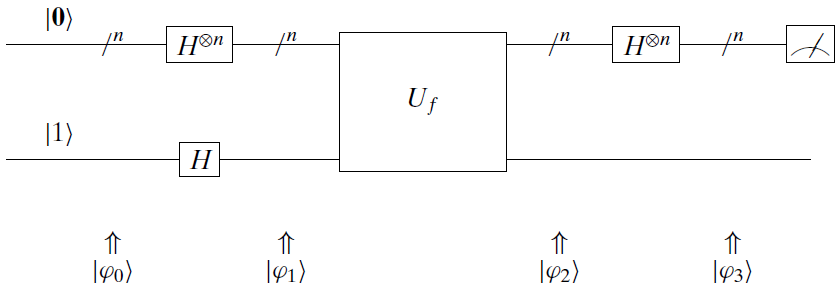
رایانش کوانتومی
الگوریتم جستجوی گراور

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان



الگوریتم دویچ–جوتزا

در نتیجه، وابستگی احتمال رمبش به $|\mathbf{0}\rangle$ به $f(\boldsymbol{x})$

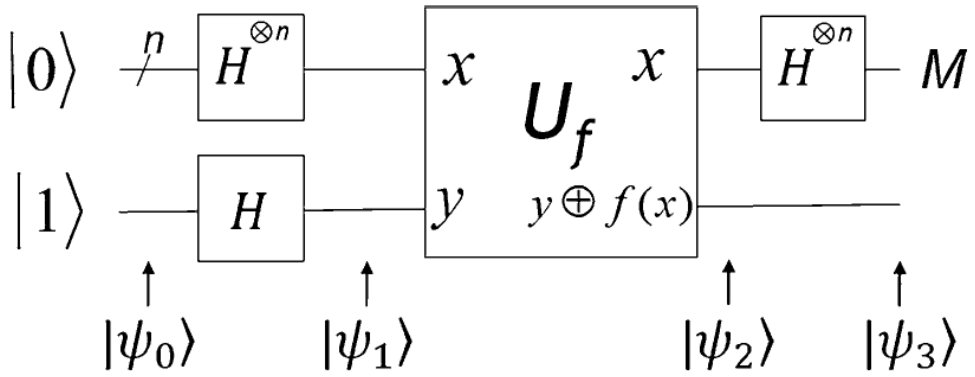
در صورت تابع ثابت بودن $f(\boldsymbol{x})$ به ۱، کیوبیت‌های بالائی برابر:

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)|\mathbf{0}\rangle}{2^n} = \frac{-(2^n)|\mathbf{0}\rangle}{2^n} = -1|\mathbf{0}\rangle.$$

در صورت تابع ثابت بودن $f(\boldsymbol{x})$ به **0**، کیوبیت‌های بالائی برابر:

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n} 1|\mathbf{0}\rangle}{2^n} = \frac{2^n|\mathbf{0}\rangle}{2^n} = +1|\mathbf{0}\rangle.$$

الگوریتم برنشتاین-وزیرانی



$$\frac{1}{۲^n}\sum_{z=0}^{۲^n-۱}\left(\sum_{x=0}^{۲^n-۱}(-۱)^{(s\oplus z).x}\right)|z\rangle\otimes\left(\frac{|0\rangle-|۱\rangle}{\sqrt{۲}}\right)$$

اگر $s \oplus \mathrm{z} = 0$ یا $z = s$ آن‌گاه بزرگی

$$\frac{1}{۲^n}\sum_{x=0}^{۲^n-۱}(-۱)^{(s\oplus z).x}$$

برابر ۱
در نتیجه

$$|\psi_۳\rangle = ۱|s\rangle\otimes\left(\frac{|0\rangle-|۱\rangle}{\sqrt{۲}}\right)$$

مقدار اندازه‌گیری‌شده برابر s
اگر $s \oplus \mathrm{z} = ۱$ یا $z \neq s$ آن‌گاه بزرگی

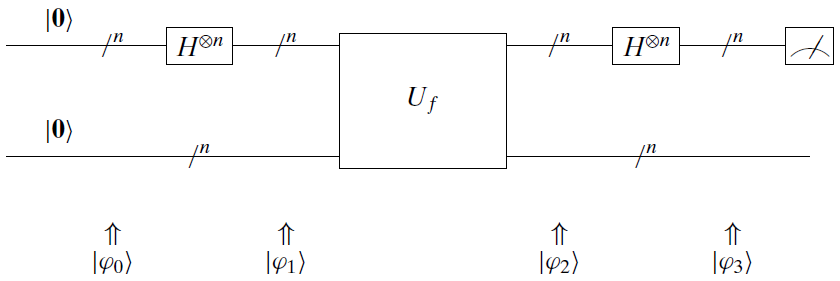
$$\frac{1}{۲^n}\sum_{x=0}^{۲^n-۱}(-۱)^{(s\oplus z).x}$$

