مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۷۷ -۶۹

محاسبات بر مبنای رایانه‌های کوانتومی و کاربرد آن برای تجزیه اعداد مرکب

علی جبار رشیدی[1*]، رحیم اصغری[2]، مصطفی اسلامی[3]

۱- دانشیار، ۲- استادیار، دانشگاه صنعتی مالک اشتر تهران ۳-استادیار، دانشگاه مازندران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

در مقاله حاضر تبدیل فوریه کوانتومی به‌عنوان جزء کلیدی در الگوریتم تجزیه اعداد طبیعی به روش کوانتومی برای استفاده در الگوریتم شر معرفی می‌گردد. پیاده‌سازی کارای الگوریتم شر که تنها الگوریتم شناخته‌شده برای تجزیه اعداد با پیچیدگی زمانی چندجمله است، هدف اصلی این مقاله است. در این مقاله، پیچیدگی محاسباتی مراحل مختلف الگوریتم تجزیه اعداد طبیعی و مدارهای کوانتومی برای اجرای تبدیل فوریه کوانتومی ارائه شده‌اند. هم‌چنین، در این مقاله تبدیل فوریه کوانتومی تعمیم و برای انجام محاسبات بهبود یافته است. الگوریتم شر بهبودیافته در نرم‌افزار میپل با استفاده از کتابخانه محاسبات کوانتومی پیاده‌سازی شده است. با استفاده از این کتابخانه مفاهیم کوانتومی درهم تنیدگی و موازی در رایانه کلاسیک شبیه‌سازی شده‌اند. مثال‌هایی از شبیه‌سازی تخمین فاز به همراه جدول و نمودار برای نمایش قابلیت برنامه ارائه کرده‌ایم. در پایان مثال‌هایی به همراه نتایج برای محاسبات الگوریتم شر بهبود داده‌شده، آورده‌ایم.

واژه‌های کلیدی: محاسبات کوانتومی، تبدیل فوریه کوانتومی، الگوریتم شر، تخمین فاز، شبیه‌سازی

۱- مقدمه[1]

تا این لحظه مهم‌ترین یافته در محاسبات کوانتومی این است که رایانه های کوانتومی می‌توانند محاسباتی را که بر روی یک رایانه کلاسیک، در زمان چندجمله‌ای قابل پیاده‌سازی نیستند، به‌طور کارآمد اجرا کنند [۱]. به‌عنوان‌مثال، پیداکردن عامل‌های اول یک عدد صحیح n بیتی با استفاده از بهترین الگوریتم‌های کلاسیک شناخته‌شده به $\exp(O(n^{\frac{1}{3}}\log^{\frac{2}{3}} n))$ عملیات نیاز دارد [۲]. بنابراین، تجزیه اعداد به عامل‌های اول روی یک کامپیوتر کلاسیک، به‌عنوان یک مسئله سخت مورد توجه قرار می‌گیرد. اهمیت رایانه کوانتومی در این‌جاست که الگوریتم شر کوانتومی (که روی یک رایانه کوانتومی اجرا می‌شود) می‌تواند این کار را با استفاده از $O(n^2 \log n \log\log n))$ عملیات انجام دهد [۳]. تجزیه اعداد مرکب به عامل‌های اول از این نظر با اهمیت است که الگوریتم رمزنگاری RSA به عنوان یکی از پرکاربردترین الگوریتم‌های رمزنگاری مبتنی بر آن است. این الگوریتم رمزنگاری به دلیل کارایی بالا در محاسبه، سال‌هاست که در مهم‌ترین مراکز امنیتی، مراکز مالی تا نهادهای نظامی و ... ، مورد استفاده قرار می‌گیرد [۴]. هم‌چنین تبدیل فوریه کوانتومی که مهم‌ترین قسمت الگوریتم شر (بخش کوانتومی) را شامل می‌شود و البته در بسیاری از محاسبات کوانتومی دیگر هم ظاهر می‌شود از اهمیت ویژه‌ای برخوردار است که به آن می پردازیم. مسئله دیگر این است که در مقاله‌ها و کتاب‌های مختلفی در رابطه با تبدیل فوریه نوشته شده است [۵-۷] ولی درک عملکرد این الگوریتم موضوعی است که در اکثر این منابع کم‌تر مورد توجه قرار می‌گیرد. مقاله حاضر در تلاش است که به این زمینه بیش‌تر بپردازد.

براساس مشاهدات فاینمن[1] [۸]، شبیه‌سازی انجام محاسبات که باید در رایانه کوانتومی صورت بپذیرد، در رایانه‌های کلاسیک ناممکن است. این مسئله را طی انجام این مقاله به‌خوبی درک کردیم. با این حال، می‌توان برای انجام محاسبات جبری و محاسبات ماتریسی به شبیه‌سازی عملگرهای کوانتومی مانند کت‌ها، گیت‌ها و عملگرهای یکانی و درنتیجه تبدیل فوریه کوانتومی در رایانه های کوانتومی پرداخت.

در مقاله [۹]، الگوریتم شر در نرم‌افزار میپل[2] شبیه‌سازی شد، ولی در آن‌جا تنها به شبیه‌سازی بخش‌های کلاسیک نرم‌افزار اکتفا شده است. در آن مقاله، یافتن مرتبه با استفاده از نرم‌افزار مرتبه‌یاب میپل انجام گرفت و با محاسبه مرتبه شبیه‌سازی الگوریتم شر صورت پذیرفت. در الگوریتم شر ذکرشده درآن مقاله، در واقع برخی از جنبه‌های خاص این الگوریتم شبیه‌سازی شده است. به‌عنوان‌مثال، عملگرهای یکانی که در رایانه کوانتومی اعمال می‌شوند، شبیه‌سازی نشده ولی نتایج حاصل از آن تبدیل‌ها را در رایانه کلاسیک (به‌صورت احتمالی "تقریباً حتماً") ساخته است.

1- Von Neumann
2- Maple

* رایانامه نویسنده مسئول: Aiorashid@yahoo.com

در مقاله حاضر برای پیاده‌سازی، نرم‌افزار میپل را انتخاب کرده‌ایم زیرا این نرم‌افزار از یک‌سو دارای ابزارهای بسیار مناسب جبر خطی است و از طرفی دیگر، کتابخانه مناسبی را برای انجام محاسبات کوانتومی توسعه داده است [۱۲-۱۰]. کتابخانه‌ای که در این مقاله مورد استفاده قرار داده‌ایم Open QUACS است که توسط کریس مک کوبین توسعه داده شد [۱۳]. این کتابخانه با وجود محدودیتی که دارد، ابزارهای لازم جهت ایجاد کت‌ها و گیت‌های لازم شبیه‌سازی مدارهای کوانتومی را در اختیار ما قرار می‌دهد. با استفاده از این کتابخانه، می‌توان تبدیل فوریه مورد نظر را به‌صورت عملگر ماتریسی ساخت که برای اختصارنویسی، از ارائه کدها صرف‌نظر کرده‌ایم.

