



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 و پس از معرفی دو الگوریتم جست‌وجو و تجزیه عدد، مورد توجه قرار گرفته است. از سوی دیگر، هندسه محاسباتی که به بررسی مسائل هندسی از منظر رایانشی 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 به شکل استفاده از الگوریتم جست‌وجوی کوانتومی بر روی مسائل بوده است که با تسریع چندجمله‌ای همراه است. مسئله قرارگیری نقطه در چندضلعی که یکی از مسائل پرکاربرد این حوزه است که تا کنون به شکل کوانتومی بررسی نشده و با رایانش کلاسی چند الگوریتم با زمان مرتبه خطی برای آن وجود دارد. در این پایان‌نامه به معرفی الگوریتمی کوانتومی برای نقطه در چندضلعی می‌پردازیم که مبتنی بر تبدیل فوری کوانتومی ست 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. همچنین نشان داده می‌شود که هیچ الگوریتم کوانتومی‌ای برای این مسئله نمی‌تواند به تسریع در حالت کلی دست بیابد.

**کلیدواژه‌ها:** رایانش کوانتومی، هندسه محاسباتی، نقطه-در-چندضلعی، تبدیل فوری کوانتومی

# فهرست مطالب

۹	۱ مقدمه
۱۰	۱-۱ تعریفِ موضوع
۱۰	۲-۱ اهمیتِ موضوع
۱۰	۳-۱ ساختار پایان‌نامه
۱۱	۲ مفاهیم اولیه
۱۱	۱-۲ حالت‌های کلاسیک و کوانتومی
۱۱	۲-۱-۱ زنجیرهٔ مارکوفی
۱۴	۲-۱-۲ گزاره‌های کوانتومی
۲۰	۳-۱-۲ تفاوت‌های سیستم‌های کوانتومی و کلاسیک
۲۲	۲-۲ رایانش کوانتومی و کلاسیک
۲۲	۱-۲-۲ مدل رایانش
۲۷	۲-۲-۲ الگوریتم‌های پایه‌ای در رایانش کوانتومی
۴۰	۳-۲-۲ شبیه‌سازی کلاسیک این سیستم‌ها
۴۰	۳-۲ هندسهٔ محاسباتی
۴۱	۱-۳-۲ الگوریتم‌های جاروب خطی/صفحه‌ای

۴۲	۲-۳-۲ الگوریتم‌های برنامه‌ریزی خطی
۴۲	۳-۳-۲ مسئله مثلث‌بندی
۴۳	۴-۳-۲ ساختمان داده لیست یال‌های دوسویه متصل
۴۴	۵-۳-۲ ساختمان داده درخت کی‌دی
۴۵	۶-۳-۲ دوگانگی
۴۶	۷-۳-۲ پیش‌پردازش‌های کاربردی، مثال دیاگرام ورونی
۴۷	۳ کارهای پیشین
۴۷	۱-۳ الگوریتم‌های کوانتومی در هندسه محاسباتی
۴۸	۱-۱-۳ مسائل مربوط به تحذب
۴۹	۲-۱-۳ مسائل مربوط به برخورد و اشتراک
۵۲	۳-۱-۳ مسائل مربوط به مجاورت
۵۳	۲-۳ مسئله قرارگیری نقطه در چندضلعی
۵۵	۴ بحث و نتایج نو
۵۵	۱-۴ معرفی یک الگوریتم کوانتومی
۵۸	۲-۴ گسترش الگوریتم برای حالت‌های دیگر
۵۸	۳-۴ حد پایین دشمن‌گونه
۶۱	۵ نتیجه‌گیری
۶۲	۱-۵ کارهای آتی

# فهرست شکل‌ها

- ۱-۲ نمایشی از الگوریتم جاروبِ خطی برای مسئلهٔ تلاقیِ پاره‌خط‌ها که رخدادها با  $e_i$  و داده‌های وضعیت با  $s_i$  مشخص شده‌اند . . . . . ۴۲
- ۲-۲ مثالی از مسئلهٔ مثلث‌بندی و پاسخِ آن . . . . . ۴۳
- ۳-۲ مثالی از دیاگرامِ ورونی برای شش نقطه در صفحه . . . . . ۴۶
- ۱-۳ نمایشِ پارامترهای استفاده شده در الگوریتم . . . . . ۵۴

