دانشگاه صنعتی شریف

دانشکده‌ی مهندسی کامپیوتر

پایان‌نامه‌ی کارشناسی

مهندسی کامپیوتر

عنوان:

الگوریتمِ کوانتومیِ نقطه در چندضلعی

نگارش:

سید سجاد کاهانی

استاد راهنما:

دکتر آبام

تیر ۱۴۰۰


بسم الله الرحمن الرحیم

به نام خدا

دانشگاه صنعتی شریف

دانشکده‌ی مهندسی کامپیوتر

پایان‌نامه‌ی کارشناسی

عنوان: الگوریتمِ کوانتومیِ نقطه در چندضلعی

نگارش: سید سجاد کاهانی

کمیته‌ی ممتحنین

استاد راهنما: دکتر آبام امضاء:

استاد مشاور: ؟؟ امضاء:

استاد مدعو: ؟؟ امضاء:

تاریخ:

چکیده

رایانشِ کوانتومی گونه‌ای از رایانش است که مبتنی بر اصل موضوع‌های مکانیک کوانتومی به وجود آمده که در دهۀ نود و پس از معرفیِ دو الگوریتمِ جست‌وجو و تجزیۀ عدد، توجه‌ها به آن افزایش یافت. از سوی دیگر، هندسۀ محاسباتی که به بررسیِ مسائلِ هندسی از منظرِ رایانشی می‌پردازد و پیچیدگی و الگوریتم‌های این مسائل را بررسی می‌کند، می‌تواند در سیاقِ رایانشِ کوانتومی نیز موردِ بررسی قرار بگیرد. از بدو پیدایشِ رایانشِ کوانتومی بررسی‌های اندکی برروی کاربردِ آن در هندسۀ محاسباتی صورت گرفته که آن بررسی‌ها هم اکثراً به شکلِ استفاده از الگوریتمِ جست‌وجوی کوانتومی برروی مسائل بوده‌است که با تسریعِ چندجمله‌ای همراه است. مسئلۀ قرارگیریِ نقطه در چندضلعی که یکی از مسائلِ پرکاربردِ این حوزه است که تا کنون به شکلِ کوانتومی بررسی نشده و با رایانشِ کلاسیک چند الگوریتم با زمانِ خطی برای آن وجود دارد در کنار الگوریتم‌های تقریبی و با پیش‌پردازشی که در زمان و پرسش زیرخطی اجرا می‌شوند. در این پایان‌نامه به معرفیِ الگوریتمی کوانتومی برای نقطه در چندضلعی می‌پردازیم که مبتنی بر تبدیلِ فوریۀ کوانتومی‌ست و می‌تواند در شرایطی که تضمینِ فاصلۀ نقطه از اضلاع وجود دارد به تسریعِ فرا‌ـچندجمله‌ای دست می‌یابد و با یک پرسش در زمانِ لگاریتمی می‌تواند پاسخ مسئله را به دست بیاورد اما در حالتِ کلی تسریعی نسبت به حالتِ کلاسیک نخواهد داشت.

کلیدواژه‌ها: رایانشِ کوانتومی، هندسۀ محساباتی، نقطه‌ـ درـ چندضلعی، تبدیلِ فوریۀ کوانتومی

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

فصل ۱

مقدمه

از ایدهٔ کامپیوترهای کوانتومی بیش از نیم قرن می‌گذرد اما عمدهٔ توجه به آن پس از دو الگوریتمِ مشهورِ شور و گروور در دههٔ نودِ میلادی بوده‌است. از آن روز تلاشِ بی‌وقفه‌ای برای یافتنِ الگوریتم‌های جدید و کاربردهای جدید از الگوریتم‌های قدیمیِ رایانشِ کوانتومی ادامه دارد. اما بخشِ اندکی از این تلاش‌ها در حوزهٔ هندسهٔ محاسباتی بوده‌است، با این وجود به نظر می‌رسد که با توجه به خواصِ هندسیِ حالت‌های کوانتومی و قیودِ هندسی که مسائلِ هندسهٔ محاسباتی را از گونه‌های دیگرِ مسائلِ محاسباتی متمایز می‌کنند، رایانشِ کوانتومی کاربردهایی بسیار گسترده‌تر از آن‌چه تا کنون شناخته‌شده است در این حوزه داشته‌باشد.

۱-۱ تعریف مسئله

مسئلهٔ این تز، در مرحلهٔ اول، بررسیِ کاربردهای الگوریتم‌های کوانتومی در هندسهٔ محاسباتی و در مرحلهٔ بعد معرفیِ الگوریتمِ جدیدی برای مسئلهٔ نقطه‌ـ‌درـ‌چندضلعی است. هرچند که برای مسئلهٔ نقطه‌ـ‌درـ‌چندضلعی الگوریتمِ خطی‌ای وجود دارد و امکانِ تسریعِ آن به شکلِ کلاسیک وجود ندارد اما به علتِ استفادهٔ گستردهٔ آن در گرافیکِ کامپیوتری، بهبودِ سرعتِ آن به شکلِ تکنیکال نیز همواره مورد توجهِ افراد بوده‌است. همچنین در ادبیاتِ الگوریتم‌های کوانتومی در هندسهٔ محاسباتی، هرچند مسئله‌های بسیاری مورد بررسی قرار گرفته اما این مسئله موردِ بررسی قرار نگرفته و از سوی دیگر، ایدهٔ اکثریتِ تسریع‌های کوانتومی در هندسهٔ محاسباتی مبتنی بر جست‌وجوی کوانتومی بوده‌است که منتجِ به تسریعِ حداکثر

مربعی می‌شود.

۱-۲ ساختار پایان‌نامه

این پایان‌نامه در پنج فصل به این موضوع می‌پردازد به این ترتیب که پس از مقدمه، در فصلِ اول مفاهیمِ اولیهٔ رایانشِ کوانتومی و هندسهٔ محاسباتی مرور می‌شود و پس از آن در فصلِ مروری بر ادبیاتِ الگوریتم‌های کوانتومیِ هندسهٔ محاسباتی صورت می‌گیرد. سپس برای الگوریتمِ نقطه‌ـ درـ چندضلعی الگوریتم‌های کلاسیک بررسی می‌شوند و در فصلِ چهارم الگوریتمِ کوانتومی‌ای تشریح می‌شود. درنهایت در فصلِ آخر به جمع‌بندی و مسیرهای پیشنهادی برای پژوهش‌های آتی پرداخته می‌شود.

فصل ۲

مفاهیم اولیه

همواره مرسوم‌ترین راه برای بیانِ فیزیکِ کوانتوم، دنبال کردنِ سیرِ تاریخیِ رخدادها بوده، اما امروزه با به وجود آمدنِ رایانشِ کوانتومی، بسیاری از منابع از اصلِ موضوع‌های رایانش و اطلاعاتِ کوانتومی برای ورود به فیزیکِ کوانتوم استفاده می‌کنند و معتقدند این درگاه، باعث کم‌تر گمراه شدنِ افراد در گزاره‌های ناسازگار با شهودِ ما از طبیعت دارد. [۱]

۲-۱ حالت‌های کلاسیک و کوانتومی

مفاهیمِ «حالت» و «گزار» در بخش‌های مختلفی از دانش استفاده شده و کاربردهای گوناگونی دارد، یکی از این کاربردها، در زنجیره‌های مارکوفی‌ست.

۲-۱-۱ زنجیرهٔ مارکوفی

این بخش تنها مقدمه و مروری بر زنجیره‌های مارکوفی‌ست.

نمایش ۱ *برای نمایشِ بردارها از حروفِ کوچک و توپر* $\mathbf{a}$ *استفاده می‌کنیم و برای نمایشِ ماتریس‌ها از حروفِ بزرگِ توپر* $\mathbf{A}$ *نشان می‌دهیم.*

برای نمایشِ ترانهاده بردارها و ماتریس‌ها از علامتِ $^{\intercal}$. *استفاده می‌کنیم.*

برای نشان دادنِ درایه‌ها نیز از زیروند به شکلِ $\mathbf{A}_{ij}$ استفاده می‌کنیم.

همچنین بردارِ $\mathbf{j}$ نشان‌دهندهٔ بردارهایی با همهٔ عناصر یک است و $\mathbf{e_i}$ برداری‌ست که تنها مؤلفهٔ iام آن یک است و باقی صفر هستند.

برای بردارهای مختلط از علامتِ *. برای مزدوج‌مختلطِ تک‌تکِ درایه‌های بردارها و ماتریس‌ها استفاده می‌کنیم.

همچنین

$$.^\dagger = .^{*\intercal} \tag{۱-۲}$$

یک زنجیرهٔ مارکوفی یک دنباله از متغیرهای تصادفی X_t بر روی مجموعهٔ گسستهٔ حالت‌ها به نامِ $\mathbf{S}$ است. با این شرط که توزیعِ متغیرِ تصادفیِ متغیر X_{t+1} امِ دنباله تنها بستگی به جملهٔ X_t ام دارد و احتمالاتِ شرطیِ این بستگی در طولِ این زنجیره ثابت هستند و می‌توان آن‌ها را با ماتریسِ گزار نشان داد به این ترتیب که برای همهٔ tها

$$(\mathbf{T})_{ij} = \Pr(X_{t+1} = j | X_t = i) \tag{۲-۲}$$

که اگر در کنارِ این ماتریس، بردارِ احتمال را تعریف کنیم

$$(\mathbf{p}^t)_i = \Pr(X_t = j) \tag{۳-۲}$$

آن‌گاه می‌توان این خاصیت‌ها را در حالتِ کلی اثبات کرد.

$$\mathbf{j}^\intercal \mathbf{p}^t = 1 \tag{۴-۲}$$

$$\mathbf{T}\mathbf{j} = \mathbf{j} \tag{۵-۲}$$

$$\mathbf{j}^\intercal \mathbf{T} = \mathbf{j}^\intercal \tag{۶-۲}$$

و همچنین به شکلِ کلی می‌توان تحول را به این شکل بیان کرد.

$$\mathbf{p}^t = \mathbf{T}^t \mathbf{p}^۰ \tag{۷-۲}$$

می‌توان معادلهٔ ۲-۶ را به شکلِ شفاهی این طور بیان کرد که جمعِ مؤلفه‌ها در گزارِ سیستم ناورداست. البته این طبیعی‌ست زیرا برای ما مطلوب است که بردارِ $\mathbf{p}^t$ همواره توزیعِ احتمال باقی بماند.

با توجه به این‌که این ماتریس گزار مثبت است خواص متعددی را می‌توان برای آن اثبات کرد، از جمله این‌که ویژه‌برداری با ویژه‌مقدارِ بیشینه (برابرِ یک) وجود دارد که حالتِ تعادلِ این سیستم پس از بی‌نهایت‌بار گزار است. [۲]

تضارب حالت‌ها

دو زنجیرهٔ مارکوفی را در نظر بگیرید که (لااقل در ابتدا) مستقلاً کار می‌کنند. زنجیرهٔ اول در حالتِ $\mathbf{p}^۱$ و زنجیرهٔ دوم را در حالتِ $\mathbf{p}^۲$ در نظر بگیرید. اگر بخواهیم مجموعِ دو زنجیره را با یک زنجیرهٔ بزرگ‌تر بیان کنیم

$$\mathbf{p}^{\text{کل}} = \mathbf{p}^۱ \otimes \mathbf{p}^۲ \tag{۸-۲}$$

که در آن $\otimes$ ضرب تانسوری‌ست. و به همین شکل

$$\mathbf{T}^{\text{کل}} = \mathbf{T}^۱ \otimes \mathbf{T}^۲ \tag{۹-۲}$$

حالا اگر بعد از تحولی به شکلِ مجزا یا به شکلِ هم‌بسته، از بردارِ حالتِ دو سیستم، به بردارِ حالتِ یکی از سیستم‌ها برسیم کافی‌ست

$$\mathbf{p}^۱_i = \sum_{j}^{\dim(\text{زنجیرهٔ دوم})} \mathbf{p}^{\text{کل}}{}_{۲} \mathbf{e}^۱_i \otimes \mathbf{e}^۲_j \tag{۱۰-۲}$$

کمیت‌های مشاهده‌پذیر

برای سیستمی که در حالتِ $\mathbf{p}$ قرار دارد، دسترسی به خودِ این بردار در عمل مقدور نیست و آن‌چه مشاهده می‌شود، کمیتِ مشاهده‌پذیری نظیرِ X است که می‌توان آن را تابعی از حالت‌های سیستم درنظر گرفت، یعنی

$$M : \{۱ \dots n\} \to \mathbb{R} \qquad (۱۱-۲)$$

که البته این تابع را می‌توان به شکلِ برداری نشان داد که در آن صورت، بیانِ کمیتی مثلِ امیدِ ریاضیِ آن ساده‌تر می‌شود

$$\mathbb{E}[M] = \mathbf{M}^{\intercal}\mathbf{p} \qquad (۱۲-۲)$$

۲-۱-۲ گزارهای کوانتومی

سیستمِ احتمالاتی‌ای را (با n حالتِ مجزا) بگیرید که برای نمایشِ آن از برداری nـ بعدی، مختلط و با اندازهٔ یک به نامِ $\mathbf{v}$ بهره می‌گیریم به طوری‌که

$$\Pr(i) = |\mathbf{v}_i|^{۲} \qquad (۱۳-۲)$$

به هر فضای برداری‌ای که یک ضربِ داخلی برروی آن تعریف شده، نظیرِ فضای برداریِ تعریف‌شده، «فضای هیلبرت» می‌گوییم.

نمایش ۲ *برای بردارهای مختلط، به جای $\mathbf{v}$ از $|v\rangle$ استفاده می‌کنیم و همچنین برای $\mathbf{v}^{\dagger}$ از $\langle v|$ استفاده می‌کنیم.*

همچنین $\langle v|u\rangle$ ضربِ داخلیِ دوبردار و $|v\rangle\,|u\rangle$ نمایشِ ساده‌ای از $|u\rangle \otimes |v\rangle$ است.

و به ازای هر $i \in \{۰, \dots, n\}$ $|i\rangle$ برداری‌ست که مؤلفهٔ iام آن یک است.

در نهایت $|v\rangle\langle u|$ همان ماتریسِ $\mathbf{v}\mathbf{u}^{\dagger}$ است.

ماتریس‌ها با علامتِ توپر نشان داده نمی‌شوند و همچنین I ماتریس همانی‌ست.

در ادامه نشان خواهیم‌داد این گونه‌حالت‌ها چیزی فراتر از زنجیرهٔ مارکوفی هستند. برای گزارِ این سیستم، باید از ماتریس‌های حافظِ اندازه (ماتریس‌های یکانی) استفاده کنیم، به این ترتیب هر $U \in SU(n)$ [۱] یک گزار برای این سیستم است.

مثال ۲-۱ (تبدیل هادامارد) *فرض کنید سیستمی با دو حالتِ مجزا داریم و آن را یک کیوبیت می‌نامیم. اگر بگیریم*

$$|۰\rangle := \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \tag{۱۴-۲}$$

$$|۱\rangle := \begin{pmatrix} ۰ \\ ۱ \end{pmatrix} \tag{۱۵-۲}$$

همچنین اگر بگیریم

$$|+\rangle := \frac{۱}{\sqrt{۲}}(|۰\rangle + |۱\rangle) \tag{۱۶-۲}$$

$$|-\rangle := \frac{۱}{\sqrt{۲}}(|۰\rangle - |۱\rangle) \tag{۱۷-۲}$$

این‌دو بردار هردو توزیعِ احتمالاتی به شکلِ $\mathbf{p} = \begin{pmatrix} ۱/۲ \\ ۱/۲ \end{pmatrix}$ *دارند.*

و اگر این تحول را در نظر بگیریم

$$H = \frac{۱}{۲}\begin{pmatrix} ۱ & ۱ \\ ۱ & -۱ \end{pmatrix} \tag{۱۸-۲}$$

[۱] $SU(n)$ گروه ماتریس‌های یکانیِ $n \times n$ هستند.

