الگوریتم جستجوی گراور [۱]

عباس محرابیان[۲]

۱ مقدمه

فرض کنید مسابقه‌ای به شکل زیر برگزار می‌شود: صد بستهٔ دربسته روبروی شما قرار دارد که نودونه‌تای آن‌ها پوچ هستند و در یکی از آن‌ها جایزه‌ای به ارزش ۲۵هزار تومان قرار دارد. شما می‌توانید هر بسته را با پرداخت هزار تومان باز کنید، و اگر جایزه در آن بود، آن را بردارید. آیا شما در این مسابقه شرکت می‌کنید؟ پس از اندکی تأمل می‌بینید که به نفع شما نیست که در این مسابقه شرکت کنید. گراور [۲] یک ریاضی‌دان هندی است که نشان داد در دنیای الگوریتم‌های کوانتوم، به نفع شماست که در این مسابقه شرکت کنید! او در حقیقت الگوریتمی کوانتومی ارائه داد که با خرج کردن حدود ۱۰هزار تومان می‌تواند بسته‌ای را که جایزه در آن است پیدا کند. در این مقاله الگوریتم جستجوی گراور را توضیح می‌دهیم، که یک الگوریتم کوانتومی[۳] است. در نیمهٔ نخست مقاله توضیحات کلی دربارهٔ الگوریتم‌های کوانتومی می‌دهیم بدون این که وارد جزئیات مربوط به نحوهٔ پیاده‌سازی آن‌ها و مباحث مکانیک کوانتومی شویم، و در نیمهٔ دوم الگوریتم گراور را توضیح می‌دهیم.

۲ الگوریتم‌های کوانتومی

در ادامه منظور از الگوریتمی *متعارف*، الگوریتمی غیرکوانتومی است. همان‌طور که در الگوریتم‌های متعارف، بیت‌ها واحدهای اطلاعاتی هستند، در الگوریتم‌های کوانتومی، کیوبیت‌ها[۴] واحدهای اطلاعاتی هستند. محتوای هر بیت می‌تواند یکی از دو عضو مجموعهٔ $\{۰,۱\}$ باشد. محتوای یک کیوبیت می‌تواند هر عضوی از مجموعهٔ

$$Q_۱ = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^۲ : |a|^۲ + |b|^۲ = ۱ \right\}$$

باشد. در فضاهای برداری که در این مقاله و به طور کلی در الگوریتم‌های کوانتوم با آن‌ها سروکار داریم، میدان همیشه مجموعهٔ اعداد مختلط است. نمادهای مخصوصی برای نشان دادن اعضای پایهٔ استاندارد $\mathbb{C}^۲$ وجود دارد: $\begin{pmatrix} ۱ \\ ۰ \end{pmatrix}$ را با $|۰\rangle$ و $\begin{pmatrix} ۰ \\ ۱ \end{pmatrix}$ را با $|۱\rangle$ نشان می‌دهیم. نمادهای $\langle$ و $|$ در این‌جا فقط مشخص می‌کنند که با یک عضو $Q_۱$ سروکار داریم که به شکل یک بردار ستونی است. در ابتدای یک الگوریتم، می‌توان هر یک از کیوبیت‌ها را با یکی از دو مقدار $|۰\rangle$ یا $|۱\rangle$ مقداردهی اولیه کرد.

یک الگوریتم متعارف را می‌توان به شکل یک مدار منطقی نشان داد که از تعدادی گیت[۵] مانند not، and، و or تشکیل شده است. ورودی هر گیت یک یا دو بیت و خروجی آن هم یک بیت است. الگوریتم‌های کوانتومی را هم می‌توان به همین صورت نشان داد. دو نوع گیت کوانتومی وجود دارد: نوع اول در ساده‌ترین حالت یک کیوبیت ورودی و یک کیوبیت خروجی دارد. فرض کنید U یک عملگر یکه[۶] دلخواه روی فضای برداری $\mathbb{C}^۲$ باشد. در این صورت می‌توان یک گیت کوانتومی متناظر با U در نظر گرفت که برای هر ورودی $|q\rangle \in Q_۱$، خروجی آن $U|q\rangle$ می‌باشد. توجه کنید که بی‌نهایت گونه گیت کوانتومی از نوع اول داریم.

