



دانشکده: فیزیک

گروه: فیزیک ذرات بنیادی

جستجوی کوانتومی

دانشجو: عادل مجیدی

استاد راهنما:

دکتر حسین موحدیان

پایان نامه ارشد جهت اخذ درجه کارشناسی ارشد

ماه و سال انتشار: خرداد ۱۳۸۸

تقدیم به پدر و مادر عزیز
و همسر مهربانم

با تشکر از راهنمایی‌های بی‌دریغ دکتر موحدیان

دانشجو تأیید می‌نماید که مطالب مندرج در این پایان‌نامه (رساله) نتیجه تحقیقات خودش می‌باشد و در صورت استفاده از نتایج دیگران مرجع آن را ذکر نموده است.

کلیه حقوق مادی مترتب از نتایج مطالعات، آزمایشات و نوآوری ناشی از تحقیق موضوع این پایان‌نامه (رساله) متعلق به دانشگاه صنعتی شاهرود می‌باشد.

خرداد ۱۳۸۸

چکیده

الگوریتم جستجوی کوانتومی که اصول اولیه‌ی آن توسط گراور کشف شد، می‌توانست یک گزینه‌ی مشخص را در یک فضای جستجو با اندازه‌ی N که اطلاعات در آن به صورت نامرتب ذخیره شده، در $O(\sqrt{N})$ مرحله بیابد. بعدها اثبات شد که نمی‌توان الگوریتم کوانتومی‌ای که از این سریع‌تر باشد نوشت، با این وجود تلاش‌ها برای افزایش دقت در الگوریتم جستجو افزایش یافت تا احتمال دستیابی به جواب بعد از اندازه‌گیری بیشتر و بیشتر شود. احمد یونس توانست با تغییراتی در روش گراور احتمال دستیابی به جواب را به حداقل 87.88% برساند در حالی که این احتمال در الگوریتم گراور حداقل برابر 50% است.

ما با اضافه کردن یک کیوبیت هدف دیگر به الگوریتم احمد یونس و ایجاد درهم‌تنیدگی بین این کیوبیت با بقیه‌ی سیستم، الگوریتم جدیدی تشکیل دادیم و سپس میانگین احتمال موفقیت برای پنج تکرار اول از الگوریتم جدید را با الگوریتم احمد یونس مقایسه کردیم. نتایج حاصل افزایش میانگین موفقیت را در تمامی پنج تکرار اول در الگوریتم جدید نشان داد. به خصوص در اولین تکرار در تمامی بازه‌ی $1 \leq M \leq N$ احتمال موفقیت در الگوریتم جدید همواره بیشتر است.

کلمات کلیدی: مکانیک کوانتومی؛ کامپیوتر کوانتومی؛ اطلاعات کوانتومی و محاسبات کوانتومی؛ جستجوی کوانتومی؛ الگوریتم گراور؛ الگوریتم احمد یونس

فهرست مطالب

۱	فصل ۱- مکانیک کوانتومی.....
۲	۱-۱- مقدمه
۲	۲-۱- اصول موضوعه‌ی مکانیک کوانتومی
۵	۳-۱- آنسامبل‌های آمیخته و ماتریس چگالی
۶	۴-۱- ضرب تانسوری و ترکیب فضاهاى هیلبرت
۸	۵-۱- درهم‌تنیدگی
۸	۶-۱- نامساوی کوشی-شوارز و مثلث
۱۰	فصل ۲- کامپیوتر کوانتومی.....
۱۱	۱-۲- مقدمه
۱۱	۲-۲- کیوبیت
۱۳	۳-۲- کره بلاخ و ماتریس‌های چگالی 2×2
۱۵	۴-۲- گیت‌های کلاسیکی و کوانتومی
۱۶	۵-۲- گیت‌های کلاسیکی
۱۶	۶-۲- گیت‌های کوانتومی
۱۷	۱-۶-۲- گیت هادامارد
۱۸	۲-۶-۲- گیت Phase Shift
۱۸	۳-۶-۲- گیت NOT
۱۹	۴-۶-۲- حالت‌های ورودی و خروجی در یک مدار
۲۰	۷-۲- گیت‌های Controlled-U
۲۱	۱-۷-۲- گیت C-NOT

۲۲	۲-۷-۲- گیت C-Phase Shift
۲۳	۲-۷-۳- گیت C-V
۲۳	۲-۷-۴- f-gate
۲۵	۲-۸- مجموعه‌ی فراگیر گیت‌ها
۲۶	۲-۹- قضیه‌ی No-Cloning
۲۷	۲-۱۰- درهم‌تنیدگی کامپیوتر با محیط
۲۹	۲-۱۱- توابع Big O, Big Ω و Big Θ
۳۱	فصل ۳- جستجوی کوانتومی
۳۲	۳-۱- مقدمه
۳۳	۳-۲- مسئله‌ی جستجوی کوانتومی
۳۳	۳-۳- الگوریتم گراور
۳۹	۳-۴- تعبیر عملگر گراور به عملگر دوران
۴۱	۳-۵- تعداد تکرارهای لازم برای رسیدن به بیشینه‌ی احتمال
۴۲	۳-۶- حداکثر احتمال خطا چقدر است؟
۴۵	۳-۷- بهینگی الگوریتم جستجوی کوانتومی
۵۱	۳-۸- تشکیل الگوریتم گراور با عملگر یکانی دلخواه
۵۶	۳-۹- تعداد نامشخص جواب‌ها
۵۸	۳-۹-۱- الگوریتم بویر
۶۲	فصل ۴- الگوریتم احمد یونس و الگوریتم پیشنهادی جدید
۶۳	۴-۱- مقدمه
۶۳	۴-۲- مدار الگوریتم احمد یونس
۷۱	۴-۳- تعداد تکرار لازم برای الگوریتم

۷۲	۴-۴-حداکثر احتمال موفقیت
۷۴	۴-۵-مثالی برای الگوریتم احمد یونس
۷۷	۴-۶-تعداد نامشخص جواب‌ها
۷۸	۴-۶-۱-الگوریتم بویر با استفاده از الگوریتم احمد یونس
۸۰	۴-۷-الگوریتم جدید بر مبنای الگوریتم احمد یونس
۸۵	۴-۸-تکرارهای بعدی الگوریتم پیشنهادی
۹۰	منابع.....
۹۲	پیوست.....

فهرست اشکال

۱۵	شکل ۱-۲- نمایش کیوبیت در کره ی بلاخ
۱۷	شکل ۲-۲- گیت هادامارد
۱۸	شکل ۳-۲- گیت Phase shift
۲۰	شکل ۴-۲- مدار یک گیت Controlled-U
۲۱	شکل ۵-۲- مدار یک گیت C-NOT
۲۲	شکل ۶-۲- مدار swap
۲۲	شکل ۷-۲- مدار یک گیت C-Phase shift
۲۳	شکل ۸-۲- مدار یک گیت f-gate
۲۴	شکل ۱-۳- مدار الگوریتم گراور
۲۴	شکل ۲-۳- مدار داخلی عملگر گراور
۳۸	شکل ۳-۳- نمایش نحوه ی عملکرد الگوریتم گراور بر دامنه ها
۴۰	شکل ۴-۳- نمودار دوران حالت سیستم تحت تأثیر عملگر گراور
۴۴	شکل ۵-۳- نمودار احتمال موفقیت الگوریتم گراور
۵۳	شکل ۶-۳- دوران کت حالت در اثر عملگر Q
۵۹	شکل ۷-۳- نمودار m_0 بر حسب $\frac{M}{N}$
۶۳	شکل ۱-۴- مدار الگوریتم احمد یونس
۷۳	شکل ۲-۴- نمودار احتمال موفقیت الگوریتم احمد یونس
۷۳	شکل ۳-۴- نمایش عملکرد P_{inv} بر زیرفضاهای سیستمی که در آن $M = \frac{N}{2}$
۸۰	شکل ۴-۴- مدار الگوریتم پیشنهادی جدید
۸۴	شکل ۵-۴- نمودار P_s در الگوریتم جدید
۸۴	شکل ۶-۴- مقایسه ی نمودارهای P_s در الگوریتم جدید و الگوریتم احمد یونس
۸۷	شکل ۷-۴- مقایسه ی نمودارهای P_s به ازای تکرارهای مختلف در دو الگوریتم

فهرست جداول

۸۵	جدول ۴-۱ : ضرایب حالت سیستم در الگوریتم جدید تا تکرار پنجم
۸۷	جدول ۴-۲ : میانگین احتمال موفقیت در دو الگوریتم تا تکرار پنجم

فصل ۱

مکانیک کوانتومی

۱-۱-مقدمه

در سال ۱۹۰۰ ماکس پلانک تئوری کوانتوم خود را به جامعه‌ی فیزیک آلمان ارائه کرد. او اعلام کرد که انرژی نیز مانند ماده در واحدهای منفرد وجود دارد. وجود این ذرات (که کوانتا نام گرفتند) اولین فرض تئوری کوانتوم بود.

در اوایل قرن بیستم، برخی از آزمایشات نشان دادند که توصیف قوانین کلاسیک از جهان پیرامون ما نمی‌تواند توصیف کاملی باشد و نیاز است تا قوانین جدیدی وضع شود. تئوری جدید که طبیعت و رفتار مواد و انرژی را در ابعاد اتمی و زیراتمی شرح می‌داد، تئوری کوانتومی نام گرفت. در سال ۱۹۲۵ شرودینگر و هایزنبرگ هر یک فرمولبندی جداگانه‌ای را برای این تئوری ارائه دادند.

برای درک مکانیک کوانتومی، قبل از هر چیز باید اصول موضوعه‌ی مربوط به آن را مورد بررسی قرار داد:

۱-۲-اصول موضوعه‌ی مکانیک کوانتومی

اصل موضوع ۱: حالت یک سیستم بوسیله‌ی یک بردار $(|\Psi\rangle)$ در یک فضای هیلبرت مشخص می‌شود و شامل تمام اطلاعاتی است که ما می‌توانیم درباره‌ی آن سیستم بدست آوریم.

اصل موضوع ۲: هر متغیر دینامیکی A که یک کمیت فیزیکی قابل اندازه‌گیری باشد، با یک عملگر هرمیتی نمایش داده می‌شود. (این کمیت را در اصطلاح مشاهده‌پذیر^۱ می‌گویند)

عملگر A را هرمیتی گویند هرگاه با الحاقی خود برابر باشد: $A = A^\dagger$. ویژه‌کتهای یک عملگر هرمیتی پایه‌های متعامد یک فضای برداری را تشکیل می‌دهند.

¹ observable

اصل موضوع ۳: در اثر اندازه‌گیری یک مشاهده‌پذیر A ، سیستم به یکی از ویژه‌کتهای این مشاهده‌پذیر فروریزش می‌کند و نتیجه‌ی آزمایش برابر ویژه‌مقدار متناظر با آن ویژه‌کت خواهد بود.

هرگاه قبل از اندازه‌گیری، کت حالت یک سیستم فیزیکی را در اختیار داشته باشیم، نمی‌توانیم به طور قطع بگوئیم که نتیجه‌ی اندازه‌گیری چه خواهد بود بلکه تنها می‌توانیم یک بیان احتمالی از آنچه بعد از اندازه‌گیری رخ می‌دهد داشته باشیم: اگر کت حالت سیستم $|\Psi\rangle$ باشد، آنگاه احتمال اینکه بعد از اندازه‌گیری مشاهده‌پذیر A ، ویژه‌مقدار a_n بدست آید برابر است با:

$$\text{prob}(a_n) = |\langle a_n | \Psi \rangle|^2 = \langle \Psi | P_n | \Psi \rangle = \text{Tr}(P_n | \Psi \rangle \langle \Psi |) \quad (1-1)$$

در صورتی که به ازای ویژه‌مقدار a_n تبهگنی داشته باشیم، احتمال دستیابی به ویژه‌مقدار a_n برابر خواهد بود با:

$$\text{prob}(a_n) = \sum_i |\langle a_i | \Psi \rangle|^2 = \text{Tr} \left(\sum_i P_i | \Psi \rangle \langle \Psi | \right)$$

که در آن P_i عملگر تصویر در امتداد ویژه‌کت $|a_i\rangle$ است و به صورت زیر تعریف می‌شود:

عملگر تصویر

عملگر تصویر از ضرب خارجی یک کت تشکیل می‌شود. برای مثال به ازای کت حالت $|\Psi\rangle$ ، عملگر تصویر را می‌توان به شکل زیر تشکیل داد:

$$P = |\Psi\rangle \langle \Psi| \quad (2-1)$$

این عملگر بوضوح هرمیتی است و همچنین در صورتی که $|\Psi\rangle$ نرمالیزه باشد، داریم $P^2 = P$

فرض کنید فضای n بعدی‌ای متشکل از کتهای پایه‌ی $\{|1\rangle, \dots, |n\rangle\}$ در اختیار داریم در آن صورت عملگر

$$P = \sum |i\rangle\langle i| \quad (3-1)$$

یک عملگر تصویر است که فضای n بعدی را به زیر فضای m بعدی متشکل از کت‌های پایه‌ی $\{|1\rangle, \dots, |m\rangle\}$ تصویر می‌کند.

همچنین هر عملگر A را می‌توان به صورت ترکیبی از عملگرهای تصویر نوشت

$$A = \sum a_i P_i \quad (4-1)$$

که در آن $|a_i\rangle$ و a_i ها به ترتیب ویژه‌کت‌ها و ویژه‌مقادیر A هستند.

مقدار چشم‌داشتی (مقدار میانگین)

مقدار چشم‌داشتی مشاهده‌پذیر A در سیستمی با کت حالت $|\Psi\rangle$ برابر است با:

$$\langle A \rangle = \langle \Psi | A | \Psi \rangle \quad (5-1)$$

اصل موضوع ۴: تحول زمانی یک سیستم کوانتومی منزوی، در تصویر شرودینگر، توسط معادله‌ی شرودینگر به صورت زیر بیان می‌شود:

$$i\hbar \frac{\partial}{\partial t} |\Psi\rangle = H |\Psi\rangle \Rightarrow |\Psi(t)\rangle = e^{\frac{-iH}{\hbar} t} |\Psi(0)\rangle \quad (6-1)$$

که در آن H عملگر هامیلتونی سیستم و معادل انرژی کل سیستم است. مقادیر انرژی‌ای که یک سیستم می‌تواند بگیرد، ویژه‌مقادیر عملگر H هستند. [1,3]

۳-۱- آنسامبل‌های آمیخته و ماتریس چگالی

مجموعه‌ای از سیستم‌ها را که همگی دارای حالت کوانتومی یکسان هستند را آنسامبل خالص می‌گویند. به دلیل یکسان بودن حالت سیستم‌ها، همگی آن‌ها را می‌توان با یک کت حالت نشان داد. اما در صورتی‌که

حالت‌ها متفاوت باشد آنگاه یک کت حالت نمی‌تواند نماینده‌ی تمام سیستم‌ها باشد. به این مجموعه از سیستم‌ها آنسامبل آمیخته گفته می‌شود. [1]

یک آنسامبل آمیخته شامل زیرمجموعه‌هایی است که هر یک حاوی سیستم‌های با حالت یکسان هستند. هر زیرمجموعه، بسته به تعداد حالت‌های یکسان که در خود جای داده، درصدی از کل آنسامبل را به خود اختصاص می‌دهد. به این درصد، جمعیت نسبی یا وزن احتمال می‌گویند. برای مثال می‌گوییم: زیرمجموعه‌ی اول در حالت $|\alpha_1\rangle$ با جمعیت نسبی w_1 است و زیرمجموعه‌ی دوم در حالت $|\alpha_2\rangle$ با جمعیت نسبی w_2 است و ...

مقدار میانگین یک مشاهده‌پذیر مانند A را در یک آنسامبل آمیخته می‌توان به راحتی محاسبه کرد:

$$\begin{aligned} \langle A \rangle &= \sum_i w_i \langle \alpha_i | A | \alpha_i \rangle \\ \rightarrow &= \sum_b \sum_b \left(\sum_i w_i \langle b'' | \alpha_i \rangle \langle \alpha_i | b' \rangle \right) \langle b' | A | b'' \rangle \end{aligned} \quad (7-1)$$

عبارت داخل پرانتز فقط مربوط به ویژگی آنسامبل آمیخته است و هیچ ارتباطی با مشاهده‌پذیر A ندارد. این عبارت این امکان را به ما می‌دهد که حالت آنسامبل‌های آمیخته را بوسیله‌ی ماتریس چگالی که به صورت

$$P = \sum w_i |\alpha_i\rangle \langle \alpha_i| \quad (8-1)$$

تعریف می‌شود، فرمولبندی کنیم. با این تعریف، میانگین $\langle A \rangle$ به شکل زیر در می‌آید:

$$\langle A \rangle \equiv \sum \langle b'' | \rho A | b'' \rangle = \text{tr}(\rho A) \quad (9-1)$$

نقش ماتریس چگالی در آنسامبل آمیخته مشابه نقش کت حالت در آنسامبل خالص است. یک ماتریس چگالی حاوی تمام اطلاعات مهم فیزیکی است که می‌توان درباره‌ی یک آنسامبل آمیخته بدست آورد.

در مورد آنسامبل خالص، با توجه به تعریف (۵-۱)، واضح است که ماتریس چگالی آن برابر است با:

$$\rho \equiv |\alpha\rangle\langle\alpha| \quad (10-1)$$

که $\rho^2 = \rho$ حالت این آنسامبل است. همچنین:

چند مورد از خواص ماتریس چگالی:

$$1. \quad \rho = \rho^\dagger \text{ یک عملگر هرمیتی است:}$$

$$2. \quad \text{رد } \rho^2 \text{ برابر 1 است: } \text{tr}(\rho) = 1$$

$$3. \quad \rho \text{ یک عملگر مثبت است.}$$

۱-۴- ضرب تانسوری و ترکیب فضاهای هیلبرت

ما در مکانیک کوانتومی معمولاً با سیستم‌های چند ذره‌ای سروکار داریم. برای بررسی یک سیستم چند ذره‌ای لازم است یک فضای هیلبرت کلی برای این سیستم تشکیل دهیم. این کار را بوسیله‌ی ضرب تانسوری فضاهای هیلبرت هر یک از ذرات انجام می‌دهیم. برای مثال اگر دو ذره به ترتیب دارای فضای هیلبرت H_A و H_B باشند، آنگاه فضای هیلبرت سیستم دو ذره‌ای برابر است با:

$$H = H_A \otimes H_B \quad (11-1)$$

کت حالت توصیف کننده‌ی سیستم دو ذره‌ای نیز در حالت کلی به شکل زیر است:

$$|\psi\rangle = \sum_i \alpha_{ii} |a_i\rangle \otimes |b_i\rangle \quad (12-1)$$

چند خاصیت از ضرب تانسوری:

$$1. \quad A \in H_A, B \in H_B \rightarrow C = A \otimes B \in H \quad (13-1)$$

$$2. \mathbf{A} \otimes \mathbf{B}(|\psi\rangle_A \otimes |\psi\rangle_R) = (\mathbf{A}|\psi\rangle_A) \otimes (\mathbf{B}|\psi\rangle_R) \quad (14-1)$$

$$3. ({}_R\langle\phi| \otimes {}_A\langle\phi|)(|\psi\rangle_A \otimes |\psi\rangle_R) = {}_A\langle\phi|\psi\rangle_A {}_R\langle\phi|\psi\rangle_R \quad (15-1)$$

۴. اگر A و B هرمیتی باشند، آنگاه $A \otimes B$ نیز هرمیتی است.

۵. اگر A و B یکانی باشند، آنگاه $A \otimes B$ نیز یکانی است.

۶. اگر A و B عملگرهای تصویر باشند، آنگاه $A \otimes B$ نیز عملگر تصویر است.

بعد یک فضای هیلبرت بزرگتر، برابر ضرب ابعاد فضاهای هیلبرت کوچکتر است: $N = N_A N_R$ ، بنابراین اگر $|\psi\rangle_A$ و $|\psi\rangle_R$ به ترتیب دارای نمایش ستونی $N \times 1$ و $M \times 1$ باشند آنگاه نمایش ستونی $|\psi\rangle_{AR}$ ، $NM \times 1$ خواهد بود و همچنین اگر عملگرهای A و B به ترتیب دارای ماتریسهای $N \times N$ و $M \times M$ باشند آنگاه $C = A \otimes B$ ماتریسی $NM \times NM$ خواهد داشت.

$$|\psi\rangle_A \otimes |\psi\rangle_B = \begin{pmatrix} a_1 |\psi\rangle_B \\ \vdots \\ a_N |\psi\rangle_B \end{pmatrix} \quad (16-1)$$

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1N}B \\ \vdots & \ddots & \vdots \\ a_{N1}B & \cdots & a_{NN}B \end{pmatrix} \quad (17-1)$$

(توجه: نمادگذاریهای $|\alpha\rangle \otimes |\beta\rangle$ ، $|\alpha\rangle|\beta\rangle$ و $|\alpha, \beta\rangle$ به یک معنی بکار گرفته می شوند.) [2]

۱-۵- درهم تنیدگی

فضای هیلبرت H را که مرکب از فضاهای هیلبرت H_A و H_R است، در نظر بگیرید. کت حالت $|x\rangle_{AR} \in H$ را تفکیک پذیر گویند هرگاه بتوان آن را به صورت $|x\rangle_{AR} = |\psi\rangle_A \otimes |\psi\rangle_R$ نوشت در غیر اینصورت می گوییم که $|x\rangle_{AR}$ یک حالت درهم تنیده از فضاهای هیلبرت A و B است. برای مثال کت حالت $|x\rangle_{AR} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_R + |1\rangle_A|1\rangle_R)$ را نمی توان به صورت ضرب تانسوری مستقیم زیر فضای A در زیر فضای

B نوشت و بنابراین درهم‌تنیده است. وقتی دو سیستم درهم‌تنیده باشند، حالت یک سیستم فقط با ارجاع به حالت سیستم دیگر قابل توصیف است.

