آلگوریتم کوانتومی جستجو

وحیدکریمی پور_ دانشکده فیزیک ـ دانشگاه صنعتی شریف

۱۰ مرداد ۱۳۹۷

۱ مقدمه

یکی از مسایلی که توسط آلگوریتم های کوانتومی درزمان کوتاه تری نسبت به آلگوریتم های کلاسیک حل می شوند مسایل مربوط به جستجو است. صورت مجرد یک مسئله جستجو را می توان به شکل زیر بیان کرد. مجموعه $S := \{x_1, x_2, \cdots x_N\}$ شامل N شی است. تابعی مثل $f : S \longrightarrow \{0, 1\}$ روی این مجموعه تعریف شده است. می دانیم که‌مقدار تابع f تنهایکی از عناصر این مجموعه که آن را با w نشان می دهیم برابربا صفر است و روی دیگر عناصر مجموعه S مقدار این تابع برابر با صفر است. w یکی از x_i هاست ولی نمی دانیم که کدام یک از آنهاست. درغیاب هرنوع اطلاعات اضافه ای، تنها کاری که باید بکنیم آن است که x_i های مختلف را یک به یک به تابع بدهیم و خروجی تابع را نگاه کنیم . هرگاه خروجی تابع f برابر با یک شد می فهمیم که عنصر داده شده به تابع w بوده است. بطور متوسط می بایست تابع را $O(\frac{N}{2})$ بار بخوانیم تا بتوانیم به w دسترسی پیداکنیم. اما با استفاده هوشمندانه ای از اصل برهم نهی و توازی کوانتومی می توان این مقدار را به $O(\sqrt{N})$ تقلیل داد که برای N های بزرگ کاهش قابل ملاحظه ای است. مسلم است که کلاس این مسئله با این ابداع تغییری نکرده است و همچنان این مسئله درکلاس مسائل چند جمله ای است،امابدلیل نقشی که یک آلگوریتم جستجو دراغلب آلگوریتم های دیگربازی می کند، این پیشرفت اهمیت زیادی دارد. دراین فصل نخست جستجو درداده های نامنظم را توضیح می دهیم و سپس به توضیح جستجو در داده های سازمان یافته می پردازیم.

■ تمرین: یک مجموعه داده نامنظم که دارای N داده است و یکی از آنها داده مطلوب ماست در نظر بگیرید. حال به یکی از این دو روش شروع به جستجوی این مجموعه داده می کنیم:

روش اول: مجموعه داده را یکی یکی به طور منظم جستجو می کنیم تا به داده مطلوب برسیم. طبیعی است که در این روش هر داده را فقط یک بار تست می کنیم.

روش دوم: مجموعه داده ها را به طور تصادفی جستجو می کنیم تا به داده مطلوب برسیم. در این روش یک داده ممکن است بیش از یک بار تست شود.

تعداد متوسط دفعاتی را که باید داده ها را تست کنیم تا به نتیجه مطلوب برسیم در هرکدام از دو روش محاسبه کنید.

---

۲ جستجو در داده های نامنظم

نخست دقت می کنیم که تابع f دریک مدار کوانتومی بصورت عملگر کوانتومی یکانی زیر نشان داده می شود:

$$U_f|x_i, y\rangle = |x_i, f(x_i) \oplus y\rangle. \qquad (۱)$$

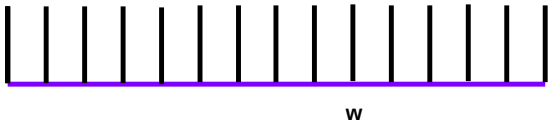
هرگاه این عملگر را روی ورودی $|x_i\rangle \otimes |-\rangle$ اثر دهیم که درآن $|-\rangle = \frac{۱}{\sqrt{۲}}(|۰\rangle - |۱\rangle)$، آنگاه براحتی دیده می شود که

$$\begin{aligned} U_f|w\rangle \otimes |-\rangle &= -|w\rangle \otimes |-\rangle \\ U_f|x_i\rangle \otimes |-\rangle &= |x_i\rangle \otimes |-\rangle \qquad x_i \neq w. \end{aligned} \qquad (۲)$$