نوع دوم، گیت *اندازه‌گیری*[۷] نام دارد، که ورودی آن یک کیوبیت و خروجی آن یک بیت است. فرض کنیم یک کیوبیت داریم که در حالت

$$\begin{pmatrix} a \\ b \end{pmatrix} = a\,|۰\rangle + b\,|۱\rangle$$

قرار دارد. اگر این کیوبیت به یک گیت اندازه‌گیری وارد شود، خروجی آن به احتمال $|a|^۲$ مقدار ۰ و به احتمال $|b|^۲$ مقدار ۱ خواهد داشت. وقتی می‌گوییم یک کیوبیت را اندازه‌گیری می‌کنیم، منظور این است که یک گیت اندازه‌گیری سر راه آن قرار می‌دهیم. توجه کنید که فقط یک گونه گیت کوانتومی از نوع دوم داریم.

ضرب تانسوری[۸] دو ماتریس را با نماد $\otimes$ نشان می‌دهیم؛ مثلاً داریم

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

---

۱ Grover's search algorithm

۲ نگارنده در سال ۱۳۸۸ مدرک کارشناسی خود را در دو رشته مهندسی کامپیوتر و ریاضیات از دانشگاه صنعتی شریف اخذ نمود و در حال حاضر دانشجوی دکتری دانشگاه واترلوی کاناداست. نشانی ای‌میل: amehrabi@uwaterloo.ca.

۳ quantum algorithm

۴ qubits

۵ gate

۶ unitary operator

۷ measurement gate

۸ tensor product

یک n–کیوبیت واحد اطلاعاتی بزرگ‌تری است که محتوای آن عضوی از مجموعهٔ

$$Q_n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{2^n} \end{pmatrix} \in \mathbb{C}^{2^n} : |x_1|^2 + |x_2|^2 + \cdots + |x_{2^n}|^2 = 1 \right\}$$

است. دقت کنید که در حقیقت، یک کیوبیت یک ۱–کیوبیت است (و از نظر فیزیکی، یک n–کیوبیت چیزی نیست جز n کیوبیت خاص و شماره‌گذاری‌شده که به صورت قراردادی به آن‌ها به شکل یک گروه منسجم نگاه می‌شود). فرض کنید n کیوبیت داشته باشیم که دارای مقادیر $|q_1\rangle, |q_2\rangle, \ldots, |q_n\rangle$ باشند. در این صورت از کنار هم قرار دادن این کیوبیت‌ها یک n–کیوبیت به دست می‌آید که محتوای آن $|q_1\rangle \otimes |q_2\rangle \otimes \cdots \otimes |q_n\rangle$ است که به اختصار آن را با $|q_1 q_2 \ldots q_n\rangle$ نشان می‌دهیم. این نمادگذاری نتیجهٔ جالبی دارد. هر عدد صحیح مانند m بین ۰ و $2^n - 1$ را می‌توان به صورت یک رشته به طول n از ۰ها و ۱ها نمایش داد (که نمایش دودویی خوانده می‌شود) که آن را با $b(m)$ نشان می‌دهیم. در این صورت می‌توان وارسی کرد که $\{|b(i)\rangle : 0 \le i \le 2^n - 1\}$ همان پایهٔ استاندارد $\mathbb{C}^{2^n}$ است. مثلاً $\{|111\rangle, |110\rangle, |101\rangle, |100\rangle, |011\rangle, |010\rangle, |001\rangle, |000\rangle\}$ پایهٔ استاندارد $\mathbb{C}^8$ است. دقت کنید که همواره از ضرب تانسوری n کیوبیت یک n–کیوبیت به دست می‌آید، ولی یک n–کیوبیت را لزوماً نمی‌توان به صورت ضرب تانسوری n کیوبیت نوشت. این یکی از ویژگی‌های عجیب مکانیک کوانتومی است و به پدیدهٔ entanglement مرتبط است، که بحث دربارهٔ آن از حوصلهٔ این مقاله خارج است.

دو نوع گیتی که برای کیوبیت‌ها تعریف کردیم، به صورت طبیعی برای n–کیوبیت‌ها نیز قابل تعریف هستند. فرض کنید U یک عملگر یکه روی فضای برداری $\mathbb{C}^{2^n}$ باشد. در این صورت متناظر با U یک گیت کوانتومی داریم که ورودی و خروجی‌اش هر دو n–کیوبیت هستند و همانند حالت $n = 1$، برای هر ورودی $|q\rangle \in Q_n$، خروجی آن $U|q\rangle$ می‌باشد. اندازه‌گیری یک n–کیوبیت به ما n بیت می‌دهد. فرض کنید $|q\rangle$ یک n–کیوبیت باشد که در پایهٔ استاندارد به صورت

$$|q\rangle = \sum_{i=0}^{2^n - 1} \alpha_i |b(i)\rangle$$

نمایش داده شود. در این صورت به احتمال $|\alpha_i|^2$ حاصل اندازه‌گیری $b(i)$ خواهد بود.