برابر صفر

الگوریتم تناوب سیمون

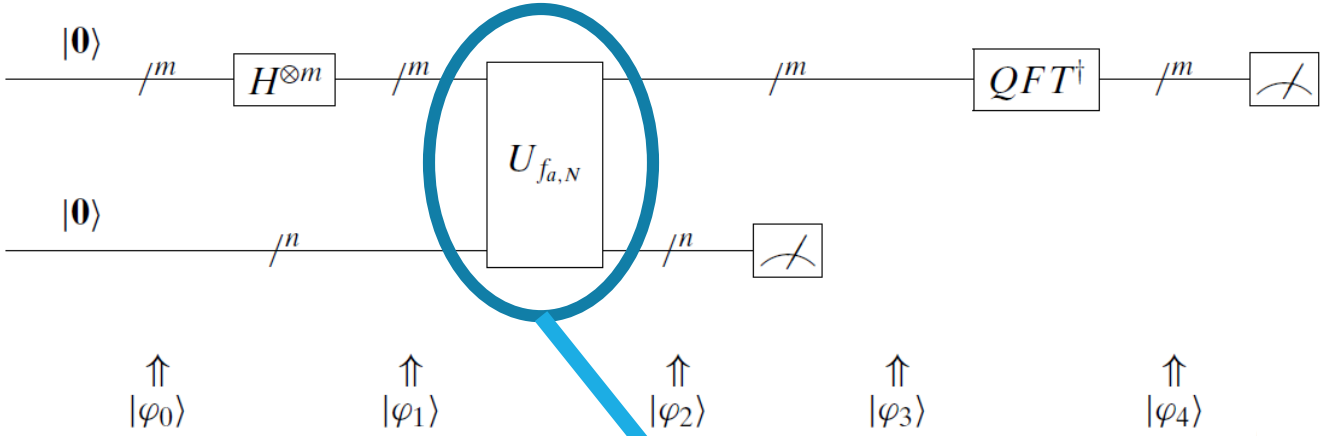
الگوریتم سیمون:

بخش کوانتومی الگوریتم نیاز به تکرار عملیات‌های زیر برای چندین بار:



نمایش ماتریسی

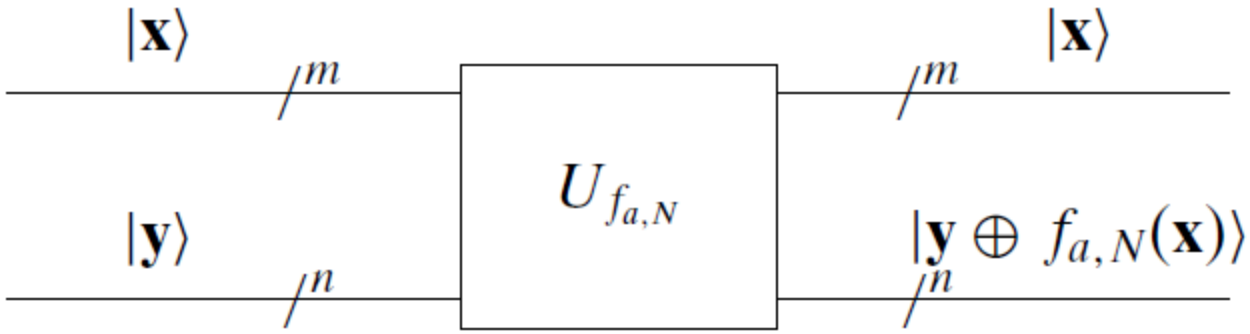
$$\left(H^{\otimes n} \otimes I\right) U_f \left(H^{\otimes n} \otimes I\right) |\mathbf{0}, \mathbf{0}\rangle$$



الگوریتم شور

مدار کوانتومی معادل $f_{a,N}$

- خروجی کمتر از N، در نتیجه تعداد بیت‌های خروجی برابر $n = \lceil logN \rceil$
- نیاز به ارزیابی $f_{a,N}$ برای حداقل N^2 مقدار از x
- نیاز به $m = logN^2 = 2logN = 2n$ بیت ورودی
- شماتیک مدار کوانتومی معادل



- انتقال از $|\boldsymbol{x},\boldsymbol{y}\rangle$ به $|\boldsymbol{x},\boldsymbol{y} \oplus f_{a,N}(\boldsymbol{x})\rangle = |\boldsymbol{x},\boldsymbol{y} \oplus a^x \% N\rangle$

الگوریتم جستجوی گراور

گلی گم کرده‌ام می‌جویم او را!