آن‌گاه تحتِ این تحول، دو بردارِ مثبت و منفی که توزیعِ احتمالِ یک‌شکل داشتند به دو بردار با توزیع‌های متفاوت می‌روند که این‌چنین رفتاری با زنجیرهٔ مارکوفی قابلِ‌توصیف نیست.

این مثال نشان می‌دهد که این تئوری اندکی با تئوریِ احتمالِ مرسوم متفاوت است.

نکتهٔ دیگری که موردِ توجه است این است که برخلافِ T، گزارِ U حتماً وارون‌پذیر است که این نکته‌ای‌ست که در بخش‌های دیگر بیشتر موردِ توجه قرار می‌گیرد.

اندازه‌گیری

یکی از بخش‌های مبهمِ مکانیکِ کوانتومی، اندازه‌گیری‌ست. تصور کنید که سیستمی کوانتومی در حالتِ $|v\rangle$ قرار دارد. اگر یک مشاهده یا اندازه‌گیریِ فیزیکی انجام بگیرد، بردارِ حالتِ سیستم با احتمالِ $\Pr(i) = |\langle e_i|v\rangle|^۲$ به بردارِ $|e_i\rangle$ تبدیل می‌شود. به این عمل «فروریزش» می‌گویند.

مثال ۲-۲ *مانندِ مثالِ قبل، یک کیوبیت را تصور کنید*

- *سیستم در حالتِ اولیهٔ $|+\rangle$ باشد.*
- *تحول H را روی آن اعمال شود.*
- *اندازه‌گیری را انجام شود.*

نتیجهٔ این فرایند به این شکل است که با احتمالِ $\Pr(۰) = ۱$ حالتِ ۰ مشاهده می‌شود.

حالا سناریوی دیگری را درنظر بگیرید که در ابتدا یک اندازه‌گیری نیز انجام می‌گیرد.

- *سیستم در حالتِ اولیهٔ $|+\rangle$ باشد.*
- *یک اندازه‌گیریِ اولیه انجام می‌شود.*
- *تحول H را روی آن اعمال شود.*
- *اندازه‌گیری را انجام شود.*

می‌توان محاسبه کرد که حاصلِ این فرایند با احتمالِ $\Pr(۰) = \frac{۱}{۲}$ *حالتِ* ۰ *و با احتمالِ* $\Pr(۱) = \frac{۱}{۲}$ *حالتِ* ۱ *مشاهده می‌شود.*

این آزمایش تأثیرِ مفهومِ رمبش را نشان می‌دهد. به این ترتیب که می‌توان آزمایشِ مشابهی برای زنجیره‌های مارکوفی تعریف کرد و خواهیم دید که اندازه‌گیری هیچ‌تأثیری در زنجیره‌های مارکوفی ندارد.

به طورِ مشابه، برای آن‌چه در خصوصِ کمیت‌های مشاهده‌پذیر در زنجیرهٔ مارکوفی گفتیم، دسترسی به بردارِ حالتِ یک سیستم $|v\rangle$ و حتی توزیع احتمالاتِ آن مقدور نیست.

در ساده‌ترین حالت در نظر بگیرید که کمیتِ مشاهده‌پذیری به نامِ M داریم که به هر حالتِ سیستم (یا به عبارتی دیگر هر بردار از پایهٔ متعامدیکهٔ فضا) مانندِ $|i\rangle$ یک عدد $\lambda_i \in \mathbb{R}$ نسبت می‌دهد.

می‌دانیم که آن‌گاه

$$\mathbb{E}[M] = \sum_i \lambda_i \Pr(i) = \sum_i \lambda_i |\langle i|v\rangle|^۲ = \sum_i \lambda_i \langle v|i\rangle \langle i|v\rangle \qquad (۱۹-۲)$$

که حالا اگر ماتریسِ زیر را تعریف کنیم

$$\hat{M} := \sum_i \lambda_i |i\rangle\langle i| \qquad (۲۰-۲)$$

آن‌گاه، می‌توان معادلهٔ ۲-۱۹ را به شکلِ زیر نوشت

$$\mathbb{E}[M] = \langle v|\hat{M}|v\rangle \qquad (۲۱-۲)$$

اما حقیقتِ ماجرا این است که در یک سیستمِ فیزیکی، ممکن است چند پایهٔ متعامدیکه برای حالت‌های مربوط به مشخصه‌های مختلف وجود داشته‌باشد.

مثال ۲-۳ (آزمایشِ اشترن‌ـ گرلاخ) *با اغماض می‌توان الکترون‌ها را آهن‌رباهای کوچکی در نظر گرفت که سه مؤلفه دارند و این سه مؤلفه جهت آهن‌ربا را مشخص می‌کند. به این کمیتِ برداری، «اسپین» می‌گوییم.* [۲]

پس مؤلفه‌های اسپین را می‌توان در هرکدام از راستاهای x *و* y *و* z *اندازه‌گیری کرد. در نتیجه باید بتوان سه عملگر به شکل* $\hat{X}$ *و* $\hat{Y}$ *و* $\hat{Z}$ *تعریف کرد.*

در آزمایش اشترن ـ گرلاخ با اندازه‌گیری پیاپی این عملگرها نتایجی دور از انتظار می‌بینیم، برای مثال اگر با اندازه‌گیری‌های پیاپی $\hat{Y}$ ببینیم که سیستم در راستای y اسپینی برابر $\frac{1}{2}$ [۳] دارد، اگر حال اندازه‌گیری $\hat{X}$ را ترتیب بدهیم، اطلاعاتی که از اسپین در راستای y به دست آورده‌ایم نیز دیگر معتبر نیست.

در نتیجهٔ این آزمایش، ساده‌ترین مدلی که این رفتار را توصیف کند به شرحِ زیر است که این سیستم علی‌رغمِ این‌که سه مؤلفه برای اندازه‌گیری دارد، حالتِ آن برداری نظیر $|\psi\rangle$ در فضای دوبعدی‌ست و عملگرهای گفته‌شده برابر با ماتریس‌هایی به شکلِ زیر است.

$$\hat{X} = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{۲۲-۲}$$

$$\hat{Y} = \frac{1}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{۲۳-۲}$$

$$\hat{Z} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{۲۴-۲}$$

یک مثالِ معروف‌تر از این، «مکان» و «تکانه» هستند که هردو پایه‌های متعامدیکه‌ای برای فضای حالت‌های یک ذره هستند. در نتیجهٔ این، نمی‌توان مکان و تکانه را همزمان اندازه‌گیری کرد و همچنین با اندازه‌گیریِ آن‌ها به ترتیب می‌توان به اصلِ عدمِ قطعیت [۴] را اثبات کرد.

---

[۳] این تعریف به هیچ‌وجه تعریف دقیقی از اسپین به عنوانِ یک کمیت ذاتی در ذرات صحیح نیست و تنها مثال ملموسی‌ست برای استفاده از آن در سیاقِ رایانشِ کوانتومی

[۳] مقدارِ دقیق‌ترِ آن $\frac{\hbar}{2}$ است که برای سادگی، مقدارِ $\hbar$ را که یک ثابتِ جهانی به نامِ ثابتِ کاهیدهٔ پلانک است، یک فرض می‌کنیم.

[۴] اصلِ عدمِ قطعیت، اصلی‌ست که بیان می‌کند هرگونه اندازه‌گیری‌ای که مکان و تکانه را به ترتیب با خطای Δx و Δp اندازه‌گیری کند، این نامساوی برقرار است

$$\Delta x \Delta p \geqslant \frac{\hbar}{2} \tag{۲۵-۲}$$

مدلِ کوانتوم‌ـاحتمالاتی

حالا می‌توان مدلی را تصور کرد که سیستم، به شکلِ احتمالاتی، در حالاتِ کوانتومیِ متعدد باشد. یعنی دنباله‌ای از حالت‌ها داریم $|v_1\rangle \dots |v_n\rangle$ داریم که سیستم با احتمالاتِ نظیرِ $p_1 \dots p_n$ در این حالات حضور داشته‌باشد.

سیستم‌های این‌چنینی را می‌توان با ترکیبِ مدلِ احتمالاتی و کوانتومی بررسی کرد، اما برای بررسیِ ساده‌تر، می‌توان کمیتِ زیر را تعریف کرد که ماتریسِ چگالی نام دارد و نمایندهٔ این توزیعِ احتمالاتی از توزیع‌هاست.

$$\rho := \sum_{i=1}^{n} p_i \, |v_i\rangle\langle v_i| \tag{۲۶-۲}$$

حالا اثرِ یک تحولِ کوانتومی که یک ماتریسِ یکانی مانند U است، برروی این ماتریسِ چگالی، به شکلِ زیر است.

$$\rho \mapsto U\rho U^{\dagger} \tag{۲۷-۲}$$

و همچنین، با اندازه‌گیریِ یک کمیت، مانندِ M امیدِ ریاضیِ آن از رابطهٔ زیر به دست می‌آید.

$$\mathbb{E}[M] = \mathrm{Tr}\left(\rho \hat{M}\right) \tag{۲۸-۲}$$

بررسیِ تحولاتِ این سیستم‌ها، با مفهومی به نامِ کانال انجام می‌گیرد که خارج از این مقال است.

تضاربِ حالت‌ها

اگر دو سیستمِ کوانتومیِ مجزا با حالت‌های $\langle v|$ و $\langle u|$ داشته‌باشیم، آن‌گاه حالتِ کلیِ سیستم $\langle u| \otimes \langle v|$ خواهدبود.

در این صورت اگر عملگری مانند U را فقط برروی سیستمِ اول اثر بدهیم، آنگاه اثرِ آن بر کلِ سیستم به شکلِ $U\otimes I$ خواهد بود. به شکلی مشابه می‌توان عملگری را فقط روی سیستمِ دوم اثر داد یا عملگری را روی هردو سیستم به شکلِ همزمان اثر داد که در نتیجهٔ آن، بردارِ حاصل، به شکلِ ضربی مثلِ $|u'\rangle\otimes|v'\rangle$ قابلِ بیان نباشد.

در کلی‌ترین حالت، برداری که متعلق به دو فضا باشد را بتوان به شکلِ زیر نوشت

$$|\psi\rangle=\sum_i |a_i\rangle\otimes|b_i\rangle \qquad (۲۹-۲)$$

حالا فرض کنید فضای دوم را در پایه‌ای دلخواه اندازه‌گیری می‌کنیم. و نتیجهٔ آن بردارِ $|b_i\rangle$ در سیستمِ آنگاه سیستم با احتمالِ $|\langle b_i|\psi\rangle|^2$ در حالتِ $\frac{\langle b_i|\psi\rangle}{|\langle b_i|\psi\rangle|}$ قرار می‌گیرد. ذکرِ این نکته لازم است که حاصلِ $\langle b_i|\psi\rangle$ یک بردار در فضای اول است و نه یک عدد.

این‌طور می‌توان گفت که پس از اندازه‌گیریِ فضای دوم، یک حالتِ احتمالاتیِ کوانتومی داریم که با آن را با یک ماتریسِ چگالی نشان می‌دهیم.

$$\rho_{\text{فضای اول}}=\sum_i |\langle b_i|\psi\rangle|^2\frac{\langle b_i|\psi\rangle}{|\langle b_i|\psi\rangle|}\frac{\langle\psi|b_i\rangle}{|\langle b_i|\psi\rangle|}=\sum_i \langle b_i|\psi\rangle\langle\psi|b_i\rangle=\text{Tr}_{\text{فضای دوم}}|\psi\rangle\langle\psi| \qquad (۳۰-۲)$$

که با ساده‌سازی به ردِ جزئی می‌رسیم.

۲-۱-۳ تفاوت‌های سیستم‌های کوانتومی و کلاسیک

همچنان که در مثالِ ۲-۱ گفته‌شد، سیستم‌های کوانتومی قابلیت‌هایی متعددی مزیدِ بر سیستم‌های کلاسیک دارند. آن‌چه در آن مثال دیده‌شد به نوعی قابلیتِ پنهان کردنِ اطلاعاتی در سیستم بود که خود را در یک اندازه‌گیریِ ساده نشان نمی‌دهد.

در ادامه در قالبِ یک مثال، به بررسیِ هم‌بستگی‌های کوانتومی می‌پردازیم که «درهم‌تنیدگی» نامیده می‌شود.

مثال ۲-۴ (آزمایشِ بل) *یک بازی را تصور کنید، که داور به هرکدام از دو بازیکن (آلیس و باب) یک*

بیت ارسال می‌کند. درنظر بگیرید x را به آلیس و y را به باب ارسال می‌کند.

آلیس و باب نمی‌توانند با هم هیچ پیامی ردوبدل کنند. حالا، آلیس و باب، هرکدام برحسبِ استراتژیِ خود یک بیت را به داور برمی‌گردانند. تصور کنید دو بیت را a و b باشند. آلیس و باب هردو با هم پیروز می‌شوند اگر و تنها اگر

$$a \,\mathrm{XOR}\, b = x \,\mathrm{AND}\, y \tag{۳۱-۲}$$

حالا یک‌بار در نظر می‌گیریم که استراتژیِ هرکدام، به شکلِ تعینی باشد، یعنی

$$\begin{cases} a_x = f(x) \\ b_y = g(y) \end{cases} \tag{۳۲-۲}$$

اگر فرض بگیریم که هریک از مقادیرِ x و y هم‌احتمال باشند، آنگاه برای احتمالِ پیروزی، برای هر استراتژی‌ای خواهیم داشت

$$\Pr(\text{پیروزی}) \leqslant \frac{۳}{۴} \tag{۳۳-۲}$$

حالا اگر استراتژیِ هرکدام از آلیس و باب، به شکلِ احتمالاتی و وابسته به یک متغیرِ تصادفیِ مشترک مانندِ λ باشد

$$\begin{cases} \Pr(a|x,\lambda) = f(a,x,\lambda) \\ \Pr(b|y,\lambda) = g(b,y,\lambda) \end{cases} \tag{۳۴-۲}$$

در این صورت، باز هم همان حد برای احتمالِ پیروزی برقرار است.

