درس دهم : آلگوریتم های کوانتومی جستجو

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.

۱ جستجو در داده های نامنظم

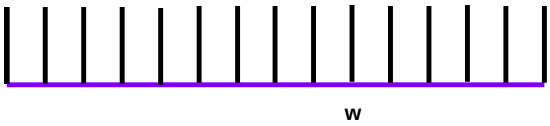
نخست دقت می کنیم که تابع f دریک مدار کوانتومی بصورت عملگر کوانتومی یکانی زیر نشان داده می شود:

$$U_f|x_i, y\rangle = |x_i, f(x_i) \oplus y\rangle. \tag{1}$$

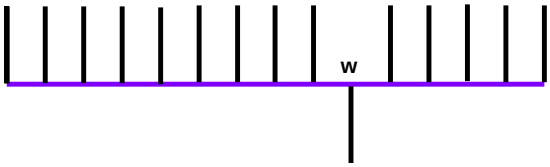
هرگاه این عملگر را روی ورودی $|x_i\rangle \otimes |-\rangle$ اثر دهیم که درآن $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$، آنگاه براحتی دیده می شود که

$$\begin{aligned} U_f|w\rangle \otimes |-\rangle &= -|w\rangle \otimes |-\rangle \\ U_f|x_i\rangle \otimes |-\rangle &= |w\rangle \otimes |-\rangle \qquad x_i \neq w. \end{aligned} \tag{2}$$

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



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 .

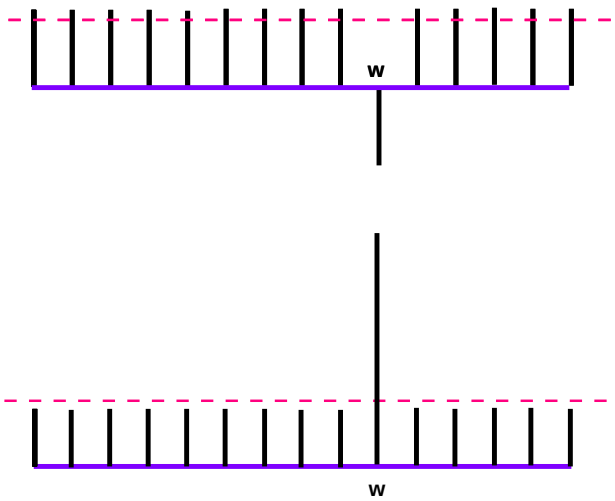
سادگی حذف می کنیم. درنتیجه می توان عملگر U_f را به شکل زیرنوشت :

$$U_f = I - 2|w\rangle\langle w|. \tag{3}$$

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.
حال فرض کنید که عملگر U_f را روی حالت

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

اثر دهیم. نخست آلگوریتم گرور را به طور کیفی توضیح می دهیم. هرگاه حالت فوق رابه شکل ۱ نشان دهیم بعداز اثر عملگر U_f به شکل ۲ 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 ۳ 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



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.

درنتیجه اندازه گیری چنین حالتی به احتمال زیاد، نتیجه اش $|w\rangle$ خواهد بود. البته پس از هرباراندازه 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 نشان می دهیم که عملگر I_s را می توان به صورت زیر نوشت :

$$I_s = I - 2|s\rangle\langle s|, \tag{5}$$

که درآن $|s\rangle$ همان حالت 4 است. برای این کار I_s را روی یک حالت دلخواه مثل x_j اثر می دهیم. باتوجه به تساوی $\langle s|x_j\rangle = \frac{1}{\sqrt{N}}$، خواهیم داشت :

$$I_s|x_j\rangle = |x_j\rangle - 2\frac{1}{\sqrt{N}}|s\rangle = |x_j\rangle - \frac{2}{\sqrt{N}}|s\rangle. \tag{6}$$

حال اگر عملگر I_s را روی $|\psi\rangle = \sum_i a_i|x_i\rangle$ اثر دهیم نتیجه عبارت خواهد بود از:

$$I_s|\psi\rangle = \sum_i a_i(|x_\rangle - \frac{2}{\sqrt{N}}|s\rangle) = \sum_i a_i|x_i\rangle - 2\overline{a}|s\rangle \tag{7}$$

