



دانشگاه صنعتی شریف
دانشکده‌ی مهندسی کامپیوتر

پایان‌نامه‌ی کارشناسی
مهندسی کامپیوتر

عنوان:

الگوریتم کوانتومی نقطه در چندضلعی

نگارش:

سید سجاد کاهانی

استاد راهنما:

دکتر آبام

تیر ۱۴۰۰

سلام

به نام خدا
دانشگاه صنعتی شریف
دانشکده‌ی مهندسی کامپیوتر

پایان‌نامه‌ی کارشناسی

عنوان: الگوریتمِ کوانتومیِ نقطه در چندضلعی

نگارش: سید سجاد کاهانی

کمیته‌ی ممحنین

امضاء:

استاد راهنما: دکتر آلام

امضاء:

استاد مشاور: ؟؟

امضاء:

استاد مدعو: ؟؟

تاریخ:

چکیده

رایانش کوانتومی گونه‌ای از رایانش است که مبتنی بر اصل موضوع‌های مکانیک کوانتومی به وجود آمده که در دهه نود و پس از معرفی دو الگوریتم جست‌وجو و تجزیه عدد، توجه‌ها بیش از پیش معطوف به آن شد. از روی دیگر، هندسه محاسباتی که به بررسی مسائل هندسی از منظر رایانش می‌پردازد و پیچیدگی و الگوریتم‌های این مسائل را بررسی می‌کند، می‌تواند در سیاق رایانش کوانتومی نیز مورد بررسی قرار بگیرد. از بدو پیدایش رایانش کوانتومی بررسی‌های اندکی بر روی کاربرد آن در هندسه محاسباتی صورت گرفته که آن بررسی‌ها هم اکثراً معطوف به استفاده از الگوریتم جست‌وجوی کوانتومی بر روی مسائل بوده‌است که با تسریع چندجمله‌ای همراه است. مسئله نقطه در چندضلعی که یکی از مسائل پرکاربرد این حوزه است تا کنون به شکل کوانتومی بررسی نشده و با رایانش کلاسیک چند الگوریتم با زمان خطی برای آن وجود دارد در کنار الگوریتم‌های تقریبی و با پیش‌پردازی که در زمان و پرسش زیرخطی اجرا می‌شوند. در این پایان‌نامه به معرفی الگوریتمی کوانتومی برای نقطه در چندضلعی می‌پردازیم که مبتنی بر تبدیل فوریه کوانتومی است و می‌تواند در شرایطی که تضمین فاصله نقطه از اضلاع وجود دارد به تسریع فرا-چندجمله‌ای دست می‌یابد و با یک پرسش در زمان لگاریتمی می‌تواند پاسخ مسئله را به دست بیاورد اما در حالت کلی تسریعی نسبت به حالت کلاسیک نخواهد داشت.

کلیدواژه‌ها: پایان‌نامه، حروف چینی، قالب، زی‌پرشین

فهرست مطالب

۹	۱ مقدمه
۹	۱-۱ تعریف مسئله
۱۰	۲-۱ ساختار پایان نامه
۱۱	۲ مفاهیم اولیه
۱۱	۱-۲ حالت های کلاسیک و کوانتومی
۱۱	۱-۱-۲ زنجیره مارکوفی
۱۴	۲-۱-۲ گزارهای کوانتومی
۲۰	۳-۱-۲ تفاوت های سیستم های کوانتومی و کلاسیک
۲۲	۲-۲ رایانش کوانتومی و کلاسیک
۲۲	۱-۲-۲ مدل رایانش
۲۷	۲-۲-۲ الگوریتم های پایه ای در رایانش کوانتومی
۳۹	۳-۲-۲ شبیه سازی کلاسیک این سیستم ها
۴۰	۳-۲ هندسه محاسباتی
۴۰	۱-۳-۲ الگوریتم های جاروب خطی/صفحه ای
۴۱	۲-۳-۲ الگوریتم های برنامه ریزی خطی

۴۱ مسئله پوش محدب	۳-۳-۲
۴۱ مسئله مثلث بندی	۴-۳-۲
۴۱ ساختمان داده لیست یال های دوسویه متصل	۵-۳-۲
۴۱ ساختمان داده درخت کی دی	۶-۳-۲
۴۱ دوگانگی	۷-۳-۲
۴۱ پیش پردازش های کاربردی، مثال دیاگرام ورونی	۸-۳-۲
۴۲	
۴۲ الگوریتم های کوانتومی در هندسه محاسباتی	۱-۳
۴۵ مسئله قرارگیری نقطه در چندضلعی	۲-۳
۴۷	
۴۷ الگوریتم کوانتومی نقطه در چندضلعی	۴
۵۰ گسترش الگوریتم برای حالت های دیگر	۱-۴
۵۱	
۵۱ نتیجه گیری	۵
۵۱ کارهای آتی	۱-۵
۵۲	
۵۲ مطالب تکمیلی	آ
۵۲ شبه کدهای کوانتومی	۱-آ

فهرست شکل‌ها

۳-۱	نمایش پارامترهای استفاده شده در الگوریتم	۴۶
-----	--	----

فهرست جدول‌ها

فصل ۱

مقدمه

از ایده کامپیوترهای کوانتومی بیش از نیم قرن می‌گذرد اما عمده توجه به آن پس از دو الگوریتم مشهور شور و گروور در دهه نود میلادی بوده است. از آن روز تلاش بی‌وقفه‌ای برای یافتن الگوریتم‌های جدید و کاربردهای جدید از الگوریتم‌های قدیمی رایانش کوانتومی ادامه دارد. اما بخش اندکی از این تلاش‌ها در حوزه هندسه محاسباتی بوده است، با این وجود به نظر می‌رسد که با توجه به خواص هندسی حالت‌های کوانتومی و قیود هندسی که مسائل هندسه محاسباتی را از گونه‌های دیگر مسائل محاسباتی متمایز می‌کند، رایانش کوانتومی کاربردهایی بسیار گسترده‌تر از آن‌چه تا کنون شناخته شده است در این حوزه داشته باشد.

۱-۱ تعریف مسئله

مسئله این‌تر، در مرحله اول، بررسی کاربردهای الگوریتم‌های کوانتومی در هندسه محاسباتی و در مرحله بعد معرفی الگوریتم جدیدی برای مسئله نقطه-در-چندضلعی است. هرچند که برای مسئله نقطه-در-چندضلعی الگوریتم خطی‌ای وجود دارد و امکان تسریع آن به شکل کلاسیک وجود ندارد اما به علت استفاده گسترده آن در گرافیک کامپیوتری، بهبود سرعت آن به شکل تکنیکال نیز همواره مورد توجه افراد بوده است. همچنین در ادبیات الگوریتم‌های کوانتومی در هندسه محاسباتی، هرچند مسئله‌های بسیاری مورد بررسی قرار گرفته اما این مسئله مورد بررسی قرار نگرفته و از سوی دیگر، ایده اکثریت تسریع‌های کوانتومی در هندسه محاسباتی مبتنی بر جست‌وجوی کوانتومی بوده است که منتج به تسریع حداکثر

مربعی می‌شود.

۱-۲ ساختار پایان‌نامه

این پایان‌نامه در پنج فصل به این موضوع می‌پردازد به این ترتیب که پس از مقدمه، در فصل اول مفاهیم اولیه راینش کوانتومی و هندسه محاسباتی مرور می‌شود و پس از آن در فصل مروری بر ادبیات الگوریتم‌های کوانتومی هندسه محاسباتی صورت می‌گیرد. سپس برای الگوریتم نقطه-در-چندضلعی الگوریتم‌های کلاسیک بررسی می‌شوند و در فصل چهارم الگوریتم کوانتومی‌ای تشریح می‌شود. در نهایت در فصل آخر به جمع‌بندی و مسیرهای پیشنهادی برای پژوهش‌های آتی پرداخته می‌شود.

فصل ۲

مفاهیم اولیه

همواره مرسوم‌ترین راه برای بیان 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 شهود ما از طبیعت دارد. [۱]

۱-۲ حالت‌های کلاسیک و کوانتومی

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

۱-۱-۲ زنجیره مارکوفی

این بخش تنها مقدمه و مروری بر زنجیره‌های مارکوفی‌ست.

نمایش ۱ برای نمایش بردارها از حروفِ کوچک و توپر a استفاده می‌کنیم و برای نمایش ماتریس‌ها از حروفِ بزرگ توپر A نشان می‌دهیم.

برای نمایش ترانزیت‌ها بردارها و ماتریس‌ها از علامت T استفاده می‌کنیم.

برای نشان دادن درایه‌ها نیز از زیروند به شکل A_{ij} استفاده می‌کنیم.

همچنین بردار \mathbf{z} نشان‌دهنده بردارهایی با همه عناصر یک است و \mathbf{e}_i برداری است که تنها مؤلفه i آن یک است و باقی صفر هستند.

برای بردارهای مختلط از علامت $*$ برای مزدوج مختلط تک تک درایه‌های بردارها و ماتریس‌ها استفاده می‌کنیم.

همچنین

$$\dagger = \cdot^* \quad (۱-۲)$$

یک زنجیره مارکوفی یک دنباله از متغیرهای تصادفی X_t بر روی مجموعه گسسته حالت‌ها به نام S است. با این شرط که توزیع متغیر تصادفی متغیر X_{t+1} ام دنباله تنها بستگی به جمله X_t ام دارد و احتمالات شرطی این بستگی در طول این زنجیره ثابت هستند و می‌توان آن‌ها را با ماتریس گزار نشان داد به این ترتیب که برای همه t ‌ها

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

که اگر در کنار این ماتریس، بردار احتمال را تعریف کنیم

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

آن‌گاه می‌توان این خاصیت‌ها را در حالت کلی اثبات کرد.

$$\mathbf{j}^T \mathbf{p}^t = ۱ \quad (۴-۲)$$

$$T \mathbf{j} = \mathbf{j} \quad (۵-۲)$$

$$\mathbf{j}^T T = \mathbf{j}^T \quad (۶-۲)$$

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

$$\mathbf{p}^t = \mathbf{T}^t \mathbf{p}^* \quad (۷-۲)$$

می‌توان معادله ۶-۲ را به شکل شفاهی این طور بیان کرد که جمع مؤلفه‌ها در گزارِ سیستم ناورداست. البته این طبیعی‌ست زیرا برای ما مطلوب است که بردار \mathbf{p}^t همواره توزیع احتمال باقی بماند. با توجه به این که این ماتریس گزار مثبت است خواص متعددی را می‌توان برای آن اثبات کرد، از جمله این که ویژه‌برداری با ویژه‌مقدار بیشینه (برابر یک) وجود دارد که حالت تعادل این سیستم پس از بی‌نهایت بار گزار است. [۲]