یافتن گلی در میان گل‌ها

بررسی تک تک گل و به دنبال یافتن گل

نا کارآمد

داشتن آرایه N-تایی در بدترین حالت از مرتبه N و در حالت متوسط N/2

الگوریتم جستجوی گراور در $\sqrt{N}$

- فرض $N = ۲^n$ پس کاهش مرتبه جستجو از ۲^n به $۲^{\frac{n}{۲}}$

عدم سرعت نمایی ولی با پیشرفتی مناسب

دارای کاربرد در شمارش و نظریه پایگاه داده و امثالهم

فرض تابع $f: \{0,۱\}^{۷} \to \{0,۱\}$ و اطمینان از وجود رشته دودویی $\mathbf{x}_0$ به طوری که

$$f(x) = \begin{cases} ۱, \boldsymbol{x} = \boldsymbol{x}_0 \\ 0, \boldsymbol{x} \neq \boldsymbol{x}_0 \end{cases}$$

الگوریتم جستجوی گراور

هدف: یافتن x_0

- در روش کلاسیکی نیاز به ارزیابی ۲^n رشتهٔ دودوئی و
- الگوریتم گروور جستجوی $\sqrt{۲^n} = ۲^{\frac{n}{۲}}$
- فرض وجود تابع f

$$f(x) = \begin{cases} ۱, x = x_0 \\ 0, x \neq x_0 \end{cases}$$

فرض بر امکان مدل تابع f با عملگر یگانی U_f

- نگاشت $|\boldsymbol{x},\boldsymbol{y}\rangle$ به $|\boldsymbol{x},f(\boldsymbol{x}) \oplus y\rangle$

$$U_f|\boldsymbol{x},y\rangle$$

الگوریتم جستجوی گراور

هدف: یافتن x_0

- در روش کلاسیکی نیاز به ارزیابی ۲^n رشتهٔ دودوئی و
- الگوریتم گروور جستجوی $\sqrt{۲^n} = ۲^{\frac{n}{۲}}$
- فرض وجود تابع f

$$f(x) = \begin{cases} ۱, x = x_0 \\ 0, x \neq x_0 \end{cases}$$

فرض بر امکان مدل تابع f با عملگر یگانی U_f

- نگاشت $|\boldsymbol{x},\boldsymbol{y}\rangle$ به $|\boldsymbol{x},f(\boldsymbol{x}) \oplus y\rangle$

$$U_f|\boldsymbol{x},y\rangle = |\boldsymbol{x},f(\boldsymbol{x}) \oplus y\rangle$$

الگوریتم جستجوی گراور

هدف: یافتن x_0

- در روش کلاسیکی نیاز به ارزیابی ۲^n رشتهٔ دودوئی و
- الگوریتم گروور جستجوی $\sqrt{۲^n} = ۲^{\frac{n}{۲}}$
- فرض وجود تابع f

$$f(x) = \begin{cases} ۱, x = x_0 \\ 0, x \neq x_0 \end{cases}$$

فرض بر امکان مدل تابع f با عملگر یگانی U_f

- نگاشت $|\boldsymbol{x},\boldsymbol{y}\rangle$ به $|\boldsymbol{x},f(\boldsymbol{x}) \oplus y\rangle$

$$U_f|\boldsymbol{x},y\rangle = |\boldsymbol{x},f(\boldsymbol{x}) \oplus y\rangle = \begin{cases} |\boldsymbol{x},۱ \oplus y\rangle, x = x_0 \\ |\boldsymbol{x},0 \oplus y\rangle, x \neq x_0 \end{cases}$$

الگوریتم جستجوی گراور

هدف: یافتن x_0

- در روش کلاسیکی نیاز به ارزیابی ۲^n رشتهٔ دودوئی و
- الگوریتم گروور جستجوی $\sqrt{۲^n} = ۲^{\frac{n}{۲}}$
- فرض وجود تابع f

$$f(x) = \begin{cases} ۱, x = x_0 \\ 0, x \neq x_0 \end{cases}$$

فرض بر امکان مدل تابع f با عملگر یگانی U_f

- نگاشت $|\boldsymbol{x},\boldsymbol{y}\rangle$ به $|\boldsymbol{x},f(\boldsymbol{x}) \oplus y\rangle$

$$U_f|\boldsymbol{x},y\rangle = |\boldsymbol{x},f(\boldsymbol{x}) \oplus y\rangle = \begin{cases} |\boldsymbol{x},۱ \oplus y\rangle, x = x_0 \\ |\boldsymbol{x},0 \oplus y\rangle, x \neq x_0 \end{cases} = \begin{cases} -۱|\boldsymbol{x},y\rangle, x = x_0 \\ +۱|\boldsymbol{x},y\rangle, x \neq x_0 \end{cases}$$