اما اگر به‌جای متغیرِ تصادفیِ مشترک، یک حالتِ کوانتومی بینِ آلیس و باب به اشتراک گذاشته شود، به طوری‌که سیستمِ کوانتومیِ مسئله، از دو زیرسیستمِ دوحالته تشکیل شده‌است که زیرسیستمِ اول در اختیارِ آلیس و زیرسیستمِ دوم در اختیارِ باب است. (که در زیر فوق با اندیس‌ها مشخص شده‌اند)

$$|\psi\rangle = \frac{۱}{\sqrt{۲}}(|۰\rangle_A |۰\rangle_B + |۱\rangle_A |۱\rangle_B) \qquad (۳۵-۲)$$

حالا اگر برای تعیینِ استراتژی هرکدام از بازیکنان از اندازه‌گیری استفاده کنند، یعنی با توجه به ورودی (x و y) یک پایهٔ متعامد برای اندازه‌گیری انتخاب کند [۵] و از نتیجهٔ آزمایش، خروجیِ خود را انتخاب کند، یعنی اگر $\{|A_۰^۰\rangle, |A_۰^۱\rangle\}$ و $\{|A_۱^۰\rangle, |A_۱^۱\rangle\}$ دو پایهٔ متعامدِ برای اندازه‌گیری در زیرسیستمِ آلیس باشند و به شکلِ مشابهی برای باب، بردارهای B را داشته‌باشیم، می‌توانیم به این شکل بنویسیم که

$$Pr(a,b|x,y) = \left|\langle\psi|A_a^x\rangle\,|B_b^y\rangle\right|^۲ \qquad (۳۶-۲)$$

دلیلِ این‌که نمی‌توان این احتمال را برای آلیس و باب به شکلِ مجزا نوشت این است که هرکدام از این‌دو، نخست اندازه‌گیری را انجام دهند، برروی استیتِ کلیِ سیستم تأثیر می‌گذارند، هرچند که این تأثیر، همچنان نمی‌توان هیچ پیامی را منتقل کرد، اما شکلِ خاصی از هم‌بستگی را به وجود می‌آورد که در سیستم‌های کلاسیک دیده نمی‌شوند و درنتیجه باعث می‌شود که احتمالِ پیروزی می‌تواند به $\frac{۱+۲\sqrt{۲}}{۴} \simeq ۰/۸۵$ برسد که این نقضِ نامساویِ ۲-۳۳ است. [۳، ناموضعیت در مکانیکِ کوانتومی]

۲-۲ رایانشِ کوانتومی و کلاسیک

۲-۲-۱ مدل رایانش

نمایش ۳ *یک الفبا مانند Σ ، یک مجموعه از علامت‌هاست. اگر $s \in \Sigma$ یکی از آن علامت‌ها باشد ss یا $s^۲$ یک کلمهٔ ساخته‌شده با تکرارِ آن علامت است و همچنین $\Sigma^۲$ مجموعهٔ کلمه‌ها با طول دو است. (و به همین‌ترتیب برای طول‌های بیشتر)*

از عملگرِ *. برای بیانِ مجموعه‌های کلمه‌های آن الفبا (با طول صفر یا بیشتر) استفاده می‌کنیم. همچنین برای هر $s \in \Sigma^*$ عملگرِ $|.|$ طولِ آن را بیان می‌کند.

[۵] اندازه‌گیری در پایهٔ متعامدِ دلخواه، هم‌ارزِ انجامِ یک تحولِ یکانیِ مناسب و سپس اندازه‌گیری در پایهٔ اصلی است. پس اگر تحول‌های یکانی همگی در دسترس باشند، اندازه‌گیری در هر پایه‌ای ممکن است. دربارهٔ در دسترس بودنِ تحول‌ها در ۲-۲-۱ بررسی می‌شود.

برای یک $s \in \Sigma^*$ اگر $\Sigma = \mathbb{Z}_N$ یعنی اعداد کوچک‌تر از N باشد، آن‌گاه عددی که این بازنمایی را در مبنای N دارد با $\bar{s}$ نمایش می‌دهیم.

مدل‌های مختلفی برای بیانِ رایانش کوانتومی وجود دارد اما پر استفاده‌ترینِ آن‌ها مدلِ مداری‌ست که به سادگی قابلِ ساخت از روی مدلِ کلاسیکِ مداری‌ست.

در مدل‌های محاسباتی، یک مسئله را به شکلی استاندارد که قابل محاسبه باشد بیان می‌کنیم. برای سادگی، در این بخش فرض می‌کنیم که مسئله‌ای که قصد حلِ آن را داریم، تابعی به شکلِ $f : \mathbb{Z}_۲^* \to \mathbb{Z}_۲$ است.

خانوادهٔ مدارهای یکنواخت و غیرِیک‌نواخت

یک مدار C، یک گرافِ جهت‌دارِ غیرِ مدور است که سه دسته گره برروی آن مشخص می‌کنیم.

- گره‌های ورودی: گره‌هایی با درجهٔ ورودیِ صفر هستند که هرکدام نمایانگر یکی از ورودی‌های مسئله است هستند.
- گره‌های گیت: گره‌هایی با درجهٔ ورودی و خروجی‌شان ناصفر هستند که هرکدام نمایانگر یک گیت از مجموعهٔ گیت‌های مجاز در مدار است که تعدادِ ورودی‌ها و تعدادِ خروجی‌های مشخصی دارد. برای ما این مجموعه شاملِ AND و OR هرکدام با دو ورودی و NOT با یک ورودی است.
- گره‌های خروجی: گره‌هایی با درجهٔ خروجی صفر که نمایندهٔ خروجیِ مسئله هستند (با توجه به تعریف تابع به شکلِ گفته شده، تنها یک گره خروجی داریم)

برروی این مدار، توابعِ زیر را تعریف می‌کنیم

- $\mathrm{size}(C)$: تعدادِ گره‌های گیت در مدار
- $\mathrm{depth}(C)$: طولِ طولانی‌ترین مسیر در مدار

با توجه به تعریفی که از مدار ارائه شد، اندازهٔ ورودی‌های آن ثابت است و برای حلِ مسئله به شکلی که گفته شد، نیاز به یک خانواده از مدارها داریم. خانوادهٔ مدار F، یک دنباله از مدارها به شکلِ $(F_۱, F_۲, \dots)$ است که F_i برای ورودی با طولِ i تابعِ f را محاسبه می‌کند.

اگر تابعِ f با یک خانوادهٔ مدار F قابلِ محاسبه باشد، به طوری که برای $\text{size}(F_i)$ (به عنوانِ تابعی از i) داشته‌باشیم $\text{size}(F_i) \in \mathcal{O}(poly(i))$ آن‌گاه می‌گوییم مسئلهٔ محاسبهٔ f عضو کلاس $\mathbf{P}/poly$ است.

مثالِ ساده‌ای وجود دارد که نشان می‌دهد این مدل از ماشین تورینگ قوی‌تر است.

مثال ۲-۵ (این مثال صرفاً به خاطرِ علاقهٔ شخصیِ نویسنده این‌جاست و بار علمی‌ای ندارد.) *فرض کنید مسئلهٔ h به شکلِ $h : \mathbb{Z}_۲^* \to \mathbb{Z}_۲$ برای ماشینِ تورینگ غیرقابل محاسبه است. (می‌دانیم چنین مسئله‌ای وجود دارد)*

می‌دانیم که به ازای هر $s \in \mathbb{Z}_۲^*$ می‌توان عددی طبیعی به آن نسبت داد که به این شکل ساخته‌می‌شود $n_s = \overline{۱s}$ به سادگی می‌توان گفت این تبدیل یک‌به‌یک و پوشاست.

حال ابتدا مسئلهٔ دیگری به شکلِ $f : ۱^* \to \mathbb{Z}_۲$ می‌سازیم که در آن

$$f(۱^{n_s}) = h(s) \tag{۳۷-۲}$$

آنگاه طبیعتاً برای هرطولی از ورودیِ f یک مدار وجود دارد که خروجیِ لازم را تولید کند. (اما تولیدِ خودِ مدار کارِ سختی‌ست و این مهم همان‌چیزی‌ست که به آن توجه نشده‌بود)

پس خانوادهٔ مدار از ماشین تورینگ قوی‌تر عمل می‌کنند.

با توجه به مثالِ گفته‌شده، خانوادهٔ مدارهای یکنواخت را تعریف می‌کنیم که در آن هرکدام از F_i ها به سادگی (در زمان چندجمله‌ای) توسط یک مدل محاسباتی قابل توصیف باشند.

حالا اگر مسئله‌ای با یک خانوادهٔ مدار یکنواخت F قابلِ محاسبه باشد، اگر $\text{size}(F_i) \in \mathcal{O}(poly(i))$ آن‌گاه می‌گوییم مسئلهٔ محاسبهٔ f عضو کلاس $\mathbf{P}$ است.

پس از آن، مسئله‌ای مانندِ g را تصور کنید که برای ورودی، علاوه‌بر x، یک رشته به نامِ w می‌گیرد به طوری که $|w| \in \mathcal{O}(poly(|x|))$ طولِ این رشته نسبت به طولِ x به شکلِ چندجمله‌ای باشد.

این ورودیِ w را به شکلِ نوعی سرِ نخ برای $f(x) = ۱$ استفاده می‌کنیم، یعنی فرض کنید

$$\begin{cases} \exists w\ g(x \cdot w) = ۱ \Leftrightarrow f(x) = ۱ \\ \forall w\ g(x \cdot w) = ۰ \Leftrightarrow f(x) = ۰ \end{cases} \tag{۳۸-۲}$$

اکنون اگر مسئلهٔ g که مسئلهٔ f به همراهِ سرنخ است (و از مسئلهٔ f آسان‌تر است) عضوِ کلاسِ **P** باشد می‌گوییم که مسئلهٔ f خود عضوِ کلاسِ **NP** است.

برای تعریفِ چند کلاسِ دیگر، تصور کنید یک مدار به شکلِ احتمالاتی کار می‌کند یا برای سازگاری با تعریف‌های قبل، این‌بار بگیرید مسئلهٔ g علاوه بر ورودیِ x، یک رشته از اعدادِ تصادفی به طولِ چندجمله‌ای را می‌گیرد که آن را r می‌نامیم. اگر g خود عضوِ **P** باشد و داشته‌باشیم

$$\Pr(g(x \cdot r) = f(x)) \geqslant \frac{۲}{۳} \qquad (۳۹-۲)$$

آن‌گاه f عضوِ کلاسِ **BPP** است. [۴] [۶]

مدارهای کوانتومی

حالا تصور کنید یه سیستمِ dـحالتهٔ کوانتومی داریم. به این سیستم «کیودیت» می‌گوییم. در حالتی که $d = ۲$ به این سیستم «کیوبیت» می‌گوییم.

اگر یک سیستم متشکل از n کیوبیت در نظر بگیریم، چنان‌چه پیشتر گفته‌شد، می‌توان تحول‌هایی را به شکلِ محلی برروی یکی یا چندتا از این کیوبیت‌ها (به عنوانِ یک زیرسیستم از سیستمی بزرگ‌تر) اعمال کرد.

از این رو می‌توان متصور شد که اگر گیت‌های پایهٔ کوانتومی را تعریف کنیم، بتوان مدارِ کوانتومی را تعریف کرد که به شکلِ مشابهی، شاملِ گره‌های زیر خواهد بود [۵]

- گره‌های ورودی: مشابهِ حالتِ قبل اما به شکلِ حالتِ کوانتومی است. (البته می‌دانیم که هر حالتِ کلاسیکی لزوماً یک حالتِ کوانتومی نیز هست)
- گره‌های خروجی: مشابهِ حالتِ قبل اما به شکلِ حالتِ کوانتومی است.
- گره‌های گیت‌های کوانتومی: مشابهِ حالتِ قبل اما ذکرِ این نکته لازم است که گیت‌های پایه در مدارهای کوانتومی، نمی‌توانند شاملِ AND و OR باشند چرا که این گیت‌ها باید فضای مبدأ و مقصد

[۶] کلاس‌های **P** ، **NP** و **BPP** هیچ‌گاه به این شکل تعریف نمی‌شوند. شکلِ اولیهٔ تعریفِ آن‌ها مبتنی بر ماشینِ تورینگ است و بعد در طیِ قضیه‌هایی، اثبات می‌شود که به این شکل قابلِ نوشتن هستند.

یکسانی داشته‌باشند (درجهٔ ورودی و خروجی‌شان یکی باشد) و تحولِ متناظر با آن‌ها وارون‌پذیر باشد. در اصل هر گیت باید یک ماتریس یکانی باشد.

- گرهِ اندازه‌گیری: یک اندازه‌گیری در پایهٔ $|۰\rangle$ و $|۱\rangle$ انجام می‌شود که طبیعتاً درجهٔ ورودیِ آن یک و درجهٔ خروجیِ آن نیز یک است.

یکی از مشهورترین مجموعهٔ گیت‌های پایه مجموعهٔ گیتِ H از مثالِ ۲-۳ و همچنین T و CNOT است که به شکلِ زیر تعریف می‌شوند. [۶]

$$T := \begin{pmatrix} ۱ & ۰ \\ ۱ & e^{i\frac{\pi}{۴}} \end{pmatrix} \tag{۲-۴۰}$$

$$\text{CNOT} := |۰\rangle\langle۰| \otimes I + |۱\rangle\langle۱| \otimes \text{NOT} \tag{۲-۴۱}$$

که در این بین، T و H عملگرهای تک‌کیوبیتی هستند اما CNOT یک عملگرِ دوکیوبیتی است.

حالا به شکلِ مشابهی همان توابع برروی مدارهای کوانتومی نیز تعریف می‌شوند و همچنین تعریفِ خانوادهٔ مدار و یکنواختی نیز به همین ترتیب تعمیم داده‌می‌شود.

کلاس‌های محاسباتی کوانتومی

به شکلِ مشابهی، برای مسئله‌ای به شکلِ $f : \{۰,۱\}^* \to \{۰,۱\}$ داریم [۷] که اگر با خانوادهٔ یکنواختی از مدارهای کوانتومی، به نامِ Q قابل محاسبه باشند، به طوری‌که $\text{size}(Q_i) \in \mathcal{O}(poly(i))$ آن‌گاه می‌گوییم که این مسئله عضوِ کلاسِ **EQP** [۸] است.

در ادامه، اگر بگیریم که مدارِ کوانتومی، همواره درست عمل نکند اما با احتمالِ خوبی پاسخِ درست بدهد، یعنی به شکلِ فرمال داشته‌باشیم

$$\Pr(f(x) = Q_i(x)) \geqslant \frac{۲}{۳} \tag{۲-۴۲}$$

[۷] می‌دانیم که مدارهای کوانتومی، فضای مبدا و مقصدِ یکسانی دارند، از این رو، پیاده‌سازیِ تابعی به شکلِ فوق، می‌تواند به این شکل انجام بگیرد که ورودی به شکلِ کوانتومی داده می‌شود و پس از انجامِ یک عملیاتِ یکانی، برروی یک کیوبیتِ خاص، اندازه‌گیری رخ می‌دهد و حاصلِ اندازه‌گیری به عنوانِ خروجیِ سیستم لحاظ می‌شود.

[۸] exact quantum polynomial

آنگاه می‌گوییم که مسئله در کلاسِ **BQP** قرار دارد.

در این‌جا بدونِ اثبات، چند گزاره درخصوصِ کلاس‌های محاسباتیِ گفته‌شده را بررسی می‌کنیم. [۷] [۸]

$$\mathbf{P} \subseteq \mathbf{EQP} \subseteq \mathbf{BQP} \tag{۴۳-۲}$$

$$\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \tag{۴۴-۲}$$

$$\mathbf{NP} \not\subset \mathbf{BQP} \tag{۴۵-۲}$$

$$\mathbf{NP} \not\supset \mathbf{BQP} \tag{۴۶-۲}$$

۲-۲-۲ الگوریتم‌های پایه‌ای در رایانش کوانتومی

برای بررسیِ الگوریتم‌های کوانتومی، نیاز به شیوه‌ای برای بیانِ آن‌ها داریم، هرچند تلاش‌های بسیاری برای طراحیِ زبان‌ها و حساب‌ها برای رایانشِ کوانتومی صورت گرفته، اما برای حفظِ یک‌پارچگی با شیوهٔ بیانِ الگوریتم‌های کوانتومی، از شیوه‌های نموداری، نظیرِ شکلِ مدارِ کوانتومی و حسابِ ZX استفاده نمی‌کنیم. [۵] [۹] [۱۰] ذکرِ این نکته هم لازم است که روش‌های شکلی تعمیم‌پذیر نیستند. از طرفی زبان‌های کوانتومی اغلب ساختارِ مشترکی در خصوصِ ساختارداده‌ها و عملیات‌های کوانتومی دارند اما از نظرِ عملیات‌های کلاسیک، تفاوت‌های بسیاری دارند. از این‌رو برای تشریحِ الگوریتم‌های کوانتومی از شبه‌کد کمک خواهیم گرفت. هرچند ساختارِ این شبه‌کد کاملاً گویاست اما برای حفظِ صحت و دقت، در پیوست آن را از نظرِ نحوی و معنایی بررسی می‌کنیم.