در این مقاله، تبدیل فوریه کوانتومی را که بخش کلیدی الگوریتم تجزیه اعداد صحیح به عوامل اول و بسیاری الگوریتم‌های کوانتومی دیگر است، مورد بررسی قرار می‌دهیم. تبدیل فوریه کوانتومی عبارت از یک الگوریتم کوانتومی مؤثر برای اجرای یک تبدیل فوریه است [۱۴]. به کمک تبدیل فوریه کوانتومی، تخمین فاز کوانتومی که تقریبی از مقادیر ویژه یک عملگر یکانی، تحت شرایط معین است، امکان‌پذیر می‌شود [۱۵]. این کار به ما اجازه می‌دهد که مسائلی مانند مسئله یافتن درجه و مسئله تجزیه اعداد صحیح به عامل‌های اول را مشابه آن‌چه در رایانه کوانتومی انجام می‌شود شبیه‌سازی کنیم. مثال‌هایی از تخمین فاز با استفاده از برنامه، ارائه شده است. در مقاله حاضر پیچیدگی زمانی مراحل مختلف الگوریتم ارائه‌شده و گام‌های الگوریتم شر برای تجزیه اعداد مرکب آورده شده‌اند.

ساختار مقاله به‌این‌ترتیب است: ابتدا در بخش ۲، تبدیل فوریه کوانتومی و نیز فرم تعمیم‌یافته آن را ارائه کرده و در بخش ۳، تخمین فاز کوانتومی براساس تبدیل فوریه کوانتومی تعمیم‌یافته، بیان شده است. در بخش ۴، مرتبه‌یابی کوانتومی را مطرح کرده و درنهایت در بخش ۵، الگوریتم شر برای تجزیه اعداد صحیح مثبت، به‌عنوان کاربردی از تبدیل فوریه کوانتومی تعمیم‌یافته، شبیه‌سازی و نتایج ارائه گردیده‌اند.

۲- تبدیل فوریه کوانتومی

یافته‌های جدید در محاسبه کوانتومی شامل انجام تبدیلاتی است که می‌توانند روی یک کامپیوتر کوانتومی، خیلی سریع‌تر از یک کامپیوتر کلاسیک اجرا شوند. این یافته، ساخت الگوریتم‌های سریع برای کامپیوترهای کوانتومی را ممکن ساخته است [۱۶]. تبدیل فوریه گسسته، یک بردار از اعداد مختلط را به عنوان ورودی و به صورت $x_0, \dots, x_{N-1}$ را (طول بردار N، یک پارامتر ثابت است) می‌گیرد. خروجی آن (داده تبدیل‌شده)، یک بردار از اعداد مختلط $y_0, \dots, y_{N-1}$ است که توسط رابطه (۱) تعریف می‌شود:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N} \qquad (۱)$$

تبدیل فوریه کوانتومی دقیقاً همان تبدیل فوریه گسسته است ولی نحوه نمادگذاری‌ها با توجه به نحوه نمادگذاری‌ها در فیزیک کوانتوم برای تبدیل فوریه کوانتومی، کمی متفاوت می‌شود. همان‌طورکه در رابطه (۲) نشان داده شده است، تبدیل فوریه کوانتومی روی پایه‌های $|0\rangle, \dots, |N-1\rangle$ تعریف می‌شود.

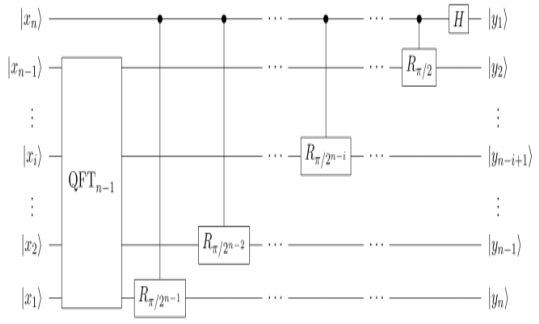
$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \qquad (۲)$$

تبدیل بالا تبدیلی یکانی است و می‌تواند بر روی یک کامپیوتر کوانتومی پیاده‌سازی شود. در این رابطه، متغیر N که برابر با 2^n است را در نظر می‌گیریم که n در آن، عددی صحیح بوده و بردارهای $|0\rangle, \dots, |2^n-1\rangle$ هم پایه‌های محاسباتی برای یک رایانه کوانتومی n کیوبیتی محسوب می‌شوند. در این صورت می‌توان حالت $|j\rangle$ را با استفاده از نمایش باینری $j = j_1 j_2 \dots j_n$ نشان داد. هم‌چنین می‌توان حالت $0.j_L j_{L+1} \dots j_m$ را به‌صورت $\frac{j_L}{2} + \frac{j_{L+1}}{4} + \dots + \frac{j_m}{2^{m-L+1}}$ نیز نمایش داد.

به کمک خواص جبری، تبدیل فوریه کوانتومی می‌تواند به‌صورت رابطه (۵-۳) ارائه شود:

$$|j_1, \dots, j_n\rangle \to \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle) \dots (|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n}|1\rangle)}{2^{n/2}} \qquad (۳)$$

این نمایش به ما اجازه پیاده‌سازی یک مدار کوانتومی کارآمد، جهت محاسبه تبدیل فوریه کوانتومی را می‌دهد. رابطه (۳)، استخراج یک مدار کارآمد برای تبدیل فوریه کوانتومی را آسان می‌سازد. یک چنین مداری در شکل (۱) نشان داده شده است [۵].



شکل (۱): مدار پیاده‌سازی تبدیل فوریه کوانتومی

گیت R_K (گیت چرخش شرطی)، بیانگر یک تبدیل یکانی است و ماتریس نظیر آن در رابطه (۴) ارائه گردیده است:

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & 2^{2\pi i/2^k} \end{bmatrix} \qquad (۴)$$

1- Cris macquin

در مدار شکل (۱)، ابتدا یک گیت هادامارد[1] و n-۱ چرخش شرطی، روی اولین کیوبیت اعمال می‌شود یعنی در مجموع n گیت مورد استفاده قرار می‌گیرد. سپس روی دومین کیوبیت، یک گیت هادامارد و n-۲ چرخش شرطی یعنی در مجموع n-۱ گیت اعمال می‌شوند.