در صورتی که ماتریس چگالی ρ ، یک حالت خالص باشد، یعنی $\rho = |\chi\rangle_{AR} \langle\chi|$ ، آنگاه می‌توان بررسی کرد که آیا $|\chi\rangle_{AR}$ درهم‌تنیده است یا خیر:

ویژه‌مقادیر ماتریس چگالی فضای هیلبرت A ($\rho_A = \text{tr}_R(\rho)$) معروف به ضرایب اشمیت هستند. اگر تعداد ضرایب غیر صفر اشمیت برابر یک باشد، در آن صورت $|\chi\rangle$ تفکیک‌پذیر است و در صورتی که بیشتر از یک باشد درهم‌تنیده می‌باشد. [3,5]

۱-۶- نامساوی‌های کوشی-شوارز و مثلث

۱. نامساوی کوشی-شوارز^۳ [2]

به ازای هر دو کت دلخواه $|\Psi\rangle$ و $|\Phi\rangle$ داریم:

$$|\langle\Phi|\Psi\rangle|^2 \leq \langle\Phi|\Phi\rangle \langle\Psi|\Psi\rangle \quad (18-1)$$

یک مثال از این نامساوی به صورت زیر است ($\mathbf{x}_i$ ها و $\mathbf{y}_i$ ها اعدادی حقیقی‌اند):

$$\left(\sum_i x_i y_i\right)^2 \leq \left(\sum_i x_i^2\right) \left(\sum_i y_i^2\right) \quad (19-1)$$

۲. نامساوی مثلث [2]

به ازای هر دو کت دلخواه $|\Psi\rangle$ و $|\Phi\rangle$ ، اندازه‌ی مجموع دو کت حالت همواره از مجموع اندازه‌ی این کت‌ها کوچکتر است:

³ Cauchy-Schwarz

$$\sqrt{\langle \Phi + \Psi | \Phi + \Psi \rangle} \leq \sqrt{\langle \Phi | \Phi \rangle} + \sqrt{\langle \Psi | \Psi \rangle} \quad (۲۰-۱)$$

فصل ۲

کامپیوتر کوانتومی

۲-۱-مقدمه

کامپیوترهای کلاسیکی ای که امروزه با آن سروکار داریم، با بکارگیری بیت‌ها که در دو حالت خاص می‌توانند وجود داشته باشند کار می‌کنند. اما کامپیوترهای کوانتومی به دو حالت خاص محدود نمی‌شوند. آن‌ها اطلاعات را بوسیله‌ی بیت‌های کوانتومی (کیوبیت‌ها) کدگذاری می‌کنند که می‌تواند بینهایت حالت را به خود بگیرد. این کامپیوترها برای پردازش اطلاعات از پدیده‌های کوانتومی هم‌چون برهم‌نهی و درهم‌تنیدگی استفاده می‌کنند که به کامپیوتر کوانتومی امکان می‌دهد تا بتواند پردازش را بصورت کاملاً موازی انجام دهد و به این ترتیب کاهش قابل توجهی در زمان انجام محاسبات رخ می‌دهد.

۲-۲-کیوبیت

واحد پایه برای انجام فرآیند پردازش اطلاعات در کامپیوترهای کلاسیک، بیت است. یک بیت می‌تواند مقادیر 0 یا 1 را به خود بگیرد. در کامپیوترهای کوانتومی نیز مانند کامپیوترهای کلاسیک یک واحد پایه وجود دارد که آن را کیوبیت می‌نامند. کیوبیت یک کت حالت در فضای هیلبرت دوبعدی به شکل زیر است:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2-1) \quad (\alpha^2 + \beta^2 = 1)$$

که $|0\rangle$ و $|1\rangle$ پایه‌های نرمالیزه و متعامد این فضای دوبعدی‌اند. در اینجا یک تفاوت بنیادی بین بیت و کیوبیت وجود دارد: یک بیت در یک زمان واحد، می‌تواند فقط 0 یا فقط 1 باشد، اما کیوبیت می‌تواند $|0\rangle$ یا $|1\rangle$ و هم یا یک برهم‌نهی از $|0\rangle$ و $|1\rangle$ باشد. در این حالت اگر یک اندازه‌گیری روی کیوبیت انجام دهیم، به احتمال $|\alpha|^2$ آن را در حالت $|0\rangle$ و با احتمال $|\beta|^2$ آن را در حالت $|1\rangle$ خواهیم یافت. تفاوت دیگر این است که بیت را می‌توان به آسانی و بدون آشفته کردن حالت آن اندازه‌گیری کرد و به اطلاعات گذشته‌ی آن دست یافت اما بعد از اندازه‌گیری از یک کیوبیت، حالت آن به یکی از حالت‌های پایه فروریزش می‌کند بنابراین دیگر نمی‌توان اطلاعات اضافی آن را بدست آورد.

نمایش ستونی کیوبیت به صورت زیر است:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad (2-2)$$

از ضرب تانسوری کیوبیت‌ها، سیستم‌های چندکیوبیتی تشکیل می‌شود. یک ضرب تانسوری به صورت $|a\rangle = |a_{n-1}\rangle \otimes |a_{n-2}\rangle \otimes \dots \otimes |a_1\rangle \otimes |a_0\rangle$ که در آن $a_i \in \{0,1\}$ است، حالت پایه‌ای از یک سیستم n کیوبیتی (با فضای هیلبرت 2^n بعدی) می‌باشد و اصطلاحاً می‌گوییم یک رجیستر کوانتومی با اندازه‌ی n است. این رجیستر را به عنوان نماینده‌ی یک عدد دهدهی^۴ از 0 تا 2^{n-1} در نظر می‌گیریم:

$$a = 2^0 a_0 + 2^1 a_1 + \dots + 2^{n-1} a_{n-1} \quad (3-2)$$

به عنوان مثال اعداد صفر تا هفت را می‌توانیم بوسیله‌ی رجیستری با اندازه‌ی سه نمایش دهیم:

$$|000\rangle \equiv |0\rangle, |001\rangle \equiv |1\rangle, |010\rangle \equiv |2\rangle, |011\rangle \equiv |3\rangle, |100\rangle \equiv |4\rangle, |101\rangle \equiv |5\rangle, \\ |110\rangle \equiv |6\rangle, |111\rangle \equiv |7\rangle$$

این اعداد را یکجا و به صورت برهم‌نهشی از آنها می‌توان در یک سیستم n کیوبیتی ذخیره کرد:

$$|\Psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \dots + \alpha_7|111\rangle \quad (4-2)$$

$$(|\alpha_0|^2 + |\alpha_1|^2 + \dots + |\alpha_7|^2 = 1) \quad (\text{بطوری که})$$

از نقطه نظر سخت افزاری، بیت یک اختلاف ولتاژ در دو سر یک خازن است: یک خازن شارژ شده نماینده‌ی بیت 1 و یک خازن خالی نماینده‌ی بیت 0 است. در کامپیوترهای کوانتومی هر سیستم دو حالتی می‌تواند به عنوان یک کیوبیت بکار گرفته شود. برای مثال اسپین یک الکترون یک سیستم دو حالتی است که می‌توان اسپین up ($|\uparrow\rangle$) در راستای محور z را $|0\rangle$ و اسپین down ($|\downarrow\rangle$) را $|1\rangle$ در نظر گرفت. در این صورت ضرایب α و β جهت‌گیری اسپین را در فضای سه بعدی x, y و z تعیین می‌کنند. این را می‌توان در کره‌ی بلاخ که یک تصویر هندسی از کیوبیت ارائه می‌دهد به خوبی درک کرد. [6,7]

^۴ decimal

۲-۳- کره بلاخ و ماتریس های چگالی 2×2

هر ماتریس هرمیتی دلخواه 2×2 را که رد آن برابر یک باشد، می توان در حالت کلی به شکل زیر نمایش داد:

$$\rho = \frac{1}{2} \begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \quad (5-2)$$

ماتریس فوق را به طور مرسوم بر حسب ماتریس های پاؤلی به صورت زیر می نویسند:

$$\rho = \frac{1}{2} (1 + \vec{r} \cdot \vec{\sigma}) \quad (6-2)$$

ماتریس ρ با توجه به خواص ماتریس های چگالی، فقط وقتی می تواند یک ماتریس چگالی باشد که ویژه-مقادیرش غیر منفی باشند و این فقط وقتی ممکن است که داشته باشیم:

$$|\vec{r}| = x^2 + y^2 + z^2 \leq 1 \quad (7-2)$$

همان طور که می بینیم این نامساوی معادل است با نامساوی مربوط به مختصات نقاط داخل یک گوی توپر به شعاع یک. بنابراین هر ماتریس چگالی را می توان با یک نقطه (x, y, z) در داخل یک گوی توپر سه بعدی متناظر دانست. در حالتی که $|\vec{r}| = 1$ باشد، گوی تبدیل به کره (تو خالی) می شود و در این حالت، هر ماتریس چگالی متناظر با یک نقطه روی یک کره سه بعدی خواهد بود. به این کره، کره بلاخ گفته می شود.

در مورد یک کیوبیت منفرد، که دارای کت حالت خالص^۵ به صورت:

$$|\Psi\rangle = \alpha |\uparrow\rangle + \beta |\downarrow\rangle \quad (8-2)$$

است، ماتریس چگالی برابر $\rho = |\Psi\rangle\langle\Psi|$ است.

⁵ pure state

کت حالت $|\Psi\rangle$ را هم‌چنین می‌توان به این صورت بیان کرد:

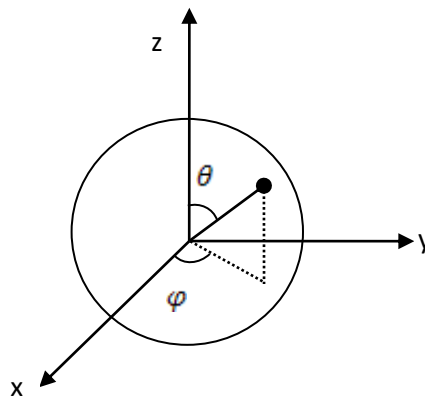
$$|\Psi(\theta, \varphi)\rangle = e^{-i\phi/2} \cos\left(\frac{\theta}{2}\right) |\uparrow\rangle + e^{i\phi/2} \sin\left(\frac{\theta}{2}\right) |\downarrow\rangle \quad (9-2)$$

که در آن:

$$\vec{r} = \hat{n} = (x, y, z) = (\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta) \quad (11-2)$$

$$|\hat{n}| = 1$$

پس می‌توان ماتریس چگالی یک کیوبیت منفرد را با یک نقطه روی یک کره بلاخ که در شکل (۱-۲) نشان داده شده است، متناظر کرد.



شکل ۱-۲- نمایش کیوبیت در کره ی بلاخ

هر نقطه‌ی داخل گوی بلاخ متناظر است با یک آنسامبل آمیخته که دارای ماتریس چگالی

$$\rho = \sum w_i |\Psi_i\rangle \langle \Psi_i|$$

است. از آنجایی که هر آنسامبل آمیخته از مجموعه‌ای از آنسامبل‌های خالص تشکیل می‌شود، با توجه به

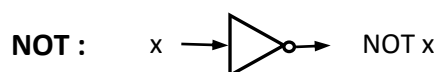
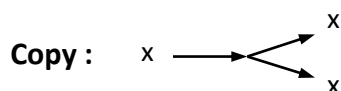
رابطه‌ی (۱۰-۲)، برای یک آنسامبل آمیخته خواهیم داشت که در آن $\vec{r} = \sum_i w_i \hat{n}_i$ و در نتیجه $|\vec{r}| \leq 1$.

[3,5,7]

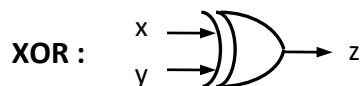
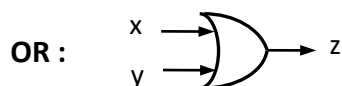
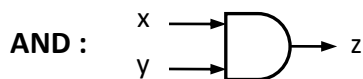
۲-۴- گیت‌های کلاسیکی و کوانتومی

گیت‌ها که اجزای اصلی یک مدار منطقی را تشکیل می‌دهند عملیات پردازش اطلاعات روی بیت‌ها در کامپیوترهای کلاسیکی و کیوبیت‌ها در کامپیوترهای کوانتومی را بر عهده دارند. در ادامه با انواع این گیت‌ها و نحوه‌ی عملشان آشنا می‌شویم.

۲-۵- گیت‌های کلاسیکی



x	NOT x
0	1
1	0



x	y	$z = x \text{ AND } y$	$z = x \text{ OR } y$	$z = x \text{ XOR } y$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

۲-۶- گیت‌های کوانتومی

گیت‌های کوانتومی تقریباً مشابه گیت‌های کلاسیکی هستند. یکی از تفاوت‌های بین این دو نوع گیت، برگشت-پذیر بودن گیت‌های کوانتومی است، به این معنا که می‌توان با استفاده از خروجی گیت‌های کوانتومی، ورودی آن‌ها را دوباره بازسازی کرد. در مورد گیت‌های کلاسیکی مانند AND، XOR، OR و NAND، ...، از آنجا که

این گیت‌ها ورودی دو بیتی را به خروجی یک بیتی تبدیل می‌کنند، بوضوح برگشت‌ناپذیرند. اما اگر یک گیت کوانتومی با عملگر U ، حالت ورودی $|\Psi_{in}\rangle$ را به $|\Psi_{out}\rangle$ تبدیل کند، می‌توان گیتی با عملگر $U^\dagger$ تشکیل داد تا $|\Psi_{out}\rangle$ را مجدداً به $|\Psi_{in}\rangle$ مبدل سازد. [6,7]

عمل یک گیت n کیوبیتی را می‌توان با عمل یک ماتریس $2^n \times 2^n$ متناظر کرد. اما بعکس هر ماتریس $2^n \times 2^n$ تنها به شرطی که یکانی باشد می‌تواند نماینده‌ی یک گیت کوانتومی باشد. برای مثال گیت یک کیوبیتی‌ای را در نظر بگیرید که روی کیوبیت $\alpha|0\rangle + \beta|1\rangle$ عمل می‌کند و حالت آن را به $\alpha'|0\rangle + \beta'|1\rangle$ تغییر می‌دهد. شرط نرمالیزه بودن ($|\alpha|^2 + |\beta|^2 = |\alpha'|^2 + |\beta'|^2 = 1$) ایجاب می‌کند که عمل این گیت عملی یکانی باشد. [4]

۲-۶-۱- گیت هادامارد H

بی‌شک این گیت یکی از مهم‌ترین گیت‌های کوانتومی است. عمل یکانی هادامارد روی کت‌های پایه‌ی محاسباتی به صورت زیر تعریف می‌شود: [6]

$$|x\rangle \longrightarrow H \longrightarrow$$

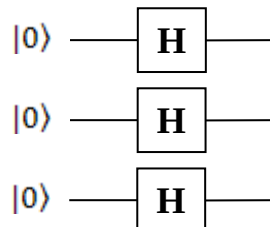
شکل ۲-۲- گیت هادامارد

$$H|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad , \quad H|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (۱۲-۲)$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (۱۳-۲)$$

^۱ Hadamard

یکی از کاربردهای جالب این گیت این است که می‌توان بوسیله‌ی آن کت پایه‌ی n بعدی $|0^{\otimes n}\rangle$ را به یک برهم‌نهی مساوی از کت‌های پایه‌ی فضای n بعدی تبدیل کرد. برای مثال به ازای $n=3$:



$$\Rightarrow H^{\otimes 3}|0^{\otimes 3}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$= \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

اگر کیوبیت را نماینده‌ی اسپین-1/2 بدانیم، آنگاه عمل هادامارد اینگونه تفسیر می‌شود: این گیت اسپین up در جهت z ($|S_x, +\rangle$) را به $|S_x, +\rangle$ و اسپین down ($|S_x, -\rangle$) را به $|S_x, -\rangle$ تبدیل می‌کند.

۲-۶-۲ گیت Phase shift (φ)

این گیت فاز کت پایه‌ی $|1\rangle$ را به اندازه‌ی φ تغییر می‌دهد. بنابراین قادر است فاز نسبی یک برهم‌نهی از $|0\rangle$ و $|1\rangle$ را تغییر دهد: [6]

The diagram shows a horizontal line representing a qubit. On the left, it is labeled $|x\rangle$. It enters a rectangular box with the Greek letter φ above it. On the right, it exits the box and is labeled $e^{ix\varphi}|x\rangle$.

شکل ۲-۳- گیت Phase shift

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|0\rangle + e^{i\varphi}\beta|1\rangle \quad (۱۴-۲)$$

$$\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \quad (۱۵-۲)$$

۲-۶-۳- گیت NOT (X)

این گیت یک حالت پایه را به حالت پایه‌ی دیگر تبدیل می‌کند: [4]

$$|0\rangle \rightarrow |1\rangle, \quad |1\rangle \rightarrow |0\rangle \quad (۱۶-۲)$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (۱۷-۲)$$

۲-۶-۴- حالت‌های ورودی و خروجی در یک مدار

مداری را در نظر بگیرید که دارای ورودی و خروجی n کیوبیتی باشد. فرض کنید این مدار حالت n کیوبیتی $|x\rangle$ را به عنوان ورودی می‌گیرد و آن را با عدد n کیوبیتی a جمع می‌کند. اما در اینجا باید توجه داشت که مجموع دو عدد n کیوبیتی همواره عددی n کیوبیتی نیست بلکه می‌تواند $n+1$ کیوبیتی باشد که در این حالت با توجه به اینکه خروجی مدار n کیوبیتی است تنها n کیوبیت سمت راست از مجموع $x+a$ به عنوان خروجی از مدار خارج می‌شود و این معادل است با این مفهوم که این مدار باقیمانده‌ی تقسیم $x+a$ بر 2^n را به عنوان خروجی از مدار بیرون می‌دهد، یعنی:

$$|x\rangle \rightarrow |(x+a) \bmod 2^n\rangle \quad (۱۸-۲)$$

که $(x+a) \bmod 2^n \equiv$ باقیمانده‌ی تقسیم $x+a$ بر 2^n .

برای مثال اگر x و a اعداد پنج کیوبیتی زیر باشند، آنگاه:

$$x = 25 \equiv 11001, \quad a = 8 \equiv 01000 \Rightarrow x+a = 33 \equiv 100001$$

همان‌طور که می‌بینیم مجموع $x+a$ یک عدد شش‌کیوبیتی است و مدار فقط پنج کیوبیت اول از سمت راست

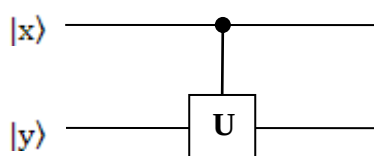
$$(00001) \text{ را می‌تواند به خروجی بدهد: } |11001\rangle \rightarrow |00001\rangle$$

این تبدیل را به صورت معادل می‌توان به صورت زیر نشان داد:

$$|x\rangle \rightarrow |(x+a) \bmod 2^5| = |33 \bmod 32| \equiv |00001\rangle$$

۲-۷- گیت‌های Controlled-U

گیت‌های Controlled-U که گیت‌های دو یا چندکیوبیتی هستند و ایجاد درهم‌تنیدگی بین کیوبیت‌های ورودی می‌کنند، از مهم‌ترین گیت‌های چندکیوبیتی می‌باشند. ورودی این گیت‌ها شامل یک کیوبیت کنترل $|x\rangle$ و یک کیوبیت هدف $|y\rangle$ است. کیوبیت کنترل تعیین می‌کند که آیا یک عمل یکانی مشخص روی کیوبیت هدف انجام شود یا خیر. [2,6]



شکل ۲-۴- مدار یک گیت Controlled-U

عملکرد این نوع گیت‌ها، به طور کلی به این صورت است:

۱. در صورتی که کیوبیت کنترل در حالت $|0\rangle$ باشد، گیت هیچ عملی روی کیوبیت هدف انجام نمی‌دهد

$$|0\rangle |y\rangle \rightarrow |0\rangle |y\rangle \text{ یعنی:}$$

^y target

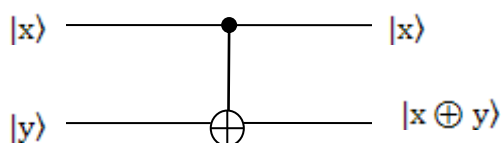
۲. در صورتی که کیوبیت کنترل در حالت $|1\rangle$ باشد، گیت عملگر یکانی U را بر کیوبیت هدف اثر می‌دهد

$$|1\rangle |y\rangle \longrightarrow |1\rangle (U|y\rangle) \quad \text{یعنی:}$$

اگر عمل عملگر U مشخص باشد، آنگاه نمایش ماتریسی این گیت دوکیوبیتی را در پایه‌های محاسباتی $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ می‌توان اینگونه تعیین کرد. در ادامه چند مورد از معروف‌ترین گیت‌های Controlled- U را آورده‌ایم:

۲-۷-۱- گیت C-NOT (Controlled-NOT)

این گیت هم‌چنین به گیت XOR نیز معروف است. کاری که این گیت انجام می‌دهد این است که کیوبیت کنترل را با کیوبیت هدف جمع کرده و باقیمانده‌ی تقسیم این جمع بر 2 را به عنوان خروجی هدف بیرون می‌دهد. به عبارت دیگر اگر کیوبیت کنترل $|1\rangle$ باشد، کیوبیت هدف را معکوس می‌کند و اگر کیوبیت کنترل $|0\rangle$ باشد، آن را بدون تغییر می‌گذارد.



شکل ۲-۵- مدار یک گیت C-NOT

$$|x\rangle |y\rangle \longrightarrow |x\rangle |x \oplus y\rangle \quad (2-20)$$

که در آن $\oplus$ به معنای باقیمانده‌ی تقسیم جمع بر 2 است.

$$\langle 00|U|00\rangle = \langle 00|00\rangle = 1, \langle 01|U|01\rangle = \langle 01|01\rangle = 1, \langle 10|U|11\rangle = \langle 10|10\rangle = 1,$$

$$\langle 11|U|10\rangle = \langle 11|11\rangle = 1$$

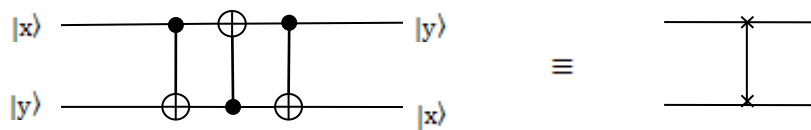
با همین روش بقیه درایه‌های ماتریس برابر صفر است. بنابراین نمایش ماتریسی این گیت به صورت زیر می‌باشد:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (21-2)$$

در حالتی که کیوبیت کنترل به صورت یک برهم‌نهی از کیوبیت‌های $|0\rangle$ و $|1\rangle$ باشد، خروجی گیت C-NOT اینگونه خواهد بود:

$$|x\rangle = \alpha|0\rangle + \beta|1\rangle : |x\rangle|y\rangle \longrightarrow |x\rangle(\alpha|0\oplus y\rangle + \beta|1\oplus y\rangle) \quad (22-2)$$

از این گیت مهم در تشکیل مدارهای زیادی استفاده می‌شود. یکی از موارد استفاده‌ی آن، در تشکیل مداری است که جای دو کیوبیت ورودی را که در حالت پایه هستند عوض می‌کند:

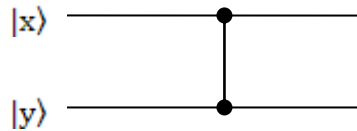


شکل ۲-۶- مدار swap

$$|x\rangle|y\rangle \rightarrow |x\rangle|x\oplus y\rangle \rightarrow |(x\oplus y)\oplus x\rangle|x\oplus y\rangle = |y\rangle|x\oplus y\rangle \rightarrow |y\rangle|y\oplus(x\oplus y)\rangle = |y\rangle|x\rangle$$

۲-۷-۲ گیت C-Phase shift

مدار این گیت را به این شکل نمایش می‌دهند:



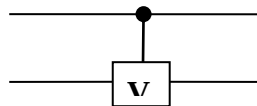
شکل ۷-۲- مدار یک گیت C-Phase shift

این گیت، فاز کیوبیت هدف را تغییر می‌دهد. ماتریس این گیت در پایه‌های محاسباتی $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ به صورت زیر است:

$$B(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} \quad (23-2)$$

$$|x\rangle|y\rangle \longrightarrow B(\phi)(|x\rangle|y\rangle) = e^{ixy\phi} |x\rangle|y\rangle \quad (24-2)$$

۲-۷-۳ گیت C-V (Controlled-V)



این گیت نوع خاصی از C-Phase shift با $\phi = \frac{\pi}{2}$ است.