ذکرِ این نکته لازم است که الگوریتم‌های کوانتومیِ گسترده‌ای برای کاربردهای متنوعی وجود دارند [۱۱] [۱۲] [۱۳] اما در این مقال، تمرکز برروی الگوریتم‌های پایه‌ای خواهندبود که به زعمِ نویسنده می‌توانند کاربردی در مسائلِ هندسهٔ محاسباتی داشته‌باشند.

الگوریتمِ دویچ–جوزا

اگر جعبه‌سیاهی داشته‌باشیم که مدارِ تابعِ $o : \mathbb{Z}_2^n \to \mathbb{Z}_2$ باشد و برای این تابع داشته‌باشیم که حتماً یکی از حالت‌های زیر برقرار است

- تابع ثابت است.
- تابع متوازن است به این معنی که به ازای نیمی از ورودی‌ها $o(x) = ۱$ و برای نیمی دیگر $o(x) = ۰$

حالا مسئله این است که تشخیص بدهیم تابعِ o در کدام‌یک از دسته‌های فوق می‌افتد.

با استفاده از هر مدلِ کلاسیکی، نظیرِ خانوادهٔ مدارها، قابلِ تصور است که برای جوابِ قطعی، نیاز به حداقل $۲^{n-۱} + ۱$ بار استفاده از جعبه‌سیاهِ مذکور داریم.

اما به شکلِ کوانتومی، اگر فرض کنیم که همین مدارِ تابعِ o را داریم و برای این‌که این مدار، خواصِ یک مدارِ کوانتومی (وارون‌پذیری و یکی‌بودنِ فضای مبدأ و مقصد) را داشته‌باشیم، تحولِ یکانیِ O را به شکلِ زیر تعریف کنیم

$$O = \sum_{x \in \mathbb{Z}_۲^n, y \in \mathbb{Z}_۲} |x, y \,\mathrm{XOR}\, o(x)\rangle\langle x, y| \qquad (۴۷-۲)$$

این تعمیم برروی $n + ۱$ کیوبیت تعریف شده‌است که n کیوبیتِ اول، نقشِ ورودیِ o را دارند و کیوبیتِ آخر، محلِ ذخیرهٔ خروجیِ o است.

حالا شبهِ‌کدی مانندِ ۱ را درنظر بگیرید.

الگوریتم ۱ دویچ–جوزا

```
H : 1 qubit gate = 1/2 * [1,  1;
                          1, -1]
function IsConstant(O: n+1 qubit gate)
    // Qubits:
    x : n qubit state
    y : 1 qubit state

    // Algorithm:
    // stage 1, initialization
    for i : integer from 1 to n
        Initiate x[i] to |0>
    Initiate y to |1>

    // stage 2, parallization
    for i : integer from 1 to n
        Apply H on x[i]

    Apply H on y

    // stage 3, query
    Apply O on x, y

    // stage 4, interfere (fourier transform)
    for i : integer from 1 to n
        Apply H on x[i]

    // stage 5, measurement
    is_constant : boolean = true
    for i from 1 to n
        result : boolean = Measure on x[i]
        if (result)
            is_constant = false

    return is_constant
```

برای تحلیلِ دقیقِ این الگوریتم، حالتِ کیوبیت‌ها را در پایانِ هر مرحله بررسی می‌کنیم

$$|\psi_۱\rangle = |۰^n\rangle_x |۱\rangle_y \tag{۴۸-۲}$$

سپس با انجام شدنِ عملگرِ H برروی تک‌تکِ گیت‌ها، خواهیم داشت

$$|\psi_۲\rangle = \frac{۱}{\sqrt{۲^{n+۱}}} \sum_{i=۰}^{۲^n-۱} |i\rangle_x (|۰\rangle_y - |۱\rangle_y) \tag{۴۹-۲}$$

$$|\psi_۳\rangle = \frac{۱}{\sqrt{۲^{n+۱}}} \sum_{i=۰}^{۲^n-۱} |i\rangle_x \left(|o(i)\rangle_y - |\mathrm{NOT}\, o(i)\rangle_y\right) \tag{۲-۵۰}$$

$$= \frac{۱}{\sqrt{۲^{n+۱}}} \sum_{i=۰}^{۲^n-۱} \left(|۰\rangle_y - |۱\rangle_y\right) \tag{۲-۵۱}$$

حالا با اعمالِ دوبارهٔ Hها برروی xها، می‌دانیم که حالتِ y تغییری نخواهد کرد.

$$|\psi_۴\rangle = (H_x^{\otimes n} \frac{۱}{\sqrt{۲^{n+۱}}} \sum_{i=۰}^{۲^n-۱} (-۱)^{o(i)} |i\rangle_x) \otimes (|۰\rangle_y - |۱\rangle_y) \tag{۲-۵۲}$$

با اضافه کردنِ این نکته که درصورتی پاسخ `is_constant` برابر با درست است که تمامِ بیت‌های خروجیِ x برابر با صفر باشند، یعنی

$$\Pr(\texttt{is\_constant}) = \|\langle ۰^n|_x |\psi_۴\rangle\|^۲ \tag{۲-۵۳}$$

$$= \left| \langle ۰^n| H_x^{\otimes n} \frac{۱}{\sqrt{۲^n}} \sum_{i=۰}^{۲^n-۱} (-۱)^{o(i)} |i\rangle_x \right|^۲ \tag{۲-۵۴}$$

$$= \frac{۱}{۲^n} \left| (\frac{۱}{\sqrt{۲^n}} \sum_{i=۰}^{۲^n-۱} \langle i|)(\sum_{i=۰}^{۲^n-۱} (-۱)^{o(i)} |i\rangle) \right|^۲ \tag{۲-۵۵}$$

$$= \frac{۱}{۲^{۲n}} \left| \sum_{i=۰}^{۲^n-۱} (-۱)^{o(i)} \right|^۲ \tag{۲-۵۶}$$

تنها نکتهٔ ریاضیاتیِ استفاده‌شده در این اثبات این است که عملگرهای H می‌توانند از نظرِ ریاضی برروی بردارِ ترانهاده/مزدوج $\langle ۰^n|$ که در سمتِ راستشان قرار گرفته‌است اثر کنند.

در نتیجه می‌بینیم که برای حالتی که o مقدارِ ثابتی دارد، این احتمال برابر با یک و برای حالتِ متوازن این احتمال دقیقاً برابر با صفر است.

پس این الگوریتم که تنها یک‌بار از جعبه‌سیاهِ مذکور استفاده می‌کند، می‌تواند به شکلِ قطعی به مسئله پاسخ بدهد. [۱۴]

برای تشریحِ بیشترِ آن‌چه که باعثِ این افزایشِ سرعت شد، می‌توان به این نکته اشاره کرد که همزمانیِ بررسیِ همهٔ حالت‌ها، در کنارِ ابزاری که عملکردی مشابهِ تبدیلِ فوریه دارد (تبدیلِ هادامارد) که در فضای کوانتومی به سرعت پیاده‌سازی می‌شود، امکانِ این نتیجه‌گیریِ سریع را فراهم آورده‌است. اما به طورِ کلی، در این الگوریتم و الگوریتم‌های بعدی، آن‌چه عمومیت دارد، ساختاری شبیه به سیستمِ احتمالاتی‌ست با این تفاوت که احتمالاتِ منفی‌ای دارد که با هم می‌توانند تداخلِ سازنده یا مخرب داشته‌باشند.

الگوریتم زیرگروهِ آبلیِ پنهان و کاربردهای آن

می‌دانیم که گروهِ محدود، به یک مجموعهٔ محدود، مانندِ G و یک تابع که آن را ضربِ گروه می‌نامیم و به شکلِ $\cdot : G \times G \to G$ تعریف می‌شود می‌گوییم که خواصِ زیر را دارا باشد

- شرکت‌پذیری: برای هر $a, b, c \in G$ داشته‌باشیم $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- عنصرِ همانی: وجود داشته‌باشد $I \in G$ که برای هر $g \in G$ داشته‌باشیم $g \cdot I = I \cdot g = ۱$
- عنصرِ وارون: برای هر عنصری نظیرِ $g \in G$ داشته‌باشیم $g^{-۱} \in G$ که $g \cdot g^{-۱} = g^{-۱} \cdot g = I$
- جابه‌جایی (تنها در گروه‌های آبلی): برای هر $a, b \in G$ داشته‌باشیم $a \cdot b = b \cdot a$

همچنین زیرگروه، گروهی‌ست که زیرمجموعهٔ گروهی بزرگ‌تر با همان ضرب است و هم‌دستهٔ یک زیرگروه مانندِ H به مجموعه‌هایی می‌گویند که برای هر $g \in G$ به شکلِ زیر تعریف می‌شوند

$$gH = \{gh | h \in H\} \qquad (۵۷-۲)$$

و مولدهای گروه، به کمینه عناصری می‌گویند که از بسترِ ضربِ آن‌ها در خود، همهٔ عناصرِ گروه به دست می‌آیند.

اگر گروهی محدود و آبلی به نامِ G داشته‌باشیم و تابعی به شکلِ $f : G \to S$ نیز داده‌شده‌است که S یک مجموعهٔ دلخواه است. اگر زیرگروهی به نامِ H وجود داشته‌باشد که برای f داشته‌باشیم که

$$f(x) = f(y) \Leftrightarrow x \text{ و } y \text{ در یک هم‌دستهٔ زیرگروه } H \text{ قرار دارند} \Leftrightarrow xH = yH \qquad (۵۸-۲)$$

آنگاه مسئله یافتنِ H (به معنای یافتنِ مولدهای آن گروه) است.

پیش از بررسیِ دقیقِ الگوریتم، به بررسیِ تعمیمِ تبدیلِ فوریه در فضای گروه‌های آبلیِ محدود می‌پردازیم. بدونِ اشاره به تئوریِ بازنماییِ گروه‌ها، مجموعهٔ توابعِ $G \to \mathbb{C}$ را در نظر بگیرید، این توابع تشکیلِ یک فضای برداری را می‌دهند، یک پایهٔ بدیهی برای این فضا، توابعِ زیر هستند

$$\delta_g(x) = \begin{cases} ۱ & g = x \\ ۰ & g \neq x \end{cases} \qquad (۵۹-۲)$$

بدونِ اثبات بپذیریم که یک پایهٔ نابدیهی برای این فضا، مجموعهٔ توابعی هستند که خواصِ زیر را دارند [؟]

$$|\chi_k(x)| = ۱ \tag{۶۰-۲}$$

$$\chi_k(I) = ۱ \tag{۶۱-۲}$$

$$\chi_k(x \cdot y) = \chi_k(x) \cdot \chi_k(y) \tag{۶۲-۲}$$

که این اعدادِ k را نیز می‌توان با عناصرِ گروه جایگزین کرد اگر یک سریِ کمینهٔ مولد برای G درنظر بگیریم و آن را $\text{gen}(G)$ بنامیم

$$\chi_I(x) = ۱ \tag{۶۳-۲}$$

$$\chi_g(g') = e^{\delta_{gg'} \frac{۲i\pi}{\text{order}(g)}} \quad g, g' \in \text{gen}(G) \text{ اگر} \tag{۶۴-۲}$$

$$\chi_{a\cdot b}(x) = \chi_a(x)\chi_b(x) \tag{۶۵-۲}$$

لازم به ذکر است که مرتبهٔ g کوچک‌ترین عددی‌ست که $g^{\text{order}(g)} = ۱$ یا به عبارتی دیگر

$$\text{order}(g) = |\{g^z | z \in \mathbb{Z}\}| \tag{۶۶-۲}$$

آن‌چه گفته‌شد، تعریفِ دو پایه برای مجموعهٔ توابعِ $G \to \mathbb{C}$ بود که همین دو پایه برای فضای حالت‌های کوانتومیِ سیستمی که حالت‌های کلاسیکِ آن همان عناصرِ G است نیز برقرار است.

از این رو، می‌توان یک تحولِ یکانی در این فضا تعریف کرد که این تغییرِ پایه را صورت می‌دهد

$$\text{QFT} := \frac{۱}{\sqrt{|G|}} \sum_{a,b} \chi_a(b) \, |b\rangle\langle a| \tag{۶۷-۲}$$

که این تعریف را تبدیلِ فوریهٔ کوانتومی می‌گیریم. لازم به ذکر است که به ازای گروهی خاص، $(\mathbb{Z}_۲)$ برابر با تبدیلِ هادامارد خواهد بود.