به این ترتیب، تعداد گیت‌های مورد نیاز در این مدار برابر با $n+(n-1)+...+1=\frac{n(n+1)}{2}$ خواهد بود. البته این تعداد گیت، بدون احتساب گیت‌های جابه‌جایی است. از طرفی به تعداد $\frac{n}{2}$ گیت جابه‌جایی نیز مورد نیاز است که هر گیت جابه‌جایی با استفاده از سه گیت CNOT، پیاده‌سازی می‌شود. بنابراین، این مدار یک الگوریتم از مرتبه $\Theta(n^2)$ برای اجرای تبدیل فوریه کوانتومی فراهم می‌کند. برعکس، بهترین الگوریتم‌های کلاسیک برای محاسبه تبدیل فوریه گسسته عبارتند از: الگوریتم‌هایی مثل تبدیل فوریه سریع (FFT[2]) که تبدیل فوریه گسسته را با استفاده از $\Theta(n2^n)$ گیت، محاسبه می‌کند [۱۷].

در نتیجه، محاسبه تبدیل فوریه روی یک کامپیوتر کلاسیک نسبت به محاسبه تبدیل فوریه کوانتومی روی یک کامپیوتر کوانتومی، به‌طور نمایی به عملگرهای بیش‌تری نیاز دارد.

۳- تعمیم تبدیل فوریه

برای به‌دست‌آوردن کارایی بهتر، می‌توان الگوریتم فوریه کوانتومی را تعمیم داد. در این‌جا به‌طور خلاصه به نحوه تعمیم الگوریتم فوریه با استفاده از چندجمله‌ای‌های متعامد (مانند لاگور[3] و هرمیت[4]) می‌پردازیم. فرض کنید تابع $f\in H$ بوده که در آن H فضای هیلبرت است. هم‌چنین فرض کنید $\{\phi_n\}_{n\in\mathbb{N}}$ خانواده‌ای از بردارها در فضای هیلبرت H باشد، در این صورت می‌توان بر اساس خانواده بردارها یک عملگر به صورت زیر تعریف کرد:

$$\forall n\in\mathbb{N}, Uf[n]=\langle f,\phi_n\rangle \qquad (۵)$$

این عملگر، اساساً یک کار انجام می‌دهد و آن اختصاص مجموعه‌ای از اعداد به تابع f است، به این صورت که n امین عدد متناظر با ضرب داخلی تابع f در φ_n (می‌توان به‌جای ضرب داخلی روابط دیگری نیز تعریف نمود) است. برای ساخت مجدد تابع f از عملگر تعریف‌شده، باید عملگر ساخته‌شده (در اینجا U) وارون‌پذیر باشد (به‌عنوان‌مثال عملگری که با استفاده از توابع سینوسی و کسینوسی مانند تبدیل فوریه معمولی ساخته می‌شود). مطلب دوم این است که نمی‌توان هر تابع دلخواه f را بازسازی کرد. دنباله ساخته‌شده قابی از فضای هیلبرت خواهد بود اگر ثابت‌های مثبت a و b برای هر $f\in H$ وجود داشته باشند به‌طوری‌که رابطه زیر برقرار باشد: [۱۸]

$$a\|f\|^2\le\sum_{n\in\mathbb{N}}\left|\langle f,\phi_n\rangle\right|^2\le b\|f\|^2 \qquad (۶)$$

از طرفی، اگر $a=b$ باشد این قاب فشرده نامیده می‌شود و عملگر به‌دست‌آمده را عملگر قاب[5] می‌نامند و ثابت می‌شود که U عملگر قاب است اگر و فقط اگر در برد خود وارون‌پذیر متناهی باشد. اکنون فرمول‌بندی در فضای پیوسته را ارائه می‌کنیم که به‌سادگی قابل‌تعمیم به حالت گسسته خواهد بود. ایده تعمیم‌دادن تبدیل فوریه کوانتومی به تحلیل آنالیز فوریه برای معادلات دیفرانسیل معمولی در مجموعه اعداد حقیقی باز می‌گردد.

در حالت ساده معادله اشتروم لیوول[6] را در نیم‌صفحه $[0,\infty)$ به صورت زیر در نظر می‌گیریم:

$$Lf=-\frac{d^2f}{dx^2}+q(x)f(x)=g(x) \qquad (۸)$$
$$\cos\alpha f(0)+\sin\alpha f'(0)=0$$

که در آن، تابع q برای $t\ge 0$ و دربازه $[0,t]$ و نه لزوماً در $[0,\infty)$ انتگرال‌پذیر است. توابع f و g هم درمجموعه اعداد حقیقی پیوسته مشتق‌پذیر هستند. هم چنین در این‌جا ممکن است به‌شرط دومی نیاز داشته باشیم که در بی‌نهایت باید برقرار باشد.

برای هرعدد مختلط λ تابع ویژه و یکتای $\phi_\lambda(x)$ ای وجود دارد به‌طوری‌که در روابط زیر صدق می کند:

$$\begin{aligned}&L\phi_\lambda=\lambda\phi_\lambda\\&\cos\alpha\phi_\lambda(0)+\sin\alpha\phi_{\lambda'}(0)=0\\&-\sin\alpha\phi_\lambda(0)+\cos\alpha\phi_{\lambda'}(0)=1\\&\phi_\lambda\in L^2[0,\infty)\end{aligned} \qquad (۹)$$

$\phi_\lambda(x)$ ممکن است در بی‌نهایت شرایطی را برآورده نماید. اگر λ به u همگرا شود، این توابع تقریباً همه‌جا دارای حد نقطه‌ای λ خواهند بود که لزوماً در فضای هیلبرت $L^2[0,\infty)$ قرار ندارند، ولی برای $t\ge 0$ و در هر بازه متناهی $[0,t]$ دارای انتگرال مرتبه دوم خواهند بود. درصورتی‌که تابع ϕ_u یک تابع ویژه متناظر با u باشد، در فضای هیلبرت $L^2[0,\infty)$ قرار خواهد گرفت.

قضیه اشتروم لیوول [۱۹]: فرض کنید عملگر Γ در دامنه $D(\Gamma)$ ، که شامل توابع پیوسته مطلق موضعی در بازه $[0,\infty)$ هستند، قرار می‌گیرد. هم‌چنین فرض می‌کنیم که این توابع شروط مورد

1- Hadamard
2- Fast Fourier Transform
3- Laguerre
4- Hermit
5- Frame operator
6- Sturm-Liouville

نیاز در نقاط صفر و ∞ را برآورده می‌کنند. در این صورت انـدازه μ روی Γ که روی طیف $\sigma(L)$ از عملگـر توزیـع مـی‌شـود به‌طوری‌که تبدیل فوریه تعمیم‌یافتـه روی $L^2[\Gamma,\mu]$ مـی باشـد، به‌صورت حد زیر خواهد بود:

$$\hat{f}(u)=\lim_{r\to\infty}\int_0^r f(x)\phi_u(x)dx \qquad (۹)$$

پـس وارون تبـدیل فوریـه کوانتـومی تعمـیم‌یافتـه هـم در $L^2[0,\infty]$ برابر با رابطه زیر خواهد بود:

$$f(u)=\lim_{r\to\infty}\int_{-r}^{r}\hat{f}(x)\phi_u(x)d\mu(u) \qquad (۱۰)$$

علاوه بر آن، با استفاده از معادله پارسوال خواهیم داشت:

$$f_{L^2}\neq\hat{f}_{L^2} \qquad (۱۱)$$

یعنی:

$$\int_{-\infty}^{\infty}\left|\hat{f}(u)\right|^2 d\mu(u)=\int_{-\infty}^{\infty}\left|f(u)\right|^2 dx \qquad (۱۲)$$