الگوریتم جستجوی گراور

هدف: یافتن x_0

- در روش کلاسیکی نیاز به ارزیابی ۲^n رشتهٔ دودوئی و
- الگوریتم گروور جستجوی $\sqrt{۲^n} = ۲^{\frac{n}{۲}}$
- فرض وجود تابع f

$$f(x) = \begin{cases} ۱, x = x_0 \\ 0, x \neq x_0 \end{cases}$$

فرض بر امکان مدل تابع f با عملگر یگانی U_f

- نگاشت $|\boldsymbol{x},\boldsymbol{y}\rangle$ به $|\boldsymbol{x},f(\boldsymbol{x}) \oplus y\rangle$

$$U_f|\boldsymbol{x},y\rangle = |\boldsymbol{x},f(\boldsymbol{x}) \oplus y\rangle = \begin{cases} |\boldsymbol{x}, ۱ \oplus y\rangle, x = x_0 \\ |\boldsymbol{x}, 0 \oplus y\rangle, x \neq x_0 \end{cases} = \begin{cases} -۱|\boldsymbol{x},y\rangle, x = x_0 \\ +۱|\boldsymbol{x},y\rangle, x \neq x_0 \end{cases} = (-۱)^{f(x)}|\boldsymbol{x},y\rangle$$

الگوریتم جستجوی گراور

- نگاشت $|x,f(x)\oplus y\rangle$ به $|x,y\rangle$

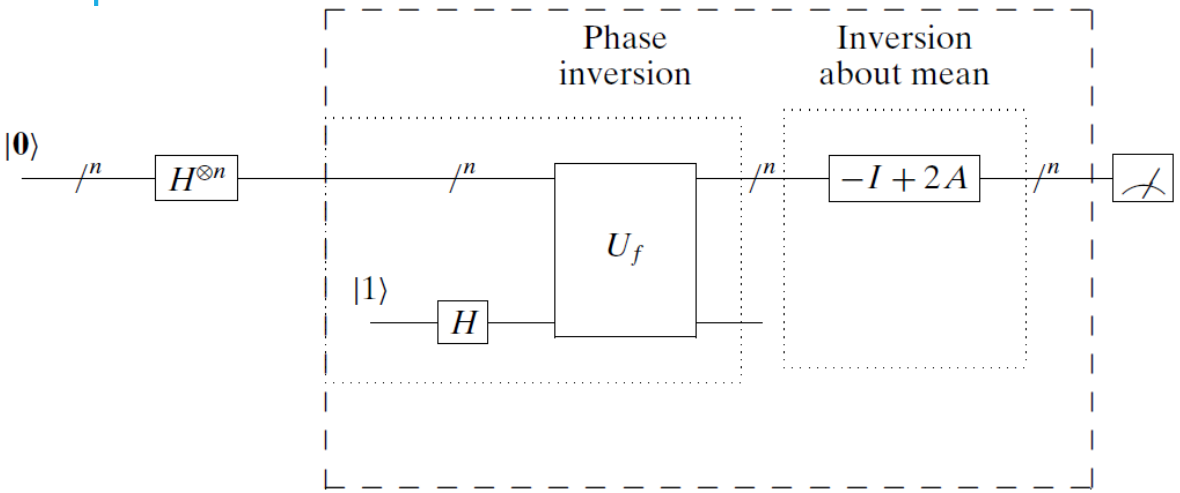
$$U_f|x,y\rangle = |x,f(x)\oplus y\rangle = \begin{cases}|x,۱\oplus y\rangle, x=x_0\\ |x,0\oplus y\rangle, x\neq x_0\end{cases}\rangle = \begin{cases}-۱|x,y\rangle, x=x_0\\ +۱|x,y\rangle, x\neq x_0\end{cases} = (-۱)^{f(x)}|x,y\rangle$$

- مثال، $n=۲$ در صورتی که f به دنبال یافتن رشته دودیی ۱۰ ، آن‌گاه U_f به صورت

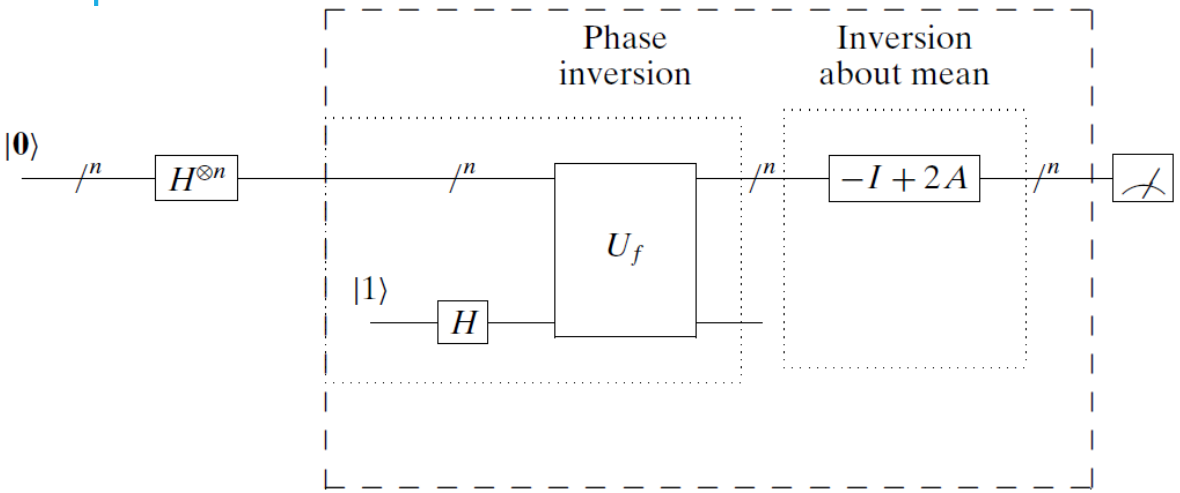
$$\begin{array}{c} \\ \mathbf{00,0}\\ \mathbf{00,1}\\ \mathbf{01,0}\\ \mathbf{01,1}\\ \mathbf{10,0}\\ \mathbf{10,1}\\ \mathbf{11,0}\\ \mathbf{11,1}\end{array}\begin{array}{c}\begin{array}{cccccccc}\mathbf{00,0} & \mathbf{00,1} & \mathbf{01,0} & \mathbf{01,1} & \mathbf{10,0} & \mathbf{10,1} & \mathbf{11,0} & \mathbf{11,1}\end{array}\\ \begin{bmatrix}1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1\end{bmatrix}\end{array}.$$