۲-۸- مجموعه‌ی فراگیر گیت‌ها^۸

^۸ universal set of gates

مجموعه‌ای از گیت‌ها را «جهانی» می‌نامیم هرگاه هر تبدیل یکانی n کیوبیتی را بتوان بوسیله‌ی این مجموعه شبیه سازی کرد.

برای مثال گیت‌های هادامارد و C-NOT به همراه تمامی گیت‌های فاز تشکیل یک مجموعه فراگیر گیت می‌دهند. البته باید توجه داشت که این مجموعه یک مجموعه‌ی نامحدود است چون تعداد گیت‌های فاز نامحدود است.

گیت هادامارد به همراه گیت C-V تشکیل یک مجموعه‌ی فراگیر محدود می‌دهد. هر تبدیل یکانی را می‌توان بوسیله‌ی تعدادی از این دو گیت شبیه‌سازی کرد. [2,6]

۲-۹- قضیه‌ی No-Cloning

فرض کنیم کیوبیت هدف در گیت C-NOT برابر $|0\rangle$ باشد آنگاه براحتی در می‌یابیم که این گیت، ورودی کنترل را کپی می‌کند:

$$|x\rangle |0\rangle \longrightarrow |x\rangle |x\rangle \quad (2-32)$$

البته این فقط برای وقتی است که $|x\rangle$ در حالت پایه باشد. در صورتی که $|x\rangle$ یک برهم‌نهی از حالت‌های پایه باشد، این گیت از کپی کردن آن عاجز است:

$$|x\rangle = \alpha |0\rangle + \beta |1\rangle : (\alpha |0\rangle + \beta |1\rangle) |0\rangle \longrightarrow \alpha |00\rangle + \beta |11\rangle \neq |x\rangle |x\rangle$$

در حالت کلی برای هر حالت خاص $|\Psi\rangle$ می‌توان یک تبدیل یکانی مانند T پیدا کرد که بتواند آن را کپی کند اما این تبدیل یکانی به غیر از $|\Psi\rangle$ تنها می‌تواند حالت‌هایی را که بر $|\Psi\rangle$ عمود هستند کپی کند. به عبارت دیگر با یک تبدیل یکانی واحد نمی‌توان دو کت حالت را که بر هم عمود نیستند کپی کرد. این قضیه به No-Cloning معروف است.

برای اثبات این قضیه از برهان خلف استفاده می‌کنیم: فرض کنیم عملگر یکانی T بتواند دو کت حالت متفاوت و نامتعامل $|\Psi'\rangle$ و $|\Psi''\rangle$ را کپی کند، یعنی:

$$T(|\Psi'\rangle|b\rangle|w\rangle) \rightarrow e^{i\Phi'} |\Psi'\rangle |\Psi'\rangle|w'\rangle$$

$$T(|\Psi''\rangle|b\rangle|w\rangle) \rightarrow e^{i\Phi''} |\Psi''\rangle |\Psi''\rangle|w''\rangle$$

که در آن $|w\rangle$ را به عنوان کت حالت بقیه‌ی جهان در نظر گرفته‌ایم. با توجه به یکانی بودن T داریم:

$$\langle\Psi'|\Psi''\rangle = e^{i(\Phi''-\Phi')} (\langle\Psi'|\Psi''\rangle)^2 \langle w'|w''\rangle$$

$$\Rightarrow |\langle\Psi'|\Psi''\rangle| = |\langle\Psi'|\Psi''\rangle|^2 \langle w'|w''\rangle \quad (33-2)$$

تساوی فوق زمانی برقرار است که $|\langle\Psi'|\Psi''\rangle|$ یا برابر صفر باشد یا برابر یک، که با فرض اولیه در تناقض است. [6,8]

۲-۱۰- درهم‌تنیدگی کامپیوتر با محیط

در بخش (۲-۲) گفتیم که کت حالت یک کیوبیت در حالت کلی به صورت رابطه‌ی (۱-۲) بیان می‌شود. ضرایب α و β علیرغم اینکه احتمال دست‌یابی به هریک از حالت‌های $|0\rangle$ و $|1\rangle$ را بعد از اندازه‌گیری بیان می‌کنند، دارای یک فاز نسبی نیز هستند که جهت‌گیری فضایی کیوبیت را مشخص می‌کند. هم‌چنین زمانی که کت حالت کامپیوتر کوانتومی، یک کت حالت چندکیوبیتی به صورت

$$|\Psi\rangle = \sum_i a_i |i\rangle \quad (34-2)$$

است نیز a_i ها فازهای نسبی بین $|i\rangle$ ها را مشخص می‌کنند.

کت حالت یک کامپیوتر کوانتومی را فقط وقتی می‌توان به صورت رابطه‌ی (۲-۳۴) نوشت که سیستم کامپیوتر با جهان اطراف خود درهم‌تنیده نباشد. به عبارت دیگر حالت کامپیوتر خالص باشد.

حال فرض کنید که بین کامپیوتر و محیط درهم‌تنیدگی وجود داشته باشد. در این صورت کت حالت در فضای هیلبرت H که ترکیبی از فضای هیلبرت کامپیوتر (H_A) و فضای هیلبرت محیط (H_R) است نوشته می‌شود:

$$|\Psi\rangle_{AR} = \sum a_{i,j} |i\rangle_A \otimes |j\rangle_R \quad (|\Psi\rangle_{AR} \in H = H_A \otimes H_R) \quad (۳۵-۲)$$

اما آنچه که مسلم است، ما تنها به حالت زیر-سیستم A و مشاهده‌پذیرهای مربوط به آن علاقه‌مندیم. مشاهده‌پذیر M_A که مربوط به زیر-سیستم A است را در نظر بگیرید. مقدار چشم‌داشتی این مشاهده‌پذیر را اینگونه محاسبه می‌کنیم:

$$\begin{aligned} \langle M_A \rangle &= {}_{AR} \langle \Psi | M_A \otimes I_R | \Psi \rangle_{AR} = \sum a_{i,v}^* ({}_A \langle j | \otimes {}_R \langle v |) (M_A \otimes I_R) \sum a_{i,u} (|i\rangle_A \otimes |u\rangle_R) \\ &= \sum a_{i,u}^* a_{i,u} {}_A \langle j | M_A | i \rangle_A \end{aligned} \quad (۳۶-۲)$$

که این دقیقاً مشابه رابطه‌ی (۴-۱)، یعنی مقدار چشم‌داشتی یک مشاهده‌پذیر در یک آنسامبل آمیخته است. و به همان ترتیب می‌توان (۳۶-۲) را به صورت

$$\langle M_A \rangle = \text{tr}(M_A \rho_A) \quad (۳۷-۲)$$

نوشت که ρ_A همان ماتریس چگالی در آنسامبل آمیخته است

$$\rho_A = \sum a_{i,u} a_{i,u}^* |i\rangle_A \langle i| \quad (۳۸-۲)$$

در حقیقت در اینجا برای بررسی یک مشاهده‌پذیر که فقط روی زیرفضای A عمل می‌کند، یک آنسامبل آمیخته از کت‌های این زیرفضا خواهیم داشت که هر یک دارای وزن احتمال مخصوص به خود هستند. همان‌طور که در بخش (۳-۱) اشاره شد، در این آنسامبل، درهم‌نهمش و فاز نسبی بین کت‌های حالت آنسامبل بی‌معنی است و در واقع همین‌جاست که بزرگترین مزیت کامپیوترهای کوانتومی را از دست می‌دهیم. فاز نسبی می‌تواند امکانات بیشتری برای نحوه‌ی ذخیره‌ی اطلاعات و پردازش آن در اختیار ما بگذارد و اگر این خصوصیت از یک کامپیوتر کوانتومی گرفته شود، قدرت آن در حد یک کامپیوتر احتمالاتی کلاسیک

کاهش می‌یابد (کامپیوتر احتمالاتی کلاسیک کامپیوتری است که در آن بیت‌ها بصورت احتمالی رخ می‌دهند، برای مثال با احتمال α بیت برابر 0 و با احتمال β برابر 1 است).

بنابراین گرچه از خاصیت درهم‌تنیدگی بین کیوبیت‌ها، بهره‌های زیادی می‌بریم اما اگر همین درهم‌تنیدگی با محیط اطراف کامپیوتر نیز وجود داشته باشد، آنگاه ما را با مشکل مواجه می‌کند. پس برای استفاده کامل از خواص یک کامپیوتر کوانتومی، لازم است که سیستم در حالت خالص باشد. [3]

۲-۱۱- توابع $Big O$ ، $Big \Omega$ و $Big \Theta$

تابع $Big O$:

می‌گوئیم $f(x) = O(g(x))$ یا $f(x) \in O(g(x))$ اگر و فقط اگر یک عدد حقیقی و مثبت C وجود داشته باشد به طوری که برای x های بزرگتر از x_0 (که یک عدد حقیقی است) داشته باشیم: [4]

$$|f(x)| \leq |C g(x)| \quad (2-39)$$

یا به عبارت دیگر:

$$f(x) = O(g(x)) \Leftrightarrow \exists (C > 0), x_0 : \forall (x > x_0) |f(x)| \leq |C g(x)| \quad (2-40)$$

چند خاصیت از $Big O$:

$$1. f_1 = O(g_1), f_2 = O(g_2) \rightarrow \begin{cases} f_1 \cdot f_2 = O(g_1 \cdot g_2) \\ f_1 + f_2 = O(g_1 + g_2) \end{cases} \quad (41-2)$$

$$2. f_1 = O(g), f_2 = O(g) \rightarrow f_1 + f_2 = O(g) \quad (42-2)$$

$$3. f \cdot O(g) = O(f \cdot g) \quad (43-2)$$

$$4. f + O(g) = O(f + g) \quad (44-2)$$

$$5. f = O(g) \rightarrow cf = O(g) \quad (45-2)$$

تابع Ω Big :

می‌گوئیم $f(x) = \Omega g(x)$ یا $f(x) \in \Omega g(x)$ اگر و فقط اگر یک عدد حقیقی و مثبت c وجود داشته باشد

به طوری که برای x های بزرگتر از x_0 (که یک عدد حقیقی است) داشته باشیم:

$$|f(x)| \geq |c g(x)| \quad (46-2)$$

تابع Θ Big :

می‌گوئیم $f(x) = \Theta g(x)$ یا $f(x) \in \Theta g(x)$ اگر و فقط اگر دو عدد حقیقی و مثبت c و c' وجود داشته باشد

به طوری که برای x های بزرگتر از x_0 (که یک عدد حقیقی است) داشته باشیم:

$$|c g(x)| \leq |f(x)| \leq |c' g(x)| \quad (47-2)$$

فصل ۳

جستجوی کوانتومی

جستجو^۹ عبارتست از پیدا کردن گزینه یا گزینه‌های مطلوب (جواب) در میان گزینه‌های دیگر که مطلوب نظر ما نیستند.

برای انجام عمل جستجو، در علم کامپیوتر الگوریتم‌هایی طراحی شده است و از آنجا که الگوریتم جستجو به عنوان یک زیرالگوریتم در دل الگوریتم‌های بسیاری بکار گرفته می‌شود از اهمیت زیادی برخوردار است به نحوی که هر چه الگوریتم جستجو سریع‌تر و بهینه‌تر باشد، به تبع آن، الگوریتم‌های دیگر که از الگوریتم جستجو بهره می‌گیرند، سریع‌تر و بهینه‌تر خواهند بود.

در روش کلاسیک که در کامپیوترهای کلاسیکی مورد استفاده قرار می‌گیرد، برای جستجوی یک گزینه در میان N گزینه، از ابتدا تک تک گزینه‌ها بصورت جداگانه و متوالی بررسی می‌شوند تا اینکه نهایتاً جواب مورد نظر حاصل شود. در این روش تا قبل از رسیدن به جواب، به طور میانگین $N/2$ بار عمل بررسی انجام می‌شود زیرا جواب ممکن است در بررسی اولین گزینه بدست آید و یا ممکن هم هست که در بررسی N امین گزینه حاصل شود، که میانگین‌اش می‌شود $N/2$.

بعد از اینکه مبحث کامپیوترهای کوانتومی ابداع شد، نشان داد که یک کامپیوتر کوانتومی حداقل می‌تواند کامپیوترهای کلاسیکی را شبیه سازی کند و از نظر قدرت با آنها برابری کند، اما بعداً چندین الگوریتم کوانتومی نوشته شد که از الگوریتم‌های متناظر کلاسیکی‌اشان بسیار سریع‌تر عمل می‌کردند که این قدرت بیشتر کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیکی را اثبات می‌کرد. یکی از این الگوریتم‌ها، الگوریتم جستجوی کوانتومی بود که توسط گراور^{۱۰} در سال ۱۹۹۶ برای اولین بار ارائه شد. این الگوریتم توانست یک

^۹ Search

^{۱۰} L.Grover

گزینه‌ی مشخص را در $O(\sqrt{N})$ مرحله^{۱۱}، در میان N گزینه پیدا کند که این نسبت به مورد کلاسیکی که در $N/2$ مرحله بود سریع تر است.

۳-۲- مسئله‌ی جستجوی کوانتومی

فرض کنید که برای مثال یک دفترچه تلفن داریم که N شماره به صورت نامرتب در آن ثبت شده و این شماره ها بوسیله‌ی اعداد 0 تا $N-1$ اندیس گذاری شده‌اند. حال می‌خواهیم از میان این شماره‌ها به دنبال یک شماره ی خاص بگردیم. واضح است که برای پیدا کردن این شماره کافیست تا فقط اندیس مربوط به آن را پیدا کنیم .

برای جستجوی کوانتومی، شماره‌های تلفن (یا هر چیز دیگر) را با کت‌های n کیوبیتی اندیس گذاری می‌کنیم . هر کدام از این کت‌ها، پایه‌ای از یک فضای 2^n بعدی است. یک سیستم n کیوبیتی می‌تواند $N = 2^n$ شماره تلفن را اندیس گذاری کند. برای مثال فرض کنید $N=8$ شماره تلفن داریم، برای اندیس گذاری این هشت شماره، نیاز به یک سیستم سه کیوبیتی داریم زیرا در این سیستم می‌توانیم هشت پایه تشکیل دهیم و هر پایه را اندیس یک شماره تلفن قرار دهیم:

اندیس ها $|111\rangle |110\rangle |101\rangle |100\rangle |011\rangle |010\rangle |001\rangle |000\rangle : |i\rangle$

بنابراین مسئله‌ی جستجوی کوانتومی عبارتست از پیدا کردن یک حالت پایه‌ی خاص در میان 2^n حالت موجود. این حالت خاص را که همان جواب مسئله است، $|w\rangle$ می‌نامیم. [9,4]

۳-۳- الگوریتم گراور

در الگوریتم جستجوی گراور، اولین مرحله تشکیل یک کت حالت است که حاصل برهم‌نهی^{۱۲} تمامی

^{۱۱} step

^{۱۲} superposition

پایه‌های فضای n بعدی (که به عنوان اندیس به کار گرفته می شوند) باشد. این کت باید با تمام این پایه‌ها هم‌پوشانی برابر داشته باشد [4]. ما آن را با $|\Psi_1\rangle$ نشان می‌دهیم:

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}} \sum_i |i\rangle \quad (1-3)$$

این حالت با اعمال عملگر $H^{\otimes n}$ روی کت $|0^{\otimes n}\rangle$ بدست می‌آید^{۱۳}:

$$H^{\otimes n} |0^{\otimes n}\rangle = \sum_i |i\rangle \quad (2-3)$$

ایده‌ی کلی در روش الگوریتم گراور افزایش تدریجی دامنهی جواب $(|w\rangle)$ و کاهش دامنهی $|i\rangle$ های دیگر است تا جایی که اندازه‌ی دامنهی جواب بسیار زیاد و اندازه‌ی دامنهی دیگر بسیار کم شود. در این صورت با اندازه‌گیری حالت سیستم، جواب مسئله‌ی جستجو با احتمال بالایی بدست می‌آید. برای این کار، بعد از اولین مرحله، الگوریتم حلقه‌ی زیر را که خود شامل چهار مرحله است بارها و بارها تکرار می‌کند [9]:

۱- عملگر I_w را اثر بده. (که حالت جواب را به اندازه‌ی π درجه تغییر فاز می‌دهد)

۲- عملگر $H^{\otimes n}$ را اثر بده.

۳- عملگر $-I_0$ را اثر بده. (که تمامی حالت‌ها را به غیر از حالت $|0^{\otimes n}\rangle$ را به اندازه‌ی π درجه تغییر فاز می‌دهد)

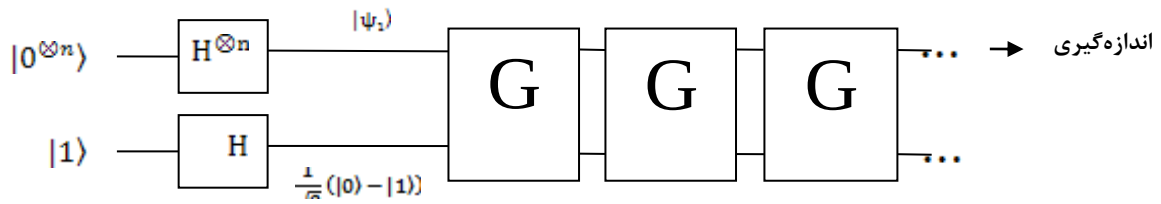
۴- عملگر $H^{\otimes n}$ را اثر بده.

در ادامه به بررسی اجزای حلقه‌ی فوق پرداخته و نشان خواهیم داد این حلقه که به حلقه‌ی تکرار گراور یا عملگر گراور معروف است در هر بار تکرار ابتدا دامنهی جواب را منفی کرده و سپس تمامی دامنه‌ها را نسبت به میانگینشان انعکاس می‌دهد که سبب افزایش دامنهی جواب و کاهش دامنه‌های دیگر می‌شود.

¹³ در مقاله‌ی گراور، عملگر $H^{\otimes n}$ به نام Walsh Hadamard معرفی شده که برابر است با:

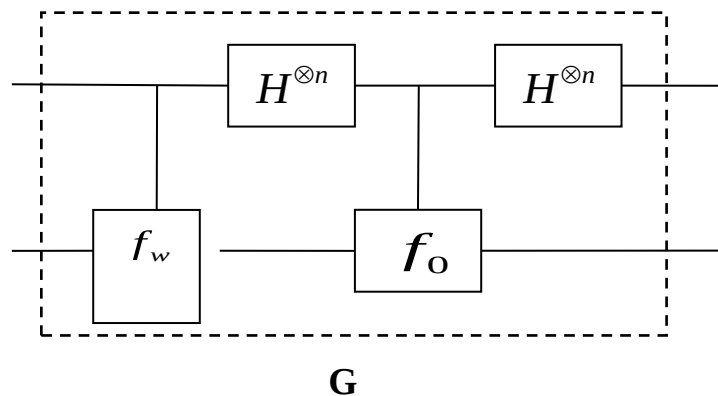
$$W_{ij} = (H^{\otimes n})_{ij} = 2^{-n/2} (-1)^{i \cdot j} \quad i, j = 0, 1, \dots, 2^n - 1$$

مداری که برای اجرای الگوریتم گراور استفاده می‌شود به طور کلی به شکل زیر است:



شکل ۳-۱ - مدار الگوریتم گراور

که در آن هر جعبه‌ی G یک مدار عملگر گراور است که ساختار داخلی آن به شکل زیر است:



شکل ۳-۲ - مدار داخلی عملگر گراور

اکنون به بررسی اجزای مدار G و عملکرد آنها می‌پردازیم.

f_w در واقع یک f -gate است. کاری که f_w انجام می‌دهد این است که ضریب $|i\rangle$ بی که جواب مسئله‌ی جستجو است ($|w\rangle$) را منفی می‌کند و ضریب $|i\rangle$ هایی که جواب نیستند را بدون تغییر باقی می‌گذارد. همان‌طور که در فصل دوم اشاره شد، یک f -gate که کیوبیت هدف آن $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ باشد، در کل به این صورت عمل می‌کند:

$$|i\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right] \rightarrow (-1)^{f_w(i)} |i\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right] \quad (3-3)$$

$$\sum_i a_i |i\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right] \rightarrow \sum_i (-1)^{f_w(i)} a_i |i\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right] \quad (4-3)$$

در عملگر گراور: $f_w(i) = \delta_{i,w}$ در نتیجه:

$$\sum_i |i\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right] \rightarrow \sum_i (-1)^{\delta_{i,w}} |i\rangle \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right] \quad (5-3)$$

همان طور که می بینیم کیوبیت هدف بعد از عمل f_w هم چنان بدون تغییر باقی مانده است و از آنجا که در ادامه نیز هرگز تغییر نمی کند، می توان آن را در محاسبات نادیده گرفت و حذف کرد.