تضارب حالت‌ها

دو زنجیره مارکوفی را در نظر بگیرید که (لااقل در ابتدا) مستقلاً کار می‌کنند. زنجیره اول در حالت \mathbf{p}^1 و زنجیره دوم را در حالت \mathbf{p}^2 در نظر بگیرید. اگر بخواهیم مجموع دو زنجیره را با یک زنجیره بزرگ‌تر بیان کنیم

$$\mathbf{p}^{\text{کل}} = \mathbf{p}^1 \otimes \mathbf{p}^2 \quad (۸-۲)$$

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

$$\mathbf{T}^{\text{کل}} = \mathbf{T}^1 \otimes \mathbf{T}^2 \quad (۹-۲)$$

حالا اگر بعد از تحولی به شکل مجزا یا به شکل هم‌بسته، از بردار حالت دو سیستم، به بردار حالت یکی از سیستم‌ها برسیم کافی‌ست

$$\mathbf{p}_i^1 = \sum_j^{\dim(\text{زنجیره دوم})} \mathbf{p}^{\text{کل}} \mathbf{e}_i^1 \otimes \mathbf{e}_j^2 \quad (۱۰-۲)$$

کمیت‌های مشاهده‌پذیر

برای سیستمی که در حالت p قرار دارد، دسترسی به خود این بردار در عمل مقدور نیست و آنچه مشاهده می‌شود، کمیت مشاهده‌پذیری نظیر X است که می‌توان آن را تابعی از حالت‌های سیستم در نظر گرفت، یعنی

$$M : \{1 \dots n\} \rightarrow \mathbb{R} \quad (11-2)$$

که البته این تابع را می‌توان به شکل برداری نشان داد که در آن صورت، بیان کمیتی مثل امید ریاضی آن ساده‌تر می‌شود

$$\mathbb{E}[M] = \mathbf{M}^T \mathbf{p} \quad (12-2)$$

۲-۱-۲ گزارهای کوانتومی

سیستم احتمالاتی‌ای را (با n حالت مجزا) بگیرید که برای نمایش آن از برداری n -بعدی، مختلط و با اندازه یک به نام \mathbf{v} بهره می‌گیریم به طوری که

$$\text{Pr}(i) = |\mathbf{v}_i|^2 \quad (13-2)$$

به هر فضای برداری‌ای که یک ضرب داخلی بر روی آن تعریف شده، نظیر فضای برداری تعریف شده، 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 $\langle v|u\rangle$ ضرب داخلی دوبردار و $|v\rangle|u\rangle$ نمایش ساده‌ای از $|v\rangle \otimes |u\rangle$ است.

و به ازای هر $i \in \{0, \dots, n\}$ برداری است که مؤلفه i ام آن یک است.

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

ماتریس‌ها با علامت توپر نشان داده نمی‌شوند و همچنین I ماتریس همانی است.

در ادامه نشان خواهیم داد این گونه‌حالت‌ها چیزی فراتر از زنجیره مارکوفی هستند. برای گزار این سیستم، باید از ماتریس‌های حافظ 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 حالت مجزا داریم و آن را یک کیوبیت می‌نامیم. اگر بگیریم

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (2-14)$$

$$|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (2-15)$$

همچنین اگر بگیریم

$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (2-16)$$

$$|-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (2-17)$$

این دو بردار هردو توزیع احتمالاتی به شکل $p = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$ دارند.

و اگر این تحول را در نظر بگیریم

$$H = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (2-18)$$

^۱ $SU(n)$ گروه ماتریس‌های یکانی $n \times n$ هستند.

آن‌گاه تحت این تحول، دو بردار مثبت و منفی که توزیع احتمال یک‌شکل داشتند به دو بردار با توزیع‌های متفاوت می‌روند که این چنین رفتاری با زنجیره مارکوفی قابل توصیف نیست. این مثال نشان می‌دهد که این تئوری اندکی با تئوری احتمال مرسوم متفاوت است.

نکته دیگری که مورد توجه است این است که برخلاف T ، گزار U حتماً وارون‌پذیر است که این نکته‌ای است که در بخش‌های دیگر بیشتر مورد توجه قرار می‌گیرد.

اندازه‌گیری

یکی از بخش‌های مبهم مکانیک کوانتومی، اندازه‌گیری است. تصور کنید که سیستمی کوانتومی در حالت $|v\rangle$ قرار دارد. اگر یک مشاهده یا اندازه‌گیری فیزیکی انجام بگیرد، بردار حالت سیستم با احتمال $Pr(i) = |\langle e_i | v \rangle|^2$ به بردار $|e_i\rangle$ تبدیل می‌شود. به این عمل رمبش یا collapse می‌گویند.

مثال ۲-۲ مانند مثال قبل، یک کیوبیت را تصور کنید

- سیستم در حالت اولیه $|+\rangle$ باشد.

- تحول H را روی آن اعمال شود.

- اندازه‌گیری را انجام شود.

نتیجه این فرایند به این شکل است که با احتمال $Pr(0) = 1$ حالت 0 مشاهده می‌شود.

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

- سیستم در حالت اولیه $|+\rangle$ باشد.

- یک اندازه‌گیری اولیه انجام می‌شود.

- تحول H را روی آن اعمال شود.

- اندازه‌گیری را انجام شود.

می‌توان محاسبه کرد که حاصل این فرایند با احتمال $\frac{1}{4}$ $\text{Pr}(0) = \frac{1}{4}$ حالت ۰ و با احتمال $\frac{1}{4}$ $\text{Pr}(1) = \frac{1}{4}$ حالت ۱ مشاهده می‌شود.

این آزمایش تأثیر مفهوم رمبش را نشان می‌دهد. به این ترتیب که می‌توان آزمایش مشابهی برای زنجیره‌های مارکوفی تعریف کرد و خواهیم دید که اندازه‌گیری هیچ تأثیری در زنجیره‌های مارکوفی ندارد.

به طور مشابه، برای آنچه در خصوص کمیت‌های مشاهده‌پذیر در زنجیره مارکوفی گفتیم، دسترسی به بردار حالت یک سیستم $|v\rangle$ و حتی توزیع احتمالات آن مقدور نیست.

در ساده‌ترین حالت در نظر بگیرید که کمیت مشاهده‌پذیری به نام M داریم که به هر حالت سیستم (یا به عبارتی دیگر هر بردار از پایه متعامدیکه فضا) مانند $|i\rangle$ یک عدد $\lambda_i \in \mathbb{R}$ نسبت می‌دهد.

می‌دانیم که آن‌گاه

$$\mathbb{E}[M] = \sum_i \lambda_i \text{Pr}(i) = \sum_i \lambda_i |\langle i|v\rangle|^2 = \sum_i \lambda_i \langle v|i\rangle \langle i|v\rangle \quad (2-19)$$

که حالا اگر ماتریس زیر را تعریف کنیم

$$\hat{M} := \sum_i \lambda_i |i\rangle\langle i| \quad (2-20)$$

آن‌گاه، می‌توان معادله ۲-۱۹ را به شکل زیر نوشت

$$\mathbb{E}[M] = \langle v|\hat{M}|v\rangle \quad (2-21)$$

اما حقیقت ماجرا این است که در یک سیستم فیزیکی، ممکن است چند پایه متعامدیکه برای حالت‌های مربوط به مشخصه‌های مختلف وجود داشته باشد.

مثال ۲-۳ (آزمایش اشتراک-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 کمیت برداری، اسپین می‌گوییم.^۲

پس مؤلفه‌های اسپین را می‌توان در هر کدام 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-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 نتیجه این آزمایش، ساده‌ترین مدلی که این رفتار را توصیف کند به شرح زیر است که این سیستم علی‌رغم این که سه مؤلفه برای اندازه‌گیری دارد، حالت آن برداری نظیر $|\psi\rangle$ در فضای دوبعدی است و عملگرهای گفته‌شده برابر با ماتریس‌هایی به شکل زیر است.

$$\hat{X} = \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (22-2)$$

$$\hat{Y} = \frac{1}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (23-2)$$

$$\hat{Z} = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (24-2)$$

یک مثال معروف‌تر از این، «مکان» و «تکانه» هستند که هردو پایه‌های متعامدیکه‌ای برای فضای حالت‌های یک ذره هستند. در نتیجه این، نمی‌توان مکان و تکانه را همزمان اندازه‌گیری کرد و همچنین با اندازه‌گیری آن‌ها به ترتیب می‌توان به اصل عدم قطعیت^۴ را اثبات کرد.

^۳ این تعریف به هیچ‌وجه تعریف دقیقی از اسپین به عنوان یک کمیت ذاتی در ذرات صحیح نیست و تنها مثال ملموسی است برای استفاده از آن در سیاقِ رایانش کوانتومی

^۳ مقدار دقیق‌تر آن $\frac{\hbar}{2}$ است که برای سادگی، مقدار \hbar را که یک ثابت جهانی به نام ثابت کاهیده پلانک است، یک فرض می‌کنیم.

^۴ اصل عدم قطعیت، اصلی است که بیان می‌کند هرگونه اندازه‌گیری‌ای که مکان و تکانه را به ترتیب با خطای Δx و Δp اندازه‌گیری کند، این نامساوی برقرار است

$$\Delta x \Delta p \geq \frac{\hbar}{2} \quad (25-2)$$

مدل کوانتوم-احتمالاتی

حالا می‌توان مدلی را تصور کرد که سیستم، به شکل احتمالاتی، در حالات کوانتومی متعدد باشد. یعنی دنباله‌ای از حالت‌ها داریم $|v_1\rangle \dots |v_n\rangle$ داریم که سیستم با احتمالات نظیر $p_1 \dots p_n$ در این حالات حضور داشته باشد.

سیستم‌های این‌چنینی را می‌توان با ترکیب مدل احتمالاتی و کوانتومی بررسی کرد، اما برای بررسی ساده‌تر، می‌توان کمیت زیر را تعریف کرد که ماتریس چگالی نام دارد و نماینده این توزیع احتمالاتی از توزیع‌هاست.

$$\rho := \sum_{i=1}^n p_i |v_i\rangle\langle v_i| \quad (26-2)$$

حالا اثر یک تحول کوانتومی که یک ماتریس یکانی مانند U است، بر روی این ماتریس چگالی، به شکل زیر است.

$$\rho \mapsto U\rho U^\dagger \quad (27-2)$$

و همچنین، با اندازه‌گیری یک کمیت، مانند M امید ریاضی آن از رابطه زیر به دست می‌آید.

$$\mathbb{E}[M] = \text{Tr}(\rho \hat{M}) \quad (28-2)$$

بررسی تحولات این سیستم‌ها، با مفهومی به نام کانال انجام می‌گیرد که خارج از این مقال است.