الگوریتم جستجوی گراور

الگوریتم جستجوی گراور



الگوریتم جستجوی گراور



شبه‌کد گروور:

۱- شروع با $|0\rangle^{\otimes n}|۱\rangle$

۲- تکرار دو عملیات زیر برای $\sqrt{N}=\sqrt{۲^n}$ دفعه

- اعمال تابع تغییر فاز $U_f\left(I^{\otimes n}\otimes H\right)$
- اعمال وارون‌سازی حول میانگین $H^{\otimes n}(۲|0\rangle\langle 0|-I)H^{\otimes n}=۲|\psi\rangle\langle\psi|-I$

۳- اندازه‌گیری

الگوریتم جستجوی گراور

شبه‌کد گروور:

۱- شروع با $|0\rangle^{\otimes n}|۱\rangle$

۲- اعمال $H^{\otimes n}H$ روی مقدار ورودی

$$H^{\otimes n}H|0\rangle^{\otimes n}|۱\rangle = \frac{۱}{\sqrt[n]{۲^۲}}\sum_{x=0}^{N-1}|x\rangle\left(\frac{|0\rangle - |۱\rangle}{\sqrt{۲}}\right) = \frac{۱}{\sqrt[n]{۲^۲}}\sum_{x=0}^{N-1}|x\rangle\,(|-\rangle)$$

۳- اعمال U_f

$$\begin{aligned}
&U_f \frac{۱}{\sqrt[n]{۲^۲}}\sum_{x=0}^{N-1}|x\rangle\,|-\rangle \\
&= \frac{۱}{\sqrt[n]{۲^۲}}\sum_{x=0}^{N-1}U_f|x\rangle\,|-\rangle \\
&= \frac{۱}{\sqrt[n]{۲^۲}}\sum_{x=0}^{N-1}|x\rangle\,|-\oplus f(x)\rangle \\
&= \frac{۱}{\sqrt[n]{۲^۲}}\sum_{x=0}^{N-1}(-۱)^{f(x)}|x\rangle\,|-\rangle
\end{aligned}$$

الگوریتم جستجوی گراور

شبه‌کد گروور:

۱- شروع با $|0\rangle^{\otimes n}|1\rangle$

۲- اعمال $H^{\otimes n}H$ روی مقدار ورودی

$$H^{\otimes n}H|0\rangle^{\otimes n}|1\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{N-1}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{N-1}|x\rangle\,(|-\rangle)$$

۳- اعمال U_f

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

تغییر فاز مقدار تحتِ جستجو

- اما ناکافی
- چرا؟
- صرفا تغییر فاز و احتمال هر حالت برابر $\frac{1}{2^n}$

الگوریتم جستجوی گراور

نیاز به تغییر میزان احتمالات

استفاده از «وارون‌گیری حول میانگین».

پس تغییر مرحله سه به صورت زیر

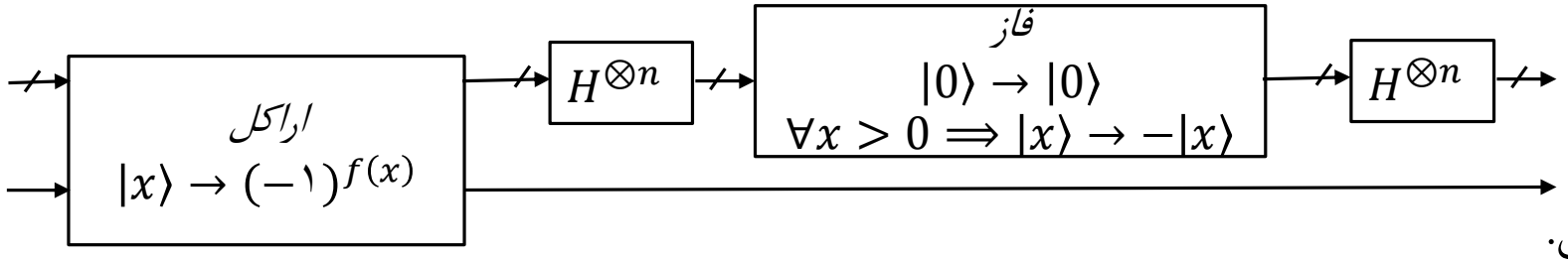
۳-

$$H^{\otimes n}(۲|0\rangle\langle 0| - I)H^{\otimes n} = ۲|\psi\rangle\langle\psi| - I$$
$$G = (۲|\psi\rangle\langle\psi| - I)U_f$$

