Psi$ да е близо до $\pm\Psi_{(1)}$**

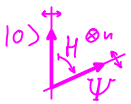
нека $2N' \approx \frac{\pi}{2\alpha}$, $G^{N'}\Psi = \cos\underbrace{(2N'+1)\alpha}_{\approx\frac{\pi}{2}}\Psi_{(0)} + \sin(2N'+1)\alpha\,\Psi_{(1)}$

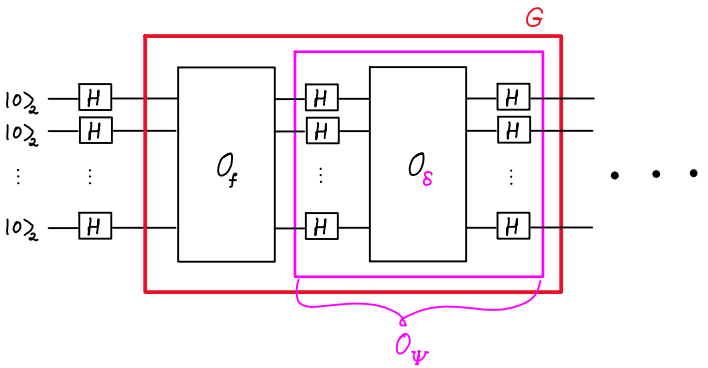
$$\alpha = \arcsin\sqrt{\frac{M}{N}} \approx \sqrt{\frac{M}{N}}, \quad N' \sim \sqrt{N}$$

Реализация $|0\rangle = |0,\dots,0\rangle \mapsto H^{\otimes n}|0\rangle = \Psi$

Оскан това: O_δ е отражение спрямо $|0\rangle$. Затова $H^{\otimes n} O_\delta H^{\otimes n} = O_\Psi$

$\delta(\ell) = \begin{cases} 0, & \ell = 0 \\ 1, & \ell \neq 0 \end{cases}$





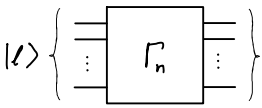
https://en.m.wikipedia.org/wiki/RSA_Factoring_Challenge

Преработена версия на онлайн-записките

2. Дискусия по понятието за квантов алгоритъм

а) Досегашното определение се базира на редица от квантови вериги (circuits)

$\{\Gamma_n\}_{n=1}^{\infty}$, n = # битове



, измерване → дава резултат l'

с вероятност $|\langle l'|\Gamma_n|l\rangle|^2$

Например, при проблема за факторизация

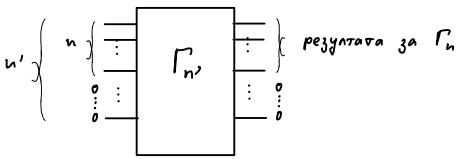
$L = PQ$ ⟼ P' – проверяваме

P Q – прости множители

Γ_n

В квантовия случай изчислителното време е нужно за постигане на верен резултат с вероятност близка до (клоняща към) 1.

б) Необходимо е, ако увеличим броя на битовете $n' > n$ да имаме съгласуваност:



-такива редици от вериги се наричат съгласувани

= uniform circuit family

в) Нужно е редицата $\{\Gamma_n\}_{n=1}^{\infty}$ от съгласувани (квантови) вериги да е породена алгоритмично (в класически смисъл).

г) Моделът на изчисления с логически вериги в класическия случай:

Илюстративни източници (аритметични цифрови вериги и анализ на тяхната сложност):

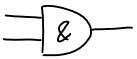
https://www.tutorialspoint.com/digital_circuits/digital_arithmetic_circuits.htm

http://www.engr.siu.edu/haibo/ece428/notes/ece428_arith.pdf

https://www.cs.tau.ac.il/~shpilka/publications/SY10.pdf

Наблюдението: в класическите вериги се използват операции (гейтове), които квантово са забранени:

 - дублиране / копиране / "клониране"

и необратими операции (гейтове)  (2 бита $\mapsto$ 1 бит)

 проблемът за обратими изчисления

https://en.wikipedia.org/wiki/Reversible_computing

[2017-Mo] Theory of reversible computing, by Juraj Morita
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2017-Mo.pdf