تضارب حالت‌ها

اگر دو سیستم کوانتومی مجزا با حالت‌های $|v\rangle$ و $|u\rangle$ داشته باشیم، آن‌گاه حالت کلی سیستم $|v\rangle \otimes |u\rangle$ خواهد بود.

در این صورت اگر عملگری مانند U را فقط بر روی سیستم اول اثر بدهیم، آنگاه اثر آن بر کل سیستم به شکل $U \otimes I$ خواهد بود. به شکلی مشابه می توان عملگری را فقط روی سیستم دوم اثر داد یا عملگری را روی هر دو سیستم به شکل همزمان اثر داد که در نتیجه آن، بردار حاصل، به شکل ضربی مثل $|v'\rangle \otimes |u'\rangle$ قابل بیان نباشد.

در کلی ترین حالت، برداری که متعلق به دو فضا باشد را بتوان به شکل زیر نوشت

$$|\psi\rangle = \sum_i |a_i\rangle \otimes |b_i\rangle \quad (2-29)$$

حالا فرض کنید فضای دوم را در پایه ای دلخواه اندازه گیری می کنیم. و نتیجه آن بردار $|b_i\rangle$ در سیستم آنگاه سیستم با احتمال $| \langle b_i | \psi \rangle |^2$ در حالت $\frac{\langle b_i | \psi \rangle}{| \langle b_i | \psi \rangle |}$ قرار می گیرد. ذکر این نکته لازم است که حاصل $\langle b_i | \psi \rangle$ یک بردار در فضای اول است و نه یک عدد.

این طور می توان گفت که پس از اندازه گیری فضای دوم، یک حالت احتمالاتی کوانتومی داریم که با آن را با یک ماتریس چگالی نشان می دهیم.

$$\rho_{\text{فضای اول}} = \sum_i | \langle b_i | \psi \rangle |^2 \frac{\langle b_i | \psi \rangle}{| \langle b_i | \psi \rangle |} \frac{\langle \psi | b_i \rangle}{| \langle b_i | \psi \rangle |} = \sum_i \langle b_i | \psi \rangle \langle \psi | b_i \rangle = \text{Tr}_{\text{فضای دوم}} |\psi\rangle \langle \psi| \quad (2-30)$$

که با ساده سازی به رد جزئی می رسیم.

۳-۱-۲ تفاوت های سیستم های کوانتومی و کلاسیک

همچنان که در مثال ۱-۲ گفته شد، سیستم های کوانتومی قابلیت هایی متعددی مزید بر سیستم های کلاسیک دارند. آنچه در آن مثال دیده شد به نوعی قابلیت پنهان کردن اطلاعاتی در سیستم بود که خود را در یک اندازه گیری ساده نشان نمی دهد.

در ادامه در قالب یک مثال، به بررسی هم بستگی های کوانتومی می پردازیم که «درهم تنیدگی» نامیده می شود.

مثال ۲-۴ (آزمایش بل) یک بازی را تصور کنید، که داور به هر کدام از دو بازیکن (آلیس و باب) یک

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

آلیس و باب نمی‌توانند با هم هیچ پیامی رد و بدل کنند. حالا، آلیس و باب، هر کدام بر حسب استراتژی خود یک بیت را به داور برمی‌گردانند. تصور کنید دو بیت a و b باشند. آلیس و باب هر دو با هم پیروز می‌شوند اگر و تنها اگر

$$a \text{ XOR } b = x \text{ AND } y \quad (۳۱-۲)$$

حالا یک بار در نظر می‌گیریم که استراتژی هر کدام، به شکل تعینی^۵ باشد، یعنی

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

اگر فرض بگیریم که هریک از مقادیر x و y هم احتمال باشند، آنگاه برای احتمال پیروزی، برای هر استراتژی‌ای خواهیم داشت

$$\Pr(\text{پیروزی}) \leq \frac{3}{4} \quad (۳۳-۲)$$

حالا اگر استراتژی هر کدام از آلیس و باب، به شکل احتمالاتی و وابسته به یک متغیر تصادفی مشترک^۶ مانند λ باشد

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

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

اما اگر به جای متغیر تصادفی مشترک، یک حالت کوانتومی بین آلیس و باب به اشتراک گذاشته شود، به طوری که سیستم کوانتومی مسئله، از دو زیرسیستم دو حالته تشکیل شده است که زیرسیستم اول در اختیار آلیس و زیرسیستم دوم در اختیار باب است. (که در زیر فوق با اندیس‌ها مشخص شده‌اند)

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) \quad (2-35)$$

حالا اگر برای تعیین استراتژی هرکدام از بازیکنان از اندازه‌گیری استفاده کنند، یعنی با توجه به ورودی (x و y) یک پایه متعامد برای اندازه‌گیری انتخاب کند^۷ و از نتیجه آزمایش، خروجی خود را انتخاب کند، یعنی اگر $\{|A_0\rangle, |A_1\rangle\}$ و $\{|B_0\rangle, |B_1\rangle\}$ دو پایه متعامد برای اندازه‌گیری در زیرسیستم آلیس باشند و به شکل مشابهی برای باب، بردارهای B را داشته باشیم، می‌توانیم به این شکل بنویسیم که

$$Pr(a, b|x, y) = |\langle\psi|A_a^x|B_b^y\rangle|^2 \quad (2-36)$$

دلیل این که نمی‌توان این احتمال را برای آلیس و باب به شکل مجزا نوشت این است که هرکدام از این دو، نخست اندازه‌گیری را انجام دهند، بر روی استیت کلی سیستم تأثیر می‌گذارند، هرچند که این تأثیر، همچنان نمی‌توان هیچ پیامی را منتقل کرد، اما شکل خاصی از هم‌بستگی را به وجود می‌آورد که در سیستم‌های کلاسیک دیده نمی‌شوند و در نتیجه باعث می‌شود که احتمال پیروزی می‌تواند به $\frac{1+\sqrt{2}}{4} \simeq 0.85$ برسد که این نقض نامساوی ۲-۳۳ است. [۳، ناموضعیت در مکانیک کوانتومی]

۲-۲ رایانش کوانتومی و کلاسیک

۱-۲-۲ مدل رایانش

نمایش ۳ یک الفبا مانند Σ ، یک مجموعه از علامت‌هاست. اگر $s \in \Sigma$ یکی از آن علامت‌ها باشد ss یا s^2 یک کلمه ساخته شده با تکرار آن علامت است و همچنین Σ^2 مجموعه کلمه‌ها با طول دو است. (و به همین ترتیب برای طول‌های بیشتر)

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

deterministic^v
shared randomness^v

^vاندازه‌گیری در پایه متعامد دلخواه، هم‌ارز انجام یک تحول یکانی مناسب و سپس اندازه‌گیری در پایه اصلی است. پس اگر تحول‌های یکانی همگی در دسترس باشند، اندازه‌گیری در هر پایه‌ای ممکن است. درباره در دسترس بودن تحول‌ها در ۱-۲-۲ 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 بیان رایانش کوانتومی وجود دارد اما پر استفاده‌ترین آن‌ها مدل مداری‌ست که به سادگی قابل ساخت از روی مدل کلاسیک 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 حل آن را داریم، تابعی به شکل $f: \mathbb{Z}_2^* \rightarrow \mathbb{Z}_2$ است.

خانواده مدارهای یکنواخت و غیریک‌نواخت

- یک مدار C ، یک گراف جهت‌دار غیر مدور است که سه دسته گره بر روی آن مشخص می‌کنیم.
- گره‌های ورودی: گره‌هایی با درجه ورودی صفر هستند که هرکدام نمایانگر یکی از ورودی‌های مسئله است هستند.
 - گره‌های گیت: گره‌هایی با درجه ورودی و خروجی شان ناصفر هستند که هرکدام نمایانگر یک گیت از مجموعه گیت‌های مجاز در مدار است که تعداد ورودی‌ها و تعداد خروجی‌های مشخصی دارد. برای ما این مجموعه شامل AND و OR هرکدام با دو ورودی و NOT با یک ورودی است.
 - گره‌های خروجی: گره‌هایی با درجه خروجی صفر که نماینده خروجی مسئله هستند (با توجه به تعریف تابع به شکل گفته شده، تنها یک گره خروجی داریم)

بر روی این مدار، توابع زیر را تعریف می‌کنیم

- $\text{size}(C)$: تعداد گره‌های گیت در مدار

- $\text{depth}(C)$: طول طولانی‌ترین مسیر در مدار

با توجه به تعریفی که از مدار ارائه شد، اندازه ورودی‌های آن ثابت است و برای حل مسئله به شکلی که گفته شد، نیاز به یک خانواده از مدارها داریم. خانواده مدار F ، یک دنباله از مدارها به شکل (F_1, F_2, \dots) است که F_i برای ورودی با طول i تابع f را محاسبه می‌کند.

اگر تابع f با یک خانواده مدار F قابل محاسبه باشد، به طوری که برای $\text{size}(F_i)$ (به عنوان تابعی از i) داشته باشیم $\text{size}(F_i) \in \mathcal{O}(\text{poly}(i))$ آن گاه می‌گوییم مسئله محاسبه f عضو کلاس P/poly است. مثال ساده‌ای وجود دارد که نشان می‌دهد این مدل از ماشین تورینگ قوی‌تر است.

مثال ۲-۵ (این مثال صرفاً به خاطر علاقه شخصی نویسنده این جاست و بار علمی‌ای ندارد). فرض کنید مسئله h به شکل $h: \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p$ برای ماشین تورینگ غیرقابل محاسبه است. (می‌دانیم چنین مسئله‌ای وجود دارد)

می‌دانیم که به ازای هر $s \in \mathbb{Z}_p^*$ می‌توان عددی طبیعی به آن نسبت داد که به این شکل ساخته می‌شود $n_s = \overline{1}s$ به سادگی می‌توان گفت این تبدیل یک به یک و پوشاست.

حال ابتدا مسئله دیگری به شکل $f: \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p$ می‌سازیم که در آن

$$f(1^{n_s}) = h(s) \quad (2-37)$$

آنگاه طبیعتاً برای هر طولی از ورودی f یک مدار وجود دارد که خروجی لازم را تولید کند. (اما تولید خود مدار کار سختی است و این مهم همان چیزی است که به آن توجه نشده بود) پس خانواده مدار از ماشین تورینگ قوی‌تر عمل می‌کنند.

با توجه به مثال گفته شده، خانواده مدارهای یکنواخت را تعریف می‌کنیم که در آن هر کدام از F_i ها به سادگی (در زمان چند جمله‌ای) توسط یک مدل محاسباتی قابل توصیف باشند.