۴- تکرار مرحلهٔ بالا به تعداد $\sqrt{N}$

۵- اندازه‌گیری

الگوریتم جستجوی گراور



نیاز به تغییر میزان احتمالات

استفاده از وارون‌گیری حول میانگین.

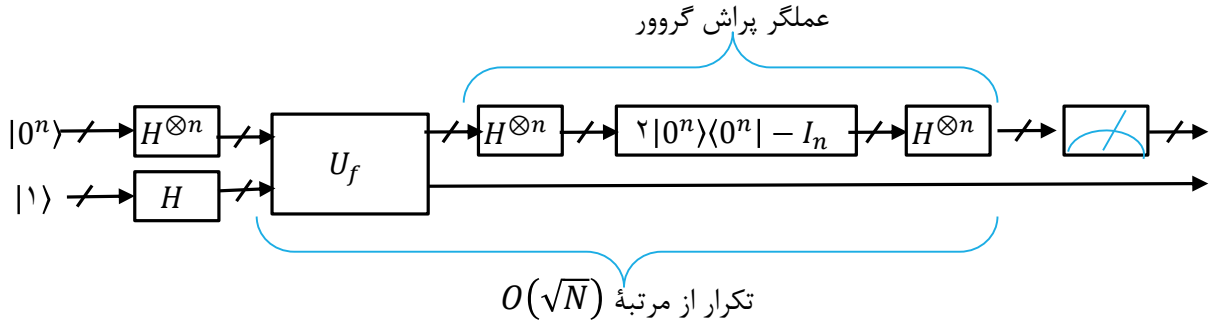
پس تغییر مرحله سه به صورت زیر

۳-

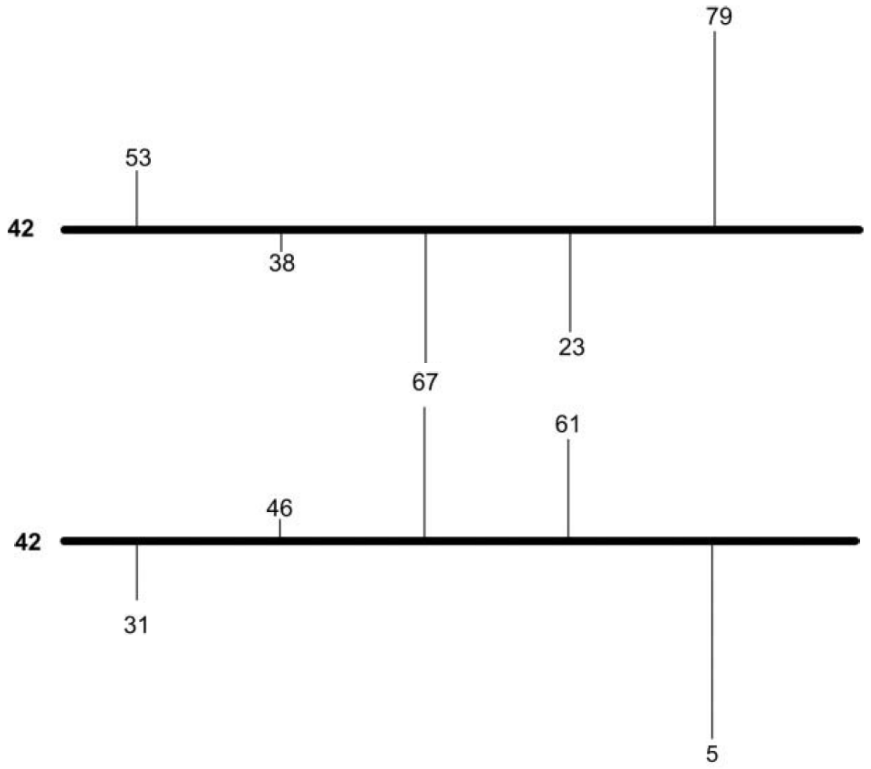
$$H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$$
$$G = (2|\psi\rangle\langle\psi| - I)U_f$$