۳ الگوریتم جستجوی گراور

فرض کنید $f : X \to \{0,1\}$ تابعی دلخواه باشد به طوری که $f^{-1}(1)$ ناتهی است. هدف پیدا کردن عنصری در $f^{-1}(1)$ است، که مجموعهٔ *جواب‌ها* نامیده می‌شود. برای سهولت در نمادگذاری فرض می‌کنیم $X = \{0,1\}^n$. طبیعت تابع f بر الگوریتم پوشیده است و در این‌جا فرض می‌کنیم تابع f به صورت یک *جعبهٔ سیاه* به الگوریتم داده شده است و الگوریتم تنها می‌تواند مقدار تابع f را در نقاط دلخواهی از دامنه‌اش بپرسد. هدف این است که با کم‌ترین پرسش از این جعبهٔ سیاه، جوابی را پیدا کند. واضح است که هر الگوریتم متعارف برای پیدا کردن جواب در حالت کلی به $\Omega(2^n)$ پرسش نیاز دارد، ولی گراور [۲] الگوریتمی کوانتومی ارائه داد که در صورتی که تعداد جواب‌ها معلوم باشد، با $O(2^{n/2})$ پرسش از جعبهٔ سیاه، جوابی برای مسئله پیدا می‌کند.

حال توضیح می‌دهیم که جعبهٔ سیاه متناظر با f چگونه کار می‌کند. از نماد $\oplus$ برای نشان دادن xor دو عنصر در $\{0,1\}$ استفاده می‌کنیم (که همان جمع در مبنای دو است). یک گیت $(n+1)$–کیوبیتی به نام F تعریف می‌کنیم که یک عملگر یکه روی $\mathbb{C}^{2^n}$ است و نقش جعبهٔ سیاه را بازی می‌کند. برای تعریف F کافی است اثر آن را روی اعضای پایه مشخص کنیم. به ازای هر $x_1, x_2, \ldots, x_n, y \in \{0,1\}$، (۱)

$$F|x_1 x_2 \ldots x_n y\rangle = |x_1 x_2 \ldots x_n\rangle \otimes |y \oplus f(x_1, x_2, \ldots, x_n)\rangle$$

در نگاه اول ممکن است نحوهٔ کار این گیت کمی عجیب به نظر برسد. در حقیقت این گیت تنها مقدار $f(x_1, x_2, \ldots, x_n)$ را با کیوبیت آخر xor می‌کند، و از این طریق مقدار f را در این نقطه به ما می‌دهد. به یاد آورید که گیت‌های کوانتومی (به جز گیت‌های اندازه‌گیری) عملگرهای یکه هستند و لذا استفاده از گیت‌هایی مثل F به عنوان جعبهٔ سیاه در الگوریتم‌های کوانتوم اجتناب‌ناپذیر است. الگوریتم گراور از $O(2^{n/2})$ کپی از گیت F استفاده می‌کند، و به احتمال بیش از یک‌سوم جوابی برای مسئله پیدا می‌کند. (شایان ذکر است که تابع f یک تابع قطعی[۹] است و الگوریتم مورد استفاده هم عمدتاً قطعی است و تنها جایی که تصادف وارد الگوریتم می‌شود انتهای الگوریتم و موقع استفاده از گیت‌های اندازه‌گیری است.) با تکرار این الگوریتم می‌توان احتمال موفقیت را به دلخواه زیاد کرد.