## فهرست جدول‌ها



# فصل ۱

## مقدمه

از مطرح شدن ایده رایانه کوانتومی توسط فاینمن [۱] بیش از نیم قرن می‌گذرد اما عمده توجه‌ها به آن پس از دو الگوریتم مشهور شور [۲] و گروور [۳] در دهه نود میلادی بوده‌است. از آن روز تلاش بی‌وقفه‌ای برای یافتن الگوریتم‌های جدید و کاربردهای جدید از الگوریتم‌های قدیمی رایانش کوانتومی ادامه دارد. در همان سال‌ها نخستین آزمایش‌های موفق مربوط به رایانش کوانتومی انجام گرفت [۴] و تا امروز، هرچند رایانه‌های کوانتومی به شکل تجاری وجود ندارند، اما با ایده‌های متعددی مبتنی بر فوتونیک، مدارهای ابررسانا یا غیره، در ابعاد ۱۰ تا ۱۰۰ کیوبیت<sup>۱</sup> ساخته شده‌اند. در سال ۲۰۱۹ نیز برای اولین بار، آزمایش برتری کوانتومی انجام شد. [۵] این آزمایش به این معنی است که محاسباتی انجام بگیرد که توسط هیچ رایانه کلاسیکی ممکن نباشد.

با این همه، تا کنون تلاش‌های اندکی در بررسی مسائل هندسه محاسباتی در سیاق رایانش کوانتومی صورت گرفته‌است. هرچند که 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 می‌کنند، رایانش کوانتومی کاربردهایی بسیار گسترده‌تر از آنچه تا کنون شناخته شده است در این حوزه داشته باشد.

---

<sup>۱</sup> معادل کوانتومی بیت

## ۱-۱ تعریف موضوع

موضوع این پایان نامه، در مرحله اول، بررسی کاربردهای شناخته شده الگوریتم های کوانتومی در هندسه محاسباتی و در مرحله بعد معرفی الگوریتم جدیدی برای مسئله نقطه در چندضلعی است. مسئله نقطه در چندضلعی، به این صورت است که چندضلعی ای در صفحه و یک نقطه در صفحه مشخص شده اند، مایلیم بدانیم که آیا نقطه درون چندضلعی قرار گرفته است یا بیرون آن. بیان ریاضی این مسئله در بخش ۲-۳ صورت خواهد گرفت.

## ۲-۱ اهمیت موضوع

اهمیت این مسئله، از دو جهت قابل بررسی است، یکی این که مسئله نقطه در چندضلعی، در هندسه محاسباتی مسئله مهمی است و از سوی دیگر کاربردهای گوناگونی در سیستم های اطلاعات جغرافیایی، گرافیک کامپیوتری و غیره دارد، از این رو تسریع در آن می تواند تفاوت های گوناگونی در فرایندهای مرسوم در این حوزه ها ایجاد کند.

از سوی دیگر، بررسی رایانه های کوانتومی و الگوریتم های آن ها هم اکنون از اهمیت زیادی برخوردار است، از این رو که قابلیت های این رایانه ها برای کاربردهای آینده نزدیک و دور شناسایی شود. رایانه های کنونی و تا آینده ای نزدیک، قابلیت حذف نطفه را ندارد و هر الگوریتمی که نسبت به آن تاب آوری داشته باشد، می تواند در ردیف اولین کاربردهای رایانش کوانتومی قرار بگیرد.

## ۳-۱ ساختار پایان نامه

این پایان نامه در پنج فصل به این موضوع می پردازد به این ترتیب که پس از مقدمه، در فصل اول مفاهیم اولیه رایانش کوانتومی و هندسه محاسباتی مرور می شود و پس از آن در فصل مروری بر ادبیات الگوریتم های کوانتومی هندسه محاسباتی صورت می گیرد. سپس برای الگوریتم نقطه - در - چندضلعی الگوریتم های کلاسیک بررسی می شوند و در فصل چهارم الگوریتم کوانتومی ای تشریح می شود. در نهایت در فصل آخر به جمع بندی و مسیرهای پیشنهادی برای پژوهش های آتی پرداخته می شود.

