Алгоритъм за търсене на Гровер / Grover, Николай М. Николов

1. Цел

Дадена е функция $f: \{0, 1, \ldots, \underbrace{2^n - 1}_{N}\} \to \{0, 1\}$, за която знаем, че има само едно решение $X \in$, такова че $f(X) = 1$

Това решение ще означим с $Z := X$

т.е. $$f(X) = \begin{cases} 0 & \text{при } X \neq Z \\ 1 & \text{при } X = Z \end{cases} \quad (\text{за } X \in \{0, 1, \ldots, 2^n - 1\})$$

Търсим $Z = ?$

Считаме, че $N \gg 1$.

Считаме също, че "проверовъчната функция" f се изчислява "бързо", т.е., за време $t = t(n)$, което има ръст на полином от n при $n \to \infty$.

Например Нека е дадено $A = YZ$ за две неизвестни прости числа $Y < Z$.
Търсим по-големия делител Z.
Проверовъчната функция е $$f(X) = \begin{cases} 0 & \text{ако } X \text{ не дели } A \\ 1 & \text{ако } X \text{ дели } A \text{ и } X^2 > A. \end{cases}$$

Деленето и вдигането на квадрат са "бързи" операции.

За повече подробности относно "бързината":

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

2. Класическа ефективност

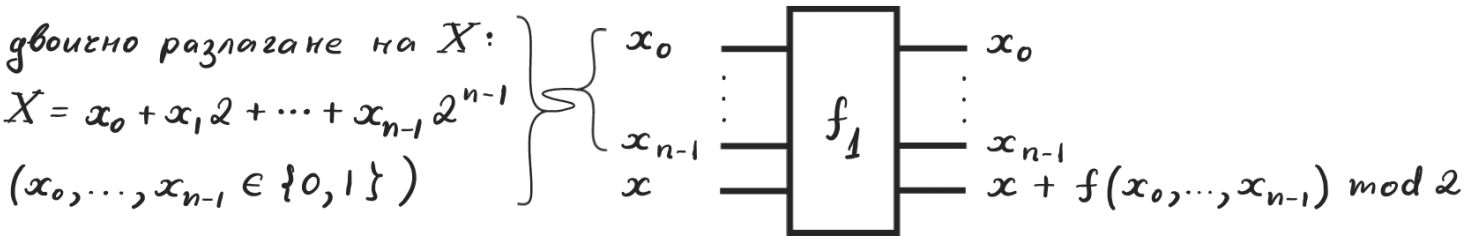
Ако f е произволна, неизвестна, то ни остава единствено да пробваме
$f(0) = ?$, $f(1) = ?$, $f(2) = ?$, ...
Следователно, времето за търсене е от порядъка на $N = 2^n$
- полиномиален ръст.

Квантовата ефективност, която ще постигнем е $\sqrt{N}$ - квадратично ускорено, но все още с експоненциален ръст.

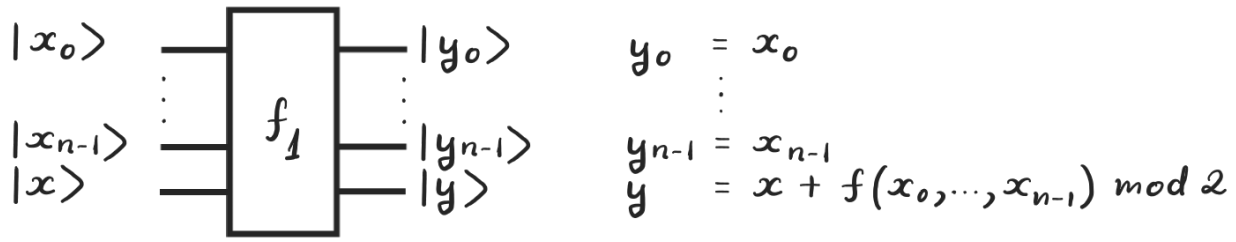
3. Квантова имплементация (внедряване) на f

Да разгледаме съответствието $(X, x) \mapsto (X, x + f(X) \bmod 2)$ за $X \in \{0, 1, \ldots, 2^n - 1\}$, $x \in \{0, 1\}$. То $\uparrow$ е обратимо (биекция е) и обратното съответствие съвпада с него.