درنتیجه، تابع $f\mapsto\hat{f}$ پوشا و یک به یـک بـوده و بنـابراین، وارون‌پذیری تبدیل فوریه کوانتومی به دسـت مـی‌آیـد. در واقـع، تبدیل فوریه، عملگر Γ را به یک‌ضرب با u تبـدیل مـی‌کنـد، بـه صورتی که $f\in D(\Gamma)$ اگر و تنها اگر داشته باشیم:

$$u\hat{f}(u)\in L^2[\Gamma,\mu] \qquad (۱۳)$$

و در این حالت، رابطه $\Gamma f(u)=u\hat{f}(u)$ برقرار می‌باشد.

درمجموع، اندازه μ می‌توانـد دارای مؤلفـه‌هـای گسسـته یـا پیوسته باشد (مانند تبدیل هنکل[1]). چنـین توسـیع‌هـایی بسـیار شبیه به توسیع تابع ویژه پیوسته است [۲۰]. به‌بیان‌دیگر، به‌جای رابطه زیر:

$$f=\sum_{\lambda_n}(f,\phi_{\lambda_n})\phi_{\lambda_n}\mu_n \qquad (۱۴)$$

رابطه زیر را داریم:

$$f=\int_{-\infty}^{\infty}(f,\phi_{\lambda_n})\phi_u(x)d\mu(u) \qquad (۱۵)$$

که درآن خواهیم داشت:

$$(f,\phi_u)=L^2_\mu\lim_{r\to\infty}\int_0^r f(x)\phi_u(x)dx \qquad (۱۶)$$

تبدیل فوریه $\hat{f}(u)=(f,\phi_u)$ چگالی طیفی f است و انـدازه آن به‌عنوان ضریب تابع ویژه ϕ_u تفسیر می‌شود که برای بازسازی f به کار می‌رود.

برای تعریف تابع دلتای دیراک[2] در حالت پیوسته داریم:

$$\sigma(x-y)=\int_{-\infty}^{\infty}e^{i2\pi\omega x}e^{i2\pi\omega x}d\omega \qquad (۱۷)$$

در نتیجه خواهیم داشت:

$$f(x)=\int_{-\infty}^{\infty}f(y)\delta(x-y)dy=$$
$$\int_{-\infty}^{\infty}e^{i2\pi\omega x}\int_{-\infty}^{\infty}f(y)e^{i2\pi\omega x}dyd\omega= \qquad (۱۸)$$
$$\int_{-\infty}^{\infty}e^{i2\pi\omega x}\hat{f}(\omega)d\omega$$

هم‌چنین، برای مقادیر ویژه عملگر دیفرانسیلی اشتروم-لیـوول، در حالت گسسته خواهیم داشت:

$$\sigma(x-y)=\sum_{n=0}^{\infty}\Psi_n(x)\Psi^*_n(y) \qquad (۱۹)$$

که در این صورت:

$$f(x)=\sum_{n=0}^{\infty}\Psi_n(x)\int_{-\infty}^{\infty}f(y)\Psi^*_n(y)dy \qquad (۲۰)$$

در این‌جا برای مقادیر $n\geq 0$، توابـع Ψ_n تـوابعی متعامـد پایه بوده و Ψ^*_n توابع دوگان آن‌ها محسوب می‌شوند. برای مثـال، با استفاده از توابع متعامد لاگور L^α_m از مرتبه α بـه‌جـای Ψ_n در حالت پیوسته خواهیم داشت:

$$\frac{(n+\alpha)!}{n!}\sigma_{mn}=\int x^\alpha e^{-x}L^\alpha_n(x)L^\alpha_m(x)dx \qquad (۲۱)$$

نتیجه می‌دهد:

$$f(x)=\sum_{n=0}^{\infty}\frac{n!L^\alpha_n(x)}{(n+\alpha)!}\hat{f}_n \qquad (۲۲)$$

$$\hat{f}_n=\int x^\alpha e^{-x}L^\alpha_n(x)f(x)dx \qquad (۲۳)$$

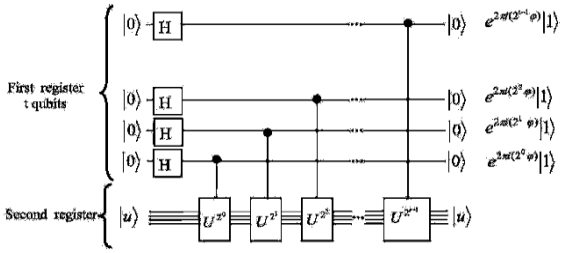
۴- تخمین فاز کوانتومی

پایه و اساس بسیاری از الگوریتم‌های کوانتومی، الگوریتم حداکثر تخمین فاز کوانتومی است [۲۱]. فرض کنید عملگر U، عملگـری یکانی می‌باشد که یک بردار ویژه $|u\rangle$ با مقدار ویژه $e^{2\pi i\phi}$ دارد. هدف الگوریتم تخمین فاز، تخمین مقدار φ است. روش تخمـین فاز کوانتومی از دو ثبات استفاده می‌کند. ثبات اول، در ابتدا t بیت کوانتومی را درحالت $|0\rangle$ دربرداردکه مقدار t وابسته به تعداد ارقام دقتی است که مـی‌خـواهیم در تخمـین داشـته باشـیم، انتخـاب می‌شود. ثبات دوم در حالت $|u\rangle$ قراردارد و تعداد بیت کوانتـومی

1- Henkel Transform

2- Dirac Delta

سه مرحله، اجرا می‌شود. ابتدا مدار نشان داده‌شده در شکل (۲) اعمال می‌شود.