حالا اگر مسئله‌ای با یک خانواده مدار یکنواخت F قابل محاسبه باشد، اگر $\text{size}(F_i) \in \mathcal{O}(\text{poly}(i))$ آن گاه می‌گوییم مسئله محاسبه f عضو کلاس P است.

پس از آن، مسئله‌ای مانند g را تصور کنید که برای ورودی، علاوه بر x ، یک رشته به نام w می‌گیرد به طوری که $|w| \in \mathcal{O}(\text{poly}(|x|))$ طول این رشته نسبت به طول x به شکل چند جمله‌ای باشد. این ورودی w را به شکل نوعی سر نخ برای $f(x) = 1$ استفاده می‌کنیم، یعنی فرض کنید

$$\begin{cases} \exists w \ g(x \cdot w) = 1 \Leftrightarrow f(x) = 1 \\ \forall w \ g(x \cdot w) = 0 \Leftrightarrow f(x) = 0 \end{cases} \quad (2-38)$$

اکنون اگر مسئله g که مسئله f به همراه سرنخ است (و از مسئله f آسان تر است) عضوِ کلاس P باشد می‌گوییم که مسئله f خود عضوِ کلاس NP است.

برای تعریف چند کلاس دیگر، تصور کنید یک مدار به شکل احتمالاتی کار می‌کند یا برای سازگاری با تعریف‌های قبل، این بار بپذیرید مسئله g علاوه بر ورودی x ، یک رشته از اعداد تصادفی به طول چندجمله‌ای را می‌گیرد که آن را r می‌نامیم. اگر g خود عضوِ P باشد و داشته باشیم

$$\Pr(g(x \cdot r) = f(x)) \geq \frac{2}{3} \quad (2-39)$$

آن‌گاه f عضوِ کلاس BPP است. [۴]^۸

مدارهای کوانتومی

حالا تصور کنید به سیستم d -حالت کوانتومی داریم. به این سیستم یک کیودیت می‌گوییم. در حالتی که $d = 2$ به این سیستم کیوبیت می‌گوییم.

اگر یک سیستم متشکل از n کیوبیت در نظر بگیریم، چنانچه پیشتر گفته شد، می‌توان تحول‌هایی را به شکل محلی بر روی یکی یا چندتا از این کیوبیت‌ها (به عنوان یک زیرسیستم از سیستمی بزرگ‌تر) اعمال کرد.

از این رو می‌توان متصور شد که اگر گیت‌های پایه کوانتومی را تعریف کنیم، بتوان مدار کوانتومی را تعریف کرد که به شکل مشابهی، شامل گره‌های زیر خواهد بود [۵]

- گره‌های ورودی: مشابه حالت قبل اما به شکل حالت کوانتومی است. (البته می‌دانیم که هر حالت کلاسیکی لزوماً یک حالت کوانتومی نیز هست)

- گره‌های خروجی: مشابه حالت قبل اما به شکل حالت کوانتومی است.

- گره‌های گیت‌های کوانتومی: مشابه حالت قبل اما ذکر این نکته لازم است که گیت‌های پایه در مدارهای کوانتومی، نمی‌توانند شامل AND و OR باشند چرا که این گیت‌ها باید فضای مبدأ و مقصد

^۸ کلاس‌های P ، NP و BPP هیچ‌گاه به این شکل تعریف نمی‌شوند. شکل اولیه تعریف آن‌ها مبتنی بر ماشین تورینگ است و بعد در طی قضیه‌هایی، اثبات می‌شود که به این شکل قابل نوشتن هستند.

یکسانی داشته باشند (درجه ورودی و خروجی شان یکی باشد) و تحول متناظر با آن‌ها وارون پذیر باشد. در اصل هر گیت باید یک ماتریس یکانی باشد.

– گره اندازه گیری: یک اندازه گیری در پایه $|0\rangle$ و $|1\rangle$ انجام می شود که طبیعتاً درجه ورودی آن یک و درجه خروجی آن نیز یک است.

یکی از مشهورترین مجموعه گیت های پایه مجموعه گیت H از مثال ۲-۳ و همچنین T و CNOT است که به شکل زیر تعریف می شوند. [۶]

$$T := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \quad (40-2)$$

$$\text{CNOT} := |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \text{NOT} \quad (41-2)$$

که در این بین، T و H عملگرهای تک کیوبیتی هستند اما CNOT یک عملگر دوکیوبیتی است. حالا به شکل مشابهی همان توابع بر روی مدارهای کوانتومی نیز تعریف می شوند و همچنین تعریف خانواده مدار و یکنواختی نیز به همین ترتیب تعمیم داده می شود.

کلاس های محاسباتی کوانتومی

به شکل مشابهی، برای مسئله ای به شکل $f: \{0, 1\}^* \rightarrow \{0, 1\}$ داریم^۹ که اگر با خانواده یکنواختی از مدارهای کوانتومی، به نام Q قابل محاسبه باشند، به طوری که $\text{size}(Q_i) \in \mathcal{O}(\text{poly}(i))$ آن گاه می گوئیم که این مسئله عضو کلاس EQP^{۱۰} است.

در ادامه، اگر بگیریم که مدار کوانتومی، همواره درست عمل نکند اما با احتمال خوبی پاسخ درست بدهد، یعنی به شکل فرمال داشته باشیم

$$\Pr(f(x) = Q_i(x)) \geq \frac{2}{3} \quad (42-2)$$

^۹ می دانیم که مدارهای کوانتومی، فضای مبدا و مقصد یکسانی دارند، از این رو، پیاده سازی تابعی به شکل فوق، می تواند به این شکل انجام بگیرد که ورودی به شکل کوانتومی داده می شود و پس از انجام یک عملیات یکانی، بر روی یک کیوبیت خاص، اندازه گیری رخ می دهد و حاصل اندازه گیری به عنوان خروجی سیستم لحاظ می شود.

^{۱۰} exact quantum polynomial

آنگاه می‌گوییم که مسئله در کلاس BQP قرار دارد.

در این جا بدون اثبات، چند گزاره در خصوص کلاس‌های محاسباتی گفته شده را بررسی می‌کنیم. [۷] [۸]

$$P \subseteq EQP \subseteq BQP \quad (۴۳-۲)$$

$$P \subseteq BPP \subseteq BQP \quad (۴۴-۲)$$

$$NP \not\subseteq BQP \quad (۴۵-۲)$$

$$NP \not\subseteq BQP \quad (۴۶-۲)$$

۲-۲-۲ الگوریتم‌های پایه‌ای در رایانش کوانتومی

برای بررسی الگوریتم‌های کوانتومی، نیاز به شیوه‌ای برای بیان آن‌ها داریم، هرچند تلاش‌های بسیاری برای طراحی زبان‌ها و حساب‌ها برای رایانش کوانتومی صورت گرفته، اما برای حفظ یک‌پارچگی با شیوه بیان الگوریتم‌های کوانتومی، از شیوه‌های نموداری، نظیر شکل مدار کوانتومی و حساب ZX استفاده نمی‌کنیم. [۵] [۹] [۱۰] ذکر این نکته هم لازم است که روش‌های شکلی تعمیم‌پذیر نیستند. از طرفی زبان‌های کوانتومی اغلب ساختار مشترکی در خصوص ساختار داده‌ها و عملیات‌های کوانتومی دارند اما از نظر عملیات‌های کلاسیک، تفاوت‌های بسیاری دارند. از این رو برای تشریح الگوریتم‌های کوانتومی از شبه‌کد کمک خواهیم گرفت. هرچند ساختار این شبه‌کد کاملاً گویاست اما برای حفظ صحت و دقت، در پیوست آن را از نظر نحوی و معنایی بررسی می‌کنیم.

ذکر این نکته لازم است که الگوریتم‌های کوانتومی گسترده‌ای برای کاربردهای متنوعی وجود دارند [۱۱] [۱۲] [۱۳] اما در این مقال، تمرکز بر روی الگوریتم‌های پایه‌ای خواهند بود که به زعم نویسنده می‌توانند کاربردی در مسائل هندسه محاسباتی داشته باشند.

الگوریتم دویچ-جوزا

اگر جعبه سیاهی^{۱۱} داشته باشیم که مدار تابع $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2^n : o$ باشد و برای این تابع داشته باشیم که حتماً یکی از حالت‌های زیر برقرار است

- تابع ثابت است.

- تابع متوازن است به این معنی که به ازای نیمی از ورودی‌ها $o(x) = 1$ و برای نیمی دیگر $o(x) = 0$

حالا مسئله این است که تشخیص بدهیم تابع o در کدام یک از دسته‌های فوق می‌افتد.

با استفاده از هر مدل کلاسیکی، نظیر خانواده مدارها، قابل تصور است که برای جواب قطعی، نیاز به حداقل $1 + 2^{n-1}$ بار استفاده از جعبه سیاه مذکور داریم.

اما به شکل کوانتومی، اگر فرض کنیم که همین مدار تابع o را داریم و برای این که این مدار، خواص یک مدار کوانتومی (وارون پذیری و یکی بودن فضای مبدأ و مقصد) را داشته باشیم، تحول یکانی O را به شکل زیر تعریف کنیم

$$O = \sum_{x \in \mathbb{Z}_2^n, y \in \mathbb{Z}_2} |x, y \text{ XOR } o(x)\rangle \langle x, y| \quad (2-47)$$

این تعمیم بر روی $n + 1$ کیوبیت تعریف شده است که n کیوبیت اول، نقش ورودی o را دارند و کیوبیت آخر، محل ذخیره خروجی o است.

حالا شبه کدی مانند ۱ را در نظر بگیرید.

^{۱۱}oracle، هرچند برای آن ترجمه پیشگو پیشنهاد شده اما به زعم نویسنده «جعبه سیاه» گویاتر است.