## 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. [۶]

## 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  $i$  ام 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 گزار 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. [۷]

### 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 گزاره‌های 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  $U \in SU(n)$ <sup>۱</sup> 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

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

<sup>۱</sup>  $SU(n)$  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 «فروریزش» 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.<sup>۲</sup>

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  $\frac{1}{2}$ <sup>۳</sup> 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<sup>۴</sup> را اثبات کرد.

<sup>۳</sup> 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

<sup>۳</sup> 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.

<sup>۴</sup> اصل عدم قطعیت، اصلی است که بیان می‌کند هرگونه اندازه‌گیری‌ای که مکان و تکانه را به ترتیب با خطای  $\Delta x$  و  $\Delta p$  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 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 مانند  $\lambda$  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 حالت 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<sup>۵</sup> 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. [۸، ناموضعیت در مکانیک کوانتومی]

## ۲-۲ رایانش کوانتومی و کلاسیک

### ۱-۲-۲ مدل رایانش

نمایش ۳ یک الفبا مانند  $\Sigma$ ، 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  $\Sigma^2$  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  $|.$  طول آن را بیان می‌کند.

<sup>۵</sup> اندازه‌گیری 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 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 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  $P/\text{poly}$  است.

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

**مثال ۲-۵ (قدرت خانواده مدار)** فرض کنید مسئله  $h$  به شکل  $h: \mathbb{Z}_2^* \rightarrow \mathbb{Z}_2$  برای ماشین تورینگ غیر قابل محاسبه است. (می‌دانیم چنین مسئله‌ای وجود دارد)

می‌دانیم که به ازای هر  $s \in \mathbb{Z}_2^*$  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  $f: \mathbb{Z}_2^* \rightarrow \mathbb{Z}_2$  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 سر نخ است (و از مسئله  $f$  آسان‌تر است) عضو کلاس  $P$  باشد می‌گوییم که مسئله  $f$  خود عضو 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 عضو  $P$  باشد و داشته باشیم

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

آن‌گاه  $f$  عضو کلاس BPP است. [۹] <sup>۶</sup>

### مدارهای کوانتومی

حالا تصور کنید به سیستم  $d$ -حالت کوانتومی داریم. به این سیستم «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 [۱۰]

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

<sup>۶</sup> 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.

• گره اندازه‌گیری: یک اندازه‌گیری در پایه  $|0\rangle$  و  $|1\rangle$  انجام می‌شود که طبیعتاً درجه ورودی آن یک و درجه خروجی آن نیز یک است.

یکی از مشهورترین مجموعه گیت‌های پایه مجموعه گیت  $H$  از مثال ۲-۳ و همچنین  $T$  و  $CNOT$  است که به شکل زیر تعریف می‌شوند. [۱۱]

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

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

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 می‌شوند و همچنین تعریف خانواده مدار و یکنواختی نیز به همین ترتیب تعمیم داده می‌شود.

### کلاس‌های محاسباتی کوانتومی

به شکل مشابهی، برای مسئله‌ای به شکل  $f: \{0, 1\}^* \rightarrow \{0, 1\}$  داریم<sup>۷</sup> که اگر با خانواده یکنواختی از مدارهای کوانتومی، به نام  $Q$  قابل محاسبه باشند، به طوری که  $\text{size}(Q_i) \in \mathcal{O}(\text{poly}(i))$  آن‌گاه می‌گوییم که این مسئله عضو کلاس  $EQP$ <sup>۸</sup> 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

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

آنگاه می‌گوییم که مسئله در کلاس  $BQP$  قرار دارد.

<sup>۷</sup> می‌دانیم که مدارهای کوانتومی، فضای مبدا و مقصد یکسانی دارند، از این رو، پیاده‌سازی تابعی به شکل فوق، می‌تواند به این شکل انجام بگیرد که ورودی به شکل کوانتومی داده می‌شود و پس از انجام یک عملیات یکانی، بر روی یک کیوبیت خاص، اندازه‌گیری رخ می‌دهد و حاصل اندازه‌گیری به عنوان خروجی سیستم لحاظ می‌شود.