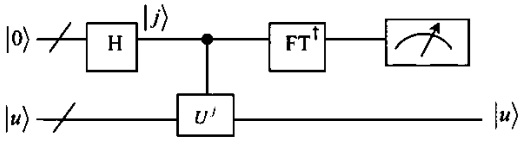


شکل (۲): مرحله اول روش تخمین فاز کوانتومی

در این مدار، ابتدا تبدیل هادامارد به اولین ثبات اعمال و سپس عملیات $Controlled-U^j$ از طریق ثبات دوم اجرا می‌گردد. بنابراین، حالت نهایی ثبات اول به‌صورت رابطه (۵) خواهد بود.

$$\frac{1}{2^{t/2}}\left(|0\rangle+e^{2\pi i 2^{t-1}\phi}|1\rangle\right)\left(|0\rangle+e^{2\pi i 2^{t-2}\phi}|1\rangle\right)\ldots\left(|0\rangle+e^{2\pi i 2^{0}\phi}|1\rangle\right)$$
$$=\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}e^{2\pi i\phi k}|k\rangle \qquad (۲۴)$$

الگوریتم تخمین فاز کوانتومی، در شکل (۳) نشان داده شده است:



شکل (۳): مراحل الگوریتم تخمین فاز کوانتومی

الگوریتم تخمین فاز کوانتومی را در زیر مشاهده می‌کنید:

الگوریتم ۱: تخمین فاز کوانتومی	
ورودی‌ها:	
جعبه سیاه، حالت ویژه $\|u\rangle$ و t بیت کوانتومی خروجی‌ها: $\tilde{\phi}_u$ به‌عنوان تقریبی از مقدار ϕ_u	
گام‌های الگوریتم :	
حالت اولیه:	$\|0\rangle\|u\rangle$
ایجاد برهم‌نهی:	$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}\|j\rangle\|u\rangle$
اعمال جعبه سیاه :	$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}\|j\rangle U^j\|u\rangle$
خروجی جعبه سیاه:	$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi i j\phi_n}\|j\rangle\|u\rangle$
اعمال تبدیل فوریه معکوس:	$\rightarrow \|\tilde{\phi}_u\rangle\|u\rangle$
اندازه‌گیری ثبات اول:	$\rightarrow \tilde{\phi}_u$

۴-۱- یافتن درجه

برای اعداد صحیح مثبت N و x که $x < N$ بوده و هیچ عامل مشترکی با هم ندارند، درجه x به پیمانه N شامل کوچک‌ترین عدد صحیح و مثبت r است که در رابطه $x^r = 1(\mathrm{mod}\, N)$ صدق می کند. مسئله یافتن درجه x عبارت از تعیین r مقدار به ازای مقادیر مشخص N است و این مسئله بر روی یک کامپیوتر کلاسیک به‌عنوان یک مسئله سخت مطرح به شمار می‌رود و این بدان معناست که حل آن بر روی یک کامپیوتر کلاسیک، از مرتبه نمایی است. در واقع، هیچ الگوریتم شناخته‌شده‌ای وجود ندارد که این مسئله را با استفاده از منابعی از مرتبه چندجمله‌ای حل نماید. به‌عبارت‌دیگر، اگر L بیت برای مشخص‌کردن N، مورد نیاز باشد هیچ الگوریتمی وجود ندارد که مسئله یافتن درجه را از مرتبه $O(L)$ حل نماید [۲۲]. در این قسمت خواهیم دید که چگونه تخمین فاز کوانتومی برای دست‌یابی به یک الگوریتم کوانتومی کارآمدیافتن درجه عدد x مورد استفاده قرار می‌گیرد.

الگوریتم کوانتومی برای یافتن درجه دقیقاً همان الگوریتم تخمین فاز است که به عملگر یکانی اعمال می‌شود. رابطه (۶) را در نظر بگیرید:

$$U|y\rangle \equiv |xy\ (\mathrm{mod}\ N)\rangle \qquad (۲۵)$$

که در آن، $y \in \{0,1\}^L$ است.

زمانی‌که $N \le y \le 2^L - 1$ باشد قرارداد می‌کنیم که $xy\ (\mathrm{mod}\ N)$ دقیقاً برابر y است.

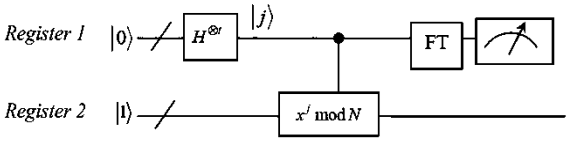
حالت‌هایی که به ازای عدد صحیح $0 \le s \le r-1$ در رابطه (۷) صدق نمایند، حالت‌های ویژه U می‌نامیم. در این رابطه، $\phi = \frac{s}{r}$ به دست می‌آید و ϕ ثابت می‌شود که رابطه (۸) برقرار است:

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi i s k}{r}\right]\left|x^k \bmod N\right\rangle \qquad (۲۶)$$

$$U|u_s\rangle \equiv \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi i s k}{r}\right]\left|x^{k+1} \bmod N\right\rangle$$
$$= \exp\left[\frac{2\pi i s}{r}\right]|u_s\rangle \qquad (۲۷)$$

در اجرای روش تخمین فاز، اگر از t بیت کوانتومی، در ثبات اول استفاده مطابق شکل (۳) و ثبات دوم را در حالت $|1\rangle$ قرار دهیم در این صورت به ازای هر s در بازه 0 تا $r-1$، یک تخمین از فاز $\phi = \frac{s}{r}$ به دست می‌آوریم.

مدار کوانتومی الگوریتم یافتن درجه را در شکل (۴) مشاهده می نمایید:



شکل (۴): مدار کوانتومی الگوریتم یافتن درجه

۴-۱- الگوریتم کسرهای متوالی

تبدیل یافتن درجه به تخمین فاز، با توصیف چگونگی به دست آوردن پاسخ مطلوب r از نتیجه الگوریتم تخمین فاز $(\phi \approx s/r)$، کامل می‌شود. ϕ یک عدد گویا است (نسبت دو عدد صحیح معین) و اگر بتوانیم نزدیک‌ترین کسر متعارف به ϕ را محاسبه کنیم، دراین صورت قادر خواهیم بود که مقدار r را هم به دست آوریم. الگوریتم کسرهای متوالی، الگوریتم کلاسیکی است که در زمان چندجمله‌ای این کار را انجام می‌دهد.

فرض کنید $\frac{s}{r}$ عددی گویا است که در شرط $\left|\frac{s}{r}-\phi\right| \le \frac{1}{2r^2}$، صدق می‌کند. در این صورت، مقدار $\frac{s}{r}$ یکی از مقادیر حاصل از اجرای الگوریتم کسرهای متوالی برای ϕ است. به‌طور خلاصه، با فرض ϕ، الگوریتم کسرهای متوالی، اعداد s' و r' را بدون هیچ برگ خرید مشترکی تولید می‌کند. به‌طوری‌که رابطه $\frac{s'}{r'}=\frac{s}{r}$ برقرار است. حدس ما برای درجه عدد r' است. با محاسبه $x^{r'} \bmod N$ می‌توان بررسی کرد که آیا این مقدار یک درجه هست یا خیر؟ اگر حاصل عبارت برابر یک شود، r' درجه x به پیمانه N خواهد بود. در الگوریتم ۲، محاسبات کوانتومی برای یافتن درجه به طورخلاصه آورده شده است.