Считаме, че имаме класическа булева верига, построена с обратими класически гейтове, която реализира това съответствие:

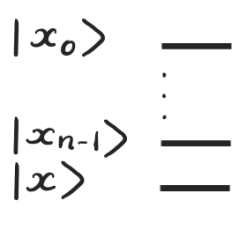


Знаем, че всяка обратима класическа верига се пренася като квантова, като класическото действие се пренесе в действие върху изчислителния базис:



Напомняме, че $|x\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ при $x = 0$ и $|x\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ при $x = 1$ е изчислителния базис на кубит.

Напомняме, че означението



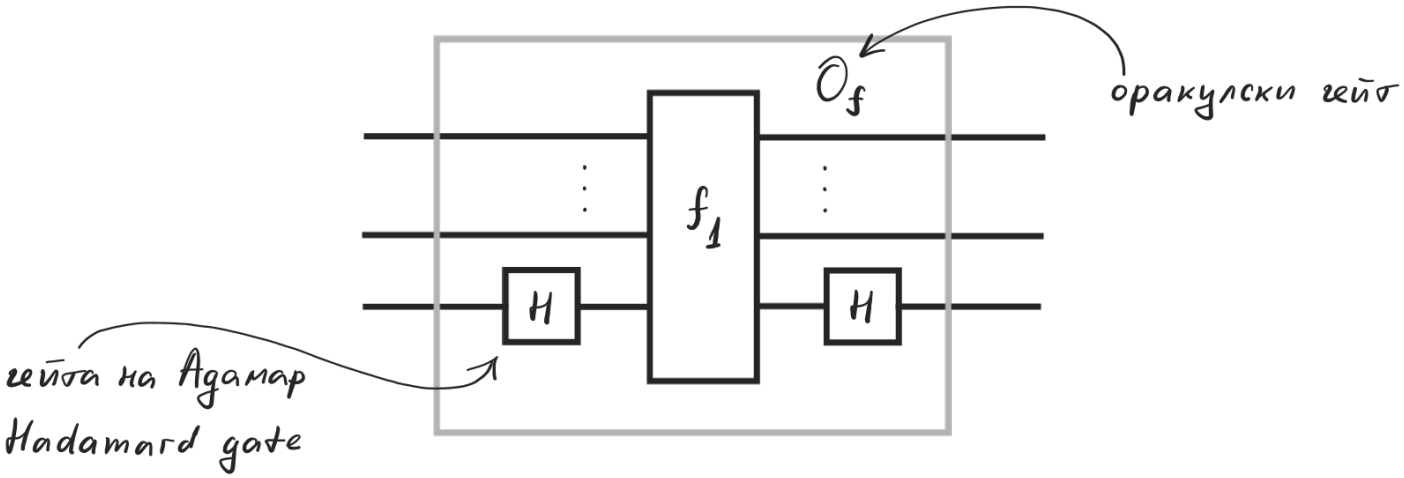
е израз на тензорно произведение:

$$|x_0\rangle \otimes \cdots \otimes |x_{n-1}\rangle \otimes |x\rangle$$

произведение на Кронекер / Kronecker

http://theo.inrne.bas.bg/~mitov/qi23_yJ4Gmi891z/NMN-QI23-08_compact-slides_v1.pdf слайдове8 11 и 49-63
https://en.m.wikipedia.org/wiki/Kronecker_product

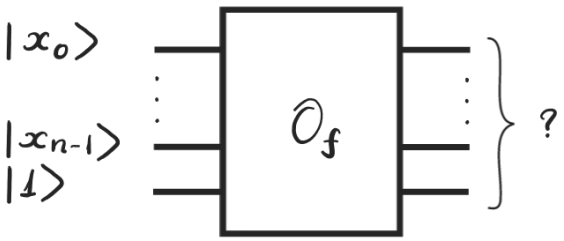
Следваща стъпка от квантовата имплементация на f е следната композиция