اینک الگوریتم گراور را توصیف می‌کنیم. تعریف کنید $N = 2^n$

[۹] deterministic

و

$$|\mathbf{h}\rangle = \sum_{\mathbf{x}\in\{۰,۱\}^n} |\mathbf{x}\rangle / \sqrt{N}\,.$$

دقت کنید که $|\mathbf{h}\rangle \in Q_n$. بردار صفر در فضای $\mathbb{C}^{۲^n}$ را با $\mathbf{O}$ نشان می‌دهیم. گیت $(n+۱)$–کیوبیتی R را چنین تعریف می‌کنیم: به ازای یک ورودی مثل $|\mathbf{z}\rangle \in Q_n$، فرض کنیم $|\mathbf{x}\rangle \in Q_n, |y\rangle \in Q_۱$، حاصل بازتاب $|\mathbf{x}\rangle$ حول خط $\mathbf{O}\,|\mathbf{h}\rangle$ باشد (در این‌جا و در ادامهٔ مقاله، منظور از $\mathbf{O}\,|\mathbf{h}\rangle$ خط گذرنده از نقاط $\mathbf{O}, |\mathbf{h}\rangle \in \mathbb{C}^{۲^n}$ است). در این صورت،

$$R\left(|\mathbf{x}\rangle \otimes |y\rangle\right) = |\mathbf{z}\rangle \otimes |y\rangle\ . \qquad (۲)$$

تعریف کنید $|-\rangle = (|۰\rangle - |۱\rangle)/\sqrt{۲} \in Q_۱$. الگوریتم گراور از یک $(n+۱)$–کیوبیت که در حالت اولیهٔ $|\mathbf{h}\rangle \otimes |-\rangle$ است شروع می‌کند و عملگرهای F و R را یکی‌درمیان k بار روی آن اعمال می‌کند تا به حالت $(RF)^k(|\mathbf{h}\rangle \otimes |-\rangle)$ برسد. مقدار دقیق k پایین‌تر تعیین خواهد شد. الگوریتم سپس $(n+۱)$–کیوبیت حاصل را اندازه‌گیری می‌کند تا به $n+۱$ بیت $x_۱, x_۲, \ldots, x_n, y$ برسد. نشان می‌دهیم می‌توان k را طوری انتخاب کرد که $k = O(\sqrt{N})$ و به احتمال بیش از یک‌سوم داشته باشیم $f(x_۱, x_۲, \ldots, x_n) = ۱$، یعنی $(x_۱, x_۲, \ldots, x_n)$ جوابی از مسئله باشد.

حالا به تحلیل این الگوریتم می‌پردازیم. تعریف می‌کنیم

$$A = f^{-۱}(۱),\ B = f^{-۱}(۰),\ \alpha = |A|,\ \beta = |B|\,.$$

هم‌چنین تعریف می‌کنیم

$$|\mathbf{a}\rangle = \sum_{\mathbf{x}\in A} |\mathbf{x}\rangle / \sqrt{\alpha},\ |\mathbf{b}\rangle = \sum_{\mathbf{x}\in B} |\mathbf{x}\rangle / \sqrt{\beta}\,.$$

ملاحظه کنید که $|\mathbf{a}\rangle$ و $|\mathbf{b}\rangle$ دو بردار عمود بر هم و یکه در $\mathbb{C}^{۲^n}$ هستند. فرض کنید $\mathcal{S} \subseteq \mathbb{C}^{۲^n}$ زیرفضای خطی تولید شده توسط این دو بردار در $\mathbb{C}^{۲^n}$ باشد که در حقیقت یک صفحه است.

لم ۱. *فرض کنید $|\mathbf{s}\rangle, |\mathbf{t}\rangle \in \mathcal{S}$ به طوری که $|\mathbf{s}\rangle$ حاصل بازتاب $|\mathbf{t}\rangle$ حول خط $\mathbf{O}\,|\mathbf{b}\rangle$ باشد. در این صورت،*

$$F(|\mathbf{s}\rangle \otimes |-\rangle) = |\mathbf{t}\rangle \otimes |-\rangle\,.$$

اثبات. چون F عملگری خطی است، کافی است نشان دهیم تأثیر آن روی اعضای پایهٔ $\mathcal{S}$ همان تأثیر مطلوب است، یعنی کافی است نشان دهیم دو تساوی زیر برقرارند.

$$F(|\mathbf{b}\rangle \otimes |-\rangle) = |\mathbf{b}\rangle \otimes |-\rangle\ , \qquad (۳)$$

$$F(|\mathbf{a}\rangle \otimes |-\rangle) = (-|\mathbf{a}\rangle) \otimes |-\rangle\ . \qquad (۴)$$