تعداد گیت‌های مورد نیاز برای اجرای تبدیل هادامارد از مرتبه $O(L)$ هست که در تبدیل فوریه معکوس، این تعداد از مرتبه $O(L^2)$ خواهد شد. عملگر $x^j \bmod N$ و الگوریتم کسرهای متوالی، هریک به $O(L^2)$ گیت نیاز دارند. بنابراین، بار محاسباتی در این مدار از مرتبه $O(L^3)$ است.

۵- الگوریتم شر

محاسبات کوانتومی، افزایش توان محاسباتی را نوید می‌دهند. پیتر شر[1] توانست از توازی موجود در کامپیوترهای کوانتومی به‌منظور عامل‌یابی اعداد استفاده کند [۱]. این الگوریتم، عملاً بسیار ساده بود. ابتدا یک عدد برای عامل‌یابی دریافت می‌شود (N) فرض این‌که N حاصل‌ضرب دو عدد اول است، این مقدار باید نسبت به N نیز اول باشد. به ازای مقادیر مختلف x، مقدار تابع $f(x)=(a^x \bmod N)$ محاسبه می شود که تمام این عملیات‌ها با توان محاسبات کوانتومی، می‌تواند در واحد زمان انجام گردد. در نتایج تابع، یک الگوی تکراری وجود دارد که دوره این تکرارها را باید پیدا کرد.

یافتن این دوره، معادل یافتن درجه است. در واقع، برای تجزیه اعداد به عوامل اول نیاز به استفاده از الگوریتم یافتن درجه داریم. خوشبختانه این کار را می‌توان به‌سرعت روی کامپیوترهای کوانتومی با یک تغییر شکل تبدیل فوریه کوانتومی انجام داد. این دوره را با نماد r نشان می‌دهیم. سپس مقادیر $\gcd(a^{r/2}+1, N)$ و $\gcd(a^{r/2}-1, N)$ محاسبه می‌شوند (تابع gcd بزرگ‌ترین مقسوم‌علیه مشترک می‌باشد). به دلیل برقراری تساوی $a' \bmod N$ خواهیم داشت:

$$a^r - 1 = (a^{r/2}-1).(a^{r/2}+1) = 0 \bmod N \qquad (۲۸)$$

به این صورت، $(a^{r/2}-1)(a^{r/2}+1)$ مضرب صحیحی از N است. در الگوریتم شر از خاصیت برهم‌نهی کوانتومی استفاده می‌شود که اجازه می‌دهد n کیوبیت در یک لحظه، تمام حالت ممکن را داشته باشند. پیتر شر نشان داد که کامپیوترهای کوانتومی قادر به محاسبه عوامل اول اعداد خیلی بزرگ، در یک‌زمان کوتاه هستند. این الگوریتم، وابسته به توازی کوانتومی و تبدیل فوریه کوانتومی است. مدارات کوانتومی، برای این الگوریتم با استفاده از کتابخانه Open QUACS [۱۱] در میپل طراحی‌شده‌اند. با انتخاب عدد صحیح N، مراحل پیاده‌سازی الگوریتم شر جهت پیداکردن عوامل اول آن به شرح زیر می‌باشند:

مرحله اول: پیداکردن عدد صحیح Q که توانی از ۲ بوده و $N^2 \le Q \le 2N^2$ باشد. این مرحله توسط رایانه‌های کلاسیک انجام می‌شود.

مرحله دوم: انتخاب عدد صحیح a که کوچک‌تر از N بوده و نسبت به آن اول باشد. این مرحله نیز توسط رایانه‌های کلاسیک انجام می‌شود.

مرحله سوم: ایجاد دو ثبات کوانتومی به نام ثبات ورودی و ثبات خروجی. ثبات ورودی باید دارای تعداد کافی کیوبیت، جهت نگهداری اعدادی به بزرگی Q-1 باشد و ثبات خروجی باید دارای تعداد کافی کیوبیت جهت نگهداری اعدادی به بزرگی N-1 باشد.

مرحله چهارم: بارگذاری ثبات ورودی با مقادیر صحیح 0 تا Q-1 و بارگذاری ثبات خروجی با مقدار 0.

مجموع حالت‌های اولیه ثبات‌های کوانتومی سیستم در این نقطه در رابطه (۲۹) بیان‌شده است.

1- Peter Shor

$$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|0\rangle \qquad (۲۹)$$

مرحله پنجم: اجرای تابع $a^x \bmod N$ برای هر عدد ذخیره‌شده در ثبات ورودی و ذخیره‌سازی نتایج آن در ثبات خروجی. به دلیل توازی کوانتومی، این مرحله در یک گام اجرا می‌شود. رایانه کوانتومی تابع $a^{|x\rangle} \bmod N$ را محاسبه می‌کند که $|x\rangle$، برهم‌نهی حالت‌های به‌دست‌آمده در مرحله چهارم است.

این مرحله، روی رایانه کوانتومی اجرا می‌شود. وضعیت ثبات‌های کوانتومی در این مرحله در رابطه (۳۰) نشان داده شده است:

$$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|a^x \bmod N\rangle \qquad (۳۰)$$

مرحله ششم: به دست آوردن ثبات خروجی با مقادیر K:

$$a^x \bmod N = K \qquad (۳۱)$$

این عمل به‌وسیله رایانه کوانتومی اجرا می‌شود. وضعیت ثبات‌های کوانتومی بعد از این مرحله عبارت است از:

$$\frac{1}{\sqrt{\|A\|}}\sum_{x'\in A}^{Q-1}|x'\rangle|k\rangle \qquad (۳۲)$$

که در آن، A مجموعه‌ای از x' است به‌طوری‌که خواهیم داشت:

$a^{x'} \bmod N = K$

و $\|A\|$ تعداد عناصر این مجموعه است.

مرحله هفتم: اعمال تبدیل فوریه کوانتومی روی ثبات ورودی. تبدیل فوریه کوانتومی باعث تغییر حالت $|x\rangle$ می‌شود همان‌طور که در رابطه (۳۳) نشان داده شده است:

$$|x\rangle \to \frac{1}{\sqrt{Q}}\sum_{c=0}^{Q-1}|C\rangle e^{2\pi ixc/Q} \qquad (۳۳)$$

این مرحله توسط رایانه کوانتومی، در یک گام به‌وسیله توازی کوانتومی اجرا می‌شود. بعد از تبدیل فوریه کوانتومی، وضعیت ثبات‌ها به‌صورت زیر است:

$$\frac{1}{\sqrt{\|A\|}}\sum_{x'\in A}^{Q-1}|C\rangle|k\rangle e^{2\pi ixc/Q} \qquad (۳۴)$$

مرحله هشتم: اندازه‌گیری ثبات ورودی. این مقدار m نامیده می‌شود. این مرحله توسط رایانه کوانتومی اجرا می‌شود.