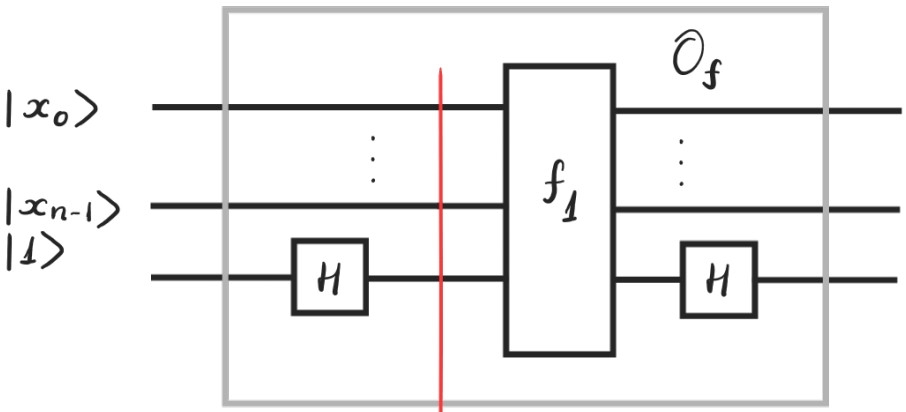


Напомняме действието на H:

$$|0\rangle \xrightarrow{H} 2^{-1/2}(|0\rangle + |1\rangle)$$
$$|1\rangle \xrightarrow{H} 2^{-1/2}(|0\rangle - |1\rangle)$$

Да пресметнем:





$|x_0\rangle$
$\otimes\ |x_{n-1}\rangle$
$\otimes\ (2^{-1/2}|0\rangle - 2^{-1/2}|1\rangle)$

линейна комбинация

$2^{-1/2}$ { $|x_0\rangle$, $\otimes\ |x_{n-1}\rangle$, $\otimes\ |0\rangle$ } → f_1 → { $|x_0\rangle$, $\otimes\ |x_{n-1}\rangle$, $\otimes\ |f(X)\rangle$ }

$-$

$2^{-1/2}$ { $|x_0\rangle$, $\otimes\ |x_{n-1}\rangle$, $\otimes\ |1\rangle$ } → f_1 → { $|x_0\rangle$, $\otimes\ |x_{n-1}\rangle$, $\otimes\ |$"не"$f(X)\rangle$ }