شکل عملگری f_w که I_w می نامیم را می توان به صورت زیر تعریف کرد:

$$I_w = I - 2|w\rangle\langle w| \quad (6-3)$$

اجزای دیگر عملگر گراور، شامل دو عملگر والش - هادامارد^{۱۴} ($H^{\otimes n}$) و یک f-gate دیگر (f_n) است. f_n همانند f_w عمل می کند با این تفاوت که ضریب همه $|i\rangle$ ها را بجای $|0^{\otimes n}\rangle$ منفی می کند. یعنی:

$$|i\rangle \rightarrow (-1)^{1+\delta_{i,0}} |i\rangle \quad (7-3)$$

با توجه به آنچه گفته شد، اکنون می توانیم عملگر گراور را تشکیل دهیم:

$$G = -H^{\otimes n} I_n H^{\otimes n} I_w = -H^{\otimes n} (I - 2|0^{\otimes n}\rangle\langle 0^{\otimes n}|) H^{\otimes n} (I - 2|w\rangle\langle w|) \quad (8-3)$$

که در آن I_n عملگری است که ضریب $|0^{\otimes n}\rangle$ را منفی و ضریب بقیه $|i\rangle$ ها را بدون تغییر باقی می گذارد:

$$I_n = I - 2|0^{\otimes n}\rangle\langle 0^{\otimes n}| \quad (9-3)$$

¹⁴ Walsh-Hadamard

از طرفی چون $H^{\otimes n} |0^{\otimes n}\rangle = |\Psi_1\rangle$ و همچنین $H^{\otimes n} H^{\otimes n} = I$ خواهیم داشت:

$$G = (2 |\Psi_1\rangle\langle\Psi_1| - I)(I - 2|w\rangle\langle w|) = I_\epsilon I_w \quad (10-3)$$

که در آن: $I_\epsilon = 2 |\Psi_1\rangle\langle\Psi_1| - I$.

می‌توان نشان داد که عملگر I_ϵ دامنه‌های هر حالت دلخواه $|\Psi'\rangle = \sum_i a_i |i\rangle$ را حول مقدار متوسط دامنه‌ها انعکاس می‌دهد:

$$I_\epsilon |i\rangle = (2 |\Psi_1\rangle\langle\Psi_1| - I) |i\rangle = 2 |\Psi_1\rangle\langle\Psi_1|i\rangle - |i\rangle \quad (11-3)$$

داریم: $\langle\Psi_1|i\rangle = \frac{1}{\sqrt{N}}$ ، در نتیجه:

$$I_\epsilon |i\rangle = 2 \frac{1}{\sqrt{N}} |\Psi_1\rangle - |i\rangle \quad (12-3)$$

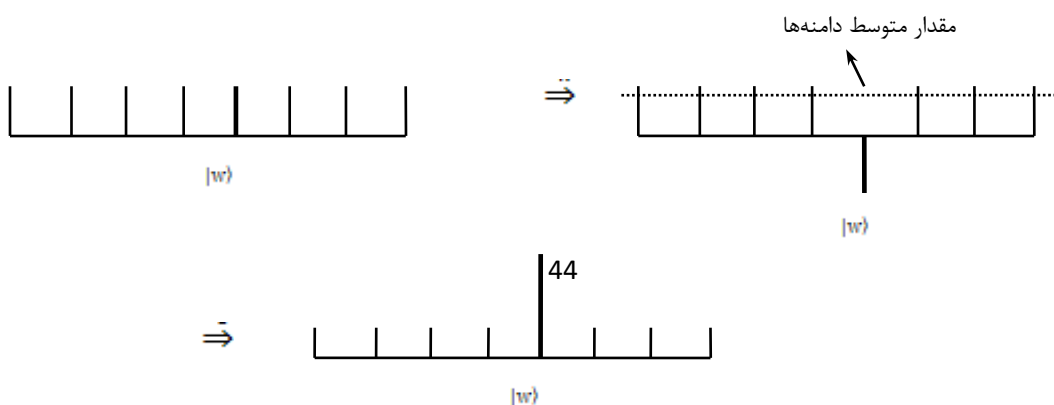
$$\Rightarrow I_\epsilon |\Psi'\rangle = 2 \frac{\sum_i a_i}{N} \sum_i |i\rangle - \sum_i a_i |i\rangle \quad (13-3)$$

در عبارت بالا $(\sum_i a_i)/N$ مقدار میانگین دامنه‌ها است و آن را با $\langle a \rangle$ نشان می‌دهیم در نتیجه:

$$I_\epsilon |\Psi'\rangle = \sum_i (2\langle a \rangle - a_i) |i\rangle \quad (14-3)$$

که این نشان می‌دهد I_ϵ دامنه‌ها را حول متوسط‌اشان انعکاس می‌دهد.

عملگر گراور در اولین حلقه را به صورت شماتیک می‌توان این‌طور نمایش داد [9]:



همان‌طور که از شکل (۳-۳) می‌بینیم دامنه‌ی جواب بطور قابل ملاحظه‌ای افزایش یافته اما دامنه‌های دیگر چون اختلاف کمی با مقدار میانگین داشتند، به مقدار کمی کاهش یافتند. با تکرار عملگر گراور، دامنه‌ی جواب بیشتر و بیشتر و دامنه‌های دیگر کمتر و کمتر می‌شود.

در مقاله‌ای که گراور ارائه کرد، فرض شده که تنها یک جواب در میان N گزینه وجود دارد، اما در صورتی که M جواب در میان N گزینه وجود داشته باشد و بخواهیم از این میان جوابی را پیدا کنیم، هم‌چنان روش گراور قابل کاربرد است، با این تفاوت که I_w یک f -gate است که بطور هم‌زمان دامنه‌ی تمام M جواب را منفی می‌کند و می‌توان آن را به صورت

$$I_w = [I - 2 |w\rangle\langle w|] \quad (۳-۱۵)$$

نمایش داد. I_w هم هیچ تغییری نمی‌کند. [9,4]

۳-۴- تغییر عملگر گراور به عملگر دوران

عملگر گراور را هم‌چنین می‌توان به صورت ایجاد یک دوران در کت $|\Psi\rangle$ در صفحه‌ی یک نمودار دوبعدی با پایه‌های $|\alpha\rangle$ و $|\beta\rangle$ تعبیر کرد [4]. که $|\alpha\rangle$ کت نرمالیزه شده‌ی برهم‌نهی $|i\rangle$ هایی است که جزو جواب نیستند و برابر است با:

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum' |i\rangle \quad (۱۶-۳)$$

که $\sum''$ یعنی جمع روی i هایی که جواب نیستند.

و $|\beta\rangle$ کت نرمالیزه شده ی برهم نهش $|i\rangle$ هایی است که جزو جوابند و برابر است با:

$$|\beta\rangle = \frac{1}{\sqrt{N}} \sum' |i\rangle \quad (۱۷-۳)$$

که $\sum'$ یعنی جمع روی i هایی که جواب هستند.

حال $|\Psi_1\rangle$ را می توان به این صورت نوشت:

$$|\Psi_1\rangle = \cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle \quad (۱۸-۳)$$

بعد از اینکه عملگر I_w اثر می کند، دامنه ی جواب ها منفی می شود و بنابراین:

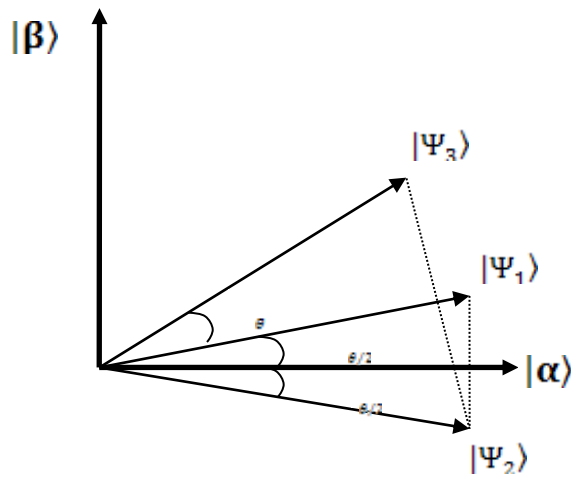
$$|\Psi_1\rangle \rightarrow |\Psi_2\rangle = \cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle \quad (۱۹-۳)$$

یعنی $|\Psi_1\rangle$ حول $|\alpha\rangle$ انعکاس می یابد.

سپس با عمل عملگر I_x بر $|\Psi_2\rangle$ ، این کت حول کت $|\Psi_1\rangle$ انعکاس می یابد:

$$\begin{aligned} I_x |\Psi_2\rangle &= (2|\Psi_1\rangle\langle\Psi_1| - I) |\Psi_2\rangle = 2\langle\Psi_1|\Psi_2\rangle |\Psi_1\rangle - |\Psi_2\rangle \\ \Rightarrow I_x |\Psi_2\rangle &= \cos\left(\frac{\theta}{2}\right) |\alpha\rangle + \sin\left(\frac{\theta}{2}\right) |\beta\rangle = |\Psi_3\rangle \end{aligned} \quad (۲۱-۳)$$

همان طور که از شکل (۴-۳) پیداست $|\Psi_3\rangle$ کت انعکاس یافته ی $|\Psi_2\rangle$ حول $|\Psi_1\rangle$ است.



شکل ۳-۴- نمودار دوران حالت سیستم تحت تأثیر عملگر گراور

کت حالت با اثر عملگر گراور همواره در این صفحه‌ی دوبعدی باقی می‌ماند و از آن خارج نمی‌شود.

نتیجه حاصل از این دو انعکاس متوالی معادل است با یک دوران به اندازه‌ی θ درجه به سمت پایه‌ی $|\beta\rangle$ بنابراین عملگر گراور معادل است با یک ماتریس دوران:

$$G = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \quad (۲۲-۳)$$

این عملگر در هر بار تکرار، کت حالت سیستم را بوسیله‌ی دوران، به $|\beta\rangle$ نزدیک و نزدیک‌تر می‌کند. کت حالت در k امین تکرار عملگر گراور برابر خواهد بود با:

$$G^k |\Psi_1\rangle = \cos\left(\frac{2k+1}{2}\theta\right) |\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right) |\beta\rangle \quad (۲۳-۳)$$

۳-۵- تعداد تکرارهای لازم برای رسیدن به بیشینه‌ی احتمال

اکنون سوال مهمی که مطرح است این است که بیشینه‌ی احتمال دست‌یابی به جواب، در چندمین تکرار حاصل می‌شود؟

حالت سیستم در الگوریتم گراور بعد از k امین تکرار با رابطه‌ی (۲۳-۳) تعیین می‌شود. با توجه به این رابطه

$$P_{\beta}^k = \sin^2 \left[(2k+1) \frac{\theta}{2} \right] \quad \text{احتمال رسیدن به جواب بعد از } k \text{ امین تکرار برابر است با:}$$

و احتمال نرسیدن به جواب (احتمال خطا) بعد از k امین تکرار برابر: $P_{n\pi}^k = \cos^2 \left((2k+1) \frac{\theta}{2} \right)$

در صورتی که k را بجای اینکه عددی صحیح باشد یک عدد حقیقی ($\bar{k}$) فرض کنیم، آنگاه حداکثر احتمال ممکن برای رسیدن به جواب برابر یک خواهد بود [10]:

$$\frac{2k+1}{2} \theta = \frac{\pi}{2}$$

$$k = \frac{\pi}{2\theta} - \frac{1}{2} \quad (24-3)$$

اما تعداد تکرارهای الگوریتم باید عددی صحیح باشد، بنابراین نزدیکترین عدد صحیح به $\bar{k}$ برابر با تعداد تکرارهای لازم برای دستیابی به حداکثر احتمال موفقیت خواهد بود (که ما آن را با R نشان می‌دهیم). واضح است که نزدیک‌ترین عدد صحیح برابر است با:

$$R = \left\lfloor \frac{\pi}{2\theta} \right\rfloor \quad (25-3)$$

زیرا $|R - \bar{k}| \leq 1/2$ است. در رابطه‌ی فوق علامت $| \cdot |$ ، عملگر جزء صحیح^{۱۵} است و همچنین θ برابر است با:

$$\theta = 2 \arcsin \sqrt{\frac{M}{N}} \quad (26-3)$$

۳-۶- حداکثر احتمال خطا چقدر است؟

از رابطه‌ی $|R - \bar{k}| \leq 1/2$ خواهیم داشت:

$$\left| (2R+1) \frac{\theta}{2} - (2k+1) \frac{\theta}{2} \right| \leq \frac{\theta}{2} \quad (27-3)$$

^{۱۵} floor operation

از طرفی داشتیم $\frac{\pi}{2} = \frac{\pi}{2} (2k+1)$ ، بنابراین:

$$\left| (2R+1)\frac{\theta}{2} - \frac{\pi}{2} \right| \leq \frac{\theta}{2} \rightarrow \left| \sin \left((2R+1)\frac{\theta}{2} - \frac{\pi}{2} \right) \right| \leq \left| \sin \left(\frac{\theta}{2} \right) \right|$$

$$\cos^2 \left((2R+1)\frac{\theta}{2} \right) \leq \sin^2 \left(\frac{\theta}{2} \right) \Rightarrow P_{ns}^R \leq \frac{M}{N} \quad (28-3)$$

بنابراین حداکثر احتمال خطا، M/N است. [10]

برای وقتی که تعداد جواب‌ها از تعداد کل گزینه‌ها خیلی کمتر باشد ($M \ll N$) آنگاه R را می‌توان با تقریب نسبتاً خوبی برحسب M/N بدست آورد:

$$R = \left\lceil \frac{\pi/2}{2 \arcsin(\sqrt{M/N})} \right\rceil \quad (29-3)$$

$$\Rightarrow R \leq \left\lceil \frac{\pi}{4} \sqrt{N/M} \right\rceil \leq \frac{\pi}{4} \sqrt{N/M}$$

$$\Rightarrow R = O(\sqrt{N/M}) \quad (30-3)$$

این اثباتی بر این مطلب است که جستجوی کوانتومی در $O(\sqrt{N/M})$ مرحله به جواب می‌رسد. اما همان‌طور که از رابطه (29-3) مشخص است برای دانستن R ، ما باید تعداد جواب (M) را بدانیم، که این به خودی خود یک ضعف برای این روش به شمار می‌رود چون در حالت کلی ممکن است M نامشخص باشد. در آن صورت نمی‌دانیم که چند بار باید الگوریتم را تکرار کنیم تا در نهایت وقتی که اندازه‌گیری می‌کنیم با بیشینه‌ی احتمال، جواب را بدست آوریم. البته بعدها روشی ابداع شد که در آن نیاز به دانستن M رفع شده و در نتیجه این ضعف را پوشش داده است.

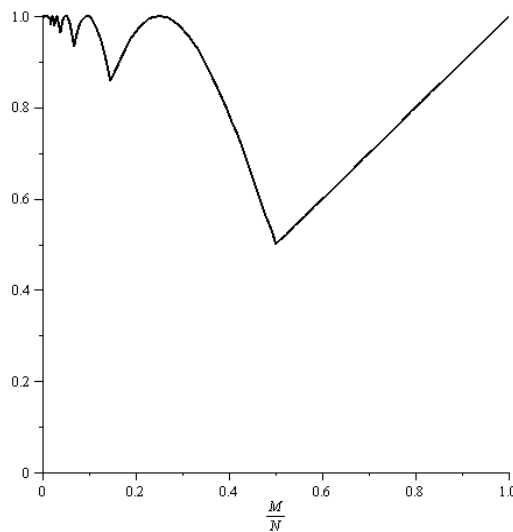
نکته‌ای که لازم است در اینجا به آن توجه کنیم این است که هم‌چنان یک احتمال ضعیف خطا وجود خواهد داشت، بنابراین برای حصول اطمینان از اینکه نتیجه‌ی حاصل از اندازه‌گیری قطعاً جواب است، لازم است حتماً نتیجه را بررسی کنیم و در صورت خطا مراحل از نو باید تکرار شود.

احتمال دستیابی به جواب (بعد از تکرار الگوریتم گراور به تعداد مناسب R)، برابر است با:

$$P_s^R = \sin^2 \left[\left(2 \left\lfloor \frac{\pi/2}{\theta} \right\rfloor + 1 \right) \frac{\theta}{2} \right]$$

$$= \sin^2 \left[\left(2 \left\lfloor \frac{\pi}{4 \arcsin(\sqrt{M/N})} \right\rfloor + 1 \right) \arcsin \sqrt{M/N} \right] \quad (3-31)$$

نمودار این احتمال بر حسب M/N به صورت زیر است:



شکل ۳-۵- نمودار احتمال موفقیت الگوریتم گراور

با توجه به این نمودار، می‌بینیم که برای مقادیری از M/N که از $1/2$ بیشتر است، P_s^R یک تابع خطی از M/N می‌باشد:

$$P_s^R = \frac{M}{N} \quad (32-3)$$

این نتیجه به این سبب است که برای این بازه، R برابر صفر است. به عبارت دیگر الگوریتم گراور برای بازه‌ی $\frac{1}{2} \leq \frac{M}{N} \leq 1$ ، کاملاً از کارآیی خود را از دست می‌دهد. این بزرگترین ضعف این الگوریتم به شمار می‌رود. در واقع همان‌طور که در نمودار می‌بینیم وقتی M/N از $1/4$ بیشتر می‌شود، P_s^R به شدت سقوط می‌کند و حدوداً فقط وقتی M/N کوچکتر از 0.4 است (که در این حالت احتمال دستیابی به جواب از 0.8 بیشتر است) می‌توان الگوریتم را کارآمد دانست.

برای پوشش دادن این ضعف، روش‌هایی پیشنهاد شده است. یک روش وقتی است که از قبل بدانیم که M قطعاً از $N/2$ بزرگتر است [4]. در این صورت کافی است که یک گزینه را از میان N گزینه به صورت تصادفی انتخاب کنیم و بررسی کنیم که آیا جواب هست یا نه؟ در این صورت با توجه به اینکه $M \geq N/2$ است، احتمال اینکه این گزینه جواب باشد، حداقل $1/2$ است. البته با توجه به اینکه M ممکن است از قبل نامشخص باشد، این روش، روش کارآیی محسوب نمی‌شود.

روش پیشنهادی دیگر که در آن از قبل نیازی به دانستن M نیست، اضافه کردن N گزینه جدید (که هیچ‌کدام جزو جواب نیستند) به N گزینه قبلی است. با این کار تعداد گزینه‌ها به $2N$ افزایش می‌یابد و در این حالت، دیگر حتماً M از $(2N)/2$ کوچکتر است. برای این کار، یک کیوبیت $|0\rangle$ به n کیوبیت قبلی اضافه می‌کنیم. این کیوبیت نیز مانند n کیوبیت دیگر از گیت هادامارد عبور می‌کند و به $(|0\rangle + |1\rangle)/\sqrt{2}$ تبدیل می‌شود:

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{N}} \left(\sum'' |i\rangle + \sum' |i\rangle \right) \\ &= \frac{1}{\sqrt{2N}} \left[\sum'' (|0\rangle \otimes |i\rangle + |1\rangle \otimes |i\rangle) + \sum' |0\rangle \otimes |i\rangle + \sum' |1\rangle \otimes |i\rangle \right] \quad (33-3) \end{aligned}$$

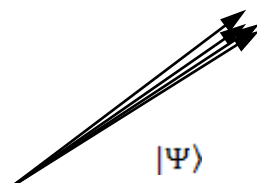
در مورد آخرین جمله باید گفت، وقتی به ابتدای یک جواب، کیوبیت $|1\rangle$ اضافه می‌شود، به طور قطع $|i\rangle \otimes |1\rangle$ دیگر جواب نخواهد بود اما اگر $|0\rangle$ به جواب اضافه شود $|i\rangle \otimes |0\rangle$ هم‌چنان یک جواب می‌باشد. در این روش با توجه به اینکه تعداد گزینه‌ها دو برابر می‌شود، تعداد تکرارهای الگوریتم هم به $\frac{2}{\sqrt{2}}$ افزایش می‌یابد. [4]

۳-۷- بهینگی الگوریتم جستجوی کوانتومی

یکی از مسائلی که در زمینه‌ی الگوریتم جستجوی کوانتومی مورد بررسی قرار گرفته، این است که آیا الگوریتم جستجویی که توسط گراور ارائه شده، الگوریتمی بهینه است یا نه؟ به عبارتی روشن‌تر آیا می‌توان برای کامپیوترهای کوانتومی الگوریتم جستجوی جدیدی طراحی کرد که سریع‌تر از $O(\sqrt{N})$ مرحله، تنها گزینه‌ی جواب را از میان N گزینه پیدا کند؟

در این بخش نشان می‌دهیم که الگوریتم گراور یک الگوریتم بهینه است.

در ابتدا مجموعه‌ای از N کامپیوتر کوانتومی را در نظر بگیرید که همگی در حالت اولیه‌ی یکسان $|\Psi\rangle$ هستند (و $|\Psi\rangle$ کت نرمالیزه شده در فضای N بعدی است).



فرض کنید هر یک از این N کامپیوتر کوانتومی، در اثر الگوریتم جستجو یکی از N گزینه را به عنوان جواب به دست می‌دهد. برای مثال اولین کامپیوتر کوانتومی اولین گزینه را، دومین کامپیوتر دومین گزینه را، ... و N امین کامپیوتر N امین گزینه را به عنوان جواب به دست می‌دهد.

الگوریتم جستجو را به صورت کلی برای هر یک از N کامپیوتر کوانتومی این‌طور نمایش می‌دهیم:

$$|\Psi_k^x\rangle \equiv U_k O_x U_{k-1} O_x \dots U_1 O_x |\Psi\rangle \quad (3-34)$$

که $|\Psi_k^x\rangle$ کت حالت x امین کامپیوتر کوانتومی بعد از k بار عمل عملگر O_x بر کت اولیه $|\Psi\rangle$ است. و O_x عملگری است که فاز جواب $|x\rangle$ را در x امین کامپیوتر کوانتومی به اندازه φ تغییر می‌دهد:

$$|x\rangle \rightarrow e^{i\varphi}|x\rangle \quad (3-35)$$

این عملگر در حالت کلی به صورت زیر نمایش داده می‌شود:

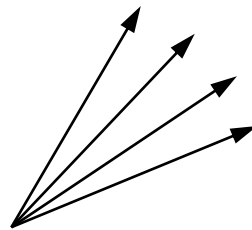
$$O_x = I - (1 - e^{i\varphi})|x\rangle\langle x| \quad (3-36)$$

U هم یک عملگر یکانی است.

برای مثال در الگوریتم گراور: $|\Psi\rangle = \sum_x (1/\sqrt{N})|x\rangle$ و $O_x = I - 2|x\rangle\langle x|$ که فاز جواب $|x\rangle$ را از $\varphi = 0$ به $\varphi = \pi$ تغییر می‌دهد. و عملگر یکانی U برابر است با:

$$U = -WI_0W \quad (3-37)$$

در اثر عمل الگوریتم جستجو، حالت‌های اولیه‌ی یکسان ($|\Psi\rangle$ ها) گسترش یافته و از هم باز می‌شوند.