از تعریف $|-\rangle$ و $|\mathbf{b}\rangle$ و به دلیل خطی بودن عملگر F داریم

$$\begin{aligned}\sqrt{۲\beta}F(|\mathbf{b}\rangle \otimes |-\rangle) &= \sqrt{۲}F\left(\sum_{\mathbf{x}\in B} |\mathbf{x}\rangle \otimes |-\rangle\right)\\ &= \sum_{\mathbf{x}\in B} \left[F\left(|\mathbf{x}\rangle \otimes |۰\rangle\right) - F\left(|\mathbf{x}\rangle \otimes |۱\rangle\right)\right]\ .\end{aligned}$$

طبق تعریف F در (۱) به ازای هر $\mathbf{x} \in B$ و هر $y \in \{۰,۱\}$ داریم

$$F\left(|\mathbf{x}\rangle \otimes |y\rangle\right) = |\mathbf{x}\rangle \otimes |f(\mathbf{x}) \oplus y\rangle = |\mathbf{x}\rangle \otimes |y\rangle\ .$$

در نتیجه داریم

$$\begin{aligned}\sqrt{۲\beta}F(|\mathbf{b}\rangle \otimes |-\rangle) &= \sum_{\mathbf{x}\in B} \left[|\mathbf{x}\rangle \otimes |۰\rangle - |\mathbf{x}\rangle \otimes |۱\rangle\right]\\ &= \sqrt{۲\beta}(|\mathbf{b}\rangle \otimes |-\rangle)\,,\end{aligned}$$

بنابراین (۳) درست است.

حال (۴) را اثبات می‌کنیم. از تعریف $|-\rangle$ و $|\mathbf{a}\rangle$ و به دلیل خطی بودن عملگر F داریم

$$\begin{aligned}\sqrt{۲\alpha}F(|\mathbf{a}\rangle \otimes |-\rangle) &= \sqrt{۲}F\left(\sum_{\mathbf{x}\in A} |\mathbf{x}\rangle \otimes |-\rangle\right)\\ &= \sum_{\mathbf{x}\in A} \left[F\left(|\mathbf{x}\rangle \otimes |۰\rangle\right) - F\left(|\mathbf{x}\rangle \otimes |۱\rangle\right)\right]\ .\end{aligned}$$

طبق تعریف F در (۱) به ازای هر $\mathbf{x} \in A$ و هر $y \in \{۰,۱\}$ داریم

$$F\left(|\mathbf{x}\rangle \otimes |y\rangle\right) = |\mathbf{x}\rangle \otimes |f(\mathbf{x}) \oplus y\rangle = |\mathbf{x}\rangle \otimes |۱ - y\rangle\ .$$

در نتیجه داریم

$$\begin{aligned}\sqrt{۲\alpha}F(|\mathbf{a}\rangle \otimes |-\rangle) &= \sum_{\mathbf{x}\in A} \left[F(|\mathbf{x}\rangle \otimes |۰\rangle) - F(|\mathbf{x}\rangle \otimes |۱\rangle)\right]\\ &= \sum_{\mathbf{x}\in A} \left[|\mathbf{x}\rangle \otimes |۱\rangle - |\mathbf{x}\rangle \otimes |۰\rangle\right]\\ &= \sum_{\mathbf{x}\in A} \left[(-|\mathbf{x}\rangle) \otimes |۰\rangle - (-|\mathbf{x}\rangle) \otimes |۱\rangle\right]\\ &= \sqrt{۲\alpha}\left(-|\mathbf{a}\rangle \otimes |-\rangle\right)\ ,\end{aligned}$$

بنابراین (۴) درست است. □

صفحهٔ $\mathcal{S}$ را در نظر بگیرید. فرض کنیم θ زاویهٔ بین خطوط $\mathbf{O}\,|\mathbf{h}\rangle$ و $\mathbf{O}\,|\mathbf{b}\rangle$ باشد (برای این که علامت زوایا را تعیین کنیم، فرض می‌کنیم که خط $\mathbf{O}\,|\mathbf{b}\rangle$ محور x و خط $\mathbf{O}\,|\mathbf{a}\rangle$ محور y باشد.) در این صورت هر بار اعمال عملگر RF شبیه اعمال یک دوران با زاویهٔ ۲θ

حول $\mathbf{O}$ در این صفحه می‌باشد. در واقع، فرض کنید $|\mathbf{x}\rangle \in \mathcal{S}$. در این صورت طبق لم ۱ داریم

$$F(|\mathbf{x}\rangle \otimes |-\rangle) = |\mathbf{y}\rangle \otimes |-\rangle \ ,$$