Следователно, след f_1 преминава линейната комбинация

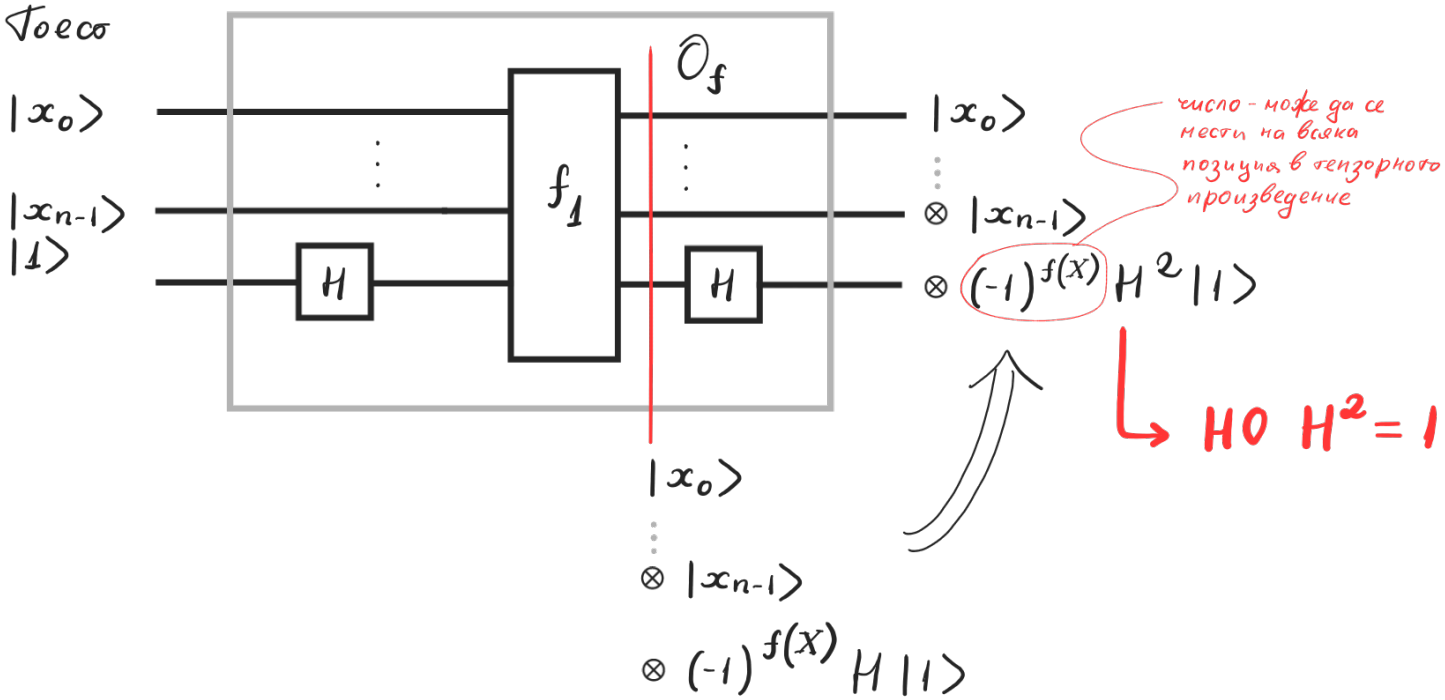
$$2^{-1/2}\,|x_0\rangle \otimes \cdots \otimes |x_{n-1}\rangle \otimes |f(X)\rangle - 2^{-1/2}\,|x_0\rangle \otimes \cdots \otimes |x_{n-1}\rangle \otimes |\text{"не"}\,f(X)\rangle$$

$$= |x_0\rangle \otimes \cdots \otimes |x_{n-1}\rangle \otimes \left(2^{-1/2}\,|f(X)\rangle - 2^{-1/2}\,|\text{"не"}\,f(X)\rangle\right)$$

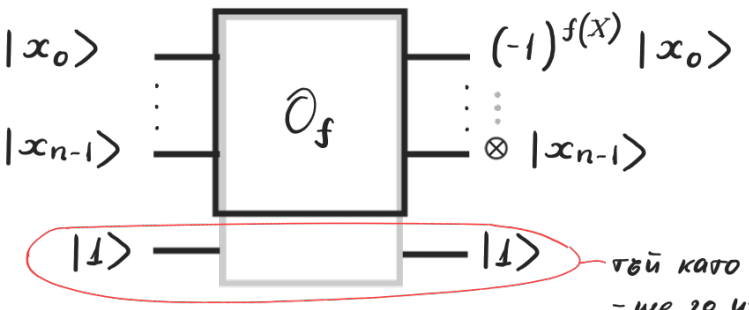
$$= \left\{ \begin{array}{ll} 2^{-1/2}|0\rangle - 2^{-1/2}|1\rangle & \text{при } f(X)=0 \\ 2^{-1/2}|1\rangle - 2^{-1/2}|0\rangle & \text{при } f(X)=1 \end{array} \right\} = (-1)^{f(X)}\left(2^{-1/2}|0\rangle - 2^{-1/2}|1\rangle\right)$$