مرحله نهم: با به کار بردن m روی رایانه‌های کلاسیک، مقدار دوره تکرار r توسط روش‌های مختلف به دست می‌آید.

مرحله دهم: با داشتن مقدار r ، عوامل اول عدد N توسط ب.م.م، مطابق رابطه (۳۵) به دست می‌آیند. این مرحله توسط رایانه‌های کلاسیک انجام می‌شود.

$$\left.\begin{aligned}\gcd(a^{r/2}+1, N) = p\\ \gcd(a^{r/2}-1, N) = q\end{aligned}\right\} \Rightarrow N = p.q \qquad (۳۵)$$

نتیجه جالبی که شر بدان دست یافت این بود که یک رایانه کوانتومی، در یک زمان از مرتبه چندجمله‌ای عمل تجزیه را انجام می‌دهد.

الگوریتم ۲: یافتن درجه به روش کوانتومی

ورودی‌ها:

۱- یک جعبه سیاه $U_{x,N}$

۲- t بیت کوانتومی که با $|0\rangle$ شروع می‌شود.

۳- L بیت کوانتومی که باحالت $|1\rangle$ شروع می‌شوند.

خروجی‌ها: یافتن درجه r

مراحل الگوریتم:

حالت اولیه: $|0\rangle|u\rangle$

ایجاد برهم‌نهی: $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle$

اعمال $U_{x,N}$ با رابطه زیر:

$$\to \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \bmod N\rangle \approx \frac{1}{\sqrt{r\,2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}e^{2\pi isj/r}|j\rangle|u_s\rangle$$

۴ - اعمال تبدیل فوریه معکوس به ثبات اول: $\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left|(\frac{\tilde{s}}{r})\right\rangle|u_s\rangle$

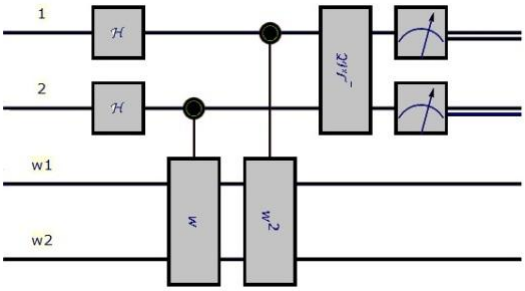
اندازه‌گیری ثبات اول: $\to (\frac{\tilde{s}}{r})$

اعمال الگوریتم کسرهای متوالی: $\to r$

۶- شبیه‌سازی در نرم‌افزار میپل

دراین بخش به عنوان مثال اول، ابتدا با درنظرگرفتن ثبات ثانویه با دو خروجی و ثبات اولیه با سه ورودی، یک مسئله ساده را در نظر گرفته‌ایم. مدار تخمین فاز برای این مثال را در شکل (۵) مشاهده می‌نمایید. در جدول (۱) نتایج مربوط به‌اندازه‌گیری با تبدیل فوریه کوانتومی و ابرحالت[1] متناظر ارائه شده است.

1- Superposition



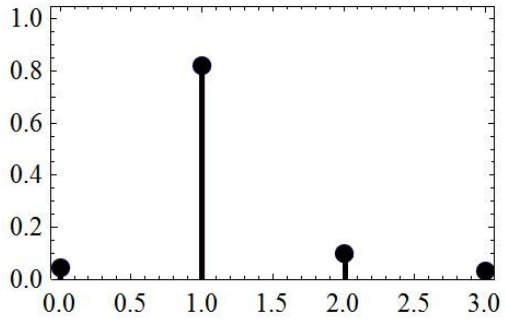
شکل (۵): مدار تخمین فاز برای مثال اول

جدول (۱): ابرحالت‌های به‌دست‌آمده در مثال اول

ابرحالت (سوپرپوزیشن)	اندازه‌گیری
$(0.0975452-0.490393i)\|0001\rangle+$ $(0.277785+0.415735i)\|0010\rangle+$ $(0.490393-0.975452i)\|0011\rangle+$ $(-0.490393+0.097545i)\|0000\rangle$	$(O_1 \quad O_2)$
$(0.415735-0.277785i)\|0101\rangle+$ $(0.0975452-0.490393i)\|0110\rangle+$ $(0.415735+0.277785i)\|0111\rangle+$ $(-0.415735-0.277785i)\|0100\rangle$	$(O_1 \quad l_2)$
$(0.0975452+0.490393i)\|1000\rangle+$ $(0.0.490393+0.0975452i)\|1001\rangle+$ $(0.415735-0.277785i)\|1010\rangle+$ $(0.0975452+0.490393i)\|1011\rangle$	$(l_1 \quad O_2)$
$-(0.277785+0.415735i)\|1101\rangle+$ $(0.490393-0.975452i)\|1110\rangle+$ $(0.277785-0.415735i)\|1111\rangle+$ $(-0.277785+0.415735i)\|1100\rangle$	$(l_1 \quad l_2)$

در شکل (۶)، احتمال متناظر با حالت‌های اندازه‌گیری‌شده در جدول (۱) نشان داده شده‌اند. حالت‌ها از بالا به پایین به ترتیب از چپ به راست با میله‌های نمودار متناظر شده‌اند.

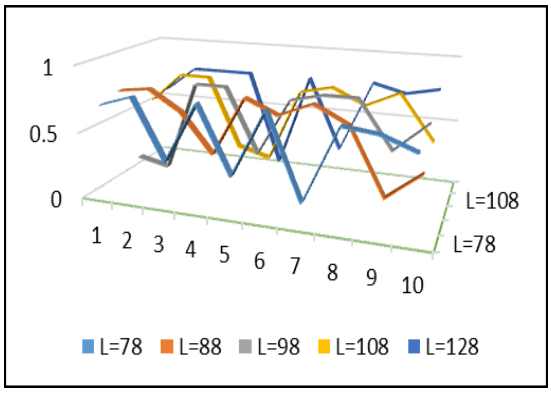
در مثال دوم، الگوریتم شر با استفاده از نرم‌افزار میپل پیاده‌سازی شده است. نتایج عددی ارائه‌شده در جدول (۲) تجزیه عدد مرکب ده رقمی N=2596466813=27751*93563 برای تعداد کیوبیت‌های درنظر گرفته‌شده در ثبات، جهت ۲ بار اجرای برنامه را نشان می‌دهد. هم‌چنین در این جدول تعداد تکرارها برای انتخاب عدد تصادفی اولیه و مرتبه به‌دست‌آمده نیز ارائه شده‌اند. نتایج تصادفی‌بودن زمان به‌دست‌آمده و هم‌چنین تعداد تکرارهای لازم برای انتخاب عدد تصادفی را که در جدول با * نشان داده شده، به‌خوبی نشان می‌دهد. الگوریتم تبدیل فوریه تعمیم‌یافته (با استفاده از چندجمله‌ای‌های متعامد) به‌خوبی الگوریتم تبدیل فوریه کوانتومی معمولی عمل می‌کند. درعین‌حال از لحاظ نظری اهمیت بیش‌تری برای تعمیم استفاده از تبدیل فوق خواهد داشت.