آنچه که موجب این بازشدگی می‌شود قطعاً عملگر O_x است زیرا عملگرهای U در تمامی N کامپیوتر یکسانند و فقط O_x است که در کامپیوترهای مختلف $|x\rangle$ های متفاوتی را به عنوان جواب تغییر فاز می‌دهد. در صورتی که عملگرهای O_x را از الگوریتم جستجو حذف کنیم، کت $|\Psi_k\rangle$ که آن را به صورت زیر تعریف می‌کنیم، در تمام N کامپیوتر هم‌چنان یکسان است:

$$|\Psi_k\rangle \equiv U_k U_{k-1} \dots U_1 |\Psi\rangle \quad (3-38)$$

بنابراین اکنون می‌توانیم D_k را به عنوان معیاری برای میزان بازشدگی (که ناشی از عمل عملگر O_x است) به صورت زیر تعریف کنیم:

$$D_k \equiv \sum_x \|\Psi_k^x - \Psi_k\|^2 \quad (3-39)$$

(در رابطه‌ی بالا برای سادگی، کت‌های $|\Psi_k^x\rangle$ و $|\Psi_k\rangle$ را به ترتیب به صورت Ψ_k^x و Ψ_k نوشته‌ایم. همچنین نماد $\|A\|$ به معنی اندازه‌ی کت $|A\rangle$ یعنی $\sqrt{\langle A|A\rangle}$ است. نماد $\langle A|B\rangle$ هم از این پس به معنی اندازه‌ی عدد مختلط حاصل از ضرب داخلی دو کت $|A\rangle$ و $|B\rangle$ استفاده می‌شود.)

حال برای بررسی بهینگی، ابتدا نشان می‌دهیم که همواره بعد از k بار عمل عملگر O_x ، داریم $D_k \leq 4k^2$. برای این کار از روش استقرا استفاده می‌کنیم [11]:

$$k=0 \rightarrow D_0=0 \quad \text{داریم} \quad (3-40)$$

$$D_k \leq 4k^2 \quad \text{فرض،} \quad (3-41)$$

$$D_{k+1} \leq 4(k+1)^2 \quad \text{اثبات می‌کنیم} \quad (3-42)$$

$$\begin{aligned} D_{k+1} &= \sum_x \|U_{k+1} O_x \Psi_k^x - U_{k+1} \Psi_k\|^2 = \sum_x \|U_{k+1} (O_x \Psi_k^x - \Psi_k)\|^2 \\ &= \sum_x \|(O_x \Psi_k^x - \Psi_k)\|^2 \end{aligned}$$

$$D_{k+1} = \sum_x \|O_x (\Psi_k^x - \Psi_k) + (O_x - I) \Psi_k\|^2 \quad (3-43)$$

با توجه به اینکه $(O_x - I)|\Psi_k\rangle = -(1 - e^{i\varphi})|x\rangle\langle x|\Psi_k\rangle$ و با استفاده از نامساوی

$$\|a+b\|^2 \leq \|a\|^2 + 2\|a\|\|b\| + \|b\|^2$$

$$D_{k+1} \leq \sum_x (\|\Psi_k^x - \Psi_k\|^2 + 2|1 - e^{i\varphi}| \|\Psi_k^x - \Psi_k\| |\langle x|\Psi_k\rangle| + |1 - e^{i\varphi}|^2 |\langle x|\Psi_k\rangle|^2)$$

و چون $|1 - e^{i\varphi}| \leq 2$ است، بنابراین:

$$D_{k+1} \leq \sum_x (\|\Psi_k^x - \Psi_k\|^2 + 4\|\Psi_k^x - \Psi_k\| |\langle x | \Psi_k \rangle| + 4|\langle x | \Psi_k \rangle|^2) \quad (44-3)$$

اکنون با استفاده از نامساوی کوشی-شوارز (بخش ۱-۶ را ببینید)، نامساوی (۴۴-۳) را می‌توانیم اینگونه بنویسیم:

$$D_{k+1} \leq D_k + 4 \left(\sum_x \|\Psi_k^x - \Psi_k\|^2 \right)^{1/2} \left(\sum_x |\langle x | \Psi_k \rangle|^2 \right)^{1/2} + 4 \quad (45-3)$$

$$D_{k+1} \leq D_k + 4\sqrt{D_k} + 4 \quad (46-3)$$

با قرار دادن فرض (۴۱-۳) در نامساوی (۴۶-۳) خواهیم داشت:

$$D_{k+1} \leq 4(k+1)^2 \quad (47-3)$$

که این نشان می‌دهد که فرض ما درست بوده است، یعنی:

$$D_k \leq 4k^2 \quad (48-3)$$

وقتی الگوریتم جستجو بیشتر و بیشتر تکرار شود، $|\Psi_k^x\rangle$ که کت حالت x امین کامپیوتر کوانتومی است به کت پایه‌ی $|x\rangle$ نزدیک و نزدیک‌تر می‌شود تا جایی که در نهایت با آن برابر می‌شود، که در این صورت احتمال دستیابی به جواب برابر یک است. در این حالت D_k برابر است با:

$$D_k = \sum_x \|x - \Psi_k\|^2 \quad (49-3)$$

$$D_k = \sum_x \langle x - \Psi_k | x - \Psi_k \rangle = \sum_x (\langle x | x \rangle + \langle \Psi_k | \Psi_k \rangle - \langle x | \Psi_k \rangle - \langle \Psi_k | x \rangle)$$

$$D_k = 2N - \sum_x \left(\langle x | \Psi_k \rangle + \langle x | \Psi_k \rangle^* \right) \quad (50-3)$$

با توجه به اینکه $|\Psi_k\rangle$ یک کت نرمالیزه شده است، بیشینه‌ی عبارت دوم در رابطه‌ی بالا وقتی رخ می‌دهد که همه‌ی $\langle x|\Psi_k\rangle$ ها برابر مقدار حقیقی و مساوی $\frac{1}{\sqrt{N}}$ باشند. بنابراین:

$$D_k \geq 2N - 2 \sum_x \frac{1}{\sqrt{N}} \Rightarrow D_k = \sum_x \|\mathbf{x} - \Psi_k\|^2 \geq 2N - 2\sqrt{N} \quad (51-3)$$

اکنون از نامساوی‌های (51-3) و (48-3)، می‌توان حد پایینی را برای k به صورت زیر تعیین کرد:

$$2N - 2\sqrt{N} \leq D_k \leq 4k^2 \quad (52-3)$$

$$\Rightarrow k \geq \sqrt{\frac{1}{2} - \frac{1}{2\sqrt{N}}} \sqrt{N} \rightarrow k \geq 0.7071\sqrt{N} \quad (53-3)$$

یعنی الگوریتم‌های جستجوی کوانتومی برای اینکه به جواب برسند باید حداقل $0.7071\sqrt{N}$ بار تکرار شوند. بنابراین هیچ الگوریتم کوانتومی‌ای نمی‌تواند در کمتر از $\Omega\sqrt{N}$ مرحله به جواب برسد که این نشان می‌دهد الگوریتم جستجوی گراور الگوریتمی بهینه است.

اما باید توجه داشته باشیم که برای اثبات رابطه‌ی (53-3) فرض کرده بودیم که $|\Psi_k^x\rangle$ نهایتاً در اثر الگوریتم جستجو به کت جواب $|\mathbf{x}\rangle$ تبدیل می‌شود و احتمال دستیابی به جواب برابر یک است. اما همیشه این‌طور نیست و معمولاً یک احتمال خطایی هم وجود دارد. حال فرض کنیم احتمال دستیابی به جواب حداقل برابر $1/2$ باشد، یعنی:

$$|\langle \mathbf{x} | \Psi_k^x \rangle|^2 \geq \frac{1}{2} \quad (54-3)$$

در این حالت هم می‌توانیم بهینگی را اثبات کنیم [4]:

$$D_k \geq \sum_x \|\Psi_k^x - \mathbf{x}\|^2 - 2 \sum_x \|\Psi_k^x - \mathbf{x}\| \|\mathbf{x} - \Psi_k\| + \sum_x \|\mathbf{x} - \Psi_k\|^2 \quad (56-3)$$

با استفاده از نامساوی کوشی-شوارز برای جمله‌ی دوم، نامساوی فوق به شکل زیر در می‌آید:

$$D_k = \sum_x \|\Psi_k^x - x\|^2 - 2 \left(\sum_x \|\Psi_k^x - x\|^2 \right)^{1/2} \left(\sum_x \|x - \Psi_k\|^2 \right)^{1/2} + \sum_x \|x - \Psi_k\|^2 \quad (57-3)$$

$$D_k \geq \left(\left(\sum_x \|x - \Psi_k\|^2 \right)^{1/2} - \left(\sum_x \|\Psi_k^x - x\|^2 \right)^{1/2} \right)^2 \quad (58-3)$$

در نامساوی فوق در مورد عبارت $\sum_x \|\Psi_k^x - x\|^2$ داریم:

$$\sum_x \|\Psi_k^x - x\|^2 = \sum_x (2 - 2|\langle x | \Psi_k^x \rangle|) \quad (59-3)$$

$$\longrightarrow \sum_x \|\Psi_k^x - x\|^2 \leq (2 - \sqrt{2})N \quad (60-3)$$

حال با استفاده از نامساوی‌های (60-3) و (51-3) در نامساوی (58-3)، خواهیم داشت:

$$D_k \geq \left(\sqrt{2 - \frac{2}{\sqrt{N}}} - \sqrt{2 - \sqrt{2}} \right)^2 N \quad (61-3)$$

$$\rightarrow D_k \geq 0.42N \quad (62-3)$$

بنابراین از روابط (62-3) و (48-3)، می‌توان حد پایین k را محاسبه کرد:

$$0.42N \leq D_k \leq 4k^2 \quad \rightarrow k \geq 0.324\sqrt{N} \quad \Rightarrow k = \Omega(\sqrt{N}) \quad (63-3)$$

۳-۸- تشکیل الگوریتم گراور با عملگر یکانی دلخواه

همان‌طور که در بخش (3-3) اشاره شد، الگوریتم گراور به کمک عملگر Walsh-Hadamard تشکیل شد و

آن را به صورت زیر تعریف کردیم:

$$G = -W I_n W I_w \quad (64-3)$$

این عملگر را به تعداد $O(\sqrt{N})$ بار روی کت حالت $W|0\rangle$ اثر می‌دادیم و در نهایت اندازه‌گیری می‌کردیم:

$$GGG \dots G(W|0\rangle) = (-W I_0 W I_w) (-W I_0 W I_w) \dots (-W I_0 W I_w) W|0\rangle \quad (65-3)$$

عملگر گراور را می‌توان هم‌چنین به شکلی دیگر تعریف کرد:

$$G = -I_0 W I_w W \quad (66-3)$$

در این صورت رابطه‌ی (65-3) به شکل زیر تفسیر می‌شود:

$$WGGG \dots G|0\rangle = W(-I_0 W I_w W) (-I_0 W I_w W) \dots (-I_0 W I_w W)|0\rangle \quad (67-3)$$

یعنی عملگر گراور را اینگونه تعبیر کرده‌ایم: الگوریتم از حالت پایه‌ی $|0\rangle$ شروع می‌شود و بعد از اینکه G به تعداد $O(\sqrt{N/M})$ بار اثر کرد، یک بار عملگر W را اثر می‌دهیم و در نهایت اندازه‌گیری می‌کنیم که در این حالت با احتمال زیاد جواب $(|w\rangle)$ بدست می‌آید.

در این بخش نشان می‌دهیم [12]:

۱. حالت پایه‌ی اولیه به جای $|0\rangle$ ، می‌تواند هر حالت پایه‌ی دلخواه دیگری مانند $|s\rangle$ باشد.
۲. در عملگر گراور به جای Walsh-Hadamard، می‌توان هر عملگر یکانی دلخواه U را جایگزین کرد با

این شرط که $U_{ws} \ll 1$ باشد (که $U_{ws} = \langle w|U|s\rangle$):

$$Q = -I_s U^{-1} I_w U \quad (68-3)$$

(توجه کنید که در رابطه‌ی (68-3) اگر $U^{-1} = U = W$ باشد، در آنصورت $Q = G$ خواهد بود).

$$Q = -(I - 2|s\rangle\langle s|)U^{-1}(I - 2|w\rangle\langle w|)U$$

$$= -I + 2U^{-1}|w\rangle\langle w|U + 2|s\rangle\langle s| - 4U_{ws}^*|s\rangle\langle w|U \quad (۶۹-۳)$$

با توجه به رابطه‌ی (۶۹-۳) می‌توان دریافت که Q را می‌توان به صورت یک ماتریس 2×2 در یک فضای دوبعدی نشان داد که پایه‌های آن $U^{-1}|w\rangle$ و $|s\rangle$ هستند:

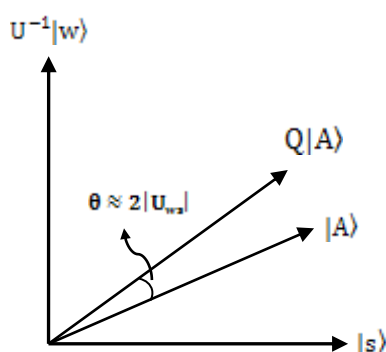
$$\left\{ \begin{array}{l} Q|s\rangle = -|s\rangle + 2U_{ws}U^{-1}|w\rangle + 2|s\rangle - 4|U_{ws}|^2|s\rangle = (1 - 4|U_{ws}|^2)|s\rangle + 2U_{ws}U^{-1}|w\rangle \\ Q(U^{-1}|w\rangle) = -U^{-1}|w\rangle + 2U^{-1}|w\rangle + 2U_{ws}^*|s\rangle - 4U_{ws}^*|s\rangle = -2U_{ws}^*|s\rangle + U^{-1}|w\rangle \end{array} \right.$$

عملگر Q هر کت حالت دلخواه $|A\rangle$ را در صفحه‌ی دو بعدی ذکر شده، با یک تبدیل در همین صفحه نگه می‌دارد.

$$|A\rangle = \alpha|s\rangle + \beta U^{-1}|w\rangle \quad (۷۰-۳)$$

$$Q \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 - 4|U_{ws}|^2 & 2U_{ws} \\ -2U_{ws}^* & 1 \end{pmatrix} \quad (۷۱-۳)$$

در اینجا نشان می‌دهیم که اگر $U_{ws} \ll 1$ باشد، عملگر Q در هر بار که بر کت $|A\rangle$ اثر می‌کند آن را تقریباً به اندازه‌ی زاویه‌ی $2|U_{ws}|$ در جهت خلاف عقربه‌های ساعت دوران می‌دهد.



شکل ۶-۳- دوران کت حالت در اثر عملگر Q

با توجه به رابطه‌ی (۷۱-۳)، بعد از k بار عمل عملگر Q ، ضرایب α_k و β_k به صورت زیرند:

$$\begin{cases} \alpha_k = (1 - 4|U_{ws}|^2) \alpha_{k-1} + 2U_{ws} \beta_{k-1} \\ \beta_k = -2U_{ws}^* \alpha_{k-1} + \beta_{k-1} \end{cases} \quad (72-3)$$

روابط (72-3) را می‌توان به صورت روابط بازگشتی زیر بازنویسی کرد:

$$\begin{cases} \alpha_k = (1 - 4|U_{ws}|^2) \alpha_{k-1} - \alpha_{k-2} \\ \beta_k = (1 - 4|U_{ws}|^2) \beta_{k-1} - \beta_{k-2} \end{cases} \quad (73-3)$$

فرض کنید که کت دلخواه $|A\rangle$ ، کت پایه‌ی $|s\rangle$ باشد. در نتیجه $\alpha_0 = 1$ و $\beta_0 = 0$ است. همچنین خواهیم داشت $\alpha_1 = 1 - 4|U_{ws}|^2$ و $\beta_1 = -2U_{ws}^*$. اکنون می‌توان با در نظر گرفتن این شرایط اولیه، روابط بازگشتی (73-3) را حل کرد.

حل معادله بازگشتی برای α_k :

$$\lambda^2 - 2(1 - 2|U_{ws}|^2)\lambda + 1 = 0 \quad (74-3)$$

$$\rightarrow \lambda_{1,2} = (1 - 2|U_{ws}|^2) \pm i\sqrt{1 - (1 - 2|U_{ws}|^2)^2}$$

$$1 - 2|U_{ws}|^2 = \cos \theta \quad \rightarrow \quad \lambda_{1,2} = \cos \theta \pm i \sin \theta = e^{\pm i\theta} \quad \text{فرض:}$$

$$\rightarrow \alpha_k = A e^{ik\theta} + B e^{-ik\theta} \quad (75-3)$$

از طرفی با توجه به تعریف $\cos \theta$ داریم $\sin \theta = 2|U_{ws}|/\sqrt{1 - |U_{ws}|^2}$ اما $U_{ws} \ll 1$ است بنابراین:

$$\sin \theta \approx 2|U_{ws}| \quad \rightarrow \quad \theta \approx \arcsin(2|U_{ws}|) \approx 2|U_{ws}| \quad (77-3)$$

در نتیجه α_k تقریباً برابر خواهد بود با:

$$\alpha_k \approx \frac{-2|U_{ws}|^2 + 2|U_{ws}|}{2|U_{ws}|} \sin(k\theta) + \cos(k\theta) - \sin(k\theta) \quad (78-3)$$

از توان دوم $|U_{ws}|$ صرف نظر می‌کنیم. در نتیجه:

$$\alpha_k \approx \cos(k\theta) \approx \cos(2k|U_{ws}|) \quad (79-3)$$

حل معادله برگشتی برای β_k :

در اینجا نیز تقریباً همان روشی را که در بدست آوردن α_k در پیش گرفتیم، استفاده می‌کنیم و نیز همان تقریب را بکار می‌بریم، با این تفاوت که در اینجا شرایط اولیه متفاوت است: $\beta_0 = 0$ و $\beta_1 = -2U_{ws}^*$. در اینصورت β_k تقریباً برابر خواهد بود با:

$$|\beta_k| \approx \sin(2k|U_{ws}|) \quad (80-3)$$

با توجه به روابط (79-3) و (80-3)، در هر بار که عملگر Q عمل می‌کند، کت حالت اولیه ($|s\rangle$) به اندازه‌ی زاویه‌ی $2|U_{ws}|$ به سمت $U^{-1}|w\rangle$ دوران می‌کند و وقتی Q به تعداد $k = \frac{\pi}{2|U_{ws}|}$ تکرار شود، کت حالت برابر $U^{-1}|w\rangle$ می‌شود و در نهایت با یک بار عمل عملگر U ، $|w\rangle$ که همان جواب است حاصل می‌شود. در نتیجه الگوریتم در $O(1/|U_{ws}|)$ به جواب می‌رسد. چون از ابتدا نمی‌دانیم $|w\rangle$ کدامیک از پایه‌ها است، بهترین نتیجه وقتی رخ می‌دهد که تمامی پایه‌ها در ابتدا در شرایط مساوی باشند، یعنی وقتی $|U|s\rangle$ دارای هم‌پوشانی مساوی با تمام پایه‌ها باشد:

$$U|s\rangle = \frac{1}{\sqrt{N}} \sum_i |i\rangle$$

$$\rightarrow \langle w|U|s\rangle = \langle w|\frac{1}{\sqrt{N}} \sum_i |i\rangle = \frac{1}{\sqrt{N}} \rightarrow O\left(\frac{1}{|U_{ws}|}\right) = O(\sqrt{N})$$

بنابراین الگوریتم بهینه می‌باشد.

۳-۹- تعداد نامشخص جواب‌ها^{۱۶}

همان‌طور که قبلاً گفتیم، وقتی تعداد جواب‌ها را از قبل ندانیم، در استفاده از الگوریتم گراور با مشکل مواجه می‌شویم. در سال ۱۹۹۸، مایکل بویِر^{۱۷} الگوریتمی را معرفی کرد که در دل خود از الگوریتم گراور استفاده می‌کرد. این الگوریتم که با $O(\sqrt{N/M})$ بار استفاده از الگوریتم گراور به جواب می‌رسد راه حلی است برای زمانی که M مشخص نباشد [10]. قبل از بررسی این الگوریتم باید به دو لم زیر توجه کنیم:

لم ۱: اگر α یک عدد حقیقی دلخواه و m یک عدد صحیح مثبت باشد، آنگاه:

$$\sum_j \cos((2j+1)\alpha) = \frac{\sin(2m\alpha)}{2\sin\alpha} \quad (۸۱-۳)$$

لم ۲: فرض کنید M تعداد جواب‌های مسئله (که نامشخص است) باشد و همچنین فرض کنید

$\sin\theta = \sqrt{M/N}$ باشد. m را هم یک عدد صحیح و مثبت دلخواه در نظر بگیرید و z هم یک عدد صحیح

باشد که به صورت تصادفی^{۱۸} از بازه‌ی $[0, m-1]$ انتخاب می‌شود. در این صورت بعد از z بار تکرار عمل الگوریتم

گراور بر روی حالت اولیه $|\Psi_1\rangle = \frac{1}{\sqrt{N}} \sum_i |i\rangle$ ، احتمال دستیابی به جواب برابر است با:

$$P_m = \frac{1}{2} - \frac{\sin(4m\theta)}{4m\sin(2\theta)} \quad (۸۲-۳)$$

و همچنین وقتی $m \geq 1/\sin(2\theta)$ آنگاه $P_m \geq 1/4$ است.

اثبات:

می‌دانیم احتمال رسیدن به جواب بعد از z بار تکرار در الگوریتم گراور برابر است با:

¹⁶ Unknown number of matches

¹⁷ Michel Boyer

¹⁸ random

$$P_s^j = \sin^2((2j+1)\theta)$$

حال اگر j عددی تصادفی در بازه‌ی $[0, m-1]$ باشد، متوسط احتمال دستیابی به جواب برابر خواهد بود با:

$$P_m = \sum_j \frac{1}{m} P_s^j = \frac{1}{m} \sum_j \sin^2((2j+1)\theta) = \frac{1}{2m} \sum_j 1 - \cos(2(2j+1)\theta) \quad (۸۳-۳)$$

با استفاده از لم ۱:

$$\Rightarrow P_m = \frac{1}{2} - \frac{\sin(4m\theta)}{4m\sin(2\theta)} \quad (۸۴-۳)$$

حال برای وقتی که $m \geq 1/\sin(2\theta)$ است، داریم:

$$\frac{1}{m\sin(2\theta)} \leq 1 \rightarrow \frac{\sin(4m\theta)}{4m\sin(2\theta)} \leq \frac{\sin(4m\theta)}{4} \leq \frac{1}{4} \rightarrow P_m \geq \frac{1}{4} \quad (۸۵-۳)$$

۳-۹-۱- الگوریتم بویر

قبل از هر چیزی فرض می‌کنیم که $1 \leq M \leq 3N/4$ باشد. (البته M می‌تواند هر بازه‌ای به صورت $1 \leq M \leq 1$ (که $1 < N$) باشد اما قطعاً تمام بازه‌ی $[1, N]$ را نمی‌تواند پوشش دهد. بعداً در این مورد بحث می‌کنیم).