که درآن $\overline{a} := \frac{1}{N}(a_1 + a_2 + \cdots a_N)$ متوسط دامنه های حالت $|\psi\rangle$ است. حالت فوق را می توان به شکل زیر نوشت:

$$I_s|\psi\rangle = \sum_i (a_i - 2\overline{a})|x_i\rangle =: \sum_i \tilde{a_i}|x_i\rangle. \tag{8}$$

که درآن $\tilde{a_i} = a_i - 2\overline{a}$ به معنای آن است که دامنه a_i حول مقدار متوسط دامنه ها یعنی $\overline{a}$ انعکاس یافته است.

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 :

$$|r\rangle = \frac{1}{\sqrt{N-1}}(\sum_{x_i \neq w} |x_i\rangle). \tag{9}$$

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:

$$|w\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad , \qquad |r\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{10}$$

و

$$|s\rangle = \frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|r\rangle = \begin{pmatrix} \frac{1}{\sqrt{N}} \\ \sqrt{\frac{N-1}{N}} \end{pmatrix}. \tag{11}$$

درنتیجه خوا هیم داشت :

$$U_f = I - 2|w\rangle\langle w| = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{12}$$

و

$$I_s = I - 2|s\rangle\langle s| = \begin{pmatrix} 1 - \frac{2}{N} & -\frac{2}{N}\sqrt{N-1} \\ -\frac{2}{N}\sqrt{N-1} & -1 + \frac{2}{N} \end{pmatrix} \tag{13}$$

درنتیجه عملگر گرور به شکل زیر درخواهد آمد:

$$G = -I_s U_f = \begin{pmatrix} 1 - \frac{2}{N} & \frac{2}{N}\sqrt{N-1} \\ -\frac{2}{N}\sqrt{N-1} & 1 - \frac{2}{N} \end{pmatrix}. \tag{14}$$

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:

$$\cos\theta = 1 - \frac{2}{N}, \sin\theta = \frac{2}{N}\sqrt{N-1}, \tag{15}$$

و به این ترتیب عملگرگرور به شکل زیر درخواهد آمد:

$$G = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{16}$$

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:

$$\langle w|G^m|s\rangle = \frac{1}{\sqrt{N}}\cos m\theta + \sqrt{\frac{N-1}{N}}\sin m\theta. \tag{17}$$

اگر قرار دهیم

$$\cos\alpha = \frac{1}{\sqrt{N}} \qquad , \qquad \sin\alpha = \sqrt{\frac{N-1}{N}} \tag{18}$$

آنگاه خواهیم داشت :

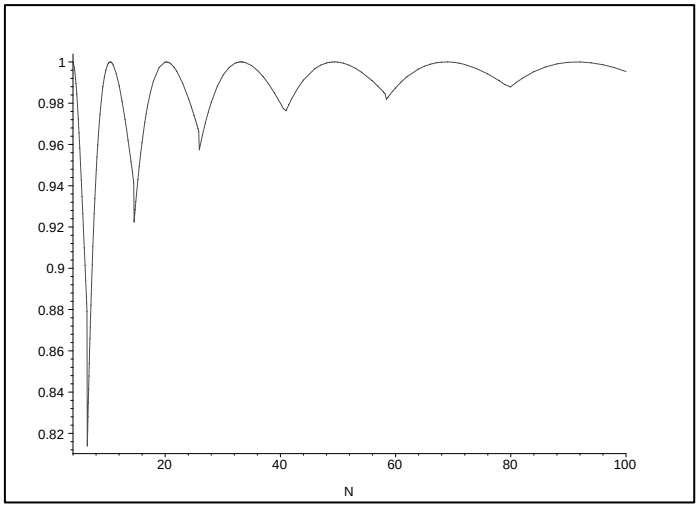
$$\langle w|G^m|s\rangle = \cos(m\theta - \alpha). \tag{19}$$