$$= (-1)^{f(X)} H\,|1\rangle$$

Тоест

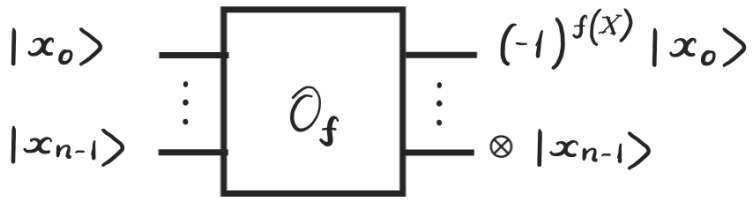


И така



тъй като не става промяна - ще го изпускаме

Резултатът: квантовата имплементация на проверовъчната функция $f(X)$ в алгоритъма на Гровер се осъществява от гейта



Забележете, че получения гейт е квантов, понеже генерирането на фазов множител $(-1)^{f(X)}$ не е класическа операция.

4. Общ сценарий на алгоритъма на Гровер

Алгоритъмът оперира върху "равномерната суперпозиция" на изчислителния базис, т.е., върху вектора

$$\Psi := 2^{-n/2} \sum_{X=0}^{2^n-1} |X\rangle$$

Това е единичен вектор $\left(\|\Psi\|^2 = 1 \right)$ с еднакви координати $2^{-n/2}$.

Да въведем следни два единични и взаимно перпендикулярни вектора:

$$|Solution\rangle := |Z\rangle$$

$$|NonSolution\rangle := \frac{1}{\sqrt{2^n-1}} \sum_{\substack{X=0 \\ X \neq Z}}^{2^n-1} |X\rangle$$

този множител докарва нормата до 1

защо е единичен? Защото тук има 2^n-1 взаимно ортогонални единични вектора. $\Rightarrow$ нормата^2 на $\sum_{X \neq Z}$ е 2^n-1.

Забележете:

$$\Psi = \underbrace{\frac{1}{\sqrt{2^n}}}_{=: \sin\theta} |Solution\rangle + \underbrace{\frac{\sqrt{2^n-1}}{\sqrt{2^n}}}_{\cos\theta} |NonSolution\rangle$$

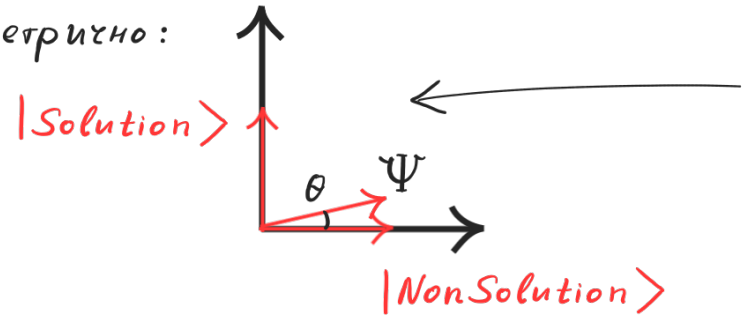
Наистина:

$$\Psi := 2^{-n/2} \sum_{X=0}^{2^n-1} |X\rangle = \frac{1}{\sqrt{2^n}} \left(|Z\rangle + \sum_{X \neq Z} |X\rangle \right)$$

$|Solution\rangle$

$\sqrt{2^n - 1}\ |NonSolution\rangle$

Геометрично:



По-нататък, действието се развива в тази равнина.

Върху вектора Ψ се прилага специално конструиран гейт G, наречен гейт на Гровер, който в горната равнина действа като въртене на ъгъл 2θ. Тоест, в горния ортонормиран базис $|NonSolution\rangle$, $|Solution\rangle$ G има матрица

$$G = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$$

Забележете $\begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix} \begin{pmatrix} \cos \varphi \\ \sin \varphi \end{pmatrix} = \begin{pmatrix} \cos(\varphi + 2\theta) \\ \sin(\varphi + 2\theta) \end{pmatrix}$ - проверете!