الگوریتم بویر شامل مراحل^{۱۹} زیر است:

۱. قرار بده: $m=1$ و $\lambda = 8/7$ ، λ می‌تواند هر عدد حقیقی دیگری در بازه‌ی $[1, 4/3]$ باشد)

۲. عدد صحیح z را به صورت تصادفی از بازه‌ی $[0, m]$ انتخاب کن.

۳. الگوریتم گراور را به تعداد z بار با حالت اولیه‌ی $|\Psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$ تکرار کن.

۴. حالت نهایی را اندازه‌گیری کن. (فرض کنیم خروجی i باشد)

۵. اگر $f(i) = 1$ بود (یعنی اگر i یک جواب بود)، آنگاه از حلقه خارج شو.

۶. در غیر این صورت قرار بده $m = \min(\lambda m, \sqrt{N})$ و سپس برو به مرحله ۲.

همان‌طور که مشخص است این الگوریتم به صورت تدریجی بازه‌ی $[0, m]$ را افزایش می‌دهد که نتیجه‌ی آن تعداد تکرارهای الگوریتم گراور به تدریج افزایش می‌یابد تا اینکه نهایتاً یک جواب بدست آید.

سوال اصلی در اینجا این است که آیا این الگوریتم کوانتومی می‌تواند در $O(\sqrt{N/M})$ مرحله به جواب برسد؟

جواب این سوال مثبت است. برای اثبات آن ابتدا m_0 را به صورت زیر تعریف می‌کنیم:

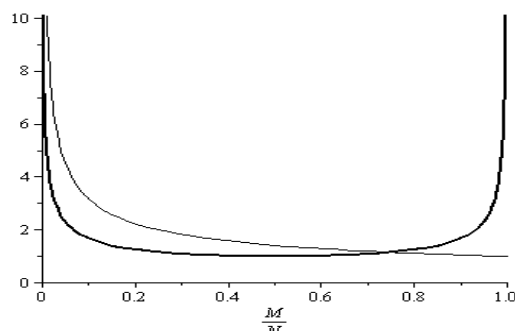
$$m_0 = \frac{1}{2\sqrt{\frac{M}{N}\left(1 - \frac{M}{N}\right)}} \quad (۸۶-۳)$$

برای وقتی $M \leq 3N/4$ باشد، داریم: $m_0 < \sqrt{N/M}$ و در نتیجه: $m_0 = O(\sqrt{N/M})$

البته برای M هایی که در بازه‌ی $3N/4 \leq M < N$ هستند هم نتیجه‌ی بالا را می‌توان بدست آورد زیرا در

این بازه، گرچه $m_0 > \sqrt{N/M}$ است اما ضریب حقیقی مثبتی (c) را می‌توان پیدا کرد (هرچند این

ضریب می‌تواند خیلی بزرگ باشد) که $m_0 < c\sqrt{N/M}$ شود که این یعنی $m_0 = O(\sqrt{N/M})$



شکل ۳-۷- نمودار m_0 بر حسب $\frac{M}{N}$

نمودار $\frac{m_0}{\sqrt{N/M}}$

اما این نتیجه را نمی‌توان برای تمام بازه‌ی $1 \leq M \leq N$ نتیجه گرفت زیرا همان‌طور که در نمودار مشخص است وقتی $M \approx N$ است آنگاه $m_0 \approx \infty$ و در آن صورت به ازای هر مقدار حقیقی از ضریب c داریم:

$$m_0 \ll c\sqrt{N/M} \quad (۸۷-۳)$$

هرگاه حلقه اصلی الگوریتم بویژه به تعدادی تکرار شود که $m \geq m_0$ گردد، آنگاه می‌گوییم که الگوریتم به مرحله‌ی بحرانی^{۲۰} رسیده است. تعداد تکرار لازم برای رسیدن به مرحله‌ی بحرانی برابر $\lceil \log_\lambda m_0 \rceil + 1$ است (که در آن $\lceil \cdot \rceil$ علامت ceiling operator است) زیرا:

مقدار m بعد از n امین تکرار $m = \lambda^{n-1}$:

$$\begin{aligned} m \geq m_0 &\Rightarrow \lambda^{n-1} \geq m_0 \Rightarrow n \geq (\log_\lambda m_0) + 1 \\ &\Longrightarrow A + 1 > [A] \quad \text{به طوری که } |[A] - A| < 1 \\ &\Rightarrow n > \lceil \log_\lambda m_0 \rceil \\ &\Rightarrow n \geq \lceil \log_\lambda m_0 \rceil + 1 \quad (۸۸-۳) \end{aligned}$$

در مرحله بحرانی همان‌طور که در لم ۲ اثبات شد، احتمال رسیدن به جواب حداقل برابر $1/4$ است.

در هر تکرار حلقه‌ی اصلی، j بار از الگوریتم گراور استفاده می‌شود و از آنجاکه j به صورت کاملاً تصادفی از بازه‌ی $0 \leq j < m$ انتخاب می‌شود، بنابراین الگوریتم گراور در هر بار تکرار حلقه اصلی، به طور میانگین $m/2$ بار تکرار می‌شود. بنابراین اکنون مقدار چشم‌داشتی تعداد تکرارهای الگوریتم گراور استفاده شده تا قبل از رسیدن به مرحله بحرانی برابر است با:

$$\sum_{n=1}^{\lceil \log_\lambda m_0 \rceil} \frac{1}{2} m = \frac{1}{2} \sum_{n=1}^{\lceil \log_\lambda m_0 \rceil} \lambda^{n-1} =$$

²⁰ critical stage

$$= \frac{1}{2} \left(\frac{\lambda^{\lceil \log_{\lambda} m_0 \rceil} - 1}{\lambda - 1} \right) \prec \frac{1}{2} \frac{\lambda^{(\log_{\lambda} m_0) + 1}}{\lambda - 1} = \frac{1}{2} \frac{\lambda m_0}{\lambda - 1} = 4m_0 \quad (۸۹-۳)$$

و از آنجا که $m_0 = O(\sqrt{N/M})$ ، بنابراین الگوریتم مذکور تا قبل از رسیدن به مرحله بحرانی در $O(\sqrt{N/M})$ مرحله به جواب می‌رسد. (البته اگر بتواند به جواب برسد)

در صورتی که تکرار از مرحله بحرانی بگذرد، آنگاه تعداد تکرارهای الگوریتم گراور مورد استفاده، از بعد از این مرحله، برابر است با:

$$\frac{1}{2} \sum_{u=0}^{\infty} \left(\frac{3}{4} \right)^u \lambda^{u + \lceil \log_{\lambda} m_0 \rceil} \prec \frac{2\lambda}{4 - 3\lambda} m_0 = 4m_0 \quad (۹۰-۳)$$

بنابراین تعداد کل الگوریتم‌های به کار گرفته شده، حداکثر برابر خواهد بود با:

$$4m_0 + 4m_0 = 8m_0 \quad (۹۱-۳)$$

پس در کل الگوریتم در $O(\sqrt{N/M})$ مرحله به جواب می‌رسد.

همان‌طور که گفتیم m_0 در تمام بازه‌ی $1 \leq M \leq N$ برابر $O(\sqrt{N/M})$ نیست. ضعف این الگوریتم هم در همین جاست. m_0 به ازای $M > 3N/4$ ، به شدت افزایش می‌یابد که این به معنی افزایش شدید استفاده از الگوریتم‌های گراور و افزایش شدید تعداد تکرارهای حلقه‌ی اصلی در الگوریتم بویر است.

فصل ۴

الگوریتم احمد یونس و الگوریتم

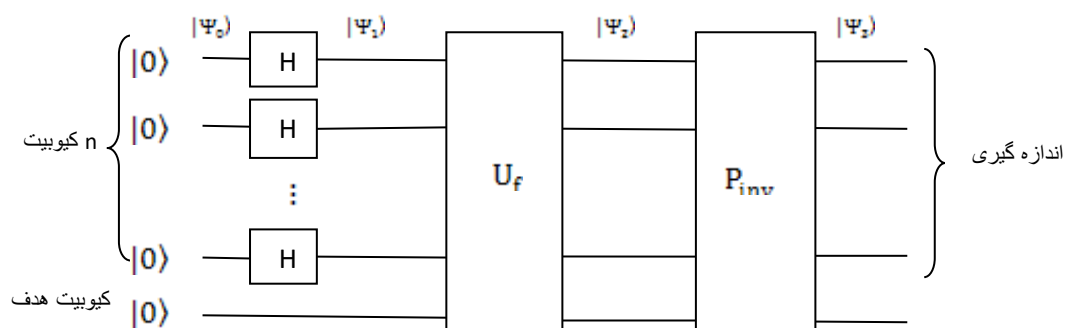
پیشنهادی جدید

۴-۱- مقدمه

در سال ۲۰۰۴ الگوریتم دیگری برای جستجوی کوانتومی پیشنهاد شد. این الگوریتم جالب که گراور هم به قوی تر بودن آن اعتراف کرده توسط احمد یونس^{۲۱} از مصر ارائه شد. در این روش بجای استفاده از عملگر I_n ، از عملگر دیگری مشابه با آن به نام "عملگر انتشار جزئی"^{۲۲} که در فضای $n+1$ کیوبیتی عمل می کند استفاده می شود، و همچنین از ایجاد درهم تنیدگی بین n کیوبیت تشکیل دهنده ی گزینه ها با کیوبیت هدف بهره می برد. احتمال دستیابی به جواب در الگوریتم جدید برای تمام مقادیر $1 \leq M \leq N$ ، حداقل برابر $0.88/0.87$ است که در مقایسه با الگوریتم گراور که حداقل برابر 0.5 می باشد بسیار کارآمدتر است. همچنین ضعف الگوریتم گراور که اشاره شد، در این الگوریتم وجود ندارد.

۴-۲- مدار الگوریتم احمد یونس

مداری که برای این الگوریتم جدید پیشنهاد شده است به صورت زیر است:



شکل ۴-۱: مدار الگوریتم احمد یونس

مشاهده می شود که این مدار از نظر ظاهری تفاوت هایی با مدار گراور دارد. ورودی این الگوریتم $|0\rangle \otimes |0^{\otimes n}\rangle$ است. کیوبیت هدف در اینجا بر خلاف الگوریتم گراور $|0\rangle$ است و مستقیماً با همین حالت به اپراتور U_f می رسد.

²¹ Ahmed Younes

²² partial diffusion operator

عملی که اپراتور U_f انجام می‌دهد نیز با I_w در الگوریتم گراور متفاوت است: در مورد عملکرد $U_{f...}$ در گراور داشتیم:

$$I_w|i\rangle\left[\frac{1}{2}(|0\rangle-|1\rangle)\right]=(-1)^{\delta_{i,w}}|i\rangle\left[\frac{1}{2}(|0\rangle-|1\rangle)\right] \quad (۱-۴)$$

و همان‌طور که قبلاً گفته شد، کیوبیت هدف در تمامی مراحل الگوریتم گراور بدون تغییر باقی می‌ماند و با n کیوبیت دیگر که $|i\rangle$ ها را می‌سازند، درهم‌تنیده نمی‌شود. اما در الگوریتم جدید، U_f بشکل زیر عمل می‌کند:

$$U_f|i,y\rangle \rightarrow |i,y \oplus f(i)\rangle \quad (۲-۴)$$

که در آن تابع $f(i)$ تابعی است که اگر i یک جواب باشد، مقدارش برابر 1 و اگر جواب نباشد، مقدارش برابر صفر است. y هم همان کیوبیت هدف است که می‌تواند 0 یا 1 باشد. در اولین تکرار الگوریتم، y برابر صفر است و:

$$U_f|i,0\rangle \rightarrow |i,0 \oplus f(i)\rangle = |i,f(i)\rangle \quad (۳-۴)$$

روند کار این الگوریتم را در اولین تکرار تا قبل از P_{inv} به طور خلاصه می‌توان اینگونه بیان کرد:

$$|\Psi_0\rangle = |0^{\otimes n}\rangle \otimes |0\rangle \longrightarrow$$

$$\rightarrow |\Psi_1\rangle = \left(\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle \rightarrow$$

$$\rightarrow |\Psi_2\rangle = U_f \left(\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |0\rangle\right) = U_f \left(\frac{1}{\sqrt{N}} |i\rangle |0\rangle + 0 \times \sum_{i=0}^{N-1} |i\rangle |1\rangle\right)$$

$$\rightarrow |\Psi_2\rangle = \left(\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} U_f |i\rangle |0\rangle + 0 \times \sum_{i=0}^{N-1} U_f |i\rangle |1\rangle\right) \rightarrow$$

$$\rightarrow |\Psi_2\rangle = \frac{1}{\sqrt{N}} \left(\sum' |i\rangle |0 \oplus f(i)\rangle + \sum'' |i\rangle |0 \oplus f(i)\rangle \right) + 0 \times \left(\sum' |i\rangle |1 \oplus f(i)\rangle + \sum'' |i\rangle |1 \oplus f(i)\rangle \right)$$

در رابطه‌ی بالا $\sum'$ جمع روی جملاتی است که در آن i یک جواب است. برای این جملات $f(i) = 1$ است. چون M جواب وجود دارد بنابراین $\sum'$ شامل M جمله است. $\sum''$ جمع روی جملاتی است که در آن i یک جواب نیست. برای این جملات $f(i) = 0$ است. $\sum''$ شامل $N-M$ جمله است.

$$|\Psi_2\rangle \equiv \left(\sum_{i=0}^{N-1} \alpha_i |i\rangle |0\rangle \right) + \left(\sum_{i=0}^{N-1} \beta_i |i\rangle |1\rangle \right)$$

همان‌طور که ملاحظه می‌شود عملکرد U_f سبب ایجاد یک درهم‌تنیدگی بین کیوبیت هدف و n کیوبیت دیگر می‌شود.

اکنون وقت آن است که P_{inv} بر روی $|\Psi_2\rangle$ عمل کند. P_{inv} (عملگر انتشار جزئی) عملگری مشابه I_n در گراور ولی در فضای $n+1$ کیوبیتی است:

$$P_{inv} = (H^{\otimes n} \otimes I) (2|0^{\otimes n+1}\rangle\langle 0^{\otimes n+1}| - I^{\otimes n+1}) (H^{\otimes n} \otimes I) \quad (4-4)$$

برای ساده‌نویسی، از این پس کت $|0^{\otimes n+1}\rangle$ را با $|0\rangle$ نشان می‌دهیم.

انتظار می‌رود که عملکرد P_{inv} هم‌چون I_n ، انعکاس دامنه‌های $|\Psi_2\rangle$ نسبت به مقدار میانگین دامنه‌ها باشد، اما این عمل را فقط روی دامنه‌های زیرفضای $|i\rangle \otimes |0\rangle$ انجام می‌دهد در حالی که دامنه‌های زیرفضای $|i\rangle \otimes |1\rangle$ را فقط منفی می‌کند:

در نتیجه:

$$|\Psi_3\rangle = P_{inv} |\Psi_2\rangle = \sum_{i=0}^{N-1} (2\langle\alpha\rangle - \alpha_i) |i\rangle |0\rangle - \sum_{i=0}^{N-1} \beta_i |i\rangle |1\rangle \quad (5-4)$$

مطلب قابل ذکر در اینجا این است که جملاتی از مجموع اول $|\Psi_2\rangle$ که ضریبشان (α_i) صفر بوده (یعنی جملاتی که $|i\rangle$ در آنها جواب بوده)، بعد از اعمال عملگر P_{inv} دیگر صفر نیست و برابر است با $2\langle\alpha\rangle - 0 = 2\langle\alpha\rangle$.

اکنون با توجه به نکته فوق و با توجه به اینکه:

$$\langle\alpha\rangle = \frac{\sum_{i=0}^{N-1} \alpha_i}{N} = \frac{(N-M) \frac{1}{\sqrt{N}} + M \times 0}{N} = \frac{N-M}{N\sqrt{N}} \quad (6-4)$$

$|\Psi_3\rangle$ را می‌توان به این صورت نوشت:

$$|\Psi_3\rangle = \left[\sum'' \left(2 \frac{N-M}{N\sqrt{N}} - \frac{1}{\sqrt{N}} \right) |i\rangle|0\rangle + \sum' \left(2 \frac{N-M}{N\sqrt{N}} - 0 \right) |i\rangle|0\rangle \right] - \sum' \frac{1}{\sqrt{N}} |i\rangle|1\rangle \quad (7-4)$$

که در رابطه‌ی فوق $\sum'$ جمع روی جملاتی است که در آن $|i\rangle$ یک جواب است و $\sum''$ جمع روی جملاتی است که $|i\rangle$ جواب نیست.

با توجه به رابطه‌ی (7-4) می‌بینیم که جملات حاوی جواب در دو زیرفضا ظاهر شده‌اند. در هر تکرار بعدی، U_F جای این دو زیرفضا را فقط در جمع‌های حاوی جواب عوض می‌کند، چون:

$$|i\rangle \otimes |0\rangle \rightarrow |i\rangle \otimes |0 \oplus 1\rangle = |i\rangle \otimes |1\rangle \quad \text{و} \quad |i\rangle \otimes |1\rangle \rightarrow |i\rangle \otimes |1 \oplus 1\rangle = |i\rangle \otimes |0\rangle$$

سپس با اعمال P_{inv} ، دامنه‌های زیرفضای $|i\rangle \otimes |0\rangle$ (اعم از جواب و غیر جواب) نسبت به میانگینشان انعکاس می‌یابند و از آنجاکه جای زیرفضاهای شامل جواب در هر تکرار توسط U_F عوض می‌شود، بنابراین در هر بار جای آن دسته از دامنه‌های جواب که باید به همراه دامنه‌های غیر جواب، نسبت به میانگینشان انعکاس یابند،

عوض می‌شود. کت حالت سیستم در k امین تکرار الگوریتم را در حالت کلی می‌توان به این صورت نمایش داد:

$$|\Psi^k\rangle = a_k \sum_{i=0}^{N-1} |i\rangle|0\rangle + b_k \sum_{i=0}^{N-1} |i\rangle|0\rangle + c_k \sum_{i=0}^{N-1} |i\rangle|1\rangle \quad (۸-۴)$$

از آنجا که عملگرهای U_f و P_{inv} که دائماً روی کت حالت عمل می‌کنند، هر دو یکانی^{۲۳} هستند و اندازه‌ی $|\Psi\rangle$ را تغییر نمی‌دهند، بنابراین همواره مجموع مجذور دامنه‌ها و در نتیجه مجموع احتمالات برابر یک است:

$$(N-M) a_k^2 + M (b_k^2 + c_k^2) = 1 \quad (۹-۴)$$

که در آن جمله‌ی اول سمت چپ تساوی، احتمال نرسیدن به جواب (P_{ns}^k) و جمله‌ی دوم احتمال رسیدن به جواب در k امین تکرار است (P_s^k).

یکانی بودن U_f

$$\text{داریم: } U_f|i\rangle|y\rangle = |i\rangle|y \oplus f(i)\rangle$$

$$\Rightarrow U_f U_f|i\rangle|y\rangle = U_f(|i\rangle|y \oplus f(i)\rangle) = |i\rangle|y \oplus f(i) \oplus f(i)\rangle$$

$$f(i) \oplus f(i) = 0 \Rightarrow U_f U_f|i\rangle|y\rangle = |i\rangle|y\rangle$$

$$\Rightarrow U_f U_f = I$$

بنابراین با توجه به هرمیتی بودن U_f ، یکانی بودن آن را می‌توانیم نتیجه بگیریم.