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 $N = 4$ باشد. دراین حالت داریم $\cos\theta = \frac{1}{2}$ و $\cos\alpha = \frac{1}{2}$ و یا

$$\alpha = \frac{\pi}{3}, \qquad \theta = \frac{\pi}{3}, \longrightarrow m = 1 \tag{20}$$

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

$$\alpha \approx \frac{\pi}{2}, \qquad \cos\theta \approx 1 - \frac{\theta^2}{2} = 1 - \frac{2}{N}, \longrightarrow \theta = \frac{2}{\sqrt{N}}, \tag{21}$$



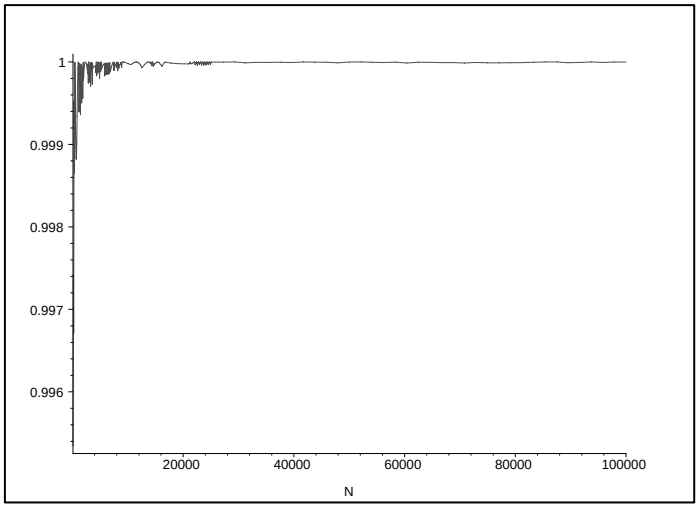
شکل ۴: احتمال یافتن یک شی دربین N با استفاده از آلگوریتم گرور به عنوان تابعی از N برای $4 \leq N \leq 100$.

ودرنتیجه $m \approx \frac{\pi}{4}\sqrt{N}$. 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 $[\frac{\pi}{4}\sqrt{N}]$ را درعبارت 19 قراردهیم. این احتمال برابراست با:

$$P(N) := \cos^2([\frac{\pi}{4}\sqrt{N}]\cos^{-1}(1-\frac{2}{N}) - \cos^{-1}(\frac{1}{\sqrt{N}})). \tag{22}$$

شکل های ۴ و ۵ این تابع را برحسب N ، نشان می دهد.

هرگاه تعداد عناصر مطلوب بیش از یکی مثلاً l تا باشد، اصلاح کوچکی دراستدلال بالا نشان می دهد که می توان درزمانی از مرتبه $O(\frac{\pi}{4}\sqrt{\frac{N}{l}})$ به یکی از عناصر مطلوب دست یافت. اثبات دقیق این امر را به عنوان یک تمرین به عهده خواننده می گذاریم.



شکل ۵: احتمال یافتن یک شی دربین N با استفاده از آلگوریتم گرور به عنوان تابعی از N برای $100 \leq N \leq 100000$.

۱.۱ 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 $I_s = I - 2|s\rangle\langle s|$. ازطرفی می دانیم که

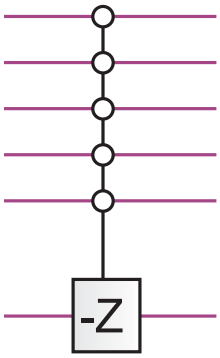
$$|s\rangle = H^{\otimes N}|0, 0, \cdots 0\rangle =: H^{\otimes N}|\overline{0}\rangle, \tag{23}$$

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

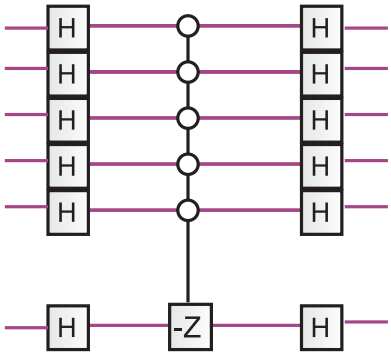
$$I_s = H^{\otimes N} I_0 H^{\otimes N} \tag{24}$$