الگوریتمِ زیر را در نظر بگیرید

الگوریتم ۲ زیرگروهِ پنهان

```
function SampleFromHperp(G : Group, f: Hilbert(G × S) gate) {
    qft : Hilbert(G) gate = QFT of G, defined above

    x : Hilbert(G) state
    y : Hiblert(S) state

    // stage 1, initialization and applying oracle
    Initiate x to |I>
    Apply qft on x
    // or any other way to make x = sum |g>
    Initiate y to |0>

    Apply f on x, y

    // stage 2, collapsing into a constant set
    Measure on y

    // stage 3, applying QFT to extract generators
    Apply qft on x

    // stage 4, select a generator
    Measure on x

}
```

در مرحلهٔ اول، ابتدا تلاش می‌شود که حالتی به شکل $\frac{۱}{\sqrt{|G|}}\sum_{g\in G}|g\rangle_x$ تولید شود که برحسبِ شکلِ ذخیره‌سازی و ساختارِ گروه، به شکل‌های متفاوتی می‌توان این کار را انجام داد، اما آن‌چه با همین ابزار قابلِ پیاده‌سازی‌ست، استفاده از تبدیلِ فوریه برروی عنصرِ همانی‌ست که این حالت را تولید می‌کند. سپس با اعمال f که تبدیل به عملیاتی یکانی شده، به حالتی به شکلِ زیر خواهیم رسید

$$|\psi_۱\rangle = \frac{۱}{\sqrt{|G|}}\sum_{g\in G}|g\rangle_x|f(g)\rangle_y \qquad (۶۸-۲)$$

سپس با اندازه‌گیری در فضای دوم، به برهم‌نهی از حالاتی می‌رسیم که مقدارِ $f(g)$ برای آن‌ها برابر بوده، یعنی یک هم‌دستهٔ H

$$|\psi_۲\rangle = \frac{۱}{\sqrt{|H|}}\sum_{h\in H}|sh\rangle_x|f(s)\rangle_y \qquad (۶۹-۲)$$

و پس از آن با اعمالِ تبدیلِ فوریهٔ مذکور، خواهیم داشت

$$|\psi_۳\rangle = \frac{۱}{\sqrt{|H||G|}} \sum_{h\in H}\sum_{g\in G} \chi_{s\cdot h}(g)\,|g\rangle_x\,|f(s)\rangle_y \tag{۷۰-۲}$$

به سادگی می‌توان اثبات کرد که

$$\sum_{k=۰}^{\text{order}(g)-۱} \chi_{g^k}(x) = \begin{cases} \text{order}(g) & \chi_g(x) = ۱ \\ ۰ & \chi_g(x) \neq ۱ \end{cases} \tag{۷۱-۲}$$

و همین تعمیم برای جمع برروی زیرگروه نیز وجود دارد که با استفاده از آن، می‌توان نوشت

$$|\psi_۳\rangle = \frac{۱}{\sqrt{|H||G|}} \sum_{g\in G}\chi_s(g) \sum_{h\in H}\chi_h(g)\,|g\rangle_x\,|f(s)\rangle_y \tag{۷۲-۲}$$

$$= \frac{\sqrt{|H|}}{\sqrt{|G|}} \sum_{g\in H^\perp} \chi_s(g)\,|g\rangle_x\,|f(s)\rangle_y \tag{۷۳-۲}$$

که در رابطهٔ فوق $H^\perp$ باید به شکلِ زیر تعریف شود

$$H^\perp := \{g \mid \chi_h(g) = ۱\ \forall h \in H\} \tag{۷۴-۲}$$

نتیجهٔ اندازه‌گیریِ آخر، همان نمونه‌گیری از گروهِ $H^\perp$ است و با دانستنِ این گروه، خودِ گروهِ H نیز دانسته می‌شود.[۱۵] [۹]

در ادامه، در یک مثالِ کاربردی، به یافتنِ دورهٔ تناوبِ یک تابع می‌پردازیم که خود در تجزیهٔ اعداد استفاده می‌شود. [۱۰]

مثال ۲-۶ (محاسبهٔ دورهٔ تناوب) *فرض کنید گروهِ اصلیِ مسئله $\mathbb{Z}_Q$ (با عملِ جمع) باشد، آن‌گاه تابعِ f را به شکلِ زیر تعریف کنیم*

$$f(x) = a^x \mod N \tag{۷۶-۲}$$

[۹] شیوهٔ یافتنِ مولدهای H با استفاده از $H^\perp$ در حالتِ کلی خارج از این مقال است

[۱۰] ارتباطِ مثالِ مذکور با تجزیهٔ عددِ N نیز به این صورت است که با دانستنِ r اگر r زوج باشد، آن‌گاه معادلهٔ زیر می‌تواند منتج به تجزیهٔ عدد شود.

$$(a^{\frac{r}{۲}}+۱)(a^{\frac{r}{۲}}-۱) \mod N = ۰ \tag{۷۵-۲}$$

که طبیعتاً اعدادِ a و N دانسته‌شده هستند به طوری‌که $\gcd(a,N)=۱$

حالا زیرگروهی که این تابع برروی آن ثابت است $\{۰,r,۲r,\dots Q-r\}$ است اگر Q/r عددِ صحیحی باشد.

اگر الگوریتمِ مذکور برروی این مسئله اجرا شود، می‌دانیم که برای گروهِ گفته‌شده

$$\chi_a(b)=e^{۲i\pi\frac{ab}{Q}} \tag{۲-۷۷}$$

که در نتیجهٔ آن، برای هر حاصلِ اندازه‌گیری مانندِ m خواهیم‌داشت

$$\chi_r(m)=۱\Rightarrow mr=kQ \tag{۲-۷۸}$$

که در آن k عددی نامعلوم اما صحیح است و اگر چندبار m را اندازه بگیریم، مسئلهٔ به دست آوردنِ r به مسئلهٔ باقی‌ماندهٔ چینی تبدیل می‌شود و قابلِ حل است.

تنها نکتهٔ باقی‌مانده این ضمانت است که $\frac{Q}{r}$ صحیح است که نشان داده‌شده حتی درصورتِ صحیح نبودنِ این نسبت، با قیدهایی، این الگوریتم با احتمالِ خوبی همچنان به‌درستی عمل می‌کند. [۱۶]

الگوریتم‌های جست‌وجو، شمارش و تقویت

یک تابع به شکلِ $D\to\mathbb{Z}_۲$ داده‌شده است که از مجموعهٔ محدودِ D به اعدادِ صفر و یک می‌رود. مسئله، پیدا کردنِ عنصر/عنصرهایی از D هستند که به ازای آن‌ها $f(s)=۱$. این مقادیر را مجموعهٔ $T:=\{s|f(s)=۱\}$ می‌نامیم و این مسئله را جست‌وجوی نامرتب نیز می‌توان نامید.

حالا در فضای هیلبرتی که پایه‌هایش اعضای D هستند می‌توانیم برداری به شکلِ زیر تعریف کنیم

$$|D\rangle=\frac{۱}{\sqrt{|D|}}\sum_{e\in D}|e\rangle \tag{۲-۷۹}$$

و همچنین یک عملگر و یک بردار به شکلِ زیر تعریف می‌کنیم به این منظور اگر تعریف کنیم این یک عملگرِ خطی در فضای x باشد

$$\mathbb{P}_T:=\sum_{x\in T}|x\rangle\langle x| \tag{۲-۸۰}$$

$$|T\rangle := \frac{۱}{\sqrt{|T|}} \sum_{x \in T} |x\rangle \tag{۸۱-۲}$$

که واضح است که $\mathbb{P}_{\mathbb{T}} \neq |T\rangle\langle T|$.

اگر فرض بگیریم مداری (تنها متشکل از گیت‌های پایه و بدونِ اندازه‌گیری) به نامِ G داریم که عملیاتِ زیر را انجام می‌دهد، و طبیعتاً می‌توان انتظار داشت که وارونِ این مدار را نیز داشته‌باشیم

$$|D\rangle = G\,|e_۱\rangle \tag{۸۲-۲}$$

که $e_۱$ یک عنصرِ دلخواه و مشخص از مجموعهٔ D باشد،

فرض می‌کنیم که f را نیز مشابهِ الگوریتم‌های قبل به شکلِ زیر داشته‌باشیم

$$F = \sum_{x \in D, y \in \mathbb{Z}_۲} |x, y \,\mathrm{XOR}\, f(x)\rangle\langle x, y| \tag{۸۳-۲}$$

همچنین عجیب نیست که به هرشکلی که برای مجموعهٔ D فضای هیلبرتی ساخته‌شود (برای مثال اگر در $\lceil \log_۲ |D| \rceil$ کیوبیت کد شود)، به سادگی می‌توان تابعِ $\delta_{e_۱}(x)$ را به شکلِ کوانتومی نیز پیاده کرد که عملگری یکانی در فضای $\mathrm{Hilbert}(D \times \mathbb{Z}_۲)$ به شکلِ زیر خواهدشد

$$\Delta_{e_۱} = \sum_{x \in D, y \in \mathbb{Z}_۲} |x, y \,\mathrm{XOR}\, \delta_{e_۱}(x)\rangle\langle x, y| \tag{۸۴-۲}$$

$$= \sum_{x \in D - \{e_۱\}, y \in \mathbb{Z}_۲} |x, y\rangle\langle x, y| + \sum_{y \in \mathbb{Z}_۲} |e_۱, \mathrm{NOT}\, y\rangle\langle e_۱, y| \tag{۸۵-۲}$$

حالا الگوریتمِ زیر را در نظر بگیرید

الگوریتم ۳ جست‌وجو

```
function SearchAndSample(G: Hilbert(D) gate,
                         Delta_e_1: Hilbert(D × boolean) gate,
                         F: Hilbert(D × boolean) gate) {

    Delta_prime_e_1 = Delta_e_1 then (I, Z) then Delta_e_1
    F_prime = F then (I, Z) then F

    mirrorD: Hilbert(D × boolean) gate = (inverse(G), I) then Delta_prime_e_1
        then (G, I)
    mirrorT: Hilbert(D × boolean) gate = F_prime

    x : Hilbert(D) state
    y : qubit state

    Initiate x to |e_1>
    Initiate y to |0>

    Apply G on x

    for i : integer from 1 to ceil(pi * sqrt(size(D)) / 4) {
        Apply mirrorT on x, y
        Apply mirrorD on x, y
    }

    result: D = Measure on x
    return result
}
```

در مرحلهٔ اول، می‌توان با انجامِ عملیاتِ زیر، این جعبه‌سیاه را به شکلِ دیگری تبدیل کرد

$$F' = F(I_x \otimes Z_y)F = \sum_{x\in D, y\in\mathbb{Z}_2} (-1)^{y \operatorname{XOR} f(x)} |x,y\rangle\langle x,y| \tag{۸۶-۲}$$

که در آن Z عملگری به شکلِ زیر است که برروی کیوبیتِ خروجیِ تابع اثر می‌کند

$$Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{۸۷-۲}$$

و به همین شکل برای $\Delta'_{e_1} = \Delta_{e_1}(I_x \otimes Z_y)\Delta_{e_1}$

$$\Delta'_{e_1} = \sum_{x\in D, y\in\mathbb{Z}_2} (-1)^{y \operatorname{XOR} \delta_{e_1}(x)} |x,y\rangle\langle x,y| \tag{۸۸-۲}$$

نکتهٔ قابلِ توجه این است که مقدارِ y در طیِ همهٔ این عملیات‌های F' و Δ'_{e_1} و همچنین $G\otimes I$ تغییر نمی‌کند، از این رو می‌توان فقط به تأثیرِ این عملگرها روی فضای x توجه کرد.

پس می‌توانیم بنویسیم

$$\langle ۰|_y \,\mathrm{mirrorT}\, |۰\rangle_y = \langle ۰|_y \, F' \, |۰\rangle_y \tag{۸۹-۲}$$

$$= \sum_{e\in D} (-۱)^{f(e)} \, |e\rangle\langle e|_x \tag{۹۰-۲}$$

$$= I - ۲\mathbb{P}_T \tag{۹۱-۲}$$

$$\langle ۰|_y \,\mathrm{mirrorS}\, |۰\rangle_y = \langle ۰|_y \, (G\otimes I)^{-۱} \Delta'_{e_۱} (G\otimes I) \, |۰\rangle_y \tag{۹۲-۲}$$

$$= G^{-۱}(I - ۲\,|e_۱\rangle\langle e_۱|)G \tag{۹۳-۲}$$

$$= I - ۲\,|D\rangle\langle D| \tag{۹۴-۲}$$

حالا تنها چیزی‌که باقی می‌ماند این است که تحولِ این بردار را بررسی کنیم

$$\begin{cases} |\psi_۰\rangle = |D\rangle \\ |\psi_{k+۱}\rangle = (I - ۲\,|D\rangle\langle D|)(I - ۲\mathbb{P}_T)\,|\psi_k\rangle \end{cases} \tag{۹۵-۲}$$

که آن‌گاه اگر تحول را در زیرفضای T و زیرفضای عمود بر آن بررسی کنیم

$$|\psi_k\rangle = \alpha_k \, |D-T\rangle + \beta_k \, |T\rangle \tag{۹۶-۲}$$

که

$$|D-T\rangle = \frac{۱}{\sqrt{|D-T|}}(\sqrt{|D|}\,|D\rangle - \sqrt{|T|}\,|T\rangle) \tag{۹۷-۲}$$

آنگاه

$$\begin{pmatrix} \alpha_{k+۱} \\ \beta_{k+۱} \end{pmatrix} = \left(\begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} - ۲ \begin{pmatrix} \sqrt{\frac{|D-T|}{|D|}} \\ \sqrt{\frac{|T|}{|D|}} \end{pmatrix} \begin{pmatrix} \sqrt{\frac{|D-T|}{|D|}} & \sqrt{\frac{|T|}{|D|}} \end{pmatrix} \right) \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \begin{pmatrix} \alpha_k \\ \beta_k \end{pmatrix} \tag{۹۸-۲}$$

$$= \begin{pmatrix} -\cos(۲\theta) & -\sin(۲\theta) \\ \sin(۲\theta) & -\cos(۲\theta) \end{pmatrix} \begin{pmatrix} \alpha_k \\ \beta_k \end{pmatrix} \qquad | \ \theta = \arcsin\left(\sqrt{\frac{|T|}{|D|}}\right) \tag{۹۹-۲}$$

که با این تبدیل می‌توان نشان داد که پس از طیِ $\frac{\pi}{۴\theta}$ مقدارِ β نزدیک به یک شده که به این ترتیب پس از اندازه‌گیری، احتمالِ دریافتِ یکی از عناصرِ داخلِ T یا همان عبارتِ $\|\mathbb{P}_T|\psi_k\rangle\|^۲$ نزدیک به یک خواهد بود.

این الگوریتم، بیانِ دیگری نیز دارد که اگر برای یک زیرفضا، یک عملگرِ بازتابی مثلِ $\text{mirrorT} = I - ۲\mathbb{P}_T$ داشته‌باشیم و یک حالتِ اولیه به نامِ $|\text{init}\rangle$ که عملگرِ بازتابیِ آن نیز وجود دارد (به بیانِ دیگر این حالت با مداری معلوم قابلِ تهیه است)، آنگاه می‌توان به حالتِ

$$|\text{final}\rangle = \frac{\mathbb{P}_T|\text{init}\rangle}{\|\mathbb{P}_T|\text{init}\rangle\|} \qquad (۱۰۰-۲)$$

نزدیک شد. به این بیان، الگوریتمِ تقویتِ دامنه می‌گویند. [؟]

الگوریتم‌های جبرخطی

احتمالاً حذف شود

الگوریتم‌های ولگشت

احتمالاً حذف شود

۲-۲-۳ شبیه‌سازیِ کلاسیکِ این سیستم‌ها

یکی از مسئله‌هایی که اشاره به آن اهمیت دارد، شبیه‌سازیِ مدارهای کوانتومی برروی سیستم‌های کلاسیک است. در حالتِ کلی شبیه‌سازیِ این مدارها، آن‌چنان که قابلِ حدس است، به شکلِ توانی سخت خواهندبود اما ایده‌های مختلفی وجود دارند که هرکدام در شرایطی خاص نشان می‌دهند که شبیه‌سازیِ چندجمله‌ای امکان‌پذیر است و در آن شرایط، طبیعتاً مدارها نمی‌توانند به برتری‌ای نسبت به کامپیوترهای کلاسیک دست بیابند.

۲-۳ هندسهٔ محاسباتی

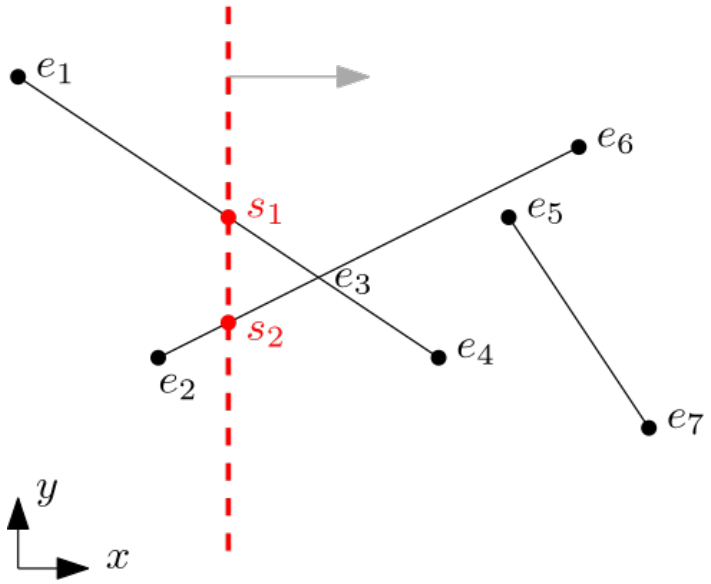
هندسهٔ محاسباتی، شاخه‌ای‌ست که به بررسیِ مسئله‌های هندسی از نظرِ محاسباتی می‌پردازد و طبیعتاً درگیرِ پیچیدگی‌ها و کلاس‌های محاسباتی در کنارِ الگوریتم‌ها و ساختمان‌های داده می‌شود. در این مقال، بیشترِ توجه معطوف به الگوریتم‌ها و ساختمان‌های داده است.