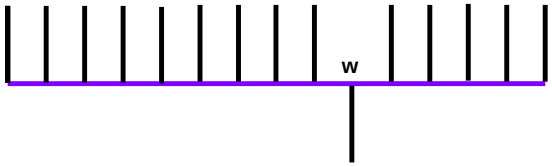
بنابراین روی زیرفضای اول اثر این عملگر به شکل یک انعکاس ظاهر می شود . یعنی این عملگر حالت $|w\rangle$ را به حالت $-|w\rangle$ برمی گرداند وبقیه حالات را دست نخورده باقی می گذارد. ازاین به بعد دربحث خود فضای دوم یعنی $|-\rangle$ را برای سادگی حذف می کنیم. درنتیجه می توان عملگر U_f را به شکل زیرنوشت :

$$U_f = I - ۲|w\rangle\langle w|. \qquad (۳)$$

دراین جا تذکر این نکته مهم است که علیرغم شکل ظاهری خود عملگر U_f بدون دانستن حالت $|w\rangle$ این انعکاس را انجام می دهد زیرا این عملگر چیزی نیست جزهمان عمل تابع f روی عناصر مجموعه S ویا حالات متناظر با آنها.



شکل ۱: بیان شماتیک بردار حالت ورودی که ترکیبی خطی از همه داده های ممکن با ضرایب مساوی است.



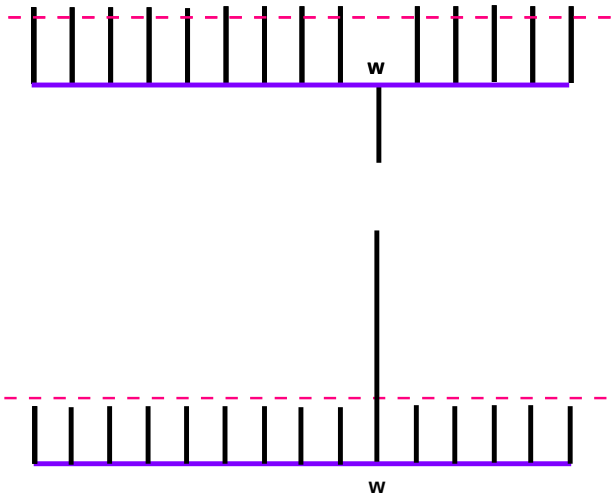
شکل ۲: بردارحالت ورودی پس از آنکه تابع یک بارآن را خوانده است .

حال فرض کنید که عملگر U_f را روی حالت

$$|s\rangle := \frac{1}{\sqrt{N}}(|x_1\rangle + |x_2\rangle + \cdots |x_N\rangle) \qquad (4)$$

اثر دهیم. نخست آلگوریتم گرور را به طور کیفی توضیح می دهیم. هرگاه حالت فوق رابه شکل 1 نشان دهیم بعداز اثر عملگر U_f به شکل 2 درخواهد آمد. حال اگر این حالت را روی متوسط خودش (که‌روی شکل به صورت خط چین نشان داده شده و بعدا به صورت دقیق تعریف خواهد شد) انعکاس دهیم، حالت نشان داده شده درشکل 3 بدست خواهد آمد.

می توان نشان داد که این انعکاس حول متوسط نیز یک عملگر یکانی است که‌آن را با I_s نشان می دهیم. خواننده می تواند به راحتی تصدیق کند که بعدازچند بار خواندن تابع و انعکاس حول متوسط، یعنی بعد از چند بار اعمال عملگر $G := I_s U_f$ شکل حالت به صورتی درخواهد آمد که درآن دامنه مربوط به $|w\rangle$ نسبت به بقیه دامنه ها افزایش قابل ملاحظه ای پیداکرده است و درنتیجه اندازه گیری چنین حالتی به احتمال زیاد،



شکل ۳: شکل بالا بردار حالت را قبل از انعکاس حول متوسط و شکل پایین بعد از انعکاس حول متوسط نشان می دهد. خط چین مقدار متوسط است.

نتیجه اش $|w\rangle$ خواهد بود. البته پس از هربارانداره گیری بااحتمال ضعیفی ممکن است که عنصری غیراز $|w\rangle$ یافت شود که دراین صورت با خوراندن آن به تابع f و بدست آمدن مقدار صفر آلگوریتم دوباره از اول طی می شود.