۴- تکرار مرحلهٔ بالا به تعداد $\sqrt{N}$

۵- اندازه‌گیری



وارون‌گیری حول میانگین



تغییر جای مقادیر شمالی به جنوبی و بالعکس

- وارون‌سازی حول میانگین
- مثال عدد ۵۳ و میانگین $\mathrm{m} = ۴۲$
  - $m - ۵۳ = -۱۱$
  - افزودن m به ۱۱− یا $m + (m - ۵۳) = ۳۱$
- در حالت کلی
  - $v_{\text{ج}} = m + \left(m - v_{\text{ق}}\right) = ۲m - v_{\text{ق}}$

وارون‌گیری حول میانگین

نمایش ماتریسی $V = [۵۳,۳۸,۱۷,۲۳,۷۹]^T$

$$M = \begin{bmatrix} \frac{۱}{۵} & \cdots & \frac{۱}{۵} \\ \vdots & \ddots & \vdots \\ \frac{۱}{۵} & \cdots & \frac{۱}{۵} \end{bmatrix}$$

$$MV = [۴۲, ۴۲, ۴۲, ۴۲, ۴۲]^T$$

$$V = -V + ۲MV = (-I + ۲M)V$$

$$(-I + ۲M) = \begin{bmatrix} (-1+\frac{2}{5}) & \frac{2}{5} & \frac{2}{5} & \frac{2}{5} & \frac{2}{5} \\ \frac{2}{5} & (-1+\frac{2}{5}) & \frac{2}{5} & \frac{2}{5} & \frac{2}{5} \\ \frac{2}{5} & \frac{2}{5} & (-1+\frac{2}{5}) & \frac{2}{5} & \frac{2}{5} \\ \frac{2}{5} & \frac{2}{5} & \frac{2}{5} & (-1+\frac{2}{5}) & \frac{2}{5} \\ \frac{2}{5} & \frac{2}{5} & \frac{2}{5} & \frac{2}{5} & (-1+\frac{2}{5}) \end{bmatrix}$$

وارون گیری حول میانگین

حالت کلی

- n کیوبیت پس 2^nحالت ممکن
- هر حالت برداری با 2^n مدخل

$$M = \begin{bmatrix} \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \end{bmatrix}$$

- M^2=M

وارون‌گیری حول میانگین

$$-I + ۲M = \begin{bmatrix} -1+\frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1+\frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & -1+\frac{2}{2^n} \end{bmatrix}$$

- $-I + ۲M$ وارون‌سازی اندازه حول میانگین
  - ماتریسی یگانی
  - اثبات کنید

تغییر فاز + وارون‌گیری حول میانگین

$$V = [۱۰,۱۰,۱۰,۱۰,۱۰]^T$$

تغییر فاز

$$V = [۱۰,۱۰,۱۰, -۱۰,۱۰]^T$$

میانگین برابر ۶

وارون‌گیری حول میانین

$$V = (-I + ۲M)V = [۲,۲,۲,۲۲,۲]^T$$

اختلاف برابر با ۲۰

تغیر فاز + وارون‌گیری حول میانگین

$$V = [۲,۲,۲,۲۲,۲]^T$$

تغییر فاز

$$V = [۲,۲,۲, -۲۲,۲]^T$$

میانگین برابر -۲.۸

وارون‌گیری حول میانین

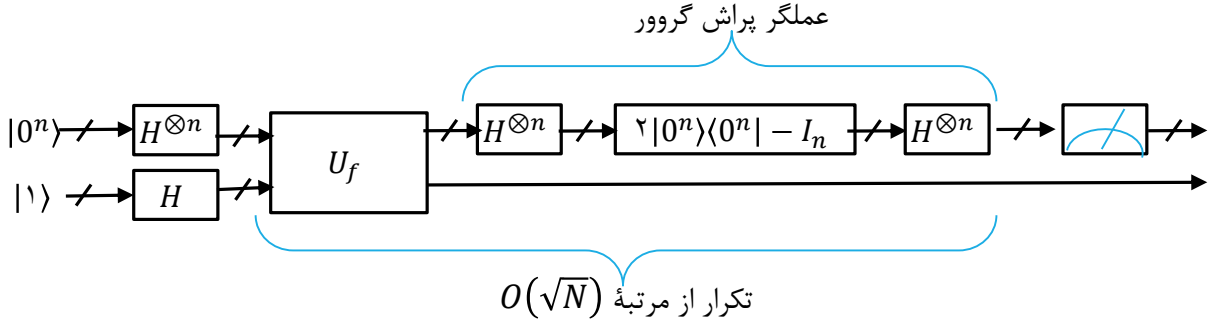
$$V = (-I + ۲M)V = [-۷.۶, -۷.۶, -۷.۶,۱۶.۴, -۷.۶]^T$$

اختلاف برابر با ۲۴

$\sqrt{۲^n}$ بار تکرار دو عملیات

- تمرین

تغییر فاز + وارون‌گیری حول میانگین



$$\begin{matrix}\mathbf{000} & \mathbf{001} & \mathbf{010} & \mathbf{011} & \mathbf{100} & \mathbf{101} & \mathbf{110} & \mathbf{111}\end{matrix}^T$$
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