الگوریتم ۱ دویچ-جوزا

```

H : 1 qubit gate = 1/2 * [1, 1;
                          1, -1]
function IsConstant(0: 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 0 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 تحلیل دقیق این الگوریتم، حالت کیوبیت‌ها را در پایان هر مرحله بررسی می‌کنیم

$$|\psi_1\rangle = |0^n\rangle_x |1\rangle_y \quad (48-2)$$

سپس با انجام شدن عملگر H بر روی تک تک گیت‌ها، خواهیم داشت

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{i=0}^{2^{n+1}-1} |i\rangle_x (|0\rangle_y - |1\rangle_y) \quad (49-2)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{i=0}^{2^n-1} |i\rangle_x (|o(i)\rangle_y - |\text{NOT } o(i)\rangle_y) \quad (50-2)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{i=0}^{2^n-1} (|0\rangle_y - |1\rangle_y) \quad (51-2)$$

حالا با اعمال دوباره H ها بر روی x ها، می دانیم که حالت y تغییری نخواهد کرد.

$$|\psi_4\rangle = (H_x^{\otimes n} \frac{1}{\sqrt{2^{n+1}}} \sum_{i=0}^{2^n-1} (-1)^{o(i)} |i\rangle_x) \otimes (|0\rangle_y - |1\rangle_y) \quad (52-2)$$

با اضافه کردن این نکته که در صورتی پاسخ `is_constant` برابر با درست است که تمام بیت های خروجی x برابر با صفر باشند، یعنی

$$\Pr(\text{is_constant}) = \|\langle 0^n |_x |\psi_4\rangle\|^2 \quad (53-2)$$

$$= \left| \langle 0^n | H_x^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{o(i)} |i\rangle_x \right|^2 \quad (54-2)$$

$$= \frac{1}{2^n} \left| \left(\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \langle i| \right) \left(\sum_{i=0}^{2^n-1} (-1)^{o(i)} |i\rangle \right) \right|^2 \quad (55-2)$$

$$= \frac{1}{2^{2n}} \left| \sum_{i=0}^{2^n-1} (-1)^{o(i)} \right|^2 \quad (56-2)$$

تنها نکته ریاضیاتی استفاده شده در این اثبات این است که عملگرهای H می توانند از نظر ریاضی بر روی بردار ترانزاده/مزدوج $|0^n\rangle$ که در سمت راستشان قرار گرفته است اثر کنند.

در نتیجه می بینیم که برای حالتی که o مقدار ثابتی دارد، این احتمال برابر با یک و برای حالت متوازن این احتمال دقیقاً برابر با صفر است.

پس این الگوریتم که تنها یک بار از جعبه سیاه مذکور استفاده می کند، می تواند به شکل قطعی به مسئله پاسخ بدهد. [۱۴]

برای تشریح بیشتر آن چه که باعث این افزایش سرعت شد، می توان به این نکته اشاره کرد که همزمانی بررسی همه حالت ها، در کنار ابزاری که عملکردی مشابه تبدیل فوریه دارد (تبدیل هادامارد) که در فضای کوانتومی به سرعت پیاده سازی می شود، امکان این نتیجه گیری سریع را فراهم آورده است. اما به طور کلی، در این الگوریتم و الگوریتم های بعدی، آن چه عمومیت دارد، ساختاری شبیه به سیستم احتمالاتی است با این تفاوت که احتمالات منفی ای دارد که با هم می توانند تداخل سازنده یا مخرب داشته باشند.

الگوریتم زیرگروه آبدلی پنهان و کاربردهای آن

می‌دانیم که گروه محدود، به یک مجموعه محدود، مانند G و یک تابع که آن را ضرب گروه می‌نامیم و به شکل $G \times G \rightarrow G$: تعریف می‌شود می‌گوییم که خواص زیر را دارا باشد

- شرکت‌پذیری: برای هر $a, b, c \in G$ داشته باشیم $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

- عنصر همانی: وجود داشته باشد $I \in G$ که برای هر $g \in G$ داشته باشیم $g \cdot I = I \cdot g = 1$

- عنصر وارون: برای هر عنصری نظیر $g \in G$ داشته باشیم $g^{-1} \in G$ که $g \cdot g^{-1} = g^{-1} \cdot g = I$

- جابه‌جایی (تنها در گروه‌های آبدلی): برای هر $a, b \in G$ داشته باشیم $a \cdot b = b \cdot a$

همچنین زیرگروه، گروهی است که زیرمجموعه گروهی بزرگ‌تر با همان ضرب است و هم‌دسته^{۱۲} یک زیرگروه مانند H به مجموعه‌هایی می‌گویند که برای هر $g \in G$ به شکل زیر تعریف می‌شوند

$$gH = \{gh | h \in H\} \quad (57-2)$$

و مولدهای گروه، به کمینه عناصری می‌گویند که از بستار ضرب آن‌ها در خود، همه عناصر گروه به دست می‌آیند.

اگر گروهی محدود و آبدلی به نام G داشته باشیم و تابعی به شکل $f: G \rightarrow S$ نیز داده شده‌است که S یک مجموعه دلخواه است. اگر زیرگروهی به نام H وجود داشته‌باشد که برای f داشته‌باشیم که

$$f(x) = f(y) \Leftrightarrow xH = yH \text{ و } y \text{ در یک هم‌دسته زیرگروه } H \text{ قرار دارند} \quad (58-2)$$

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

پیش از بررسی دقیق الگوریتم، به بررسی تعمیم تبدیل فوری در فضای گروه‌های آبدلی محدود می‌پردازیم. بدون اشاره به تئوری بازنمایی گروه‌ها، مجموعه توابع $G \rightarrow \mathbb{C}$ را در نظر بگیرید، این توابع تشکیل یک فضای برداری را می‌دهند، یک پایه بدیهی برای این فضا، توابع زیر هستند

^{۱۲} coset

$$\delta_g(x) = \begin{cases} 1 & g = x \\ 0 & g \neq x \end{cases} \quad (۵۹-۲)$$

بدون اثبات بپذیریم که یک پایه نابدیهی برای این فضا، مجموعه توابعی هستند که خواص زیر را دارند [۴]

$$|\chi_k(x)| = 1 \quad (۶۰-۲)$$

$$\chi_k(I) = 1 \quad (۶۱-۲)$$

$$\chi_k(x \cdot y) = \chi_k(x) \cdot \chi_k(y) \quad (۶۲-۲)$$

که این اعداد k را نیز می‌توان با عناصر گروه جایگزین کرد اگر یک سری کمینه مولد برای G در نظر بگیریم و آن را $\text{gen}(G)$ بنامیم

$$\chi_I(x) = 1 \quad (۶۳-۲)$$

$$\chi_g(g') = e^{\delta_{gg'} \frac{2i\pi}{\text{order}(g)}} \quad \text{اگر } g, g' \in \text{gen}(G) \quad (۶۴-۲)$$

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

لازم به ذکر است که مرتبه g کوچک‌ترین عددی است که $g^{\text{order}(g)} = 1$ یا به عبارتی دیگر

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

آنچه گفته شد، تعریف دو پایه برای مجموعه توابع $\mathbb{C} \rightarrow G$ بود که همین دو پایه برای فضای حالت‌های کوانتومی سیستمی که حالت‌های کلاسیک آن همان عناصر G است نیز برقرار است. از این رو، می‌توان یک تحول یکانی در این فضا تعریف کرد که این تغییر پایه را صورت می‌دهد

$$\text{QFT} := \frac{1}{\sqrt{|G|}} \sum_{a,b} \chi_a(b) |b\rangle\langle a| \quad (۶۷-۲)$$

که این تعریف را تبدیل فوریه کوانتومی می‌گیریم. لازم به ذکر است که به ازای گروهی خاص، (\mathbb{Z}_2) برابر با تبدیل هادامارد خواهد بود.

الگوریتم زیر را در نظر بگیرید

الگوریتم ۲ زیرگروه پنهان

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

  x : Hilbert(G) state
  y : Hilbert(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 مرحله اول، ابتدا تلاش می‌شود که حالتی به شکل $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_x$ تولید شود که بر حسب شکل ذخیره‌سازی و ساختار گروه، به شکل‌های متفاوتی می‌توان این کار را انجام داد، اما آنچه با همین ابزار قابل پیاده‌سازی است، استفاده از تبدیل فوریه بر روی عنصر همانی است که این حالت را تولید می‌کند. سپس با اعمال f که تبدیل به عملیاتی یکانی شده، به حالتی به شکل زیر خواهیم رسید

$$|\psi_1\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_x |f(g)\rangle_y \quad (2-68)$$

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

$$|\psi_2\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |sh\rangle_x |f(s)\rangle_y \quad (2-69)$$

و پس از آن با اعمال تبدیل فوریه مذکور، خواهیم داشت

$$|\psi_3\rangle = \frac{1}{\sqrt{|H||G|}} \sum_{h \in H} \sum_{g \in G} \chi_{s \cdot h}(g) |g\rangle_x |f(s)\rangle_y \quad (70-2)$$

به سادگی می‌توان اثبات کرد که

$$\sum_{k=0}^{\text{order}(g)-1} \chi_{g^k}(x) = \begin{cases} \text{order}(g) & \chi_g(x) = 1 \\ 0 & \chi_g(x) \neq 1 \end{cases} \quad (71-2)$$

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

$$|\psi_3\rangle = \frac{1}{\sqrt{|H||G|}} \sum_{g \in G} \chi_s(g) \sum_{h \in H} \chi_h(g) |g\rangle_x |f(s)\rangle_y \quad (72-2)$$

$$= \frac{\sqrt{|H|}}{\sqrt{|G|}} \sum_{g \in H^\perp} \chi_s(g) |g\rangle_x |f(s)\rangle_y \quad (73-2)$$

که در رابطه فوق H^\perp باید به شکل زیر تعریف شود

$$H^\perp := \{g \mid \chi_h(g) = 1 \ \forall h \in H\} \quad (74-2)$$

نتیجه اندازه‌گیری آخر، همان نمونه‌گیری از گروه H^\perp است و با دانستن این گروه، خود گروه H نیز دانسته می‌شود. [۱۵] ۱۳

در ادامه، در یک مثال کاربردی، به یافتن دوره تناوب یک تابع می‌پردازیم که خود در تجزیه اعداد استفاده می‌شود. ۱۴

^{۱۳} شیوه یافتن مولدهای H با استفاده از H^\perp در حالت کلی خارج از این مقال است
^{۱۴} ارتباط مثال مذکور با تجزیه عدد N نیز به این صورت است که با دانستن r اگر r زوج باشد، آن‌گاه معادله زیر می‌تواند منتج به تجزیه عدد شود.

$$(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) \bmod N = 0 \quad (75-2)$$

مثال ۲-۶ (محاسبه دوره تناوب) فرض کنید گروه اصلی مسئله \mathbb{Z}_Q (با عمل جمع) باشد، آنگاه تابع f را به شکل زیر تعریف کنیم

$$f(x) = a^x \pmod{N} \quad (۷۶-۲)$$

که طبیعتاً اعداد a و N دانسته شده هستند به طوری که $\gcd(a, N) = 1$

حالا زیرگروهی که این تابع بر روی آن ثابت است $\{1, r, r^2, \dots, Q-r\}$ است اگر Q/r عدد صحیحی باشد.

اگر الگوریتم مذکور بر روی این مسئله اجرا شود، می‌دانیم که برای گروه گفته شده

$$\chi_a(b) = e^{2i\pi \frac{ab}{Q}} \quad (۷۷-۲)$$

که در نتیجه آن، برای هر حاصل اندازه گیری مانند m خواهیم داشت

$$\chi_r(m) = 1 \Rightarrow mr = kQ \quad (۷۸-۲)$$

که در آن k عددی نامعلوم اما صحیح است و اگر چندبار m را اندازه بگیریم، مسئله به دست آوردن r به مسئله باقی مانده چینی تبدیل می‌شود و قابل حل است.

تنها نکته باقی مانده این ضمانت است که $\frac{Q}{r}$ صحیح است که نشان داده شده حتی در صورت صحیح بودن این نسبت، با قیدهایی، این الگوریتم با احتمال خوبی همچنان به درستی عمل می‌کند. [۱۶]

الگوریتم‌های جست‌وجو، شمارش و تقویت

یک تابع به شکل $\mathbb{Z}_2 \rightarrow D$ داده شده است که از مجموعه محدود D به اعداد صفر و یک می‌رود. مسئله، پیدا کردن عنصر/عنصرهایی از D هستند که به ازای آن‌ها $f(s) = 1$. این مقادیر را مجموعه $T := \{s | f(s) = 1\}$ می‌نامیم و این مسئله را جست‌وجوی نامرتب نیز می‌توان نامید.

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

$$|D\rangle = \frac{1}{\sqrt{|D|}} \sum_{e \in D} |e\rangle \quad (۷۹-۲)$$

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

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

$$|T\rangle := \frac{1}{\sqrt{|T|}} \sum_{x \in T} |x\rangle \quad (۸۱-۲)$$

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

اگر فرض بگیریم مداری (تنها متشکل از گیت‌های پایه و بدون اندازه‌گیری) به نام G داریم که عملیات زیر را انجام می‌دهد، و طبیعتاً می‌توان انتظار داشت که وارون این مدار را نیز داشته باشیم

$$|D\rangle = G |e_1\rangle \quad (۸۲-۲)$$

که e_1 یک عنصر دلخواه و مشخص از مجموعه D باشد،

فرض می‌کنیم که f را نیز مشابه الگوریتم‌های قبل به شکل زیر داشته باشیم

$$F = \sum_{x \in D, y \in \mathbb{Z}_2} |x, y \text{ XOR } f(x)\rangle\langle x, y| \quad (۸۳-۲)$$

همچنین عجیب نیست که به هر شکلی که برای مجموعه D فضای هیلبرتی ساخته شود (برای مثال اگر در $\lceil \log_2 |D| \rceil$ کیوبیت کد شود)، به سادگی می‌توان تابع $\delta_{e_1}(x)$ را به شکل کوانتومی نیز پیاده کرد که عملگری یکانی در فضای $\text{Hilbert}(D \times \mathbb{Z}_2)$ به شکل زیر خواهد شد

$$\Delta_{e_1} = \sum_{x \in D, y \in \mathbb{Z}_2} |x, y \text{ XOR } \delta_{e_1}(x)\rangle\langle x, y| \quad (۸۴-۲)$$

$$= \sum_{x \in D - \{e_1\}, y \in \mathbb{Z}_2} |x, y\rangle\langle x, y| + \sum_{y \in \mathbb{Z}_2} |e_1, \text{NOT } y\rangle\langle e_1, y| \quad (۸۵-۲)$$

حالا الگوریتم زیر را در نظر بگیرید