حال آنچه را که به طور کیفی گفتیم بطور دقیق بازگو می کنیم. نخست می بایست ببینیم آیا انعکاس حول مقدار متوسط را واقعا می توان با یک عملگر یکانی نشان داد. حالتی مثل

$$|\psi\rangle = \sum_x \psi_x |x\rangle \qquad (۵)$$

را در نظر بگیرید. متوسط این حالت برابر است با:

$$\overline{\psi} = \frac{۱}{N} \sum_x \psi_x. \qquad (۶)$$

و انعکاس حول متوسط $|\psi\rangle$ حول متوسط آن به صورت زیر است:

$$I_s|\psi\rangle := \sum_x (\psi_x - ۲(\psi_x - \overline{\psi}))|x\rangle = \sum_x (۲\overline{\psi} - \psi_x)|x\rangle \qquad (۷)$$

و در نتیجه

$$I_s|\psi\rangle := \sum_x (۲\overline{\psi} - \psi_x)|x\rangle = ۲\overline{\psi}\sqrt{N}|s\rangle - |\psi\rangle. \quad (۸)$$

اما می دانیم که

$$\overline{\psi} = \frac{۱}{\sqrt{N}}\langle s|\psi\rangle. \quad (۹)$$

بنابراین

$$I_s|\psi\rangle := ۲|s\rangle\langle s|\psi\rangle - |\psi\rangle = (۲|s\rangle\langle s| - I)|\psi\rangle. \quad (۱۰)$$

بنابراین عملگر I_s را می توان به صورت زیر نوشت :

$$I_s = ۲|s\rangle\langle s| - I, \quad (۱۱)$$

عملگرترکیبی $G := I_s U_f$ را به ا فتخار کاشف این آلگوریتم عملگر گرور می خوانیم . دراین قسمت می خواهیم نشان دهیم که با اثر عملگر گرور به تعداد $O(\sqrt{N})$ بار روی حالت اولیه $|s\rangle$ می توانیم به حالتی برسیم که دامنه $|w\rangle$ درآن بسیارافزایش یافته است. برای این کار درفضای حالت ها، حالت زیر را تعریف می کنیم :

$$|r\rangle = \frac{۱}{\sqrt{N-۱}}(\sum_{x_i \neq w} |x_i\rangle). \quad (۱۲)$$

حال دقت می کنیم که هردو عملگر I_s و U_f را می توان تنها برحسب بردارهای $|w\rangle$ و $|r\rangle$ نوشت. درواقع تمام دینامیک ازاول تا به آخر درزیرفضایی طی می شود که توسط این دوبردار جاروب می شوند. ازآنجا که این دوبرداربرهم عمودند می توانیم نمایش زیر را برای آنها انتخاب کنیم:

$$|w\rangle = \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \quad , \quad |r\rangle = \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} \quad (۱۳)$$

و

$$|s\rangle = \frac{۱}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-۱}{N}}|r\rangle = \begin{pmatrix} \frac{۱}{\sqrt{N}} \\ \sqrt{\frac{N-۱}{N}} \end{pmatrix}. \quad (۱۴)$$

درنتیجه خوا هیم داشت :

$$U_f = I - ۲|w\rangle\langle w| = \begin{pmatrix} -۱ & ۰ \\ ۰ & ۱ \end{pmatrix}, \tag{۱۵}$$

و

$$I_s = ۲|s\rangle\langle s| - I = \begin{pmatrix} \frac{۲}{N} - ۱ & \frac{۲}{N}\sqrt{N-۱} \\ \frac{۲}{N}\sqrt{N-۱} & ۱ - \frac{۲}{N} \end{pmatrix} \tag{۱۶}$$

درنتیجه عملگر گرور به شکل زیر درخواهد آمد:

$$G = I_s U_f = \begin{pmatrix} ۱ - \frac{۲}{N} & \frac{۲}{N}\sqrt{N-۱} \\ -\frac{۲}{N}\sqrt{N-۱} & ۱ - \frac{۲}{N} \end{pmatrix}. \tag{۱۷}$$

خواننده براحتی می تواند تحقیق کند که این عملگریک عملگر متعامد است یعنی $G^tG = I$ و درنتیجه چیزی جزیک دوران درصفحه جاروب شده توسط $|r\rangle$ و $|w\rangle$ نیست. برای ادامه تحلیل، پارامتر دوران θ را به شکل زیر تعریف می کنیم:

$$\cos\theta = ۱ - \frac{۲}{N}, \qquad \sin\theta = \frac{۲}{N}\sqrt{N-۱}, \tag{۱۸}$$