یکانی بودن P_{inv}

$$P_{inv} = (H^{\otimes n} \otimes I)(2|0\rangle\langle 0| - I^{\otimes n+1})(H^{\otimes n} \otimes I)$$

$$P_{inv}^\top = (H^{\otimes n} \otimes I)^\top (2|0\rangle\langle 0| - I^{\otimes n+1})^\top (H^{\otimes n} \otimes I)^\top \\ = (H^{\otimes n} \otimes I)(2|0\rangle\langle 0| - I^{\otimes n+1})(H^{\otimes n} \otimes I) = P_{inv}$$

$$P_{inv}^\top P_{inv} = (H^{\otimes n} \otimes I)(2|0\rangle\langle 0| - I^{\otimes n+1})(H^{\otimes n} \otimes I)(H^{\otimes n} \otimes I)(2|0\rangle\langle 0| - I^{\otimes n+1})(H^{\otimes n} \otimes I)$$

²³ Unitary

$$(H^{\otimes n} \otimes I)(H^{\otimes n} \otimes I) = I^{\otimes n+1}$$

$$\begin{aligned} \Rightarrow P_{inv}^T P_{inv} &= (H^{\otimes n} \otimes I)(2|0\rangle\langle 0| - I^{\otimes n+1})(2|0\rangle\langle 0| - I^{\otimes n+1})(H^{\otimes n} \otimes I) = \\ &= (H^{\otimes n} \otimes I)(4|0\rangle\langle 0|0\rangle\langle 0| - 2|0\rangle\langle 0| - 2|0\rangle\langle 0| + I^{\otimes n+1})(H^{\otimes n} \otimes I) \\ &= (H^{\otimes n} \otimes I)I^{\otimes n+1}(H^{\otimes n} \otimes I) = I^{\otimes n+1} \Rightarrow P_{inv}^T P_{inv} = I^{\otimes n+1} \end{aligned}$$

حال ثابت می‌کنیم که رابطه‌ی بین دامنه‌های $|\Psi^k\rangle$ به صورت بازگشتی زیر است:

$$\begin{cases} a_k = 2\langle \alpha_k \rangle - a_{k-1} \\ b_k = 2\langle \alpha_k \rangle - c_{k-1} \\ c_k = -b_{k-1} \end{cases} \quad (10-4)$$

که در آن :

$$\langle \alpha_k \rangle = \frac{(N-M)a_{k-1} + Mc_{k-1}}{N} \quad (11-4)$$

با حل معادلات بازگشتی (10-4) به روش استقرا به راحتی می‌توان a_k را و سپس b_k و c_k را محاسبه کرد:

$$a_k = \frac{1}{\sqrt{N}} \left(\frac{\sin((k+1)\theta)}{\sin(\theta)} - \frac{\sin(k\theta)}{\sin(\theta)} \right) \quad (12-4)$$

$$b_k = \frac{1}{\sqrt{N}} \left(\frac{\sin((k+1)\theta)}{\sin(\theta)} \right) \quad (13-4)$$

$$c_k = -\frac{1}{\sqrt{N}} \left(\frac{\sin(k\theta)}{\sin(\theta)} \right) \quad (14-4)$$

$$\sin \theta = \sqrt{2 \left(\frac{M}{N} \right) - \left(\frac{M}{N} \right)^2} \quad \text{و} \quad \cos \theta = 1 - \frac{M}{N}. \quad \text{که در آن}$$

در نتیجه برای احتمال موفقیت در k امین تکرار داریم:

$$P_s^k = M(b_k^2 + c_k^2) = (1 - \cos \theta) \left[\frac{\sin^2((k+1)\theta)}{\sin^2 \theta} - \frac{\sin^2(k\theta)}{\sin^2 \theta} \right] \quad (15-4)$$

۴-۳- تعداد تکرار لازم برای الگوریتم

برای پیدا کردن تعداد تکرار لازم، همانند روشی که در الگوریتم گراور در پیش گرفتیم، ابتدا فرض کنیم که k یک عدد حقیقی باشد (که آن را با $\bar{k}$ نشان می‌دهیم). اکنون حداکثر مقدار برای P_s به ازای $\bar{k}$ های مختلف برابر یک است. پس:

$$P_s = 1 \rightarrow \sin^2((k+1)\theta) + \sin^2(k\theta) = \frac{\sin^2 \theta}{1 - \cos \theta} = 1 + \cos \theta$$

$$\rightarrow \left[\frac{1}{2} - \frac{\cos(2(k+1)\theta)}{2} \right] + \left[\frac{1}{2} - \frac{\cos(2k\theta)}{2} \right] = 1 + \cos \theta$$

$$\rightarrow \cos(2(k+1)\theta) + \cos(2k\theta) + 2\cos \theta = 0$$

$$\rightarrow \cos \theta [\cos((2k+1)\theta) + 1] = 0$$

$$\Rightarrow \cos((2k+1)\theta) = -1 = \cos(\pi) \rightarrow k = \frac{\pi}{2\theta} - \frac{1}{2} \quad (16-4)$$

اکنون تعداد تکرار لازم (R) برابر با نزدیکترین عدد صحیح به $\bar{k}$ است، یعنی:

$$R = \left\lfloor \frac{\pi}{2\theta} \right\rfloor \quad (17-4)$$

و به ازای $M \ll N$ است، نیز داریم:

$$\theta = \arcsin \sqrt{2 \left(\frac{M}{N} \right) - \left(\frac{M}{N} \right)^2} \approx \sqrt{2 \left(\frac{M}{N} \right)}$$

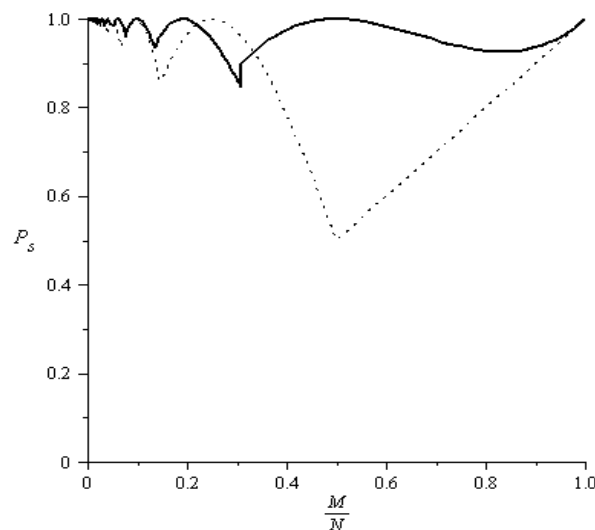
$$R \leq \frac{\pi}{2\theta} \approx \frac{\pi}{2\sqrt{2}} \sqrt{\frac{N}{M}} \rightarrow R = O\left(\sqrt{\frac{N}{M}}\right) \quad (18-4)$$

۴-۴- حداکثر احتمال موفقیت

با جایگذاری رابطه‌ی (۴-۱۷) به جای k در رابطه‌ی (۴-۱۵) حداکثر احتمال موفقیت در این الگوریتم به دست می‌آید:

$$P_s = (1 - \cos \theta) \left(\frac{\sin^2 \left(\left(\left\lfloor \frac{\pi}{2\theta} \right\rfloor + 1 \right) \theta \right)}{\sin^2 \theta} + \frac{\sin^2 \left(\left\lfloor \frac{\pi}{2\theta} \right\rfloor \theta \right)}{\sin^2 \theta} \right) \quad (۴-۱۹)$$

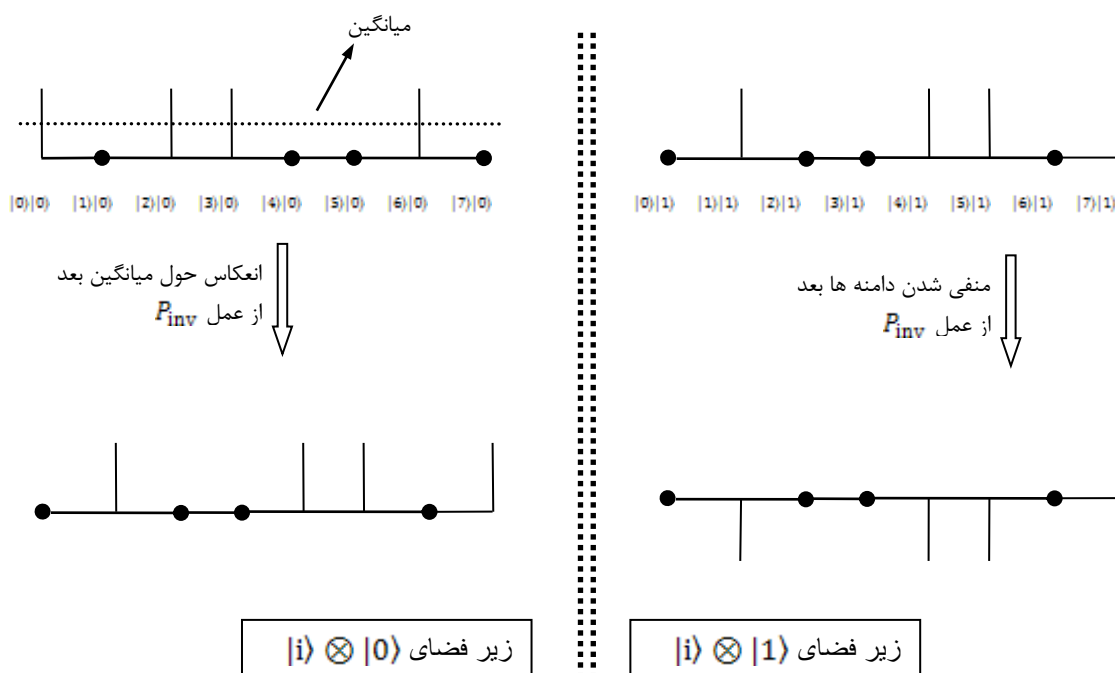
اکنون با جایگذاری $\theta = \arccos \left(1 - \frac{M}{N} \right)$ در رابطه‌ی (۴-۱۹)، می‌توان P_s را برحسب M/N رسم کرد. با مقایسه دو الگوریتم در شکل (۴-۲)، موفقیت الگوریتم احمد یونس به وضوح مشخص است. این الگوریتم هم‌چنین مشکل کارایی نداشتن الگوریتم گراور برای بازه‌ی $M \geq N/2$ را ندارد و برای $M \geq N/3$ ، یک بار تکرار می‌شود.



شکل ۴-۲: نمودار احتمال موفقیت الگوریتم احمد یونس

..... نمودار احتمال موفقیت الگوریتم گراور

دلیل این امر این است که در اولین تکرار و بعد از اینکه $|\Psi_1\rangle$ بوسیله‌ی عملگر U_F به دو زیرفضا تقسیم شد، حالت‌های غیر جواب در زیرفضای $|0\rangle \otimes |i\rangle$ تنها با حالت‌های جواب از همین زیرفضا (که دامنه‌ی همگی‌اشان صفر است) نسبت به میانگین‌اشان انعکاس می‌یابند که نتیجه‌اش کاهش دامنه‌ی حالت‌های غیر جواب است:



اما در الگوریتم گراور شکل ۴-۳: نمایش عملکرد P_{inv} بر زیر فضاهای سیستمی که در آن $M = N/2$ حالت‌های غیر جواب می‌شود.

۴-۶- تعداد نامشخص جواب‌ها

با توجه به رابطه‌ی (۴-۱۷) در می‌یابیم که در الگوریتم احمد یونس هم هم‌چون الگوریتم گراور نیاز داریم تا تعداد جواب‌ها را از قبل بدانیم. در مواردی که M مشخص نباشد می‌توانیم از الگوریتم بویر استفاده کنیم با این تفاوت که در آن بجای الگوریتم گراور، الگوریتم احمد یونس را جایگزین می‌کنیم. الگوریتم بویر جدید این مزیت را نسبت به قبلی دارد که برای تمام بازه‌ی $1 \leq M \leq N$ قابل استفاده است. ابتدا باید به لم زیر توجه کنیم:

لم: فرض کنید M تعداد جواب‌های مسئله باشد (که مقدارش نامشخص است) و θ در رابطه‌ی

$\cos(\theta) = 1 - M/N$ صدق کند. m عدد صحیح و مثبت باشد و k هم یک عدد صحیح و تصادفی از بازه‌ی

$[0, m-1]$ باشد. آنگاه احتمال دستیابی به جواب بعد از k بار تکرار الگوریتم احمد یونس بر روی حالت

اولیه‌ی $|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle$ برابر است با:

$$P_m = \frac{1}{1 + \cos \theta} \left(1 - \frac{\cos \theta \sin(2m\theta)}{2m \sin \theta} \right) \quad (۲۰-۴)$$

و هم‌چنین برای $m \geq 1/\sin(\theta)$ داریم: $P_m \geq 0.2725$.

اثبات:

احتمال موفقیت الگوریتم احمد یونس بعد از k بار تکرار از رابطه‌ی (۴-۱۵) بدست می‌آید. اکنون اگر k عدد

تصادفی در بازه‌ی $[0, m-1]$ باشد آنگاه متوسط احتمال دستیابی به جواب برابر است با:

$$P_m = \frac{1}{m} \sum_{k=0}^{m-1} P_s^k = \frac{1}{m(1 + \cos \theta)} \sum_{k=0}^{m-1} \sin^2((k+1)\theta) + \sin^2 k\theta$$

با انجام محاسبات مثلثاتی جبری می‌توان اثبات کرد:

$$\sum_{k=0}^{m-1} \sin^2((k+1)\theta) + \sin^2(k\theta) = m - \frac{\cos \theta \sin(2m\theta)}{2 \sin \theta}$$

بنابراین:

$$P_m = \frac{1}{1 + \cos \theta} \left(1 - \frac{\cos \theta \sin(2m\theta)}{2m \sin \theta} \right)$$

اکنون برای وقتی که $m \geq 1/\sin(\theta)$ است داریم:

$$P_m \geq \frac{1}{1+\cos\theta} \left(1 - \frac{1}{2} \cos\theta \sin(2m\theta) \right) = \frac{1}{1+\cos\theta} - \frac{1}{2} \frac{\cos\theta}{1+\cos\theta} \sin(2m\theta)$$

در عبارت فوق چون $0 \leq \cos(\theta) = 1 - M/N \leq 1$ است بنابراین $1/(1+\cos(\theta)) \geq 1/2$ و $\cos(\theta)/(1+\cos(\theta)) \leq 1/2$ است. در نتیجه مینیمم عبارت بالا در $\theta \approx 0$ یا به عبارت دیگر در $M \ll N$ رخ می‌دهد. از طرفی برای تمام مقادیر θ داریم $\sin(2(1/\sin(\theta))\theta)$ ، در نتیجه با توجه به اینکه $m \geq 1/\sin(\theta)$ است، آنگاه وقتی $\theta \approx 0$ باشد داریم: $\sin(2m\theta) \leq 0.91$ ، پس:

$$P_m \geq \frac{1}{2} - \frac{1}{2} \times \frac{1}{2} \times 0.91$$

بنابراین وقتی $m \geq 1/\sin(\theta)$ باشد، برای تمام بازه‌ی $1 \leq M \leq N$ داریم: $P_m \geq 0.2725$.

۴-۶-۱- الگوریتم بویر با استفاده از الگوریتم احمد یونس

دقیقاً همان الگوریتم قبلی بویر که در بخش ۳-۹-۱ معرفی کردیم را بکار می‌گیریم با این تفاوت که در خط سوم، بجای الگوریتم گراور، الگوریتم احمد یونس به تعداد k بار با حالت اولیه‌ی $|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle$ تکرار می‌شود.

حالت بحرانی وقتی شروع می‌شود که $m \geq m_0$ گردد. که در آن:

$$m_0 = \frac{1}{\sin\theta} = \frac{1}{\sqrt{2\left(\frac{M}{N}\right) - \left(\frac{M}{N}\right)^2}} \leq \frac{1}{\sqrt{2}} \sqrt{\frac{N}{M}} \rightarrow m_0 = O\left(\sqrt{\frac{N}{M}}\right) \quad (۴-۲۱)$$

در این مرحله است که احتمال دستیابی به جواب حداقل 0.2725 است. همانند قبل حلقه‌ی اصلی الگوریتم بویر به تعداد $\lceil \log_2 m_0 \rceil$ بار باید تکرار شود تا الگوریتم به مرحله بحرانی برسد.

تعداد تکرارهای الگوریتم احمد یونس که در الگوریتم بویر تا رسیدن به مرحله‌ی بحرانی، بکار برده می‌شود، برابر است با:

$$\sum_{n=1}^{\lceil \log_{\lambda} m_0 \rceil} \frac{1}{2} m = \frac{1}{2} \sum_{n=1}^{\lceil \log_{\lambda} m_0 \rceil} \lambda^{n-1} = \frac{1}{2} \left(\frac{\lambda^{\lceil \log_{\lambda} m_0 \rceil} - 1}{\lambda - 1} \right) < \frac{1}{2} \frac{\lambda m_0}{\lambda - 1} = 4m_0 \quad (22-4)$$

و تعداد تکرارهای الگوریتم بکار برده شده از پس از رسیدن به مرحله‌ی بحرانی برابر است با:

$$\frac{1}{2} \sum_{u=0}^{\infty} (0.7275)^u \lambda^{u + \lceil \log_{\lambda} m_0 \rceil} < \frac{1}{2} \left(\frac{m_0}{(1 - 0.7275)\lambda} \right) = 2.9m_0 \quad (23-4)$$

بنابراین تعداد کل تکرارهای الگوریتم استفاده شده برابر است با: $6.9m_0$ ، که برابر است با: $O(\sqrt{N/M})$. در اینجا چون m_0 برای تمامی بازه‌ی $1 \leq M \leq N$ برابر $O(\sqrt{N/M})$ است، بنابراین این الگوریتم به ازای تمامی مقادیر M می‌تواند مورد استفاده قرار گیرد.

منابع استفاده شده از بخش ۴-۱ تا ۴-۶: [13,14]

۴-۷- الگوریتم جدید بر مبنای الگوریتم احمد یونس

در این قسمت الگوریتم جدیدی را بر مبنای روش الگوریتم احمد یونس ارائه می‌دهیم. روشی که ما در پیش خواهیم گرفت این است که در این الگوریتم بعد از اولین تکرار در الگوریتم احمد یونس، یک کیوبیت هدف دیگر به مدار اضافه کرده و نتایج را برای احتمال موفقیت در دو الگوریتم مقایسه می‌کنیم. در نهایت خواهیم دید کیوبیت هدف جدید سبب افزایش زیرفضاهای جواب از دو زیرفضا به چهار زیرفضا و در نتیجه باعث افزایش احتمال دستیابی به جواب خواهد شد. در الگوریتم پیشنهادی که مدار آن در شکل (۴-۴) نمایش داده شده است، دو کیوبیت هدف در دو مرحله با n کیوبیت ورودی درهم‌تنیده می‌شوند. عملگرهای U_f و P_{inv} دقیقاً همان عملگرهای یکانی بکار برده شده در الگوریتم احمد یونس هستند و در فضای $n+1$ کیوبیتی عمل می‌کنند و عملگرهای P'_{inv} و U'_f نیز عملگرهای یکانی مشابه هستند با این تفاوت که در فضایی با اندازه‌ی $n+2$ عمل می‌کنند:

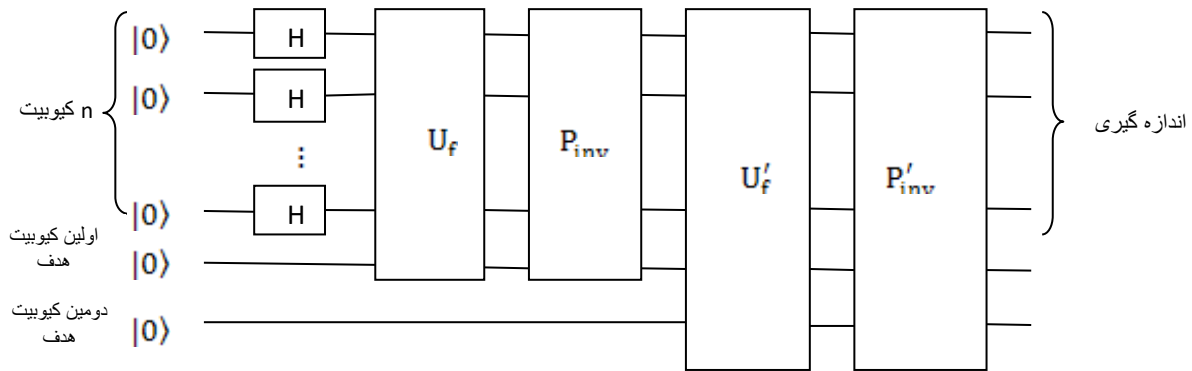
$$U'_f(|i\rangle \otimes |y\rangle \otimes |z\rangle) = (U_f(|i\rangle \otimes |z\rangle)) \otimes |y\rangle \rightarrow (|i\rangle \otimes |z \oplus f(i)\rangle) \otimes |y\rangle \quad (24-4)$$

$$f(i) = \begin{cases} 1 & \text{if } i \text{ is solution} \\ 0 & \text{if } i \text{ is not solution} \end{cases} \quad \text{که}$$

$$P'_{inv} = (H^{\otimes n} \otimes I \otimes I) (2|0^{\otimes n+2}\rangle\langle 0^{\otimes n+2}| - I^{\otimes n+2}) (H^{\otimes n} \otimes I \otimes I) \quad (25-4)$$

(در رابطه‌ی (۲۴-۴) y و z به ترتیب اولین و دومین کیوبیت هدف هستند و i هم همان رجیستر n کیوبیتی است.)

عملگر P'_{inv} سیستمی که از زیرفضاهای $|i\rangle \otimes |0\rangle \otimes |1\rangle$ ، $|i\rangle \otimes |1\rangle \otimes |0\rangle$ ، $|i\rangle \otimes |0\rangle \otimes |0\rangle$ و $|i\rangle \otimes |1\rangle \otimes |1\rangle$ تشکیل شده است را به این صورت تغییر می‌دهد: دامنه‌های زیرفضای $|i\rangle \otimes |0\rangle \otimes |0\rangle$ را نسبت به میانگین‌اشان منعکس می‌کند و دامنه‌های زیرفضاهای دیگر را فقط منفی می‌کند.



شکل ۴-۴: مدار الگوریتم پیشنهادی جدید

حالت سیستم بعد از اولین تکرار الگوریتم احمد یونس با توجه به آنچه در بخش (۲-۴) گفته شد، برابر است با:

$$|\Psi\rangle = \sum_{i=0}^{N-1} (2\langle\alpha\rangle - \alpha_i) |i\rangle |0\rangle - \sum_{i=0}^{N-1} \beta_i |i\rangle |1\rangle \quad (26-4)$$

که در آن :

$$\alpha_i = \begin{cases} 0 & \text{if } f(i) = 1 \\ \frac{1}{\sqrt{N}} & \text{if } f(i) = 0 \end{cases}, \quad \beta_i = \begin{cases} 0 & \text{if } f(i) = 0 \\ \frac{1}{\sqrt{N}} & \text{if } f(i) = 1 \end{cases}, \quad \langle\alpha\rangle = \frac{N-M}{N\sqrt{N}}$$

با اضافه شدن کیوبیت هدف جدید که (در حالت $|0\rangle$ قرار دارد)، حالت سیستم اینگونه خواهد شد:

$$\begin{aligned} |\phi\rangle = |\Psi\rangle|0\rangle &= \sum_{i=0}^{N-1} (2\langle\alpha\rangle - \alpha_i) |i\rangle|0\rangle|0\rangle - \sum_{i=0}^{N-1} \beta_i |i\rangle|1\rangle|0\rangle = \\ &= \sum_{i=0}^{N-1} (2\langle\alpha\rangle - \alpha_i) |i\rangle|0\rangle|0\rangle + \sum_{i=0}^{N-1} 0 \times |i\rangle|0\rangle|1\rangle \quad (27-4) \\ &\quad - \sum_{i=0}^{N-1} \beta_i |i\rangle|1\rangle|0\rangle + \sum_{i=0}^{N-1} 0 \times |i\rangle|1\rangle|1\rangle \end{aligned}$$

با جدا کردن جملات حاوی جواب از جملاتی که حاوی جواب نیستند خواهیم داشت:

$$\begin{aligned} |\phi\rangle &= \sum'' \left(2\langle\alpha\rangle - \frac{1}{\sqrt{N}} \right) |i\rangle|0\rangle|0\rangle + \sum' 2\langle\alpha\rangle |i\rangle|0\rangle|0\rangle + \\ &\quad + \sum'' 0 \times |i\rangle|0\rangle|1\rangle + \sum' 0 \times |i\rangle|0\rangle|1\rangle + \quad (28-4) \\ &\quad + \sum'' 0 \times |i\rangle|1\rangle|0\rangle - \sum' \frac{1}{\sqrt{N}} |i\rangle|1\rangle|0\rangle + \\ &\quad + \sum'' 0 \times |i\rangle|1\rangle|1\rangle + \sum' 0 \times |i\rangle|1\rangle|1\rangle \end{aligned}$$

اکنون عملگرهای U_f' و P_{inv}' را باید به ترتیب روی $|\phi\rangle$ اثر دهیم. با توجه به نحوه عمل این عملگرها (روابط (24-4) و (25-4)) براحتی می توان دریافت که ضرب جملات سوم و پنجم و هفتم همواره صفر باقی می ماند و بنابراین از این پس از نوشتن آنها صرف نظر می کنیم:

$$\begin{aligned} U_f' |\phi\rangle &= \sum'' \frac{1}{\sqrt{N}} \left(1 - \frac{2M}{N} \right) |i\rangle|0\rangle|0\rangle + \sum' 2 \frac{1}{\sqrt{N}} \left(1 - \frac{M}{N} \right) |i\rangle|0\rangle|1\rangle + \\ &\quad + \sum' 0 \times |i\rangle|0\rangle|0\rangle - \sum' \frac{1}{\sqrt{N}} \times |i\rangle|1\rangle|1\rangle + \sum' 0 \times |i\rangle|1\rangle|0\rangle \end{aligned}$$

همان طور که اشاره شد، عملگر P_{inv}' دامنه های زیرفضای $|i\rangle \otimes |0\rangle \otimes |0\rangle$ را نسبت به میانگین اشان انعکاس می دهد و دامنه ی بقیه ی زیرفضاها را در یک منفی ضرب می کند. میانگین زیرفضای $|i\rangle \otimes |0\rangle \otimes |0\rangle$ برابر است با:

$$\langle mean \rangle = \frac{(N-M) \frac{1}{\sqrt{N}} \left(1 - \frac{2M}{N}\right) + M \times 0}{N} = \frac{(N-M)(N-2M)}{N^2 \sqrt{N}} \quad (29-4)$$

$$\begin{aligned} P_{inv}'(U_f'|\varphi) &= \sum' \left(2\langle mean \rangle - \frac{1}{\sqrt{N}} \left(1 - \frac{2M}{N}\right) \right) |i\rangle|0\rangle|0\rangle + \\ &+ \sum' (2\langle mean \rangle - 0) |i\rangle|0\rangle|0\rangle - \sum' 2 \frac{1}{\sqrt{N}} \left(1 - \frac{M}{N}\right) |i\rangle|0\rangle|1\rangle + \\ &+ \frac{1}{\sqrt{N}} \sum' |i\rangle|1\rangle|1\rangle + \sum' 0 \times |i\rangle|1\rangle|0\rangle = \\ &= \sum' \frac{(N-2M)^2}{N^2 \sqrt{N}} |i\rangle|0\rangle|0\rangle + \sum' \frac{2(N-M)(N-2M)}{N^2 \sqrt{N}} |i\rangle|0\rangle|0\rangle - \\ &- \frac{2(N-M)}{N \sqrt{N}} \sum' |i\rangle|0\rangle|1\rangle + \frac{1}{\sqrt{N}} \sum' |i\rangle|1\rangle|1\rangle + \sum' 0 \times |i\rangle|1\rangle|0\rangle \end{aligned}$$

با توجه به آنکه هر چهار عملگر U_f و P_{inv} و U_f' و P_{inv}' یکانی هستند همواره باید اندازه‌ی کت حالت برابر یک بماند، در نتیجه باید:

$$\left[(N-M) \left(\frac{(N-2M)^2}{N^2 \sqrt{N}} \right)^2 \right] + \left[M \left(\frac{2(N-M)(N-2M)}{N^2 \sqrt{N}} \right)^2 + M \left(\frac{2(N-M)}{N \sqrt{N}} \right)^2 + M \left(\frac{1}{\sqrt{N}} \right)^2 \right] = 1 \quad (31-4)$$

که به راحتی با کمی محاسبات جبری می‌توان درستی آن را تأیید کرد.