برای مطالعه‌ای مروری بر هندسهٔ محاسباتی، ابتدا چند الگوریتمِ پایه‌ای و پرکاربرد را مرور می‌کنیم.

۲-۳-۱ الگوریتم‌های جاروبِ خطی/صفحه‌ای

این دسته الگوریتم‌ها که مبتنی بر ایدهٔ مشترکی کار می‌کنند کاربردهای گوناگونی از تشخیصِ برخوردِ پاره‌خط‌ها تا تشکیلِ دیاگرامِ ورونی (بحث شده در بخش ۲-۳-۸) دارند. بدونِ درنظر گرفتنِ جزئیات، این الگوریتم با استفاده از یک صفِ رخداد و یک درخت (یا هر داده‌ساختارِ دیگری) به نامِ وضعیت کار می‌کند. به این ترتیب که اگر خطی موازیِ محورِ y در نظر بگیریم که از $x \to -\infty$ به سمتِ $x \to \infty$ حرکت می‌کند، در طیِ این حرکت، همواره داده‌ساختارِ وضعیت را به‌روز نگه می‌دارد، به این ترتیب که نقاطی که ممکن است وضعیت تغییر کند را رخداد می‌نامیم و به محضِ کشف، آن‌ها را در صفِ رخداد قرار می‌دهیم و به ترتیبِ کم‌ترین x از صفِ رویدادها انتخاب می‌کنیم و خط را تا آن‌جا جلو می‌بریم و تغییر وضعیت را اعمال می‌کنیم.

برای مثال، در مسئلهٔ برخوردِ پاره‌خط‌ها (تعریف‌شده در ۳-۱)، وضعیت، یک درختِ دودوییِ متوازن از عرضِ محلِ برخوردِ پاره‌خط‌ها با خطِ جاروب است که در شروع و پایانِ پاره‌خط‌ها و در نقاطِ تلاقی وضعیت تغییر می‌کند. می‌توان نشان داد که این الگوریتم در $\mathcal{O}(N \log N + I \log N)$ برای N پاره‌خط که با هم I نقطهٔ تلاقی دارند عمل می‌کند. ذکرِ این نکته خالی از لطف نیست که در این الگوریتم‌های هندسهٔ محاسباتی، بستگیِ پیچیدگیِ الگوریتم به خروجی را به کرات می‌بینیم. به این دسته از الگوریتم‌ها «حساس‌به‌خروجی» می‌گویند. [۱۷]



شکل ۲-۱: نمایشی از الگوریتمِ جاروبِ خطی برای مسئلهٔ تلاقیِ پاره‌خط‌ها که رخدادها با e_i و داده‌های وضعیت با s_i مشخص شده‌اند.

۲-۳-۲ الگوریتم‌های برنامه‌ریزیِ خطی

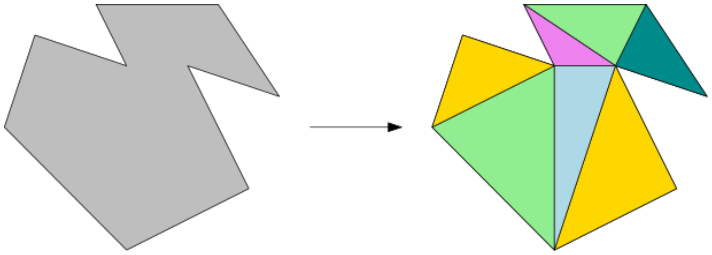
طبیعی‌ست که به دلیلِ وجودِ خط‌های راست در مسائلِ هندسی، بسیاری از مسائل به شکلِ برنامه‌ریزی‌های خطی یا برنامه‌ریزی‌های خطیِ تعمیم‌یافته خواهندبود. برای مثال، هر پاره‌خط نظیرِ یک سه قیدِ خطی‌ست و به سادگی می‌توان متصور شد که مسئلهٔ وجودِ تلاقیِ پاره‌خط‌ها (تعریف‌شده در ۳-۱) یا اشیاءِ محدب به سادگی قابلِ تعبیر به مسئلهٔ امکان‌پذیریِ قیودِ برنامه‌ریزیِ خطی باشد. مثالِ دیگری از این دست مسئلهٔ کوچک‌ترین توپِ شامل (تعریف‌شده در ۳-۱) است که به شکلِ برنامه‌ریزیِ خطیِ تعمیم‌یافته قابلِ بیان است. [۱۷]

۲-۳-۳ مسئلهٔ پوشِ محدب

احتمالاً حذف شود.

۲-۳-۴ مسئلهٔ مثلث‌بندی

مسئلهٔ مثلث‌بندی: یک Nـ ضلعی در صفحه با نقاطِ p_1 تا p_N مشخص شده‌اند، مطلوب است لیستی از مثلث‌های t_1 تا t_{N-2} به طوری‌که نقطه‌های مثلث‌ها همان نقاطِ چندضلعی باشند و مثلث‌ها بدونِ اشتراک و هم‌پوشانی همهٔ چندضلعی را بپوشانند.



شکل ۲-۲: یک مثال از مسئلهٔ مثلث‌بندی و پاسخِ آن

جوابِ این مسئله یکتا نیست و هرچندضلعی ممکن است به شیوه‌های گوناگونی مثلث‌بندی شود. از این رو مسائلی سخت‌تر از مثلث‌بندی وجود دارند که جوابِ مشخصی دارند، نظیرِ مثلث‌بندی‌ای که مجموعِ طولِ اضلاعِ مثلث‌ها کمینه شود که آن‌را مثلث‌بندیِ کمینه‌وزن می‌نامند. [۱۸]

یک الگوریتم برای این مسئله، تقسیمِ چندضلعی به چندضلعی‌های یکنوا و پس از آن مثلث‌بندی‌ست که پیچیدگیِ زمانیِ $\mathcal{O}(N \log N)$ خواهدداشت.

مسئلهٔ مثلث‌بندی به عنوانِ یک پیش‌پردازشِ کاربردی برای حلِ مسئلهٔ وجودِ نقطه در چندضلعی (تعریف شده در ؟؟) یا دیگر مسائلِ برخورد نظیرِ دنبال کردنِ پرتو استفاده می‌شود و از این‌رو اهمیتِ فراوانی در هندسهٔ محاسباتی و گرافیکِ کامپیوتری دارد. [۱۷]

۲-۳-۵ ساختمانِ دادهٔ لیستِ یال‌های دوسویه متصل

این داده‌ساختار را می‌توان ساده‌ترین و مهم‌ترین داده‌ساختار در ذخیره‌سازیِ اشکالِ هندسی در صفحه دانست. این داده‌ساختار برای افرازهای صفحه استفاده کرد.

این افرازِ صفحه را می‌توان به شکلِ یک گرافِ مسطح دید که برروی آن گره‌ها، یال‌ها و ناحیه‌ها همان نقاط، پاره‌خط‌ها و چندضلعی‌ها هستند که افرازهای صفحه را تشکیل می‌دهند. این گراف غیرجهت‌دار خواهدبود اما می‌توانیم هر یالِ آن را با دو یالِ جهت‌دار که در جهتِ عکسِ یکدیگر قرار گرفته‌اند جایگزین

کنیم و به هر یالِ این گرافِ جدید «نیم‌یال» می‌گوییم. دلیلِ این تعریف آن است که آن‌گاه ناحیهٔ چپِ هر نیم‌یال را می‌توانیم به شکلِ دقیقی تعریف کنیم.

این داده‌ساختار متشکل از سه لیست است:

۱. لیستی از نقاط که برای هر نقطه توابعِ زیر تعریف شده‌اند

- تابعِ $\text{Coordinates}(v)$ که مختصاتِ نقطهٔ v را بازمی‌گرداند.
- تابعِ $\text{IncidentEdge}(v)$ که نیم‌یالی دلخواه را بازمی‌گرداند که نقطهٔ شروعش v باشد.

۲. لیستی از نیم‌یال‌ها که برای هر نیم‌یال توابعِ زیر تعریف شده‌اند

- تابعِ $\text{Origin}(e)$ که نقطهٔ شروعِ نیمی‌یال را مشخص می‌کند.
- تابعِ $\text{Twin}(e)$ که نیم‌یالی را بازمی‌گرداند که دقیقاً برعکسِ eست.
- تابعِ $\text{IncidentFace}(e)$ ناحیه‌ای که در چپِ نیم‌یال قرار گرفته‌است را بازمی‌گرداند.
- تابعِ $\text{Next}(e)$ نیم‌یالی را بازمی‌گرداند که شروعش نقطهٔ پایانِ e باشد و ناحیهٔ سمتِ چپِ این‌دو نیم‌یال با هم یکی باشد.
- تابعِ $\text{Prev}(e)$ نیم‌یالی را بازمی‌گرداند که پایانش نقطهٔ شروعِ e باشد و ناحیهٔ سمتِ چپِ این‌دو نیم‌یال با هم یکی باشد.

۳. لیستی از ناحیه‌ها که برای هر ناحیه توابعِ زیر تعریف شده‌اند

- تابعِ $\text{OuterComponent}(f)$ اگر ناحیه‌ای وجود دارد که این ناحیه را به طورِ کامل دربر گرفته‌است آن را بازمی‌گرداند.
- تابعِ $\text{InnerComponents}(v)$ لیستی از ناحیه‌هایی که به طورِ کامل در این ناحیه قرار گرفته‌اند (و با یکدیگر و با ناحیهٔ بیرونی برخورد ندارند) بازمی‌گرداند.

قابل دریاف

۲-۳-۶ ساختمانِ دادهٔ درختِ کِی‌دی

۲-۳-۷ دوگانگی

۲-۳-۸ پیش‌پردازش‌های کاربردی، مثالِ دیاگرامِ ورونی

فصل ۳

کارهای پیشین

۳-۱ الگوریتم‌های کوانتومی در هندسهٔ محاسباتی

استفاده از ابزارِ رایانشِ کوانتومی در هندسهٔ محاسباتی از بدوِ پیدایشِ این شاخه و توسعهٔ الگوریتم‌های مشهورِ آن، موردِ بررسی قرار گرفته [؟] اما با این‌حال تا امروزه ادبیاتِ کاملاً محدودی وجود دارد که الگوریتم‌ها و حدهایی در آن به صورتِ موردی بررسی شده‌اند. هرچند تعدادِ این حدود و الگوریتم‌ها کم نیست اما هنوز تلاش‌ها در جهتِ تعمیم و کلیت‌بخشی به این گزاره‌ها چندان زیاد نبوده‌اند.

همچنین نکتهٔ مهمی که حائزِ اهمیتِ بیشتری‌ست این است که بیشترِ تلاش‌ها در این حوزه معطوف به استفاده از الگوریتم‌های جست‌وجو، شمارش و یا ولگشت‌های کوانتومی هستند که بهبودِ سرعتِ آن‌ها در نهایت می‌تواند به شکلِ مربعی [۱] باشد. و به نظر می‌رسد هنوز از الگوریتم‌هایی که بهبودِ سرعتِ توانی [۲] دارند در این حوزه استفاده‌ای نشده‌است. [؟][۱۹][۲۰][؟][؟]

در ادامه به بررسیِ الگوریتم‌ها و حدود در تلاش‌های پیشین می‌پردازیم.

از آن‌جا که هدف از این بررسی‌ها، بستگیِ پیچیدگیِ محاسباتی به پارامترهایی نظیرِ بعد و دقتِ ارقام نیست، در مرتبهٔ الگوریتم‌ها و حدها ثابت فرض شده‌اند و نوشته‌نشده‌اند.

مسئلهٔ برخوردِ اجسامِ محدب: در فضای dـ بعدی در نظر بگیرید که N شکلِ محدب داریم، هدف

---

[۱] quadratic

[۲] exponential

فهمیدنِ این است که آیا وجود دارد دوتایی از این اجسام که با هم تلاقی داشته‌باشند. [؟]

- الگوریتمِ کلاسیک:
- حدِ کلاسیک:
- الگوریتمِ کوانتومی:
- حد کوانتومی:

مسئلهٔ پوش محدب

مسئلهٔ چیدمانِ ابرصفحه‌ها[۳]

مسئلهٔ محاسبهٔ فاصلهٔ هاسدورف

مسئلهٔ نزدیک‌ترین زوج: N نقطه در فضای dـبعدی و یک تابعِ فاصله $d : \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}^+$ داده‌شده‌اند، مطلوب است زوجی که کم‌ترین فاصله را دارند. [۲۱، فصل پنجم][۱۹]

- الگوریتمِ کلاسیک: با استفاده از تقسیم و حل، با $\Theta(N \log N)$ مقایسه (بینِ فاصلهٔ زوج‌نقاط) امکانِ حل وجود دارد. البته برای الگوریتم‌های تصادفی، الگوریتم با امیدریاضیِ تعدادِ مقایسه‌ها $\Theta(N)$ ممکن است.
- حدِ کلاسیک: با استفاده از یکتاییِ عناصر، مقایسه‌ها باید از مرتبهٔ $\Omega(N \log N)$ باشند.
- الگوریتمِ کوانتومی: با استفاده از کاهش (با سربارِ لگاریتمی) به الگوریتمِ پیدا کردنِ کمینهٔ کوانتومی، با $\Theta(N^{\frac{2}{3}} \log N)$ پرسشِ مقایسه، مسئله حل می‌شود.
- حد کوانتومی: با استفاده از یکتاییِ عناصر به شکلِ کوانتومی به حدِ $\mathcal{O}(N^{\frac{2}{3}})$ خواهیم رسید.

مسئلهٔ دورترین زوج: N نقطه در فضای dـبعدی و یک تابعِ فاصله $d : \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}^+$ داده‌شده‌اند، مطلوب است زوجی که بیشترین فاصله را دارند.

نتایجِ آن مشابهِ مسئلهٔ نزدیک‌ترین زوج هستند.[۱۹]

[۳] arrangement of hyperplanes

مسئلهٔ نزدیک‌ترین زوجِ دورنگ: N نقطهٔ آبی و M نقطهٔ قرمز و یک تابعِ فاصله $d : \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}^+$ داده‌شده‌اند، مطلوب است زوجِ ناهم‌رنگی که کم‌ترین فاصله را دارند. [۱۹][۲۲، Minimum Geometric Spanning Trees]

- الگوریتمِ کلاسیک: با استفاده از زیردرختِ پوششیِ کمینهٔ هندسی، برای فاصله‌های خاصی نظیرِ L_1 در زمانِ $\mathcal{O}((N+M)\log(N+M))$ امکانِ حل وجود دارد.

  با استفاده از الگوریتم‌های تصادفی نیز در زمانِ $\mathcal{O}((NM\log N\log M)^{\frac{2}{3}} + N\log^2 M + M\log^2 N)$ حل می‌شود.

- حدِ کلاسیک: چون این مسئله از مسئلهٔ نزدیک‌ترین زوج سخت‌تر است حدهای قبلی برقرار هستند.