[2010-dV] Reversible Computing Fundamentals, Quantum Computing, and Applications, by Alexis De Vos
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2010-dV.pdf

[2020-Pr] Reversible Computation 12th International Conference, RC 2020, Oslo, Norway, July 9-10
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2020-Pr.pdf

[2019-Pr] Reversible Computation 11th International Conference, RC 2019, Lausanne, Switzerland, June 24–25
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2019-Pr.pdf

[2018-Pr] Reversible Computation 10th International Conference, RC 2018, Leicester, UK, September 12-14
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2018-Pr.pdf

[2017-Pr] Reversible Computation 9th International Conference, RC 2017, Kolkata, India, July 6-7
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2017-Pr.pdf

[2016-Pr] Reversible Computation 8th International Conference, RC 2016, Bologna, Italy, July 7-8
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2016-Pr.pdf

[2015-Pr] Reversible Computation 7th International Conference, RC 2015, Grenoble, France, July 16-17
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2015-Pr.pdf

[2014-Pr] Reversible Computation 6th International Conference, RC 2014, Kyoto, Japan, July 10-11
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2014-Pr.pdf

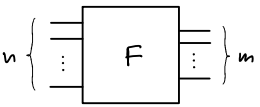
[2013-Pr] Reversible Computation 5th International Conference, RC 2013, Victoria, BC, Canada, July 4-5
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2013-Pr.pdf

[2012-Pr] Reversible Computation 4th International Workshop, RC 2012, Copenhagen, Denmark, July 2-3
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2012-Pr.pdf

[2011-Pr] Reversible Computation 3d International Workshop, RC 2011, Gent, Belgium, July 4-5
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2011-Pr.pdf

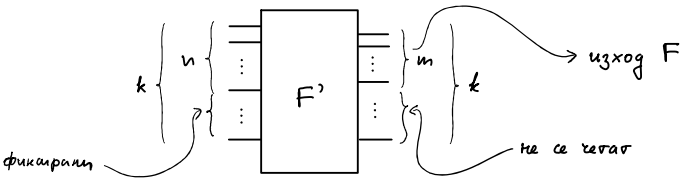
[2020-Re] Reversible Computation-Extending Horizons of Computing, Selected Results of the COST Action IC1405
http://theo.inrne.bas.bg/~mitov/qi21/notes_df34g2tb3/2020-Re.pdf

Проблем: дадена логическа верига :



$$F: \{0,\dots,N-1\} \to \{0,\dots,M-1\}, \quad N = 2^n, \quad M = 2^m$$

да се реализира (вложи) във верига на обратима функция



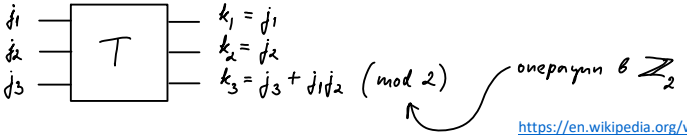
$$F': \{0,\dots,K-1\} \to \{0,\dots,K-1\}, \quad K = 2^k$$

обратима

F' може да се конструира от един елементарен, обратим, класически гейт

https://en.wikipedia.org/wiki/Toffoli_gate

- гейт на Тофоли



https://en.wikipedia.org/wiki/GF%282%29

Обратимост: $j_1 = k_1$
$j_2 = k_2$
$j_3 = k_3 + k_1 k_2$

Забележка: обратимото изображение на бинарни гейтове

$$\{0,1,2,3\} \longleftrightarrow \{0,1,2,3\}$$

- общо $4! = 24$

- всички те са линейни спрямо аритметиката в $\mathbb{Z}_2$

3. Преглед на понятието за класическо изчисление и алгоритъм и възможните му пренасяния в квантовия случай

https://plato.stanford.edu/entries/turing-machine/

https://en.wikipedia.org/wiki/Turing_machine

https://encyclopediaofmath.org/wiki/Quantum_Turing_machine

https://royalsocietypublishing.org/doi/pdf/10.1098/rspa.2018.0767

Понятието за квантова машина на Тюринг

f: (tape symbol, head state) $\longmapsto$ (tape symbol, head state, direction)

↓ квантово пренасяне

амплитуди на вероятности за преход

↳ transition matrix

https://en.wikipedia.org/wiki/Computational_complexity_of_mathematical_operations