Следователно:

$$G^k \Psi = \sin(2k+1)\theta\ |Solution\rangle + \cos(2k+1)\theta\ |NonSolution\rangle$$

Защо?

Нека k е такова, че $(2k+1)\theta \approx \frac{\pi}{2}$, т.е., $k :=$ цялата част на $\frac{\pi}{4\theta} - \frac{1}{2}$

Тогава, след k-кратно прилагане на G ще получим $G^k \Psi \approx |Solution\rangle$ и ако тогава направим измерване, то с вероятност близка до 1 ще получим $|Z\rangle$, т.е., на изходните регистри ще измерим битовете на решението Z.

5. Начало на алгоритъма на Гровер : получаване на състоянието с вектор

$$\Psi := 2^{-n/2} \sum_{X=0}^{2^n-1} |X\rangle$$

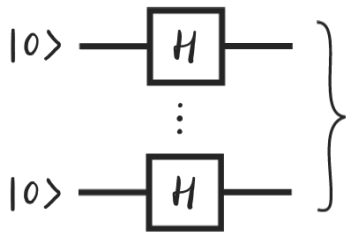
Тук прилагаме трика : $(H \otimes \cdots \otimes H)(|0\rangle \otimes \cdots \otimes |0\rangle) = \Psi$

$H^{\otimes n}$ $|0\rangle^{\otimes n}$

Виж :

http://theo.inrne.bas.bg/~mitov/qi23_yJ4Gmi891z/NMN-QI23-12_compact-slides_v01.pdf слайдове 12-15

Схематично :



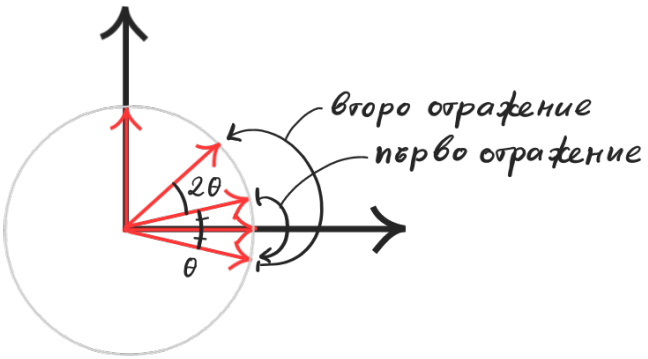
$$\Psi := 2^{-n/2} \sum_{X=0}^{2^n-1} |X\rangle$$

6. Реализация на гейта на Гровер.

а) Обща стратегия

Гейта на Гровер G трябва да действа като ротация на ъгъл 2θ в равнината разпъната от $|NonSolution\rangle$, $|Solution\rangle$

Ще използване идеята от геометрията , че последователното прилагане на две отражения в равнината е равносилно на определена ротация



Първото отражение е O_f (действието на оракула).

Това е отражение спрямо $|NonSolution\rangle$:

наистина: $O_f |Solution\rangle = (-1)^1 |Solution\rangle = -|Solution\rangle$

$O_f |NonSolution\rangle = (-1)^0 |NonSolution\rangle = +|NonSolution\rangle$

Второто отражение ще бъде спрямо вектора Ψ.

За да обясним как се конструира то с гейтове ще дадем допълнително пояснение.

б) Конструиране на отражения - формула на Хаусхолдер (Hausholder)

Нека Φ е произволен единичен вектор в Хилбертово пространство.

Припомняме, че $|\Phi\rangle\langle\Phi|$ е ортогонален проектор върху Φ

- наистина, за произволен вектор χ имаме

$$|\Phi\rangle\langle\Phi| \cdot |\chi\rangle = \langle\Phi|\chi\rangle |\Phi\rangle = \begin{cases} |\Phi\rangle \equiv \Phi & \text{ако } \chi = \Phi \\ 0 & \text{ако } \chi \perp \Phi \end{cases}$$

(виж също: http://theo.inrne.bas.bg/~mitov/qi23_yJ4Gmi891z/NMN_QI23_04_WB_notes_v1.pdf стр. 4-5)

Тогава матрицата $\overbrace{\hat{1} - 2|\Phi\rangle\langle\Phi|}^{\text{формула на Хаусхолдер}}$ задава отражение спрямо подпространството, което е $\perp$ на Φ.