- الگوریتمِ کوانتومی: به شکلِ تقریباً مشابهی با مسئلهٔ نزدیک‌ترین زوج، با تعداد پرسشِ مقایسه $\mathcal{O}((M+N)^{\frac{2}{3}}\log(M+N))$ حل می‌شود.

- حد کوانتومی: چون این مسئله از مسئلهٔ نزدیک‌ترین زوج سخت‌تر است حدهای قبلی برقرار هستند.

مسئلهٔ کوچک‌ترین توپِ شامل: در فضای dـ بعدی N نقطه داریم، مطلوب است یافتنِ ابرکره‌ای dـ بعدی با کوچک‌ترین شعاعِ ممکن که همهٔ نقاط داخلِ آن قرار بگیرند.[۱۷، فصل چهارم][۱۹]

- الگوریتمِ کلاسیک: در فضای دوبعدی با اضافه‌کردنِ تدریجیِ نقاط، با امیدریاضیِ زمانِ $\Theta(N)$ این مسئله حل می‌شود. این الگوریتم که قابلِ تعمیم به همهٔ مسئله‌های بهینه‌سازیِ LP-type است در ابعادِ بالاتر نیز به‌درستی عمل می‌کند.

- حد کوانتومی: با کاهشِ این مسئله به مسئلهٔ OR حدِ پایینِ $\Omega(\sqrt{N})$ اثبات می‌شود.

مسئلهٔ وجود تلاقیِ پاره‌خط‌ها: در فضای دوبعدی، N پاره‌خط داریم، مطلوب است این‌که وجود دارند دوپاره‌خطی که با هم تلاقی داشته‌باشند.[۱۷، فصل دوم][۱۹]

- الگوریتمِ کلاسیک: با تکنیک‌های نظیرِ جاروبِ خطی (در بخشِ ۲-۳-۱) متعددی می‌توان در زمانِ $\mathcal{O}(N\log N)$ به جوابِ مسئله رسید.

- الگوریتمِ کوانتومی: با کاهشِ مسئله به یکتاییِ عناصرِ کوانتومی که خود با استفاده از ولگشت‌های کوانتومی حل می‌شود، مسئله با استفاده از $\Theta(N^{۲/۳})$ پرسش از موقعیتِ پاره‌خط‌ها حل می‌شود.

مسئلهٔ سه‌نقطه هم‌خط [؟]

۳-۲ مسئلهٔ قرارگیریِ نقطه در چندضلعی

مسئلهٔ قرارگیریِ نقطه در چندضلعی: تصور کنید در یک صفحه، نقطهٔ p را داریم و Nـ ضلعیِ G که به‌ترتیب مشتکل از نقاطِ $q_۰ \dots q_{N-۱}$ است.

اگر بدونِ هیچ پیش‌پردازشی، بخواهیم برای همین یک نقطه، بودن یا نبودن داخلِ چندضلعی را به دست بیاوریم، دو ایدهٔ مشهور وجود دارد. **ایدهٔ نخست** این است که اگر هر نیم‌خطی از این نقطه رسم کنیم، اضلاعِ چندضلعی را در فرد نقطه قطع می‌کند اگر و تنها اگر نقطه درونِ چندضلعی باشد.

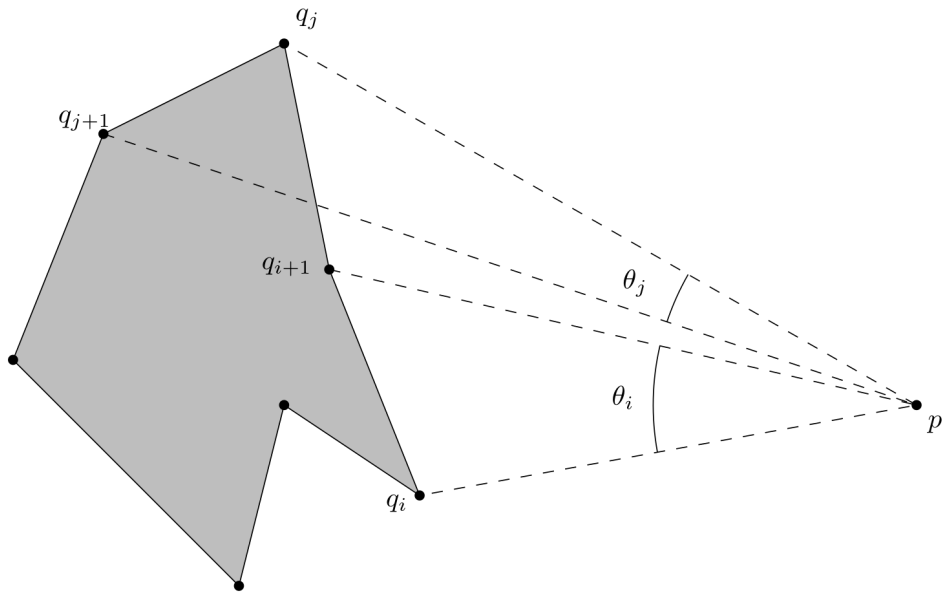
با این ایده می‌توان در مرتبهٔ $\Theta(N)$ مسئلهٔ مذکور را حل کرد.

ایدهٔ دوم به این این ترتیب است که اگر زاویهٔ خطِ $q_i\ q_{i+۱}$ [۴] از دید p را θ_i

در نظر بگیریم، همچنین به آن خط عدد s_i را نسبت دهیم که

$$\begin{cases} s_i = ۰ & \text{اگر } p \text{ در سمتِ راستِ خطِ } q_i\ q_{i+۱} \text{ باشد} \\ s_i = ۱ & \text{اگر } p \text{ در سمتِ چپِ خطِ } q_i\ q_{i+۱} \text{ باشد} \end{cases} \tag{۳-۱}$$

[۴] لازم است برای حالتی که $i = N$ دقتی به خرج بدهیم که اگر جمع را به پیمانهٔ N فرض کرده‌باشیم، تمامِ معادلات برای آن حالت نیز معتبر خواهندبود.



شکل ۳-۱: نمایشِ پارامترهای استفاده شده در الگوریتم

حالا می‌دانیم که مسئلهٔ قرارگیریِ نقطه در چندضلعی به مسئلهٔ قولی [۵] به شکلِ زیر تبدیل می‌شود.

$$\left|\sum \theta_i s_i\right| = \begin{cases} ۲\pi & \text{نقطه داخلِ چندضلعی‌ست} \\ ۰ & \text{نقطه بیرونِ چندضلعی‌ست} \end{cases} \qquad (۲-۳)$$

که به این شکل با این ایده در مرتبهٔ $\Theta(N)$ مسئلهٔ مذکور را حل کرد. البته برخلافِ ایدهٔ قبل، نیاز به محاسبهٔ توابعِ وارون‌مثلثاتی‌ست که این کار، سرعتِ این الگوریتم را در واقعیت نسبت به الگوریتمِ قبلی کاهش می‌دهد و از همین‌رو به این ترتیب استفاده نمی‌شود. اما تصحیحاتی بر این الگوریتم وجود دارد که با استفاده از تقریب‌هایی دقت را کاهش می‌دهد اما امکانِ محاسبهٔ سریع را می‌دهد.[؟]

[۵] promise

فصل ۴

بحث و نتایجِ نو

۴-۱ معرفیِ یک الگوریتمِ کوانتومی

می‌بینیم صورت‌بندیِ ایدهٔ دوم که در فصلِ پیشین مطرح شد، شباهتِ زیادی به مسئلهٔ مربوط به الگوریتمِ دویچ–جوزا دارد، اما وجودِ وزن‌ها، امکانِ استفاده از الگوریتمِ دویچ‌جوزا را به ما نمی‌دهد.

اما می‌دانیم اگر حالتی به شکلِ زیر داشته‌باشیم

$$|\phi_۱\rangle := \frac{۱}{\sqrt{N-۱}} \sum_{q_i q_{i+۱} \in \text{segments}} \kappa \theta_i s_i \, |q_i q_{i+۱}\rangle \tag{۴-۱}$$

که در آن κ یک ضریب برای بهنجارسازی‌ست، آنگاه با استفاده از تبدیلِ فوریه، می‌توانیم به حالتی برسیم که دامنهٔ حالتِ $|۰\rangle$ یا همان عنصرِ همانیِ گروه، در آن به شکلِ زیر باشد

$$\langle ۰ | \, \mathrm{QFT} \, |\psi\rangle = \frac{۱}{N-۱} \sum_{q_i q_{i+۱} \in \text{segments}} \kappa \theta_i s_i \tag{۴-۲}$$

که از آن‌جا که برای هرتبدیلِ فوریه‌ای این مهم برقرار است، می‌توان به جای QFT قرار داد $H^{\otimes \log(N-۱)}$ و فرض بگیریم که $N-۱$ توانی از دو است.

پس برای احتمالِ اندازه‌گیریِ ۰ پس از تبدیلِ فوریه داریم

$$\Pr\Big(\text{اندازه‌گیریِ } ۰\Big) = \Big|\langle ۰ | \, H^{\otimes \log(N-۱)} \, |\psi\rangle\Big|^۲ = \begin{cases} \frac{۴\kappa^۲\pi^۲}{(N-۱)^۲} & \text{نقطه داخلِ چندضلعی‌ست} \\ ۰ & \text{نقطه بیرونِ چندضلعی‌ست} \end{cases} \tag{۴-۳}$$

اما حالا ضریبِ κ مربوط به فرایندِ تولیدِ این حالت است. اگر فرض کنیم ابتدا حالتی بسازیم که

$$|\phi_{۰}\rangle = \frac{۱}{\sqrt{N-۱}} \sum_{q_i q_{i+۱} \in \text{segments}} \theta_i s_i \, |q_i q_{i+۱}\rangle \tag{۴-۴}$$

سپس به سادگی با استفاده اضافه کردنِ کیوبیت، از جعبه‌سیاه‌ها و تعمیمِ مدارهای کلاسیک، می‌توانیم به حالتِ زیر برسیم

$$|\phi_{۰}\rangle = \frac{۱}{\sqrt{N-۱}} \sum_{q_i q_{i+۱} \in \text{segments}} |q_i q_{i+۱}\rangle \, |\arcsin \kappa\theta_i\rangle \, |s_i\rangle \tag{۵-۴}$$

و پس از آن با استفاده از ایده‌هایی مرسوم، نظیرِ ایده‌های استفاده شده در بخشِ ۲-۲-۲ به حالتِ $|\phi_{۱}\rangle$ رسید. [۱]

پس با توجه به نکاتِ گفته‌شده لازم است که $\kappa\theta_i \leqslant ۱$ که نتیجه می‌دهد بدیهی‌ترین انتخاب $\kappa = \frac{۱}{\pi}$ باشد زیرا که زاویهٔ یک پاره‌خط در مقابلِ یک نقطه حداکثر به نیم‌صفحه می‌رسد. در این صورت این احتمال نیز به شکلِ $\mathcal{O}(\frac{۱}{N^{۲}})$ کوچک خواهدبود.

اما اگر قولی وجود داشته‌باشد که $\theta_i \leqslant \frac{\gamma}{N} \in \mathcal{O}(\frac{۱}{N})$ که هم‌ارزِ این قول است که نقاطی که بررسی می‌کنیم به اضلاع بیش‌ازحد نزدیک نباشند و این فاصله از مرتبهٔ طولِ اضلاع باشد، آن‌گاه می‌توان $kappa$ را برابرِ $\frac{N}{\gamma\pi}$ قرار داد که در نتیجه احتمالِ تشخیصِ نقطه درونِ چندضلعی در معادلهٔ ۴-۳ برابر با عددی ثابت خواهدشد که این یعنی با در این حالت تنها با یک پرسش می‌توان با خطای محدود به پاسخِ مسئله رسید.

---

[۱] ایدهٔ تبدیلِ s_i به $(-۱)^{s_i}$ دقیقاً مشابهِ آن‌چیزی‌ست که در بخشِ مذکور بحث شد، همچنین برای قسمتِ θ_i یک فرضِ طبیعی این است که مقدارِ $\arcsin(\kappa\theta_i)$ در چندکیوبیت به شکلِ دودویی ذخیره شده‌است و آن را می‌توان به شکلِ $\overline{r_{۲d} r_{۲d-۱} \dots r_{۲} r_{۱}}$ که یکان و دوگان و الی آخر باشند. سپس، یک گیتِ شناخته‌شده و قابلِ پیاده‌سازی که به طورِ معمول در مدارهای کوانتومی نظیرِ تبدیلِ فوریه برای گروه‌های عددی استفاده می‌شود، گیتِ $\text{C}{-}R_x$ است که عملکردِ آن به شکلِ زیر است

$$\begin{cases} \text{C}{-}R_x \, |۱\rangle \, |۰\rangle = |۱\rangle \, (\cos(x) \, |۰\rangle + \sin(x) \, |۱\rangle) \\ \text{C}{-}R_x \, |۱\rangle \, |۰\rangle = |۰\rangle \, |۰\rangle \end{cases} \tag{۶-۴}$$

حالا با در دست داشتنِ مدارهایی از این جنس، می‌توان حالتِ مذکور را تدارک دید. یک نکتهٔ مهم فرایندِ پاک کردنِ اطلاعات کیوبیت‌های مورداستفاده θ_i و s_i که با استفادهٔ دوباره از جعبه‌سیاه ممکن می‌شود و کیوبیت‌های مذکور به حالتِ صفر و جدا می‌روند و می‌توان آن‌ها را از فرایند حذف کرد.

این الگوریتم را می‌توان به شکلِ زیر بازنویسی کرد

```
function IsPointInPolygonPromised(gamma: Double,
             coordsOfSeg: Hilbert(log(N-1) qubit × D qubit × D qubit) gate)
    index : log(N - 1) qubit state
    coordsStart : D qubit state
    coordsEnd : D qubit state
    arcsinTheta : D qubit state
    side : 1 qubit state

    function ClassicalCircuitForTheta(coordStart, coordEnd) =
        arcsin(norm(coordStart - coordEnd) / norm((coordStart + coordEnd) / 2 -
            P)
             * N / gamma / pi)
    function ClassicalCircuitForS(coordStart, coordEnd) =
        sign(cross(P - (coordStart + coordEnd) / 2, coordEnd - coordStart).z)

    gate EncodedAngleFromP = quantum(ClassicalCircuitForTheta)
    gate SideFromP = quantum(ClassicalCircuitForS)

    // stage 1, initialization
    Initiate coordStart to 0
    Initiate coordEnd to 0
    Initiate arcsinTheta to 0
    Initiate side to 0
    for i : integer from 1 to log(N-1) {
        Initiate index[i] to 0
        Apply H on x[i]
    }

    // stage 2, pplying oracles
    Apply EncodedAngleFromP on coordStart, coordEnd, arcsinTheta
    Apply EncodedAngleFromS on coordStart, coordEnd, side
    // stage 3, Transforming oracle informations
    for i : integer from 1 to D {
        Apply C-R(2^(-i)) on arcsinTheta[i]
    }
    Apply Z on side
    // stage 4, pplying oracles again to remove data
    Apply EncodedAngleFromP on coordStart, coordEnd, arcsinTheta
    Apply EncodedAngleFromS on coordStart, coordEnd, side

    // stage 5, Hadamard transform and measurement
    for i : integer from 1 to log(N-1)
        Apply H on x[i]

    is_in : boolean = true
    for i : integer from 1 to log(N-1)
        result : boolean = Measure on x[i]
        if (result)
            is_in = false

    return is_in
```

۴-۲ گسترشِ الگوریتم برای حالت‌های دیگر

می‌دانیم که برای عملکردِ درستِ الگوریتم لازم است که احتمالی که در معادلهٔ ۴-۳ افزایش یابد و به مقدارِ ثابتی برسد. از این رو، می‌توان از الگوریتمِ تقویتِ دامنه که در بخشِ ۲-۲-۲ تعریف شده‌است کمک بگیریم. اگر کلِ فرایندِ الگوریتمِ قبل را تا پیش از اندازه‌گیری G بنامیم، همچنین $\mathbb{P}_{\mathbb{T}}$ را تصویر برروی عددِ ۰ باشد (که احتمالِ آن موردِ نظر است)، آن را تقویت کرد. تعدادِ مراحلِ لازم برای این تقویت از مرتبهٔ $\mathcal{O}(\frac{N}{\kappa})$ خواهدبود که این نشان می‌دهد اگر κ عدد ثابتی باشد، این الگوریتم هیچ تسریعی نمی‌تواند داشته‌باشد.