و به این ترتیب عملگرگرور به شکل زیر درخواهد آمد:

$$G = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{۱۹}$$

هرگاه روی حالت اولیه $|s\rangle$ عملگر گرور را m بار اثردهیم یعنی اینکه آن حالت را به اندازه زاویه $m\theta$ چرخانده ا یم. برای اینکه ببینم این حالت چه مقدار به حالت مطلوب یعنی $|w\rangle$ نزدیک شده است می بایست عنصر ماتریسی $\langle w|G^m|s\rangle$ را حساب کنیم که برابر خواهد شد با:

$$\langle w|G^m|s\rangle = \frac{۱}{\sqrt{N}}\cos m\theta + \sqrt{\frac{N-۱}{N}}\sin m\theta. \tag{۲۰}$$

اگر قرار دهیم

$$\cos\alpha = \frac{۱}{\sqrt{N}} \qquad , \qquad \sin\alpha = \sqrt{\frac{N-۱}{N}} \tag{۲۱}$$

آنگاه خواهیم داشت :

$$\langle w|G^m|s\rangle = \cos(m\theta - \alpha). \qquad (۲۲)$$

برای این که این همپوشانی به حداکثر خود برسد تقاضا می کنیم که $m \approx \frac{\alpha}{\theta}$.

یک نتیجه خیلی جالب که زود می توان دریافت مربوط به حالتی است که $N = ۴$ باشد. دراین حالت داریم $\cos\theta = \frac{۱}{۲}$ و $\cos\alpha = \frac{۱}{۲}$ و یا

$$\alpha = \frac{\pi}{۳}, \qquad \theta = \frac{\pi}{۳}, \longrightarrow m = ۱ \qquad (۲۳)$$

یعنی می توان دراین حالت تنها با یک بارخواندن تابع به w آنهم با احتمال یک دست یافت.

برای وقتی که N خیلی بزرگ است داریم

$$\alpha \approx \frac{\pi}{۲}, \qquad \cos\theta \approx ۱ - \frac{\theta^۲}{۲} = ۱ - \frac{۲}{N}, \longrightarrow \theta = \frac{۲}{\sqrt{N}}, \qquad (۲۴)$$

ودرنتیجه $m \approx \frac{\pi}{۴}\sqrt{N}$. به این ترتیب پس از $O(\sqrt{N})$ مرتبه می توانیم با احتمال خیلی خوب شی مورد نظر را دردرون داده ها پیدا کنیم.

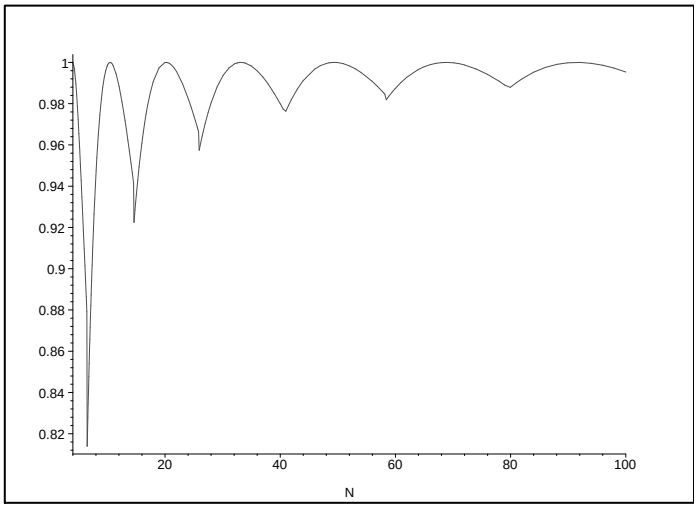
برای اینکه این احتمال را پیدا کنیم کافی است که مقدار صحیح m یعنی $[\frac{\pi}{۴}\sqrt{N}]$ را درعبارت 22 قراردهیم. این احتمال برابراست با:

$$P(N) := \cos^۲([\frac{\pi}{۴}\sqrt{N}]\cos^{-۱}(۱ - \frac{۲}{N}) - \cos^{-۱}(\frac{۱}{\sqrt{N}})). \qquad (۲۵)$$

شکل های 4 و 5 این تابع را برحسب N ، نشان می دهد.