Наистина:

$$\left(\hat{1} - 2|\Phi\rangle\langle\Phi|\right)\chi = \begin{cases} -\chi \text{ ако } \chi = \Phi \\ +\chi \text{ ако } \chi \perp \Phi \end{cases}$$

в) Конструиране на второто отражение

Съгласно б), матрицата $-\left(\hat{1} - 2|\Psi\rangle\langle\Psi|\right) = 2|\Psi\rangle\langle\Psi| - \hat{1}$.

ще извършва отражение спрямо Ψ.

Съгласно т. 5 : $H^{\otimes n}|0\rangle^{\otimes n} = \Psi$ и $|\Psi\rangle = (\Psi)^* = \left(H^{\otimes n}|0\rangle^{\otimes n}\right)^*$

$= \langle 0|^{\otimes n} H^{\otimes n}$

понеже $|0\rangle^* = \langle 0|$ и $H^* = H$ (H е едновременно унитарна и ермитова)

Тогава $2|\Psi\rangle\langle\Psi| - \hat{1} = 2H^{\otimes n}\underbrace{|0\rangle_{2^n}\langle 0|_{2^n}}_{|0\rangle^{\otimes n}} H^{\otimes n} - \underbrace{H^{\otimes n} H^{\otimes n}}_{\hat{1}}$

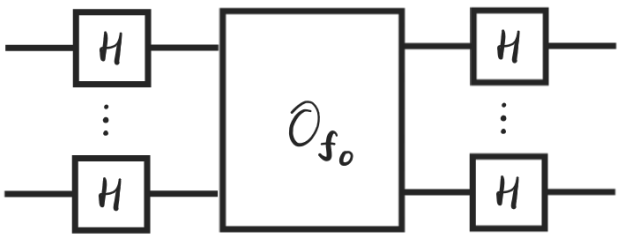
понеже $H^2 = 1$

Тоест : $2|\Psi\rangle\langle\Psi| - \hat{1} = H^{\otimes n}\underbrace{\left(2|0\rangle\langle 0| - 1\right)}_{\text{отражение спрямо } |0\rangle_{2^n} = |0\rangle^{\otimes n}} H^{\otimes n}$

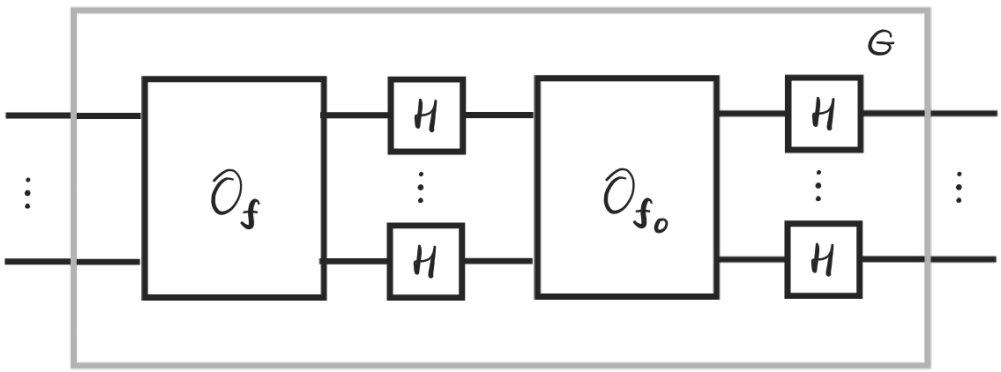
Но тогава това е оракул $\mathcal{O}_{f_0}$ за простата проверовъчна функция :

$$f_0(X) = \begin{cases} 0 & \text{при } X \neq 0 \\ 1 & \text{при } X = 0 \end{cases} \quad (\text{за } X \in \{0, 1, \ldots, 2^n - 1\})$$