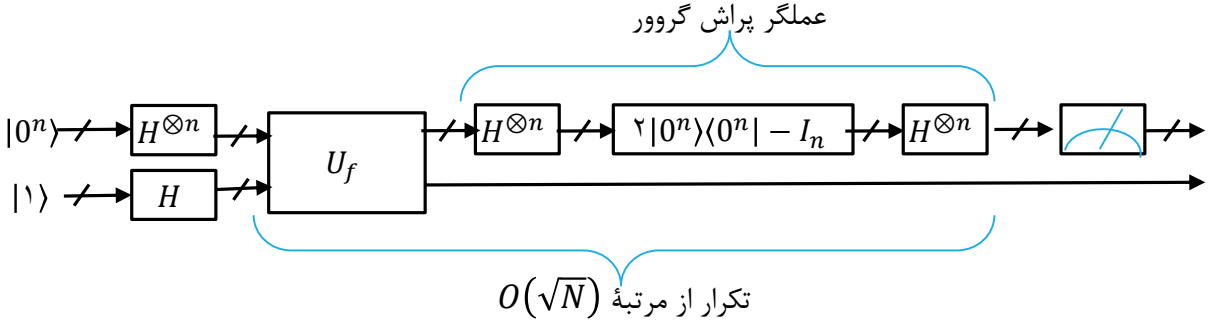
$$\begin{matrix}000 & 001 & 010 & 011 & 100 & 101 & 110 & 111\end{matrix}^T$$
$$\begin{bmatrix} \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}} \end{bmatrix}$$

$$\begin{matrix}000 & 001 & 010 & 011 & 100 & 101 & 110 & 111\end{matrix}^T$$
$$\begin{bmatrix} \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & -\frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}}, & \frac{1}{\sqrt{8}} \end{bmatrix}$$
تغییر فاز

$$M = \frac{۳}{۴\sqrt{۸}}$$

$$\begin{matrix}\mathbf{000} & \mathbf{001} & \mathbf{010} & \mathbf{011} & \mathbf{100} & \mathbf{101} & \mathbf{110} & \mathbf{111}\end{matrix}^T$$
$$\begin{bmatrix} \frac{1}{2\sqrt{8}}, & \frac{1}{2\sqrt{8}}, & \frac{1}{2\sqrt{8}}, & \frac{1}{2\sqrt{8}}, & \frac{1}{2\sqrt{8}}, & \frac{5}{2\sqrt{8}}, & \frac{1}{2\sqrt{8}}, & \frac{1}{2\sqrt{8}} \end{bmatrix}$$
وارون‌گیری حول میانگین

تغییر فاز + وارون‌گیری حول میانگین



$$\left[\frac{1}{2\sqrt{8}}_{\mathbf{000}}, \frac{1}{2\sqrt{8}}_{\mathbf{001}}, \frac{1}{2\sqrt{8}}_{\mathbf{010}}, \frac{1}{2\sqrt{8}}_{\mathbf{011}}, \frac{1}{2\sqrt{8}}_{\mathbf{100}}, \frac{5}{2\sqrt{8}}_{\mathbf{101}}, \frac{1}{2\sqrt{8}}_{\mathbf{110}}, \frac{1}{2\sqrt{8}}_{\mathbf{111}}\right]^T$$

$$\left[\frac{1}{2\sqrt{8}}_{\mathbf{000}}, \frac{1}{2\sqrt{8}}_{\mathbf{001}}, \frac{1}{2\sqrt{8}}_{\mathbf{010}}, \frac{1}{2\sqrt{8}}_{\mathbf{011}}, \frac{1}{2\sqrt{8}}_{\mathbf{100}}, -\frac{5}{2\sqrt{8}}_{\mathbf{101}}, \frac{1}{2\sqrt{8}}_{\mathbf{110}}, \frac{1}{2\sqrt{8}}_{\mathbf{111}}\right]^T$$ تغییر فاز

$$M = \frac{1}{8\sqrt{8}}$$

$$\left[\frac{-1}{4\sqrt{8}}_{\mathbf{000}}, \frac{-1}{4\sqrt{8}}_{\mathbf{001}}, \frac{-1}{4\sqrt{8}}_{\mathbf{010}}, \frac{-1}{4\sqrt{8}}_{\mathbf{011}}, \frac{-1}{4\sqrt{8}}_{\mathbf{100}}, \frac{11}{4\sqrt{8}}_{\mathbf{101}}, \frac{-1}{4\sqrt{8}}_{\mathbf{110}}, \frac{-1}{4\sqrt{8}}_{\mathbf{111}}\right]^T$$ وارون‌گیری حول میانگین

$$\frac{11}{4\sqrt{8}} \cong 0.9723 \qquad \frac{-1}{4\sqrt{8}} \cong -0.0884$$

منابع

مانوچچی

ؤانگ

نیلسن (نیک و آیک)

شنکار