۴-۳ حدِ پایینِ دشمن‌گونه

این‌طور که پیداست، مسئلهٔ نقطه در چندضلعی در حالتِ کلی نمی‌تواند تسریعی با استفاده از رایانشِ کوانتومی را تجربه کند. این موضوع به شکلِ تئوری نیز قابلِ بررسی‌ست.

تا به این‌جای بحث، محدودیتی برروی سادگی یا غیرِسادگیِ چندضلعی‌ها مشخص نشده و قابلِ حدس است که تمامِ بحث‌های گفته‌شده برروی هردو دستهٔ چندضلعی‌ها برقرار باشند. اما در این بخش، استدلالی برای حدِ پایینِ پرسش‌های کلاسیک و کوانتومیِ لازم برای حلِ مسئلهٔ مذکور بیان می‌شود که تنها برای چندضلعی‌های غیرساده معتبر است و درصورتِ محدودیتِ مسئله به چندضلعی‌های ساده، این حدود غیرمعتبر خواهندبود.

برای بیانِ این حد از حدِ پایینِ دشمن‌گونه استفاده می‌کنیم که به این ترتیب است که اگر برای مسئله‌ای به شکلِ $f : S \to \mathbb{Z}_2$ دسترسیِ الگوریتم به ورودی از طریقِ جعبه‌سیاه باشد؛ یعنی برای هر ورودیِ مسئله مانندِ $s \in S$ الگوریتم با استفاده از جعبه‌سیاهی مانندِ O_s به جوابِ مسئله برسد، و همچنین دو زیر مجموعهٔ دلخواهِ زیر را داشته‌باشیم

$$X \subseteq \{s|f(s) = 1\} Y \subseteq \{s|f(s) = 0\} \quad (۴-۷)$$

و رابطه‌ای به شکلِ $R \subseteq X \times Y$ که

$$xRy \Leftrightarrow O_x(i) \neq O_y(i) i \text{ تنها برای یک مقدارِ} \quad (۴-۸)$$

از طرفِ دیگر می‌توانیم رابطهٔ R_i را نیز به شکلی تعریف کنیم که

$$xR_iy \Leftrightarrow O_x(i) \neq O_y(i) \text{ و } \forall j \neq i \; O_x(j) = O_y(j) \tag{۹-۴}$$

که در این صورت

$$R = \bigcup_i R_i \tag{۱۰-۴}$$

حالا اگر گرافِ دوبخشیِ معادل با R را در نظر بگیریم، کمینه درجهٔ رئوسِ بخشِ X و بخشِ Y را به ترتیب m و m' بنامیم، از سوی دیگر، برای R_i ها بیشینهٔ درجهٔ رئوس را به شکل l_i و l'_i را تعریف کنیم و بگیریم

$$l := \max_i l_i \tag{۱۱-۴}$$

$$l' := \max_i l'_i \tag{۱۲-۴}$$

آن‌گاه پیچیدگیِ محاسباتیِ پرسش های این مسئله از مرتبهٔ $\Omega(\sqrt{\frac{mm'}{ll'}})$ خواهد بود. که بدونِ اثبات آن را خواهیم‌پذیرفت [؟]

حالا برای استفاده از حدِ دشمن‌گونه، مسئلهٔ زیر را تعریف می‌کنیم

اگر یک $N-$ضلعیِ منتظم Q را درنظر بگیریم که نقطهٔ P مرکزِ آن باشد، حالا چندضلعیِ Q' را با مقیاس کردنِ Q به مرکزِ P و با ضریبِ $\frac{1}{2}$ و سپس قرینهٔ نقطه‌ای کردن آن حولِ P بسازیم، آن‌گاه به ازای هر رشتهٔ $N-$بیتیِ s یک چندضلعیِ $Q^{(s)}$ خواهیم داشت که رئوسِ آن به این ترتیب به دست می‌آیند

$$q_i^{(s)} = \begin{cases} q_i & s_i = ۱ \\ q'_i & s_i = ۰ \end{cases} \tag{۱۳-۴}$$

حالا مسئلهٔ وجودِ نقطهٔ P در چندضلعیِ $Q^{(s)}$ برابرِ مسئلهٔ زوج بودنِ وزنِ همینگِ s خواهد بود. برای اثباتِ این برابری، می‌توان از استقرای ریاضی استفاده کرد به این ترتیب که به ازای $s = ۰$ این برابری به سادگی برقرار است و با تغییرِ هر بیت از s می‌توان به سادگی نشان داد که همچنان برابری حفظ می‌شود و درنتیجه برای تمامِ رشته‌ها برقرار است.

از سوی دیگر، برای مسئلهٔ زوج بودنِ وزنِ همینگِ s، می‌توانیم از حدِ دشمن‌گونه به این ترتیب استفاده کنیم که X همهٔ رشته‌ها با وزنِ زوج و Y همهٔ رشته‌ها با وزنِ فرد باشند، آن‌گاه m و m' هردو

برابر با طولِ رشته و برابر با N خواهندبود و مقادیرِ l و l' نیز که مربوط همسایه‌هایی هستند که تنها در پرسشِ خاصِ i (بخوانید بیتِ iام) با هم تفاوت دارند برابر با ۱ خواهند بود، درنتیجه، این مسئله نیاز به $\Omega(N)$ پرسش خواهدداشت.

از آن‌جا که مسئلهٔ زوج بودنِ وزنِ همینگ قابلِ کاهش به وجودِ نقطه در چندضلعی‌ست پس حداقل پرسش برای مسئلهٔ نقطه در چندضلعی نیز برابرِ $\Omega(N)$ خواهدبود.

فصل ۵

نتیجه‌گیری

در این پایان‌نامه سعی شد که به بررسیِ رایانشِ کوانتومی و هندسهٔ محاسباتی و تلاقیِ این دو حیطه پرداخته‌شود. آن‌چه به نظر می‌رسد این است که تلاش‌های کمی در ترکیبِ این دو حوزه صورت گرفته‌است. حال آن‌که به خاطرِ ارتباطِ گستردهٔ هندسه (به‌خصوص در ابعادِ بالا) و رایانشِ کوانتومی پتانسیلِ خوبی برای تسریع‌های کوانتومی در مسائلِ هندسی وجود دارد. همچنین نظیرِ آن‌چه در این پایان‌نامه گفته شد، بسیاری از تسریع‌های کوانتومی در حضورِ قیدها و قول‌ها به دست می‌آیند که در این حوزه به خاطرِ ذاتِ هندسیِ مسائل، همواره قیدهایی برروی ورودی وجود خواهند داشت و این هم‌خوانی حتماً قابلِ استفاده خواهدبود.

آن‌چه ماحصلِ این پژوهش بوده‌است، به طورِ خاص برای مسئلهٔ نقطه در چندضلعی، به این ترتیب است که نشان داده‌شده هیچ الگوریتمِ کوانتومی‌ای نخواهدتوانست درحالتِ کلی، سریع‌تر از الگوریتم‌های کلاسیک به پاسخِ این مسئله دست پیدا کند. اما با اندکی تغییرِ مسئله و ایجادِ یک قول، مبتنی بر فاصله داشتنِ نقطه از اضلاع، یا حتی با قدری کاهشِ حساسیت نسبت به خطا در نزدیکیِ خطوطِ چندضلعی، می‌توان از الگوریتمِ پیشنهادشده استفاده کرد که از آن‌جا که مبتنی بر تبدیلِ فوریهٔ کوانتومی بوده‌است می‌تواند باعثِ تسریعِ فراـچندجمله‌ای بشود و تعدادِ پرسش‌ها را تا $\Theta(1)$ و پیچیدگیِ زمانی را تا $\Theta(\log(n))$ کاهش دهد.

نکتهٔ حائزِ اهمیتِ دیگر این است که از این الگوریتم می‌تواند به مقدارِ دلخواهی خطا را کم و به پیچیدگیِ محاسباتی اضافه کند تا به دقت و سرعتِ الگوریتمِ کلاسیک برسد.

۵-۱ کارهای آتی

در این پژوهش جای خالیِ شبیه‌سازی و نمایشِ خروجی‌ها برای مشاهدهٔ شرایطِ قول و مقدارِ خطا وجود دارد. همچنین بررسیِ الگوریتم‌های تقریبیِ کلاسیک و طراحیِ الگوریتم‌های کلاسیک برای همان شرایطِ قول می‌تواند منجر به مقایسهٔ دقیق‌تری بینِ راه‌حلِ کلاسیک و کوانتومی در این مسئله بشود. از سوی دیگر، بررسیِ کاربردهای مسئلهٔ قولی در هندسهٔ محاسباتی و حوزه‌های دیگری نظیرِ گرافیکِ کامپیوتری همچنان موردِ سؤال است.

فراتر از این، همچنان بسیاری از مسائل در هندسهٔ محاسباتی هستند که هیچ راه‌حلِ کوانتومی‌ای برای آن‌ها پیشنهاد نشده و از سوی دیگر، مسائلی که راه‌حل یا حدِ کوانتومی دارند نیز، نیازمندِ جمع‌بندی و تدوین هستند تا ابزاری یکپارچه شوند. برای مثال، بررسیِ شیوهٔ ورودی گرفتنِ اشکالِ کوانتومی یا پیدا کردنِ فرایندهای مشترک در الگوریتم‌های کوانتومیِ این حوزه، از موضوعاتِ ارزشمند برای پژوهش‌های آتی هستند.

پیوست آ

مطالب تکمیلی

آـ۱ شبه‌کدهای کوانتومی

مراجع

[1] S. Aaronson. *Quantum Computing since Democritus*. Cambridge University Press, 2013.

[2] C. M. Grinstead and J. L. Snell. *Introduction to Probability*. American Mathematical Society, 2nd edition edition, 1997.

[3] V. Karimipour. Lecture notes on quantum computation and information. http://physics.sharif.edu/~vahid/teachingQC.html, 2021. Accessed: 2021-06-25.

[4] S. Arora and B. Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[5] D. E. Deutsch and R. Penrose. Quantum computational networks. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 425(1868):73–90, 1989.

[6] P. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. A new universal and fault-tolerant quantum basis. *Information Processing Letters*, 75(3):101–107, 2000.

[7] J. Watrous. Quantum computational complexity. version: 1.

[8] S. Aaronson. 6.845 quantum complexity theory. MIT OpenCourseWare.

[9] M. Backens. The ZX-calculus is complete for stabilizer quantum mechanics. *New Journal of Physics*, 16(9):093021, 2014.

[10] P. Selinger and B. Valiron. A lambda calculus for quantum computation with classical control. In P. Urzyczyn, editor, *Typed Lambda Calculi and Applications*, pages 354–368. Springer Berlin Heidelberg, 2005.

[11] A. J., A. Adedoyin, J. Ambrosiano, P. Anisimov, A. Bärtschi, W. Casper, G. Chennupati, C. Coffrin, H. Djidjev, D. Gunter, S. Karra, N. Lemons, S. Lin, A. Malyzhenkov,

D. Mascarenas, S. Mniszewski, B. Nadiga, D. O'Malley, D. Oyen, S. Pakin, L. Prasad, R. Roberts, P. Romero, N. Santhi, N. Sinitsyn, P. J. Swart, J. G. Wendelberger, B. Yoon, R. Zamora, W. Zhu, S. Eidenbenz, P. J. Coles, M. Vuffray, and A. Y. Lokhov. Quantum algorithm implementations for beginners, 2018.

[12] A. Montanaro. Quantum algorithms: an overview. 2(1):1–8. Number: 1 Publisher: Nature Publishing Group.

[13] S. Jordan. Quantum algorithm zoo. https://quantumalgorithmzoo.org/. Accessed: 2021-07-08.

[14] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439(1907):553–558, 1992.

[15] A. Y. Kitaev. Quantum measurements and the abelian stabilizer problem. 1995-11-20.

[16] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Comput. Soc. Press.

[17] M. d. Berg, editor. *Computational geometry: algorithms and applications*. Springer, 3rd ed edition.

[18] C. D. Toth, J. O'Rourke, and J. E. Goodman. Handbook of discrete and computational geometry, third edition. page 1951.

[19] N. Volpato. Bounds for quantum computational geometry problems. page 12.

[20] M. Lanzagorta and J. Uhlmann. Quantum algorithmic methods for computational geometry. 20(6):1117–1125. Publisher: Cambridge University Press.

[21] F. P. Preparata and M. I. Shamos. *Computational geometry: an introduction*. Texts and monographs in computer science. Springer, 6. print edition.

[22] Encyclopedia of algorithms: with 379 figures and 51 tables.

واژه‌نامه

الف

برنامه‌ریزیِ خطیِ تعمیم‌یافته ... generalized linear programming

پ

پرسش ... query

ت

تعینی ... deterministic

تقویت دامنه ... amplitude amplification

ج

جعبه‌سیاه ... oracle

ح

حساس‌به‌خروجی ... output-sensetive

حدِ پایینِ دشمن‌گونه ... adversarial lower bound

ر

رایانش ... computation

ز

زنجیرهٔ مارکوفی ... markov chain

ف

فروریزش ... collapse

م

متغیرِ تصادفیِ مشترک ... shared randomness

مدلِ رایانش ... computational model

مولد ... generator

و

ولگشت ... random walk

ه

هم‌دسته ... coset

ی

یکانی ..... unitary

Abstract

Quantum computing is a computational model based on quantum mechanics principles. After introducing the Grover algorithm and Shor algorithm in the late 90s, quantum computing became a trend in both theoretical and experimental fields. On the other hand, computational geometry is a branch of computer science that analyses geometrical problems from computational prospectives, like algorithms, complexity classes, and orders. By emerging these two fields, those problems could also be analyzed in the quantum model. Efforts in this emerging field had begun with the trend and are continued till today, but almost all of the efforts were done in Grover-based speedups that are maximum quadratic. Point-In-Polygon problem which is a useful problem in computational geometry and computer graphics is not studied yet in the quantum model but it's well-studied in the classical regime with a few linear algorithms that and tight bounds on the complexity. This thesis introduces a new algorithm, based on quantum Fourier transform, that in with a promise of distance from edges, achives a superpolynomial speedup and solves the problem just with a query, but in the general case, it comes with no speed up and it's also proved that no algorithm can do such.

Keywords: Quantum Computing, Computational Geometry, Winding Number, Point in Polygon, Quantum Fourier Transform

Sharif University of Technology

Department of Computer Engineering

B.Sc. Thesis

A Quantum Algorithm for Point in Polygon

By:

Seyed Sajad Kahani

Supervisor:

Dr. Abam

July 2021