```

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 مرحله اول، می‌توان با انجام عملیات زیر، این جعبه سیاه را به شکل دیگری تبدیل کرد

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

که در آن Z عملگری به شکل زیر است که بر روی کیوبیت خروجی تابع اثر می‌کند

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

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

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

نکته قابل توجه این است که مقدار y در طی همه این عملیات‌های F' و Δ'_{e_1} و همچنین $G \otimes I$ تغییر نمی‌کند، از این رو می‌توان فقط به تأثیر این عملگرها روی فضای x توجه کرد.

پس می‌توانیم بنویسیم

$$\langle \bullet |_y \text{mirrorT} | \bullet \rangle_y = \langle \bullet |_y F' | \bullet \rangle_y \quad (۸۹-۲)$$

$$= \sum_{e \in D} (-1)^{f(e)} |e\rangle \langle e|_x \quad (۹۰-۲)$$

$$= I - \mathfrak{P}_T \quad (۹۱-۲)$$

$$\langle \bullet |_y \text{mirrorS} | \bullet \rangle_y = \langle \bullet |_y (G \otimes I)^{-1} \Delta'_{e_1} (G \otimes I) | \bullet \rangle_y \quad (۹۲-۲)$$

$$= G^{-1} (I - \mathfrak{P} |e_1\rangle \langle e_1|) G \quad (۹۳-۲)$$

$$= I - \mathfrak{P} |D\rangle \langle D| \quad (۹۴-۲)$$

حالا تنها چیزی که باقی می‌ماند این است که تحول این بردار را بررسی کنیم

$$\begin{cases} |\psi_\bullet\rangle = |D\rangle \\ |\psi_{k+1}\rangle = (I - \mathfrak{P} |D\rangle \langle D|) (I - \mathfrak{P}_T) |\psi_k\rangle \end{cases} \quad (۹۵-۲)$$

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

$$|\psi_k\rangle = \alpha_k |D - T\rangle + \beta_k |T\rangle \quad (۹۶-۲)$$

که

$$|D - T\rangle = \frac{1}{\sqrt{|D - T|}} (\sqrt{|D|} |D\rangle - \sqrt{|T|} |T\rangle) \quad (۹۷-۲)$$

آنگاه

$$\begin{pmatrix} \alpha_{k+1} \\ \beta_{k+1} \end{pmatrix} = \left(\begin{pmatrix} 1 & \cdot \\ \cdot & 1 \end{pmatrix} - \mathfrak{P} \begin{pmatrix} \sqrt{\frac{|D-T|}{|D|}} \\ \sqrt{\frac{|T|}{|D|}} \end{pmatrix} \begin{pmatrix} \sqrt{\frac{|D-T|}{|D|}} & \sqrt{\frac{|T|}{|D|}} \end{pmatrix} \right) \begin{pmatrix} 1 & \cdot \\ \cdot & -1 \end{pmatrix} \begin{pmatrix} \alpha_k \\ \beta_k \end{pmatrix} \quad (۹۸-۲)$$

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

که با این تبدیل می‌توان نشان داد که پس از طی $\frac{\pi}{4\theta}$ مقدار β نزدیک به یک شده که به این ترتیب پس از اندازه‌گیری، احتمال دریافت یکی از عناصر داخل T یا همان عبارت $\|\mathbb{P}_T |\psi_k\rangle\|^2$ نزدیک به یک خواهد بود.

این الگوریتم، بیان دیگری نیز دارد که اگر برای یک زیرفضا، یک عملگر بازتابی مثل $\text{mirrorT} = I - 2\mathbb{P}_T$ داشته باشیم و یک حالت اولیه به نام $|\text{init}\rangle$ که عملگر بازتابی آن نیز وجود دارد (به بیان دیگر این حالت با مداری معلوم قابل تهیه است)، آنگاه می‌توان به حالت

$$|\text{final}\rangle = \frac{\mathbb{P}_T |\text{init}\rangle}{\|\mathbb{P}_T |\text{init}\rangle\|} \quad (2-100)$$

نزدیک شد. به این بیان، الگوریتم تقویت دامنه^{۱۵} می‌گویند.

الگوریتم‌های جبرخطی

احتمالاً حذف شود

الگوریتم‌های ولگشت

احتمالاً حذف شود

۲-۲-۳ شبیه‌سازی کلاسیک این سیستم‌ها

یکی از مسئله‌هایی که اشاره به آن اهمیت دارد، شبیه‌سازی مدارهای کوانتومی بر روی سیستم‌های کلاسیک است. در حالت کلی شبیه‌سازی این مدارها، آن‌چنان که قابل حدس است، به شکل توانی سخت خواهند بود اما ایده‌های مختلفی وجود دارند که هرکدام در شرایطی خاص نشان می‌دهند که شبیه‌سازی چندجمله‌ای امکان‌پذیر است و در آن شرایط، طبیعتاً مدارها نمی‌توانند به برتری‌ای نسبت به کامپیوترهای کلاسیک دست یابند.

^{۱۵}amplitude amplification

۳-۲ هندسه محاسباتی

هندسه محاسباتی، شاخه‌ای است که به بررسی مسئله‌های هندسی از نظر محاسباتی می‌پردازد و طبیعتاً درگیر پیچیدگی‌ها و کلاس‌های محاسباتی در کنار الگوریتم‌ها و ساختمان‌های داده می‌شود. در این مقال، بیشتر توجه معطوف به الگوریتم‌ها و ساختمان‌های داده است.

برای مطالعه‌ای مروری بر هندسه محاسباتی، ابتدا چند الگوریتم پایه‌ای و پرکاربرد را مرور می‌کنیم.

۱-۳-۲ الگوریتم‌های جاروب خطی/صفحه‌ای

این دسته الگوریتم‌ها که مبتنی بر ایده مشترکی کار می‌کنند کاربردهای گوناگونی از تشخیص برخورد پاره‌خط‌ها تا تشکیل دیاگرام ورونی (بحث شده در بخش ۲-۳-۸) دارند. بدون در نظر گرفتن جزئیات، این الگوریتم با استفاده از یک صف رخداد و یک درخت (یا هر داده ساختار دیگری) به نام وضعیت کار می‌کند. به این ترتیب که اگر خطی موازی محور y در نظر بگیریم که از $x \rightarrow -\infty$ به سمت $x \rightarrow \infty$ حرکت می‌کند، در طی این حرکت، همواره داده ساختار وضعیت را به روز نگه می‌دارد، به این ترتیب که نقاطی که ممکن است وضعیت تغییر کند را رخداد می‌نامیم و به محض کشف، آن‌ها را در صف رخداد قرار می‌دهیم و به ترتیب کم‌ترین x از صف رویدادها انتخاب می‌کنیم و خط را تا آن جا جلو می‌بریم و تغییر وضعیت را اعمال می‌کنیم.