هرگاه تعداد عناصر مطلوب بیش از یکی مثلاً l تا باشد، اصلاح کوچکی در استدلال بالا نشان می دهد که می توان درزمانی از مرتبه $O(\frac{\pi}{۴}\sqrt{\frac{N}{l}})$ به یکی از عناصر مطلوب دست یافت. اثبات دقیق این امر را به عنوان یک تمرین به عهده خواننده می گذاریم.

■ تمرین: یک مجموعه داده نامنظم که دارای N داده است و k تا از داده های مطلوب ما هستند در نظر بگیرید. هدف ما این است که یکی از این داده های مطلوب را به روش کلاسیک پیدا کنیم. حال به یکی از این دو روش شروع به جستجوی این مجموعه داده می کنیم:



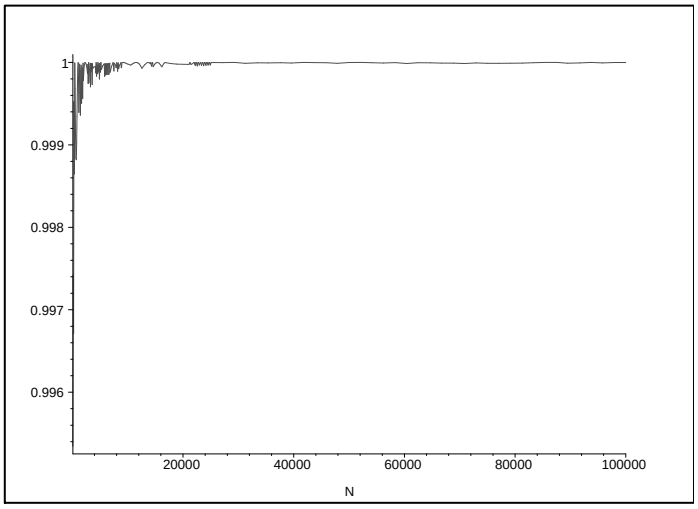
شکل ۴: احتمال یافتن یک شی دربین N با استفاده از آلگوریتم گرور به عنوان تابعی از N برای $۴ \leq N \leq ۱۰۰$.

روش اول: مجموعه داده را یکی یکی به طور منظم جستجو می کنیم تا به داده مطلوب برسیم. طبیعی است که در این روش هر داده را فقط یک بار تست می کنیم.

روش دوم: مجموعه داده ها را به طور تصادفی جستجو می کنیم تا به داده مطلوب برسیم. در این روش یک داده ممکن است بیش از یک بار تست شود.

تعداد متوسط دفعاتی را که باید داده ها را تست کنیم تا به نتیجه مطلوب برسیم در هرکدام از دو روش محاسبه کنید. در روش اول یک عبارت بسته و ساده برای وقتی که $k = ۲$ است بدست بیاورید.

■ تمرین: یک مجموعه داده نامنظم که دارای N داده است و دارای k داده مطلوب است در نظر بگیرید. می خواهیم یکی از این داده ها را پیدا کنیم. نشان دهید که یک آلگوریتم کوانتومی می تواند این کار را در زمانی از مرتبه $\sqrt{\frac{N}{k}}$ پیدا کند.



شکل ۵: احتمال یافتن یک شی دربین N با استفاده از آلگوریتم گرور به عنوان تابعی از N برای $۱۰۰ \leq N \leq ۱۰۰۰۰۰$.

۱.۲ مدار کوانتومی آلگوریتم گرور

دراین قسمت نشان می دهیم که عملگرگرور را می توان با ترکیب تعدادی از عملگرهای یک بیتی و دوبیتی کوانتومی به نحو کارآیی ساخت.
می دانیم که $I_s = I - ۲|s\rangle\langle s|$. ازطرفی می دانیم که

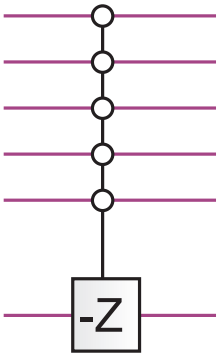
$$|s\rangle = H^{\otimes N}|۰, ۰, \cdots ۰\rangle =: H^{\otimes N}|\bar{۰}\rangle, \qquad (۲۶)$$

که درآن H عملگر هادامارد است. بنابراین می توان نوشت :