که درآن $I_0 = I - 2|\overline{0}\rangle\langle\overline{0}|$. بنابراین هرگاه که مدارِ I_0 را بسازیم می توانیم از روی آن مدار I_s را بسازیم. راه ساختن مدارِ I_0 آن است که به شکل ماتریسی آن توجه کنیم. به عنوان مثال برای سه تا کیوبیت I_0 به صورت زیر عمل می کند:

$$\begin{aligned} I_0|000\rangle &= -|000\rangle \\ I_0|001\rangle &= |001\rangle \\ I_0|010\rangle &= |010\rangle \\ &\cdots \end{aligned} \tag{25}$$



شکل ٦: مدار عملگرِ I_0.



شکل ٧: مدار عملگرِ I_s.

پس معلوم است که I_0 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 ٦ و ٧ رسم شده است. دایره سفید به این معناست که بیت کنترلی مربوطه با مقدارِ 0 فعال می شود.

٢.١ عدم حساسیت آلگوریتم نسبته به حالت اولیه

اغلب اوقات اتفاق می افتد که یک حالت مطلوب که برای منظور خاصی تهیه شده است دچار خطاهای کوچکی شده واز شکل اولیه خود فاصله گرفته است. به عنوان مثال حالت $|s\rangle$ درآلگوریتم گرورممکن است با آن دقت دردسترس نباشد. می توان پرسید که اگر به جای حالت $|s\rangle$ آلگوریتم گرور را با حالتی نزدیک به آن شروع کنیم چه اتفاقی می افتد و چقدر به کیفیت این

آلگوریتم آسیب می رسد. برای بررسی این موضوع فرض کنید که حالت مورد استفاده ما، حالت بهنجار زیراست :

$$|\tilde{s}\rangle = \sum_{i1}^{N} a_i |x_i\rangle, \tag{26}$$

که درآن $\sum_{i=1}^{N} |a_i|^2 = 1$. دراین صورت بازهم آلگوریتم را مثل گذشته طی می کنیم با این تفاوت که حالت $|r\rangle$ اکنون عبارت است از:

$$|r\rangle = \frac{1}{\sqrt{1-|a_w|^2}} \sum_{x_i \neq w} a_i |x_i\rangle. \tag{27}$$

طبیعی است که بازهم $\langle r|w\rangle = 0$. با همان نمایش دومولفه ای که دربخش قبلی برای بردارهای $|w\rangle$ و $|r\rangle$ داشتیم بردار حالت $|\tilde{s}\rangle$ به شکل زیر درخواهد آمد:

$$|\tilde{s}\rangle = \begin{pmatrix} a_w \\ \sqrt{1-|a_w|^2} \end{pmatrix}, \tag{28}$$

و درنتیجه خواهیم داشت

$$I_{\tilde{s}} = I - 2|s\rangle\langle s| = \begin{pmatrix} 1-2|a_w|^2 & -2a_w\sqrt{1-|a_w|^2} \\ -2{a_w}^*\sqrt{1-|a_w|^2} - \frac{2}{N}\sqrt{N-1} & 2|a_w|^2 - 1 \end{pmatrix}, \tag{29}$$

و ازآنجا عملگر گرور به شکل زیردرخواهد آمد:

$$G = -I_{\tilde{s}} U_f = \begin{pmatrix} 1-2|a_w|^2 & 2a_w\sqrt{1-|a_w|^2} \\ -2{a_w}^*\sqrt{1-|a_w|^2} - \frac{2}{N}\sqrt{N-1} & 1-2|a_w|^2 \end{pmatrix}. \tag{30}$$

این عملگر یک عملگر یکانی است ومی توان آن را به شکل زیر پارامتربندی کرد:

$$G = \begin{pmatrix} \cos\theta & \sin\theta e^{i\phi} \\ -\sin\theta e^{-i\phi} & \cos\theta \end{pmatrix}, \tag{31}$$