برای مثال، در مسئله برخورد پاره‌خط‌ها (تعریف شده در ۱-۳)، وضعیت، یک درخت دودویی متوازن از عرض محل برخورد پاره‌خط‌ها با خط جاروب است که در شروع و پایان پاره‌خط‌ها و در نقاط تلاقی وضعیت تغییر می‌کند. می‌توان نشان داد که این الگوریتم در $O(N \log N + I \log N)$ برای N پاره‌خط که با هم I نقطه تلاقی دارند عمل می‌کند. ذکر این نکته خالی از لطف نیست که در این الگوریتم‌های هندسه محاسباتی، بستگی پیچیدگی الگوریتم به خروجی را به کرات می‌بینیم. به این دسته از الگوریتم‌ها حساس به خروجی^{۱۶} می‌گویند. [۱۷]

^{۱۶}output sensitive

۲-۳-۲ الگوریتم‌های برنامه‌ریزی خطی

طبیعی است که به دلیل وجود خط‌های راست در مسائل هندسی، بسیاری از مسائل به شکل برنامه‌ریزی‌های خطی یا برنامه‌ریزی‌های خطی تعمیم‌یافته^{۱۷} خواهند بود. برای مثال، هر پاره‌خط نظیر یک سه قید خطی است و به سادگی می‌توان متصور شد که مسئله وجود تلاقی پاره‌خط‌ها (تعریف‌شده در ۳-۱) یا اشیاء محدب به سادگی قابل تعبیر به مسئله امکان‌پذیری قیود برنامه‌ریزی خطی باشد. مثال دیگری از این دست مسئله کوچک‌ترین توپ شامل (تعریف‌شده در ۳-۱) است که به شکل برنامه‌ریزی خطی تعمیم‌یافته قابل بیان است. [۱۷]

۳-۳-۲ مسئله پوش محدب

احتمالاً حذف شود.

۴-۳-۲ مسئله مثلث‌بندی

مسئله مثلث‌بندی: یک N -ضلعی در صفحه با نقاط p_1 تا p_N مشخص شده‌اند، مطلوب است لیستی از مثلث‌های t_1 تا t_{N-2} به طوری که نقطه‌های مثلث‌ها همان نقاط چندضلعی باشند و مثلث‌ها بدون اشتراک و هم‌پوشانی همه چندضلعی را بپوشانند.

یک الگوریتم برای این مسئله، تقسیم چندضلعی به چندضلعی‌های یکنوا و پس از آن مثلث‌بندی است. [۱۷]

۵-۳-۲ ساختمان داده لیست یال‌های دوسویه متصل

۶-۳-۲ ساختمان داده درخت کی‌دی

۷-۳-۲ دوگانگی

۸-۳-۲ پیش‌پردازش‌های کاربردی، مثال دیاگرام ورونی

^{۱۷}generalized linear programming

فصل ۳

کارهای پیشین

۱-۳ الگوریتم‌های کوانتومی در هندسه محاسباتی

استفاده از ابزارِ رایانشِ کوانتومی در هندسه محاسباتی از بدو پیدایش این شاخه و توسعه الگوریتم‌های مشهور آن، مورد بررسی قرار گرفته [؟] اما با این حال تا امروزه ادبیات کاملاً محدودی وجود دارد که الگوریتم‌ها و حدهایی در آن به صورتِ موردی بررسی شده‌اند. هرچند تعداد این حدود و الگوریتم‌ها کم نیست اما هنوز تلاش‌ها در جهتِ تعمیم و کلیت‌بخشی به این گزاره‌ها چندان زیاد نبوده‌اند.

همچنین نکته مهمی که حائز اهمیت بیشتری است این است که بیشتر تلاش‌ها در این حوزه معطوف به استفاده از الگوریتم‌های جست‌وجو، شمارش و یا ولگشت‌های کوانتومی هستند که بهبود سرعتِ آن‌ها در نهایت می‌تواند به شکلِ مربعی^۱ باشد. و به نظر می‌رسد هنوز از الگوریتم‌هایی که بهبود سرعتِ توانی^۲ دارند در این حوزه استفاده‌ای نشده‌است. [؟][۱۸][۱۹][۲۰][؟]

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

از آن‌جا که هدف از این بررسی‌ها، بستگی پیچیدگی محاسباتی به پارامترهایی نظیر بعد و دقتِ ارقام نیست، در مرتبه الگوریتم‌ها و حدها ثابت فرض شده‌اند و نوشته نشده‌اند.

مسئله برخورد اجسام محدب: در فضای d -بعدی در نظر بگیرید که N شکل محدب داریم، هدف

^۱quadratic
^۲exponential

فهمیدن این است که آیا وجود دارد دوتایی از این اجسام که با هم تلاقی داشته باشند. [۹]

– الگوریتم کلاسیک:

– حد کلاسیک:

– الگوریتم کوانتومی:

– حد کوانتومی:

مسئله پوش محدب

مسئله چیدمان ابرصفحه‌ها^۳

مسئله محاسبه فاصله هاسدورف

مسئله نزدیک‌ترین زوج: N نقطه در فضای d -بعدی و یک تابع فاصله $d : \mathbb{R}^d \times \mathbb{R}^d \rightarrow \mathbb{R}^+$ داده شده‌اند، مطلوب است زوجی که کم‌ترین فاصله را دارند. [۲۱، فصل پنجم][۱۸]

– الگوریتم کلاسیک: با استفاده از تقسیم و حل، با $\Theta(N \log N)$ مقایسه (بین فاصله زوج نقاط) امکان حل وجود دارد. البته برای الگوریتم‌های تصادفی، الگوریتم با امید ریاضی تعداد مقایسه‌ها $\Theta(N)$ ممکن است.

– حد کلاسیک: با استفاده از یکتایی عناصر، مقایسه‌ها باید از مرتبه $\Omega(N \log N)$ باشند.

– الگوریتم کوانتومی: با استفاده از کاهش (با سربار لگاریتمی) به الگوریتم پیدا کردن کمینه کوانتومی، با $\Theta(N^{\frac{1}{2}} \log N)$ پرسش مقایسه، مسئله حل می‌شود.

– حد کوانتومی: با استفاده از یکتایی عناصر به شکل کوانتومی به حد $\mathcal{O}(N^{\frac{1}{2}})$ خواهیم رسید.

مسئله دورترین زوج: N نقطه در فضای d -بعدی و یک تابع فاصله $d : \mathbb{R}^d \times \mathbb{R}^d \rightarrow \mathbb{R}^+$ داده شده‌اند، مطلوب است زوجی که بیشترین فاصله را دارند.

نتایج آن مشابه مسئله نزدیک‌ترین زوج هستند. [۱۸]

^۳ arrangement of hyperplanes

مسئله نزدیک‌ترین زوج دورنگ: N نقطه آبی و M نقطه قرمز و یک تابع فاصله $d : \mathbb{R}^d \times \mathbb{R}^d \rightarrow \mathbb{R}^+$ داده شده‌اند، مطلوب است زوج ناهم‌رنگی که کم‌ترین فاصله را دارند. [۱۸] [۲۲]، Minimum [Geometric Spanning Trees]

- الگوریتم کلاسیک: با استفاده از زیردرخت پوششی کمینه هندسی، برای فاصله‌های خاصی نظیر L_1 در زمان $\mathcal{O}((N+M) \log(N+M))$ امکان حل وجود دارد.

با استفاده از الگوریتم‌های تصادفی نیز در زمان $\mathcal{O}((NM \log N \log M)^{\frac{1}{3}} + N \log^2 M + M \log^2 N)$ حل می‌شود.

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

- الگوریتم کوانتومی: به شکل تقریباً مشابهی با مسئله نزدیک‌ترین زوج، با تعداد پرسش مقایسه $\mathcal{O}((M+N)^{\frac{1}{3}} \log(M+N))$ حل می‌شود.

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

مسئله کوچک‌ترین توپ شامل: در فضای d -بعدی N نقطه داریم، مطلوب است یافتن ابرکره‌ای d -بعدی با کوچک‌ترین شعاع ممکن که همه نقاط داخل آن قرار بگیرند. [۱۷]، فصل چهارم [۱۸]

- الگوریتم کلاسیک: در فضای دوبعدی با اضافه کردن تدریجی نقاط، با امید ریاضی زمان $\Theta(N)$ این مسئله حل می‌شود. این الگوریتم که قابل تعمیم به همه مسئله‌های بهینه‌سازی LP-type است در ابعاد بالاتر نیز به درستی عمل می‌کند.

- حد کوانتومی: با کاهش این مسئله به مسئله OR حد پایین $\Omega(\sqrt{N})$ اثبات می‌شود.

مسئله وجود تلاقی پاره‌خطها: در فضای دوبعدی، N پاره‌خط داریم، مطلوب است این که وجود دارند دو پاره‌خطی که با هم تلاقی داشته باشند. [۱۷]، فصل دوم [۱۸]

- الگوریتم کلاسیک: با تکنیک‌های نظیر جاروب خطی (در بخش ۲-۳-۱) متعددی می‌توان در زمان $\mathcal{O}(N \log N)$ به جواب مسئله رسید.

– الگوریتم کوانتومی: با کاهش مسئله به یکتایی عناصر کوانتومی که خود با استفاده از ولگشت‌های کوانتومی حل می‌شود، مسئله با استفاده از $\Theta(N^{2/3})$ پرسش از موقعیت پاره‌خط‌ها حل می‌شود.

مسئله سه‌نقطه هم خط [۲۰]

۲-۳ مسئله قرارگیری نقطه در چندضلعی

مسئله قرارگیری نقطه در چندضلعی: تصور کنید در یک صفحه، نقطه p را داریم و N –ضلعی G که به ترتیب مشکل از نقاط q_0, \dots, q_{N-1} است.

اگر بدون هیچ پیش‌پردازشی، بخواهیم برای همین یک نقطه، بودن یا نبودن داخل چندضلعی را به دست بیاوریم، دو ایده مشهور وجود دارد. ایده نخست این است که اگر هر نیم‌خطی از این نقطه رسم کنیم، اضلاع چندضلعی را در فرد نقطه قطع می‌کند اگر و تنها اگر نقطه درون چندضلعی باشد.

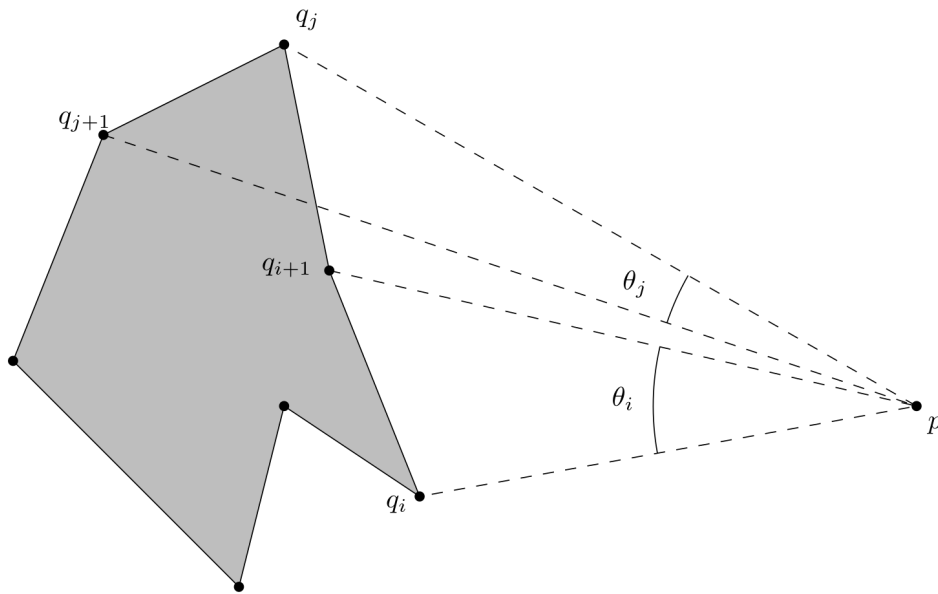
با این ایده می‌توان در مرتبه $\Theta(N)$ مسئله مذکور را حل کرد.