که در آن $|\mathbf{y}\rangle$ حاصل بازتاب $|\mathbf{x}\rangle$ حول $\mathbf{O}\,|\mathbf{b}\rangle$ می‌باشد. به علاوه، طبق تعریف R در (۲) داریم

$$F(|\mathbf{y}\rangle \otimes |-\rangle) = |\mathbf{z}\rangle \otimes |-\rangle \ ,$$

که در آن $|\mathbf{z}\rangle$ حاصل بازتاب $|\mathbf{y}\rangle$ حول $\mathbf{O}\,|\mathbf{h}\rangle$ می‌باشد. ترکیب دو بازتاب با محورهای $\mathbf{O}\,|\mathbf{b}\rangle$ و $\mathbf{O}\,|\mathbf{h}\rangle$ معادل دورانی با زاویهٔ 2θ حول $\mathbf{O}$ می‌باشد، بنابراین $|\mathbf{z}\rangle$ حاصل دوران $|\mathbf{x}\rangle$ حول $\mathbf{O}$ و با زاویهٔ 2θ در صفحهٔ $\mathcal{S}$ است. توجه کنید که

$$|\mathbf{h}\rangle = \sqrt{\alpha/N}\,|\mathbf{a}\rangle + \sqrt{\beta/N}\,|\mathbf{b}\rangle \ ,$$

بنابراین $|\mathbf{h}\rangle \in \mathcal{S}$ و چون $\alpha > 0$ و $\beta \geq 0$ پس $0 < \theta \leq \pi/2$. نتیجهٔ زیر حاصل می‌شود.

نتیجه ۲. *داریم $(RF)^k(|\mathbf{h}\rangle \otimes |-\rangle) = |\mathbf{h}'\rangle \otimes |-\rangle$ که در آن $|\mathbf{h}'\rangle$ حاصل دوران $|\mathbf{h}\rangle$ حول $\mathbf{O}$ با زاویهٔ $2k\theta$ در صفحهٔ $\mathcal{S}$ است.*

یک نکتهٔ جالب در این‌جا این است که کیوبیت آخر همیشه در حالت $|-\rangle$ می‌ماند و هیچ‌گاه در طول الگوریتم تغییری نمی‌کند، با این حال نمی‌توان این کیوبیت را از الگوریتم حذف کرد!

لم ۳. *فرض کنید $|\mathbf{q}\rangle \in Q_n \cap \mathcal{S}$ و ψ زاویهٔ بین خطوط $\mathbf{O}\,|\mathbf{q}\rangle$ و $\mathbf{O}\,|\mathbf{b}\rangle$ باشد. فرض کنید پس از اندازه‌گیری $(n+1)$—کیوبیت $|\mathbf{q}\rangle \otimes |-\rangle$، بیت‌های $x_1, x_2, \ldots, x_n, y$ به دست آیند. در این صورت احتمال $f(x_1, \ldots, x_n) = 1$ لااقل $\sin^2(\psi)$ است.*

اثبات. فرض کنید

$$|\mathbf{q}\rangle = \sum_{\mathbf{x}\in\{0,1\}^n} \mathbf{q}_\mathbf{x}\,|\mathbf{x}\rangle$$

نمایش $|\mathbf{q}\rangle$ در پایهٔ استاندارد باشد. چون $A = f^{-1}(1)$، احتمال مورد نظر برابر است با $\sum_{\mathbf{x}\in A} \mathbf{q}_\mathbf{x}^2$. فرض کنید ϕ زاویهٔ بین خطوط $\mathbf{O}\,|\mathbf{q}\rangle$ و $\mathbf{O}\,|\mathbf{a}\rangle$ باشد. چون $\mathbf{O}\,|\mathbf{a}\rangle$ بر $\mathbf{O}\,|\mathbf{b}\rangle$ عمود است، داریم $\cos^2(\phi) = \sin^2(\psi)$. طبق نامساوی کوشی—شوارز،

$$\begin{aligned}
\sum_{\mathbf{x}\in A} \mathbf{q}_\mathbf{x}^2 &= \left(\sum_{\mathbf{x}\in A} \mathbf{q}_\mathbf{x}^2\right)\left(\sum_{\mathbf{x}\in A} \frac{1}{\alpha}\right) \\
&\geq \left(\sum_{\mathbf{x}\in A} \mathbf{q}_\mathbf{x}/\sqrt{\alpha}\right)^2 \\
&= \langle |\mathbf{q}\rangle, |\mathbf{a}\rangle\rangle^2 = \| |\mathbf{q}\rangle \|^2 \cdot \| |\mathbf{a}\rangle \|^2 \cdot \cos^2(\phi) \\
&= \cos^2(\phi) = \sin^2(\psi) \ .
\end{aligned}$$