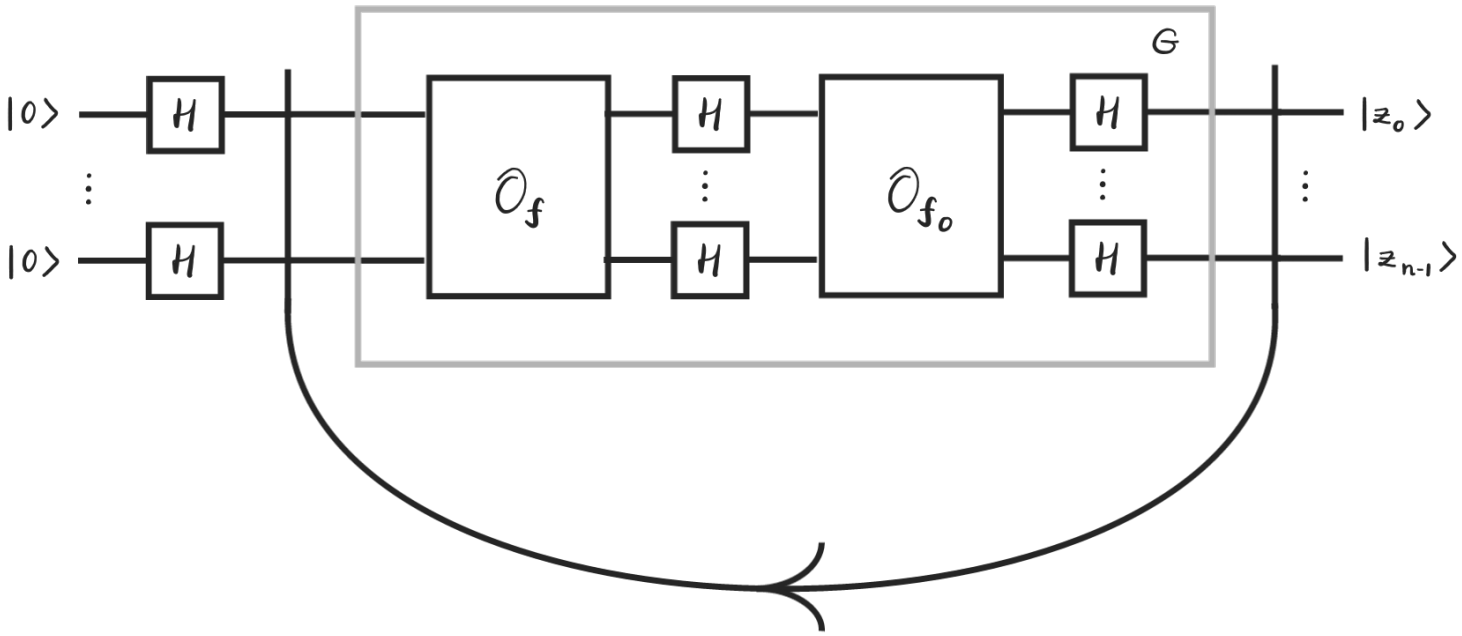
Така второто отражение е :



Пълният гейт на Гровер е :



Пълната схема на алгоритъма на Гровер е



k кратно изпълнение,

където k = цялата част на $\frac{\pi}{4\theta} - \frac{1}{2}$

$$\sin\theta = \frac{1}{\sqrt{N}}, \quad N = 2^n$$

Ако $N \gg 1$, то $\sin\theta \to 0$ и от анализа знаем, че тогава $\theta \approx \sin\theta = \frac{1}{\sqrt{N}}$

Следователно k е цялата част $\frac{\pi}{4}\sqrt{N} - \frac{1}{2} \sim \sqrt{N}$.

Тоест, потвърждаваме, че времето за изпълнение на алгоритъма е $\sim \sqrt{N}$.