ایده دوم به این ترتیب است که اگر زاویه خط $q_i q_{i+1}$ از دید p را θ_i

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

$$\begin{cases} s_i = 0 & \text{اگر } p \text{ در سمت راست خط } q_i q_{i+1} \text{ باشد} \\ s_i = 1 & \text{اگر } p \text{ در سمت چپ خط } q_i q_{i+1} \text{ باشد} \end{cases} \quad (۱-۳)$$

^۴ لازم است برای حالتی که $i = N$ دقتی به خرج بدهیم که اگر جمع را به پیمانه N فرض کرده باشیم، تمام معادلات برای آن حالت نیز معتبر خواهند بود.



شکل ۳-۱: نمایش پارامترهای استفاده شده در الگوریتم

حالا می دانیم که مسئله قرارگیری نقطه در چندضلعی به مسئله قولی^۵ به شکل زیر تبدیل می شود.

$$\left| \sum \theta_i s_i \right| = \begin{cases} 2\pi & \text{نقطه داخل چندضلعی است} \\ 0 & \text{نقطه بیرون چندضلعی است} \end{cases} \quad (۲-۳)$$

که به این شکل با این ایده در مرتبه $\Theta(N)$ مسئله مذکور را حل کرد. البته برخلاف ایده قبل، نیاز به محاسبه توابع وارون مثلثاتی است که این کار، سرعت این الگوریتم را در واقعیت نسبت به الگوریتم قبلی کاهش می دهد و از همین رو به این ترتیب استفاده نمی شود. اما تصحیحاتی بر این الگوریتم وجود دارد که با استفاده از تقریب هایی دقت را کاهش می دهد اما امکان محاسبه سریع را می دهد. [۴]

فصل ۴

الگوریتم کوانتومی نقطه در چندضلعی

می‌بینیم صورت‌بندی ایده دوم که در فصل پیشین مطرح شد، شباهت زیادی به مسئله مربوط به الگوریتم دویچ-جوزا دارد، اما وجود وزن‌ها، امکان استفاده از الگوریتم دویچ-جوزا را به ما نمی‌دهد.

اما می‌دانیم اگر حالتی به شکل زیر داشته باشیم

$$|\phi_1\rangle := \frac{1}{\sqrt{N-1}} \sum_{q_i q_{i+1} \in \text{segments}} \kappa \theta_i s_i |q_i q_{i+1}\rangle \quad (1-4)$$

که در آن κ یک ضریب برای بهنجارسازی است، آنگاه با استفاده از تبدیل فوریه، می‌توانیم به حالتی برسیم که دامنه حالت $|\bullet\rangle$ یا همان عنصر همانی گروه، در آن به شکل زیر باشد

$$\langle \bullet | \text{QFT} | \psi \rangle = \frac{1}{N-1} \sum_{q_i q_{i+1} \in \text{segments}} \kappa \theta_i s_i \quad (2-4)$$

که از آن‌جا که برای هر تبدیل فوریه‌ای این مهم برقرار است، می‌توان به جای QFT قرار داد $H^{\otimes \log(N-1)}$ و فرض بگیریم که $N-1$ توانی از دو است.

پس برای احتمال اندازه‌گیری \bullet پس از تبدیل فوریه داریم

$$\Pr(\bullet \text{ اندازه‌گیری}) = \left| \langle \bullet | H^{\otimes \log(N-1)} | \psi \rangle \right|^2 = \begin{cases} \frac{4\kappa^2 \pi^2}{(N-1)^2} & \text{نقطه داخل چندضلعی است} \\ 0 & \text{نقطه بیرون چندضلعی است} \end{cases} \quad (3-4)$$

اما حالا ضریب κ مربوط به فرایند تولید این حالت است. اگر فرض کنیم ابتدا حالتی بسازیم که

$$|\phi_0\rangle = \frac{1}{\sqrt{N-1}} \sum_{q_i q_{i+1} \in \text{segments}} \theta_i s_i |q_i q_{i+1}\rangle \quad (4-4)$$

سپس به سادگی با استفاده اضافه کردن کیوبیت، از جعبه سیاه‌ها و تعمیم مدارهای کلاسیک، می‌توانیم به حالت زیر برسیم

$$|\phi_0\rangle = \frac{1}{\sqrt{N-1}} \sum_{q_i q_{i+1} \in \text{segments}} |q_i q_{i+1}\rangle |\arcsin \kappa \theta_i\rangle |s_i\rangle \quad (5-4)$$

و پس از آن با استفاده از ایده‌هایی مرسوم، نظیر ایده‌های استفاده شده در بخش ۲-۲-۲ به حالت $|\phi_1\rangle$ رسید.^۱

پس با توجه به نکات گفته شده لازم است که $\kappa \theta_i \leq 1$ که نتیجه می‌دهد بدیهی‌ترین انتخاب $\kappa = \frac{1}{\pi}$ باشد زیرا که زاویه یک پاره خط در مقابل یک نقطه حداکثر به نیم صفحه می‌رسد. در این صورت این احتمال نیز به شکل $O(\frac{1}{N^2})$ کوچک خواهد بود.

اما اگر قوی وجود داشته باشد که $\theta_i \leq \frac{\gamma}{N} \in O(\frac{1}{N})$ که هم‌ارز این قول است که نقاطی که بررسی می‌کنیم به اضلاع بیش از حد نزدیک نباشند و این فاصله از مرتبه طول اضلاع باشد، آن‌گاه می‌توان $kappa$ را برابر $\frac{N}{\gamma\pi}$ قرار داد که در نتیجه احتمال تشخیص نقطه درون چندضلعی در معادله ۴-۳ برابر با عددی ثابت خواهد شد که این یعنی با در این حالت تنها با یک پرسش می‌توان با خطای محدود به پاسخ مسئله رسید.

این الگوریتم را می‌توان به شکل زیر بازنویسی کرد

^۱ ایده تبدیل s_i به $(-1)^{s_i}$ دقیقاً مشابه آن چیزی است که در بخش مذکور بحث شد، همچنین برای قسمت θ_i یک فرض طبیعی این است که مقدار $\arcsin(\kappa \theta_i)$ در چندکیوبیت به شکل دودویی ذخیره شده است و آن را می‌توان به شکل $r_{\gamma d} r_{\gamma d-1} \dots r_{\gamma 1}$ که یکان و دوگان و الی آخر باشند. سپس، یک گیت شناخته شده و قابل پیاده‌سازی که به طور معمول در مدارهای کوانتومی نظیر تبدیل فوری برای گروه‌های عددی استفاده می‌شود، گیت $C-R_x$ است که عملکرد آن به شکل زیر است

$$\begin{cases} C-R_x |1\rangle |0\rangle = |1\rangle (\cos(x)|0\rangle + \sin(x)|1\rangle) \\ C-R_x |1\rangle |0\rangle = |0\rangle |0\rangle \end{cases} \quad (6-4)$$

حالا با در دست داشتن مدارهایی از این جنس، می‌توان حالت مذکور را تدارک دید. یک نکته مهم فرایند پاک کردن اطلاعات کیوبیت‌های مورد استفاده θ_i و s_i که با استفاده دوباره از جعبه سیاه ممکن می‌شود و کیوبیت‌های مذکور به حالت صفر و جدا می‌روند و می‌توان آن‌ها را از فرایند حذف 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

```

۴-۱ گسترش الگوریتم برای حالت‌های دیگر

می‌دانیم که برای عملکرد درست الگوریتم لازم است که احتمالی که در معادله ۴-۳ افزایش یابد و به مقدار ثابتی برسد. از این رو، می‌توان از الگوریتم تقویت دامنه که در بخش ۲-۲-۲ تعریف شده است کمک بگیریم. اگر کل فرایند الگوریتم قبل را تا پیش از اندازه‌گیری G بنامیم، همچنین \mathbb{P}_T را تصویر بر روی عدد ۰ باشد (که احتمال آن مورد نظر است)، آن را تقویت کرد. تعداد مراحل لازم برای این تقویت از مرتبه $\mathcal{O}(\frac{N}{\kappa})$ خواهد بود که این نشان می‌دهد اگر κ عدد ثابتی باشد، این الگوریتم هیچ تسریعی نمی‌تواند داشته باشد.

فصل ۵

نتیجه گیری

در این پایان نامه سعی شد که به بررسیِ رایانشِ کوانتومی و هندسهٔ محاسباتی و تلاقیِ این دو حیطه پرداخته شود. آنچه به نظر می‌رسد این است که تلاش‌های کمی در ترکیبِ این دو حوزه صورت گرفته حال آن که به علتِ شکلِ مسائل در هندسه و وجودِ قول‌های متعددی که به خاطرِ ذاتِ هندسیِ مسائل، پتانسیل‌های زیادی برای بررسیِ مسائل و البته جمع‌بندی و تعمیمِ راه‌حل‌ها و الگوریتم‌ها وجود دارد.

از سوی دیگر، همان‌طور که گفته شد، اکثرِ تلاش‌هایی که برای طراحیِ الگوریتم و حدود صورت گرفته است مبتنی بر استفاده از الگوریتمِ جست‌وجو بوده‌اند و از این رو، اکثرِ نتایجِ بهبودهای مربعی و چندجمله‌ای هستند. اما این کار از جهتِ استفاده از الگوریتم‌هایی با تسریعِ فرا-چندجمله‌ای (که مبتنی بر تبدیلِ فوریِ کوانتومی هستند) می‌تواند متفاوت و مفید قلمداد شود.

۱-۵ کارهای آتی

پیوست آ

مطالب تکمیلی

آ-۱ شبه کدهای 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. [Homepage of VK](#), 2021.
- [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. Bäertschi, 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] Quantum algorithm zoo.
- [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.
- [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] N. Volpato. Bounds for quantum computational geometry problems. page 12.
- [19] M. Lanzagorta and J. Uhlmann. Quantum algorithmic methods for computational geometry. 20(6):1117–1125. Publisher: Cambridge University Press.
- [20] A. Ambainis and N. Larka. Quantum algorithms for computational geometry problems.
- [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

ب

پ

Abstract

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