□

اکنون ابزارهای لازم را برای انتخاب k مناسب و تحلیل الگوریتم گراور داریم. طبق تعریف $|\mathbf{h}\rangle$ و $|\mathbf{b}\rangle$ داریم

$$\cos\theta = \langle |\mathbf{h}\rangle, |\mathbf{b}\rangle\rangle = \sum_{\mathbf{x}\in B} 1/\sqrt{N\beta} = \sqrt{\beta/N} \ .$$

در نتیجه داریم $\sin\theta = \sqrt{\alpha/N} \geq 1/\sqrt{N}$. چون تعداد جواب‌های مسئله برابر α است و بر الگوریتم معلوم است، θ نیز بر الگوریتم معلوم است. می‌دانیم $\mathbf{O}\,|\mathbf{h}\rangle$ با $\mathbf{O}\,|\mathbf{b}\rangle$ زاویهٔ θ می‌سازد و k بار اعمال RF معادل دوران به اندازهٔ $2k\theta$ حول $\mathbf{O}$ می‌باشد. بنابراین طبق نتیجه ۲ پس از k بار اعمال این عملگر به $(n+1)$—کیوبیتی مانند $|\mathbf{h}'\rangle \otimes |-\rangle$ می‌رسیم به طوری که $\mathbf{O}\,|\mathbf{h}'\rangle$ با $\mathbf{O}\,|\mathbf{b}\rangle$ زاویهٔ $(2k+1)\theta$ را می‌سازد. طبق لم ۳ با اندازه‌گیری این $(n+1)$—کیوبیت به احتمال لااقل $\sin^2((2k+1)\theta)$ جوابی از مسئله را پیدا می‌کنیم.

اگر $\pi/4 \leq \theta \leq \pi/2$، کافی است k را برابر صفر انتخاب کنیم، در این صورت احتمال موفقیت الگوریتم گراور لااقل یک‌دوم خواهد بود. اگر $0 < \theta < \pi/4$، فرض کنید k کوچک‌ترین عدد طبیعی باشد که $(2k+1)\theta \geq \pi/4$. در این صورت

$$(2k-1)/\sqrt{N} \leq (2k-1)\sin\theta \leq (2k-1)\theta < \pi/4$$

در نتیجه $k < (\pi\sqrt{N}+4)/8 < \sqrt{N}$. از طرف دیگر داریم $(2k+1)\theta \leq 3\pi/4$؛ لذا با انتخاب این k، احتمال موفقیت الگوریتم گراور لااقل یک‌دوم خواهد بود.

۴ مؤخره

در بخش ۳ مسئلهٔ جستجویی تعریف کردیم و الگوریتمی کوانتومی برای حل آن ارائه دادیم. البته این مسئلهٔ دقیقاً با مسابقه‌ای که در مقدمه مطرح کردیم متناظر نیست؛ به‌هرحال الگوریتم ارائه‌شده بسیار جالب‌توجه است و تفاوت بارزی را بین قدرت الگوریتم‌های کوانتومی و الگوریتم‌های متعارف نشان می‌دهد.

گراور [۲] نشان داد هر الگوریتم کوانتومی که برای مسئلهٔ جستجوی بالا ارائه شود که احتمال موفقیتش لااقل یک‌سوم باشد، از $\Omega(\sqrt{N})$ گیت جعبه‌سیاه استفاده می‌کند و بنابراین مرتبهٔ[۱۰] تعداد پرسش‌های الگوریتم او بهینه است.

نویسندگان مقالهٔ [۱] نشان دادند که تعداد گیت‌های جعبه‌سیاه الگوریتم گراور بهینه است. هم‌چنین آن‌ها الگوریتمی ارائه دادند که مسئلهٔ جستجوی بالا را در حالتی که تعداد جواب‌ها مثبت ولی نامعلوم است حل می‌کند و از $O(\sqrt{N})$ گیت جعبه‌سیاه استفاده می‌کند.

[۱۰] order

مراجع

[١] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4–5):493–505,1998.

[٢] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (STOC 1996)*, pages 212–219, New York, 1996, ACM.