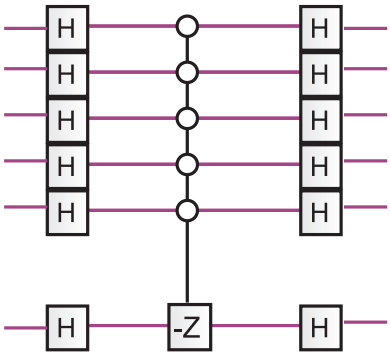
$$I_s = H^{\otimes N} I_. H^{\otimes N} \qquad (۲۷)$$

که درآن $I_. = ۲|\bar{۰}\rangle\langle\bar{۰}| - I$. بنابراین هرگاه که مدارِ $I_.$ را بسازیم می توانیم از روی آن مدار I_s را بسازیم. راه ساختن مدارِ $I_.$ آن است که به شکل ماتریسی آن توجه کنیم. به عنوان مثال برای سه تا کیوبیت $I_.$ به صورت زیر عمل می کند:

$$I_.|۰۰۰\rangle = |۰۰۰\rangle$$
$$I_.|۰۰۱\rangle = -|۰۰۱\rangle$$



شکل ۶: مدار عملگرِ $-I_{\cdot}$.



شکل ۷: مدار عملگرِ $-I_s$.

$$-I_{\cdot}|\cdot\cdot\rangle = -|\cdot\cdot\rangle$$

$$\ldots \qquad (۲۸)$$

پس معلوم است که $-I_{\cdot}$ یک عملگر کنترلی فاز $ControlledPhaseGate$ است که فقط وقتی دو کیوبیت اول برابر با صفر باشند عملگر $-Z$ روی کیوبیت آخر عمل می کند. مدار این عملگر و در نتیجه مدار عملگرِ $-I_s$ در شکل های ۶ و ۷ رسم شده است. دایره سفید به این معناست که بیت کنترلی مربوطه با مقدارِ ۰ فعال می شود.

۳ بهینه بودن آلگوریتم گرور

. فرض کنید که آلگوریتم جستجو را به شکل زیر تغییردهیم. حالت اولیه رایک حالت دلخواه مثل $|\psi(۰)\rangle$ می گیریم که دیگر یک حالت یکنواخت نیست. عملگرگرور را نیز درمرحله t ام با $G_t := K_t U_f$ نشان می دهیم. طبیعی است که از خواندن تابع درهرمرحله گریزی نیست و بنابراین U_f همچنان بخش اول عملگر گرور را تشکیل می دهد اما بخش دوم آن بجای انعکاس حول متوسط با یک عملگر مناسب دیگر مثل K_t که درهرمرحله نیز می تواند متفاوت بامرحله قبل باشد تشکیل شده است. می خواهیم نشان دهیم که با عوض کردن حالت یکنواخت اولیه و هم چنین عملگر گرور با یک عملگر دیگر نمی توان جستجو را به صورت بهتری انجام داد. هرگاه عملگرهای گرور را T بار روی حالت اولیه اثر دهیم خواهیم داشت :

$$\begin{aligned} |\psi_w(T)\rangle &= G_T G_{T-۱} G_۳ G_۲ G_۱ |\psi(۰)\rangle \\ &= K_T U_f K_{T-۱} U_f \cdots K_۳ U_f K_۲ U_f K_۱ U_f |\psi(۰)\rangle \end{aligned} \qquad (۲۹)$$

دلیل این که حالت سمت چپ را با $|\psi_w(T)\rangle$ نشان داده ایم این است که این حالت قرار است به حالت $|w\rangle$ نزدیک شود. برای ادامه کار احتیاج به چند لم و قضیه احتیاج داریم.

■ **قضیه:** قرار می دهیم

$$|\psi(T)\rangle := K_T K_{T-۱} \cdots K_۲ K_۱ |\psi(۰)\rangle. \qquad (۳۰)$$

این حالت حالتی است که بعد از T با ر عمل اپراتورهای K_i بدست می آید بدون این که در هیچ مرحله ای تابع U_f فراخوانی شده باشد. می خواهیم ثابت کنیم که

$$\| \, |\psi_w(T)\rangle - |\psi(T)\rangle \, \|^۲ \leq ۴ \left(\sum_{t=۰}^{T-۱} |\langle w|\psi(t)\rangle| \right)^۲ . \qquad (۳۱)$$