شکل (۶): احتمال متناظر با حالت‌های اندازه‌گیری‌شده جدول (۱)

جدول (۲): نتایج به‌دست‌آمده از اجرای الگوریتم

تکرار	۱		۲	
	زمان (*)	مرتبه	زمان (*)	مرتبه
L=78	42.510(2)	27750	25.459(3)	38850
L=88	11.560(3)	40098	79.077(8)	12950
L=98	119.075(12)	30750	203.113(19)	12062
L=108	36.692(7)	40750	70.856(6)	40750
L=128	29.859(8)	30750	52.291(3)	12062



شکل (۷): احتمال متناظر با فازهای تخمین زده‌شده

در شکل (۷)، احتمال متناظر با فازهای تخمین زده‌شده برای همه اجراها نشان داده شده‌اند. به این صورت که برای هر پنج شبیه‌سازی، بردار و مقدار ویژه حالت ظاهرشده به‌دست‌آمده و درنتیجه مقدار فاز تخمین زده‌شده برای فاز متناظر و اندازه حالتی که احتمال رخداد آن را نشان می‌دهد در جدول (۲) آورده شده است. با توجه به شکل می‌توان دید که با کاهش تعداد کیوبیت‌های درنظر گرفته‌شده در ثبات (L)، احتمال رخداد حالت در اجراها تغییر زیادی پیدا می‌کند. با افزایش L، احتمال رخداد

فاز بیش‌تر می‌شود و در اجراهای مختلف تفاوت کم‌تری نشان داده می‌دهد و این در واقع همان چیزی است که انتظار داریم، گرچه این موضوع را نمی‌توان در پنج اجرای متفاوت به‌خوبی و به‌طور کامل نشان داد.

باید توجه داشت با تغییر L نمی‌توان درباره سرعت انجام شبیه‌سازی اظهارنظر کرد. ولی به‌طورکلی با افزایش تعداد کیوبیت‌ها (مقدار L) زمان اجرای شبیه‌سازی افزایش می‌یابد.

۷- نتیجه‌گیری

در مقاله حاضر مسئله تجزیه اعداد مرکب صحیح و مثبت با استفاده از رایانه کوانتومی مورد مطالعه قرار گرفت. الگوریتم تجزیه که توسط پیتر شر برای رایانه‌های کوانتومی معرفی شد، از دو بخش کوانتومی و کلاسیک تشکیل می‌شود. بخش کوانتومی الگوریتم شر که شامل تخمین فاز کوانتومی و تبدیل فوریه کوانتومی و عملگرهای یکانی کوانتومی است برای پیاده‌سازی نیاز به رایانه کوانتومی دارد. تبدیل فوریه کوانتومی و تعمیم آن مورد مطالعه و بررسی قرار گرفت. در ادامه عملگرهای یکانی، به‌ویژه تبدیل فوریه کوانتومی را با کمک نرم‌افزار میپل و با استفاده از کتابخانه Open QUACS شبیه‌سازی کردیم. توازی و درهم تنیدگی دو ویژگی اساسی رایانه‌های کوانتومی است که در رایانه کلاسیک قابل پیاده‌سازی نیستند ولی با استفاده از کت‌هایی، نتیجه این دو پدیده را می‌توان شبیه‌سازی کرد. برای اندازه‌گیری نیز از توابع کتابخانه معرفی‌شده به‌کارگیری گردید. برخی نتایج شبیه‌سازی تخمین فاز و اندازه‌گیری‌های صورت گرفته‌شده در شکل‌ها و جدول‌ها ارائه شده‌اند. برای پژوهش‌های آینده می‌توان کتابخانه را با استفاده از تبدیل فوریه سریع نیز مجهز کرد و یا برنامه را برای تعداد کیوبیت‌های بیش‌تر توسعه بخشید.

۸- مراجع

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484-1509, 1997.

[2] R. Cleve, "The query complexity of order-finding," In Computational Complexity," 2000 Proceedings, 15th Annual IEEE Conference on IEEE, pp. 54-59, 2000.

[3] A. Y. Kitaev, A. Shen, and M. N. Vyalyi, "Classical and quantum computation," Providence: American Mathematical Society, 2002.

[4] A. Ekert and R. Jozsa, "Quantum computattion and Shor's factoring algorithm," Rev. Mod. Phys., vol. 68, pp. 733-53, 1996.

[5] M. L. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, New York, 2000.

[6] S. A. teane, "Quantum Computing," Rept. Prog. Phys., vol. 61, pp. 117-173, 1998.

[7] A. J. Menezes. P. C. Van Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," CRC press, 1996.

[8] R. P. Feynman, "Simulating physics with computers," Int. J. Theor. Phys. 21, pp. 467-88, 1982.

[9] J. F. Schneiderman, M. E. Stanley, and P. K. Aravind, "A pseudo-simulation of Shor's quantum factoring algorithm," arXiv preprint quant-ph/0206101, 2002.

[10] T. Raditik, "Simulation of n-qubit quantum systems, I. Quantum registers and quantum gates," http://cpc.cs.qub.ac.uk/summaries/ADWE

[11] "List of QC simulators," http://web.archive.org

[12] Quantum information, "Controlled Quantum Dynamics," http://www3.imperial.ac.uk/ /research/downloads

[13] C. B. McCubbin, "Openquacs, an open-source quantum computation simulator in maple," Ph.D. dissertation, University of Maryland, Baltimore County, 2000.

[14] Y. S. Weinstein, M. A. Pravia, E. M. Fortunato, E. M. Lloyd, and D. G. Cory, "Implementation of the quantum Fourier transform," Phys. Rev. Letter., vol. 86, no. 9, pp. 18-89, 2001.

[15] L. Hales and S. Hallgren, "An improved quantum Fourier transform algorithm and applications," In Foundations of Computer Science, 2000.

[16] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, "The fractional Fourier transform," Wiley, Chichester, 2001.

[17] J. S. Walker, "Fast fourier transforms," CRC press, 1996.

[18] S. Mallat, "A wavelet tour of signal processing," Academic press, 1999.

[19] A. Zettl, "Sturm-liouville theory," American Mathematical Society, 2010.

[20] M. A. Al-Gwaiz, "Sturm-Liouville theory and its applications," Springer, 2008.

[21] G. M. D'Ariano, C. Macchiavello, and M. F. Sacchi, "On the general problem of quantum phase estimation," Phys. Letter A, vol. 248, no. 2, pp. 103-108, 1998.

[22] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," In Proceedings of the forty-third annual ACM symposium on Theory of computing, ACM, pp. 333-342, 2011.