در عبارت فوق جمله‌ی اول برابر احتمال خطاست یعنی احتمال اینکه بعد از اندازه‌گیری روی n کیوبیت اول، گزینه‌ای غیر از گزینه‌ی جواب را بدست آوریم (P_{ns}) و مجموع سه جمله‌ی بعدی برابر احتمال رسیدن به جواب یا به عبارتی دیگر احتمال موفقیت است (P_s):

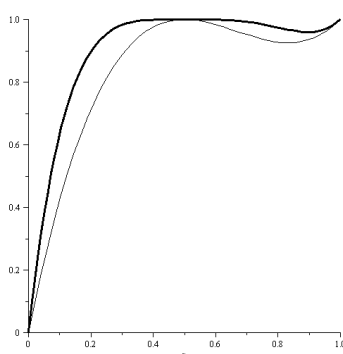
$$P_{ns} + P_s = 1$$

P_s را می‌توان بر حسب $x \equiv M/N$ به صورت زیر بازنویسی کرد:

$$P_{\pi} = 4x((1-x)(1-2x))^4 + 4x(1-x)^2 + x \quad (32-4)$$

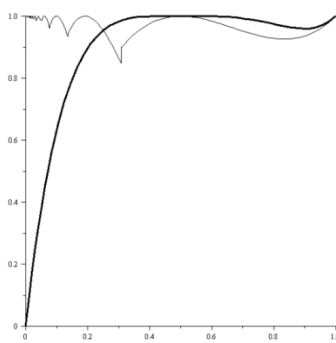
در شکل (۴-۵) نمودار P_{π} در الگوریتم پیشنهادی با نمودار اولین تکرار الگوریتم احمد یونس برای مقایسه شده است. همان طور که بوضوح مشخص است، الگوریتم جدید در تمام بازه‌ی x دارای احتمال موفقیت بیشتر از الگوریتم احمد یونس است.

همچنین در شکل (۴-۶) نمودار P_{π} با نمودار الگوریتم احمد یونس (به ازای حداکثر احتمال موفقیت) مقایسه شده است. با توجه به شکل در بازه‌ی $M \geq \frac{N}{4}$ الگوریتم احمد یونس دارای احتمال موفقیت حداقل ۰/۸۷۸۸ است در صورتی که در الگوریتم جدید این احتمال به ۰/۹۵۳۱۲۵ افزایش یافته است و بیش از ۷٪ از احتمال خطا در این بازه کاسته شده است.



شکل ۴-۵: نمودار P_{π} در الگوریتم جدید _____

نمودار P_{π} بعد از اولین تکرار در الگوریتم احمد یونس _____



شکل ۴-۶: نمودار P_{π} بر حسب x در الگوریتم جدید _____

نمودار P_{π} در الگوریتم احمد یونس (به ازای حداکثر احتمال موفقیت) _____

۴-۸- تکرارهای بعدی الگوریتم پیشنهادی

در این بخش نتایج الگوریتم پیشنهادی را به ازای چندین بار تکرار عملگر $P'_{inv} U'_f$ مورد بررسی قرار می‌دهیم. حالت سیستم را بعد از k بار تکرار این عملگر می‌توان به طور کلی به صورت

$$|\varphi^k\rangle = (P'_{inv} U'_f)^k |\varphi\rangle = \sum_k a_k |i\rangle |0\rangle |0\rangle + \sum_k b_k |i\rangle |0\rangle |0\rangle + \sum_k c_k |i\rangle |0\rangle |1\rangle + \sum_k d_k |i\rangle |1\rangle |0\rangle + \sum_k e_k |i\rangle |1\rangle |1\rangle \quad (۴-۳۳)$$

نمایش داد. در هر بار تکرار $P'_{inv} U'_f$ ، ابتدا جای ضرایب b_k و c_k و هم‌چنین جای ضرایب d_k و e_k و سپس دامنه‌های زیرفضای $|i\rangle |0\rangle |0\rangle$ نسبت به میانگین‌اشان منعکس می‌شوند. در جدول (۴-۱) ضرایب کت حالت $|\varphi^k\rangle$ را تا تکرار پنجم آورده‌ایم.

جدول ۴-۱: ضرایب حالت سیستم در الگوریتم جدید تا تکرار پنجم

	a_k
k=0	$\frac{1}{\sqrt{12}}(N-2M)$
k=1	$\frac{1}{\sqrt{12}}(N-2M)^2$
k=2	$\frac{1}{\sqrt{12}}(N^2-10N^2M+16NM^2-8M^2)$
k=3	$\frac{1}{\sqrt{12}}(N^4-16N^2M+48N^2M^2-48NM^2+16M^4)$
k=4	$\frac{1}{\sqrt{12}}(N^5-26N^4M+112N^2M^2-184N^2M^2+128NM^4-32M^5)$
k=5	$\frac{1}{\sqrt{12}}(N^6-36N^5M+288N^4M^2-544N^2M^2+608N^2M^4-320NM^5+64M^6)$

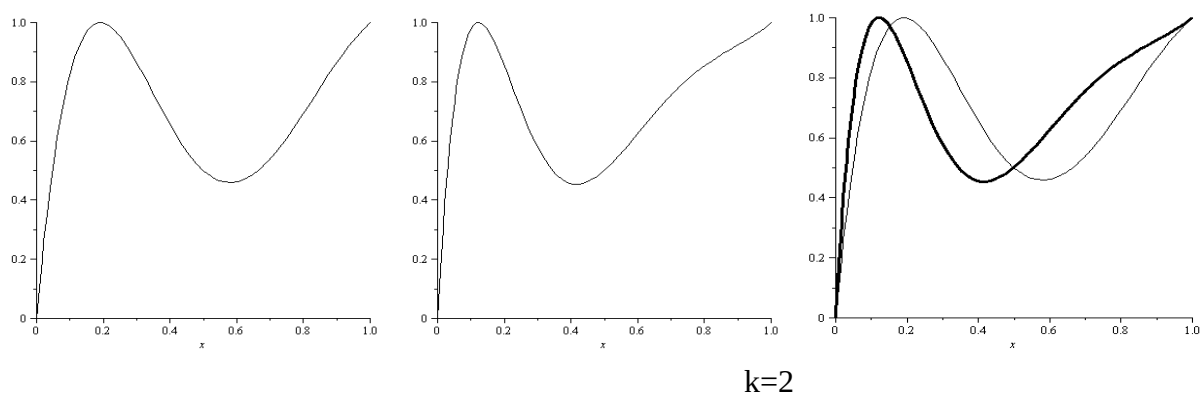
	b_k	c_k	d_k	e_k
--	-------	-------	-------	-------

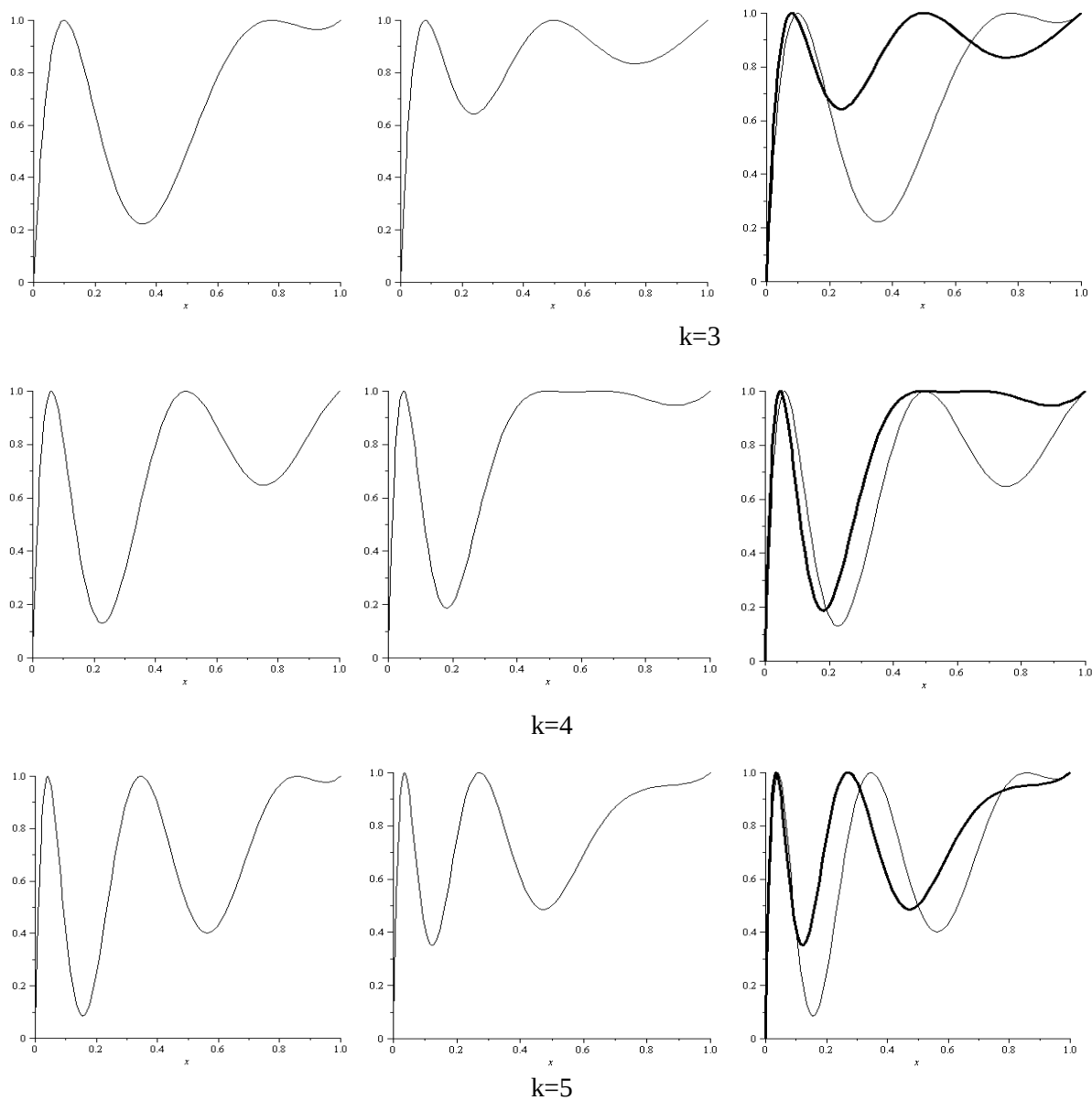
k=0	$\frac{\mathcal{L}}{32\pi^{1/2}}(N-M)$	0	$-\frac{1}{\sqrt{\pi}}$	0
k=1	$\frac{\mathcal{L}}{32\pi^{1/2}}(N-M)(N-2M)$	$-\frac{\mathcal{L}}{32\pi^{1/2}}(N-M)$	0	$\frac{1}{\sqrt{\pi}}$
k=2	$\frac{\mathcal{L}}{32\pi^{1/2}}(N-M)(N^2-3NM+2M^2)$	$-\frac{\mathcal{L}}{32\pi^{1/2}}(N-M)(N-2M)$	$-\frac{1}{\sqrt{\pi}}$	0
k=3	$\frac{\mathcal{L}}{32\pi^{1/2}}(N-M)(N^2-7N^2M+10NM^2-4M^2)$	$-\frac{\mathcal{L}}{32\pi^{1/2}}(N-M)(N^2-3NM+2M^2)$	0	$\frac{1}{\sqrt{\pi}}$
k=4	$\frac{\mathcal{L}}{32\pi^{1/2}}(3N^5-29N^4M+90N^3M^2-120N^2M^3+72NM^4-16M^5)$	$-\frac{\mathcal{L}}{32\pi^{1/2}}(N-M)(N^2-7N^2M+10NM^2-4M^2)$	$-\frac{1}{\sqrt{\pi}}$	0
$\frac{k=5}{4\pi^{1/2}}$	$(3N^5-47N^4M+204N^3M^2-392N^2M^3+376NM^4-176M^5)+32\pi^{1/2}\frac{\mathcal{L}}{32\pi^{1/2}}(3N^5-29N^4M+90N^3M^2-120N^2M^3+72NM^4-16M^5)$	0	$\frac{1}{\sqrt{\pi}}$	

در هر تکرار، احتمال موفقیت بعد از اندازه‌گیری از n کیویت اول، برابر است با:

$$P_s^k = M(b_k^2 + c_k^2 + d_k^2 + e_k^2) \quad (34-4)$$

نمودارهای احتمال موفقیت برای تکرارهای دوم تا پنجم در شکل (۷-۴) بر حسب $x \equiv \frac{\pi t}{2}$ آورده شده و با نمودارهای معادل از الگوریتم احمد یونس مقایسه شده است. با توجه به نمودارها، به طور شهودی می‌توان دریافت که احتمال موفقیت در بازه‌ی $0 \leq x \leq 1$ برای الگوریتم پیشنهادی دارای میانگین بالاتری نسبت به الگوریتم احمد یونس است. مقادیر این میانگین در جدول (۲-۴) برای هر دو الگوریتم به ازای هر بار تکرار آورده شده است.





شکل ۴-۷: ستون چپ: نمودارهای احمد یونس - ستون وسط: نمودارهای الگوریتم جدید

ستون راست: مقایسه ی دو نمودار

جدول ۴-۲: میانگین احتمال موفقیت در دو الگوریتم تا تکرار پنجم

	الگوریتم احمد یونس	الگوریتم پیشنهادی جدید
k=1	۰/۸۳۳۳	۰/۹۰۰۰
k=2	۰/۷۰۰۰	۰/۷۱۹۰
k=3	۰/۷۰۹۵	۰/۸۵۵۵
k=4	۰/۶۹۶۸	۰/۸۱۸۳
k=5	۰/۶۹۸۸	۰/۷۶۴۷

جدول ۲-۴ نشان می‌دهد که میانگین احتمال موفقیت در تمامی پنج تکرار اول در الگوریتم جدید بیشتر است و به نظر می‌رسد که در تکرارهای بعدی نیز همین وضعیت وجود داشته باشد. با توجه به اینکه در الگوریتم جدید، در اولین گام از یک حلقه‌ی الگوریتم احمد یونس نیز استفاده می‌کند، شاید این‌طور به نظر برسد که باید k امین تکرار از الگوریتم جدید را با $k+1$ امین تکرار الگوریتم احمد یونس مقایسه کنیم، که در این صورت هم الگوریتم جدید احتمال بالاتری را به دست می‌دهد. برای مثال میانگین احتمال موفقیت در اولین تکرار الگوریتم جدید ۰/۹۰ است در حالی که در دومین تکرار الگوریتم احمد یونس این احتمال برابر ۰/۷۰ است و به همین ترتیب برای سایر تکرارها درست است.

علت این افزایش را می‌توان این‌طور توضیح داد: تا قبل از اولین تکرار در الگوریتم جدید، ضرایب c_k که مربوط به زیرفضای $|i\rangle|0\rangle|1\rangle$ هستند، همگی صفرند و بعد از اولین تکرار، این ضرایب با انعکاس حول میانگین به همراه ضرایب a_k ، افزایش بیشتری نسبت به الگوریتم احمد یونس می‌یابند و موجب کاهش بیشتر ضرایب a_k می‌شوند زیرا با توجه به رابطه‌ی (۴-۵) در الگوریتم احمد یونس، ضرایبی که در تکرار دوم از زیرفضای جواب حول میانگین منعکس می‌شوند، برابر $\frac{1}{\sqrt{N}}$ هستند و بنابراین تحت انعکاس، ضرایب a_k کاهش کمتری (نسبت به ضرایب صفر) می‌یابند. به علاوه در الگوریتم جدید ضرایب زیرفضاهای $|i\rangle|1\rangle|0\rangle$ و $|i\rangle|1\rangle|1\rangle$ (یعنی d_k و e_k) نیز در احتمال موفقیت اضافه می‌شوند. این ضرایب تنها مقادیر صفر و $\frac{1}{\sqrt{N}}$ را به خود می‌گیرند و همان‌طور که در جدول نشان داده شده است، در تکرارهای بعدی فقط جای این ضرایب با هم عوض می‌شود.

بنابراین با افزودن یک کیوبیت هدف جدید به سیستم و افزایش زیرفضاهای جواب از دو زیرفضا در الگوریتم احمد یونس به چهار زیرفضا در الگوریتم جدید، می‌توان میانگین احتمال دستیابی به جواب را افزایش داد.

- [1] J.J.Sakurai,(revised edition 1999), “**Modern quantum mechanics**” , Addison-Wesley,USA
- [2] David McMahon,(2008), “**Quantum computing explained**”, John Wiley & Sons, Inc.,USA
- [3] John Preskill,(1998), “**Lecture notes for physics 229: Quantum Information and Computation**”,California Institute of Technology.
- [4] M. Nielsen, I. Chuang,(2000), “**Quantum Computation and Quantum Information**”,Cambridge, United Kingdom .
- [5] Ingemar Bengtsson and Karol Zyczkowski,(2006), “**Geometry of Quantum States**”, Cambridge, pp 137-139,383-389
- [6] Artur Ekert, Patrick Hayden and Hitoshi Inamori,(2007), “**Basic concepts in quantum computation**”, University of Oxford, Oxford OX1 3PU, United Kingdom
- [7] Ashok Chatterjee,(2003), “**Introduction to Quantum Computation**” , Saha Institute of Nuclear Physics, Kolkata, India,e-print: quant-ph/0312111
- [8] Robert B. Griffiths,(2006), “**Dense Coding, Teleportation, No Cloning**”
- [9] L.Grover,(1996), “**A fast quantum mechanical algorithm for database search**”, In Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, pp 212–219
- [10] M.Boyer, G.Brassard, P.Høyer, A.Tapp,(1996), “**Tight bounds on quantum searching**”, Proceedings, PhysComp 1996.
- [11] L.Grover ,(1997), “**Quantum search on structured problems**”
- [12] L.Grover,(1997), “**A framework for fast quantum mechanical algorithms**”
- [13] A. Younes, J. Rowe, J. Miller,(2004), “**Quantum search algorithm with more reliable behavior using partial diffusion**”,in: Proc. of the 7th Int. Conf on Quantum Communication, Measurement and Computing, pp 171-174 .

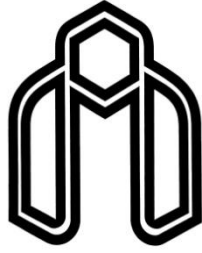
[14] A. Younes, J. Rowe, J. Miller,(2008), “**Enhanced quantum searching via entanglement and partial diffusion** ”,physica D 237, 1074-1078 .

Abstract

The quantum search algorithms whose basic principles were discovered by L.K.Grover, was able to find a specific element from an unstructured search space of size N , using approximately $\sqrt{N}$ steps. Later, it was proved that there is no quantum search algorithm faster than this. Nevertheless, efforts continued to increase the accuracy of quantum search so that the probability of finding the answer becomes more and more. Ahmed Younes by modifying Grover’s method increased the probability of success from at least 50% in Grover’s algorithms to at least 87.88%.

We formed a new algorithm by adding an extra target to younes’s algorithms and creating entanglement between new target with other qubits of system. Afterwards, we compared the first five iterations of two algorithms. Results of comparison showed that in all iterations the average of probability of success in new algorithms is more than pervious algorithms. Especially in first iteration, the probability of success for $1 \leq M \leq N$ is ever more than corresponding iteration of younes’s algorithms.

Keywords: quantum mechanic; quantum computer; quantum computation and quantum information; quantum search; Grover’s algorithms; Ahmed younes’s algorithms.



Shahrood University of Technology

Faculty: Physics

Quantum Search

Adell Majidi

Supervisor:

Dr.Hossein Movahhedian

Date: June 2009