به عبارت دیگر داریم:

$$\begin{aligned} \| \, |\psi_w(۱)|\rangle - |\psi(۱)\rangle \, \| &\leq ۲ \, (|\langle w|\psi(۰)\rangle|) \\ \| \, |\psi_w(۲)|\rangle - |\psi(۲)\rangle \, \| &\leq ۲ \, (|\langle w|\psi(۰)\rangle| + |\langle w|\psi(۱)\rangle|) \end{aligned}$$

$$\| |\psi_w(۳)\rangle - |\psi(۳)\rangle \| \leq ۲ (|\langle w|\psi(۰)\rangle| + |\langle w|\psi(۱)\rangle| + |\langle w|\psi(۲)\rangle|)$$
$$\cdots \qquad \cdots \tag{۳۲}$$

■ **اثبات:** برای فهم این قضیه کافی است که چند حالت ساده را بررسی کنیم تا به یک نظم کلی دست پیداکنیم.

به ازای $T = ۱$ داریم :

(۳۳)

$$\| |\psi_w(۱)\rangle - |\psi(۱)\rangle \| = \| K_۱U_f|\psi(۰)\rangle - K_۱|\psi(۰)\rangle \| = \| (U_f - I)|\psi(۰)\rangle \| = \| ۲|w\rangle\langle w|\psi(۰)\rangle \| = ۲|\langle w|\psi(۰)\rangle|,$$

که درآن از یکانی بودن عملگر $K_۱$ وهم چنین تساوی $U_f = I - ۲|w\rangle\langle w|$ استفاده کرده ایم .

به ازای $T = ۲$ بدست می آوریم:

$$\| |\psi_w(۲)\rangle - |\psi(۲)\rangle \| = \| K_۲U_fK_۱U_f|\psi(۰)\rangle - K_۲K_۱|\psi(۰)\rangle \| = \| U_fK_۱U_f|\psi(۰)\rangle - K_۱|\psi(۰)\rangle \|, \tag{۳۴}$$

که در آن از یکانی بودن $K_۲$ استفاده کرده ایم.

حال یک جمله مناسب به جمله داخل $\| \quad \|$ اضافه و کم می کنیم و از نامساوی $\| a + b \| \leq \| a \| + \| b \|$ استفاده کرده و بدست می آوریم:

$$\| |\psi_w(۲)\rangle - |\psi(۲)\rangle \| \leq \| U_fK_۱U_f|\psi(۰)\rangle - U_fK_۱|\psi(۰)\rangle \| + \| U_fK_۱|\psi(۰)\rangle - K_۱|\psi(۰)\rangle \| . \tag{۳۵}$$

حال در طرف راست این نامساوی از یکانی بودن U_f و $U_fK_۱$ و اینکه یک عملگر یکانی نرم بردارها را تغییر نمی دهد استفاده می کنیم و بدست می آوریم

$$\begin{aligned} \| |\psi_w(۲)\rangle - |\psi(۲)\rangle \| &\leq \| U_f|\psi(۰)\rangle - |\psi(۰)\rangle \| + \| U_fK_۱|\psi(۰)\rangle - K_۱|\psi(۰)\rangle \| \\ &= \| (U_f - I)|\psi(۰)\rangle \| + \| (U_f - I)K_۱|\psi(۰)\rangle \| . \end{aligned} \tag{۳۶}$$

حال از این که $U_f - I = -۲|w\rangle\langle w|$ استفاده کرده و نامساوی بالا را به شکل زیر می نویسیم:

$$\| |\psi_w(۲)\rangle - |\psi(۲)\rangle \| \leq ۲ \| |w\rangle\langle w||\psi(۰)\rangle \| + ۲ \| |w\rangle\langle w|K_۱|\psi(۰)\rangle \|$$

$$= \quad ۲|\langle w|\psi(۰)\rangle| + ۲|\langle w|\psi(۱)\rangle| \qquad (۳۷)$$

باتکراراین استدلال برای T دلخواه رابطه (۳۱) ثابت می شود.

■ تمرین: نامساوی (۳۱) را برای $T = ۳$ ثابت کنید.

حال به لم زیر توجه می کنیم:

■ **لم ۱:** هرگاه $a_۱$ تا a_N اعداد مثبت باشند آنگاه

$$(a_۱ + a_۲ + \cdots a_N)^۲ \leq N(a_۱^۲ + a_۲^۲ + \cdots a_N^۲). \qquad (۳۸)$$

اثبات: این نامساوی چیزی نیست جز نامساوی کوشی شوارتز برای دو بردار $u = (a_۱, a_۲, \cdots a_N)$ و $v = (۱, ۱, \cdots ۱)$.