که درآن

$$\begin{aligned} \cos\theta &= 1-2|a_w|^2 \\ , a_w &= |a_w| e^{i\phi}. \end{aligned} \tag{32}$$

براحتی می توان دریافت که

$$G^m = \begin{pmatrix} \cos m\theta & \sin m\theta e^{i\phi} \\ -\sin m\theta e^{-i\phi} & \cos m\theta \end{pmatrix}, \tag{33}$$

و درنتیجه

$$\langle w|G^m|\tilde{s}\rangle = a_w \cos m\theta + \sqrt{1-|a_w|^2}e^{i\phi}\sin m\theta. \tag{34}$$

و باتوجه به ا ینکه $a_w = |a_w|e^{i\phi}$ ،

$$\langle w|G^m|\tilde{s}\rangle = e^{i\phi}\left(|a_w|\cos m\theta + \sqrt{1-|a_w|^2}\sin m\theta\right). \tag{35}$$

حال اگر قرار دهیم $|a_w| = \cos\alpha$، بدست می آوریم :

$$P_m = |\langle w|G^m|\tilde{s}\rangle|^2 = \cos^2(m\theta - \alpha). \tag{36}$$

از این رابطه می توان فهمید که تعداد دفعات لازم برای نزدیک شدن P_m به یک برابراست با $m \approx \frac{\alpha}{\theta}$. امااز‌آنجاییکه حالت $|\tilde{s}\rangle$ تنها تفاوت کمی با حالت $|s\rangle$ دارد همه دامنه های a_{x_i} ازجمله a_w اندازه ای درحدود $\frac{1}{\sqrt{N}}$ دارند. درنتیجه بقیه استدلال درست مثل همان حالت قبل پیش می رود یعنی این که

$$m \approx \frac{\pi}{4}\sqrt{N}. \tag{37}$$

۳.۱ بهینه بودن آلگوریتم گرور

. فرض کنید که آلگوریتم جستجو را به شکل زیر تغییردهیم. حالت اولیه رایک حالت دلخواه مثل $|\psi_0\rangle$ می گیریم و 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. هرگاه عملگرهای گرور را T بار روی حالت اولیه اثر دهیم خواهیم داشت :

$$\begin{aligned} |\psi_{w(T)}\rangle &= G_T G_{T-1}\cdots G_3 G_2 G_1|\psi_0\rangle \\ &= K_T U_f K_{T-1} U_f \cdots K_3 U_f K_2 U_f K_1 U_f|\psi_0\rangle \end{aligned} \tag{38}$$

قضیه: هرگاه قراردهیم

$$|\phi_T\rangle := K_T K_{T-1}\cdots K_2 K_1|\psi(0)\rangle \tag{39}$$

آنگاه

$$\| \, |\psi_{w(T)}\rangle - |\phi\rangle \, \|^2 \leq 4 \left(\sum_{t=1}^{T} |\langle w|\psi_{w(t)}\rangle| \right)^2 . \tag{40}$$

اثبات: برای فهم این قضیه کافی است که چند حالت ساده را بررسی کنیم تا به یک نظم کلی دست پیداکنیم.
به ازای $T = 1$ داریم :

$$\| \, |\psi_{w(1)}\rangle - |\phi_1\rangle \, \| = \| \, K_1 U_f |\psi(0)\rangle - K_1 |\psi(0)\rangle \, \| = \| \, (U_f - I)|\psi(0)\rangle \, \| = \| \, 2|w\rangle\langle w|\psi(0)\rangle \, \| = 2|\langle w|\psi(0)\rangle|, \tag{41}$$

که درآن از یکانی بودن عملگر K_1 وهم چنین تساوی $U_f = I - 2|w\rangle\langle w|$ استفاده کرده ایم.
به ازای $T = 2$ بدست می آوریم:

$$\begin{aligned} & \| \, |\psi_{w(2)}\rangle - |\phi_2\rangle \, \| = \| \, K_2 U_f K_1 U_f |\psi(0)\rangle - K_2 K_1 |\psi(0)\rangle \, \| = \| \, U_f K_1 U_f |\psi(0)\rangle - K_1 |\psi(0)\rangle \, \| \\ \leq \; & \| \, U_f K_1 U_f |\psi(0)\rangle - K_1 U_f |\psi(0)\rangle \, \| + \| \, K_1 U_f |\psi(0)\rangle - K_1 |\psi(0)\rangle \, \| = \| \, (U_f - I)|\chi\rangle \, \| + \| \, (U_f - I)|\psi(0)\rangle \, \| \end{aligned}$$

که درآن $|\chi\rangle = K_1 U_f |\psi(0)\rangle$. حال می توان طرف راست تساوی آخر را به شکل زیر نوشت :

$$\begin{aligned} & \| \, (U_f - I)|\chi\rangle \, \| + \| \, (U_f - I)|\psi(0)\rangle \, \| = 2|\langle w|\chi\rangle| + 2|\langle w|\psi(0)\rangle| \\ = \; & 2|\langle w|K_1 U_f|\psi(0)\rangle| + 2|\langle w|\psi(0)\rangle| \\ = \; & 2|\langle w|\psi(1)\rangle| + 2|\langle w|\psi(0)\rangle|. \end{aligned} \tag{42}$$

باتکراراین استدلال برای T دلخواه بدست می آوریم:

$$\| \, |\psi_{w(T)}\rangle - |\phi\rangle \, \| \leq 2 \left(\sum_{t=1}^{T} |\langle w|\psi_{w(t)}\rangle| \right), \tag{43}$$

و ازآنجا به رابطه 40 می رسیم .

حال به یک نکته توجه می کنیم و آن اینکه اگر انتظار داشته باشیم که $|\psi_w(T)\rangle$ ها به ازای w های مختلف از یک دیگر تمیز پذیر باشند می بایست تشکیل یک پایه متعامد بدهند. (این نیاز از آنجا ناشی می شود که ما می خواهیم آلگوریتم گرور بتواند اشیای مختلف را پیدا کند.) از این خاصیت بعداً استفاده های مهمی خواهیم کرد. برای ادامه کار به دو لِم احتیاج داریم.

لم ۱ : هرگاه a_1 تا a_N اعداد مثبت باشند آنگاه

$$(a_1 + a_2 + \cdots a_N)^2 \leq N(a_1^2 + a_2^2 + \cdots a_N^2). \tag{44}$$

اثبات: این نامساوی چیزی نیست جز نامساوی کوشی شوارتز برای دو بردار $u = (a_1, a_2, \cdots a_N)$ و $v = (1, 1, \cdots 1)$.

لم ۲: هرگاه یک مجموعه بردار های متعامد یکه مثل $\{|u_1\rangle, |u_2\rangle, \cdots |u_N\rangle\}$ داشته باشیم آنگاه به ازای هربرداریکه دیگر مثل $|v\rangle$ نامساوی زیر برقراراست :

$$\sum_{i=1}^{N}(\langle u_i|v\rangle + \langle v|u_i\rangle) \leq 2\sqrt{N}. \tag{45}$$

اثبات: کافی است که برداریکه زیر را تعریف کنیم:

$$|s\rangle := \frac{1}{\sqrt{N}}(|u_1\rangle + |u_2\rangle + \cdots |u_N\rangle), \tag{46}$$

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

$$|\langle v|u_1\rangle + \langle v|u_2\rangle + \cdots \langle v|u_N\rangle| \leq \sqrt{N}. \tag{47}$$

امامی دانیم که برای هر عدد مختلط a

$$a + a^* = 2\ Re(a) \leq 2|a|, \tag{48}$$

بنابراین با ترکیب این نامساوی با نامساوی قبلی به رابطه‌ی 45 می رسیم. این لم را به شکل زیر نیز می توان بازنویسی کرد:

$$\sum_{i=1}^{N} |||u_i\rangle - |v\rangle||^2 \geq 2N - 2\sqrt{N}. \tag{49}$$

ادامه دارد.....