با استفاده از این لم می توانیم نامساوی (۳۱) را به صورت زیر بنویسیم:

$$| \, |\psi_w(T)\rangle - |\psi(T)\rangle \, |^۲ \leq ۴T \left(\sum_{t=۰}^{T-۱} |\langle w|\psi_w(t)\rangle|^۲ \right). \qquad (۳۹)$$

دقت کنید که نامساوی (۴۰) قرار است برای هر کدام از w ها به طور جداگانه برقرار باشد به این معنی که ممکن است داده مورد نظر که در جستجوی آن هستیم هر کدام از حالت های $|۱\rangle$ تا $|N\rangle$ باشد . این حالت ها همه برهم عمود بوده و یک پایه کامل تشکیل می دهند بنابراین می توانیم طرفین رابطه (۴۰) را روی w ها جمع بزنیم و بدست آوریم:

$$\begin{aligned} \sum_w \| \, |\psi_w(T)\rangle - |\psi(T)\rangle \, \|^۲ &\leq ۴T \sum_w \sum_{t=۰}^{T-۱} |\langle w|\psi(t)\rangle|^۲ \\ &= ۴T \sum_{t=۰}^{T} \sum_w |\langle w|\psi(t)\rangle|^۲ = ۴T \sum_{t=۰}^{T} \langle \psi(t)|\psi(t)\rangle = \sum_{t=۰}^{T-۱} ۱ = ۴T^۲ \end{aligned} \qquad (۴۰)$$

بنابراین تا کنون بدست آورده ایم که

$$\sum_w \| \, |\psi_w(T)\rangle - |\psi(T)\rangle \, \|^۲ \leq ۴T^۲. \qquad (۴۱)$$

بقیه استدلال این است که نشان دهیم طرف چپ نامساوی بالا از $۲N - ۲\sqrt{N}$ بزرگ تر است که به معنای آن است که تعداد دفعات خواندن تابع یعنی T حتما در نامساوی زیر صدق می کند

$$۲N - ۲\sqrt{N} \leq ۴T^{۲}. \tag{۴۲}$$

این همان چیزی است که می خواستیم به آن برسیم . در واقع در حد N های بزرگ که $\sqrt{N}$ در مقابل N کوچک است بدست می آوریم که

$$\sqrt{\frac{N}{۲}} \leq T.$$

به این ترتیب باقی می ماند که نامسای قول داده شده را ثابت کنیم. این نامساوی چیزی نیست جز یک تمرین ساده در جبر خطی که در پایان به آن می پردازیم.

■ **لم ۲:** هرگاه یک مجموعه بردار های متعامد یکه مثل $\{|u_۱\rangle, |u_۲\rangle, \cdots |u_N\rangle\}$ داشته باشیم آنگاه به ازای هربرداریکه دیگر مثل $|Y\rangle$ نامساوی زیر برقراراست :

$$\sum_{i=۱}^{N}(\langle u_i|Y\rangle + \langle Y|u_i\rangle) \leq ۲\sqrt{N}. \tag{۴۳}$$

اثبات: کافی است که برداریکه زیر را تعریف کنیم:

$$|s\rangle := \frac{۱}{\sqrt{N}}(|u_۱\rangle + |u_۲\rangle + \cdots |u_N\rangle), \tag{۴۴}$$

ونامساوی کوشی شوارتز را برای این بردار و بردار $|Y\rangle$ بنویسیم. بدست می آوریم

$$|\langle Y|u_۱\rangle + \langle Y|u_۲\rangle + \cdots \langle Y|u_N\rangle| \leq \sqrt{N}. \tag{۴۵}$$

امامی دانیم که برای هر عدد مختلط a

$$a + a^* = ۲\ Re(a) \leq ۲|a|, \tag{۴۶}$$

بنابراین با ترکیب این نامساوی با نامساوی قبلی یعنی (۴۵) به رابطه‌ی ۴۳ می رسیم.

■ تمرین: از ترکیب این دو نامساوی واقعا نشان دهید که رابطه (۴۳) بدست می آید. سپس نشان دهید که این نامساوی را به شکل زیر نیز می توان نوشت:

$$\sum_{i=1}^{N} |||u_i\rangle - |Y\rangle||^2 \geq 2N - 2\sqrt{N}. \qquad (47)$$