<sup>۸</sup> exact quantum polynomial

در این جا بدون اثبات، چند گزاره درخصوص کلاس های محاسباتی گفته شده را بررسی می کنیم. [۱۲] [۱۳]

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

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

$$NP \not\subseteq BQP \quad (۴۵-۲)$$

$$NP \not\subseteq BQP \quad (۴۶-۲)$$

## ۲-۲-۲ الگوریتم های پایه ای در رایانش کوانتومی

برای بررسی الگوریتم های کوانتومی، نیاز به شیوه ای برای بیان آن ها داریم، هرچند تلاش های بسیاری برای طراحی زبان ها و حساب ها برای رایانش کوانتومی صورت گرفته، اما برای حفظ یک پارچگی با شیوه بیان الگوریتم های کوانتومی، از شیوه های نموداری، نظیر شکل مدار کوانتومی و حساب ZX استفاده نمی کنیم. [۱۰] [۱۴] [۱۵] ذکر این نکته هم لازم است که روش های شکلی تعمیم پذیر نیستند. از طرفی زبان های کوانتومی اغلب ساختار مشترکی در خصوص ساختار داده ها و عملیات های کوانتومی دارند اما از نظر عملیات های کلاسیک، تفاوت های بسیاری دارند. از این رو برای تشریح الگوریتم های کوانتومی از شبه کد کمک خواهیم گرفت. ساختار این شبه کد خود گویاست و تنها از دو گونه حالت، به نمایندگی از فضای حالت های یک زیرسیستم کوانتومی و گیت، به عنوان یک تحول یکانی بر روی یک زیرسیستم استفاده می کند. عبارت  $\text{Apply } X \text{ on } Y$  تحول  $X$  را بر روی زیرسیستم  $Y$  اعمال می کند و  $\text{Measure } Y$  حالت زیرسیستم  $Y$  را در پایه مربوطه اندازه گیری می کند.

ذکر این نکته لازم است که الگوریتم های کوانتومی گسترده ای برای کاربردهای متنوعی وجود دارند [۱۶] [۱۷] [۱۸] اما در این مقال، تمرکز بر روی الگوریتم های پایه ای خواهند بود که به زعم نویسنده می توانند کاربردی در مسائل هندسه محاسباتی داشته باشند.

## الگوریتم دویچ-جوزا

اگر جعبه‌سیاهی داشته‌باشیم که مدار تابع  $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2^n : o$  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  $o(x) = 1$  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 خانواده‌ی مدارها، قابل تصور است که برای جواب قطعی، نیاز به حداقل  $1 + 2^{n-1}$  بار استفاده از جعبه‌سیاه 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 (وارون‌پذیری و یکی بودن فضای مبدأ و مقصد) را داشته‌باشیم، 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 شده‌است که  $n$  کیوبیت اول، نقش ورودی  $o$  را دارند و کیوبیت آخر، محل ذخیره خروجی  $o$  است.

حالا شبه‌کدی مانند ۱ را در نظر بگیرید.

## 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 : integer from 1 to n
    result : boolean = Measure 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. [۱۰]

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 یک زیرگروه مانند  $H$  به مجموعه‌هایی می‌گویند که برای هر  $g \in G$  به شکل زیر تعریف می‌شوند

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

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 داشته باشد که برای  $f$  داشته باشیم که

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

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

$$\delta_g(x) = \begin{cases} 1 & g = x \\ 0 & g \neq x \end{cases} \quad (2-59)$$

بدون اثبات بپذیریم که یک پایه نابدیهی برای این فضا، مجموعه توابعی هستند که خواص زیر را دارند [۱۹]

$$|\chi_k(x)| = 1 \quad (۶۰-۲)$$

$$\chi_k(I) = 1 \quad (۶۱-۲)$$

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

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  $G \rightarrow \mathbb{C}$  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 y

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

  // stage 4, select a generator
  Measure 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 برحسب 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

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

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. [۲۰]<sup>۹</sup>

در ادامه، در یک مثال کاربردی، به یافتن دوره تناوب یک تابع می‌پردازیم که خود در تجزیه اعداد استفاده می‌شود. <sup>۱۰</sup>

**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

$$f(x) = a^x \pmod{N} \quad (76-2)$$

<sup>۹</sup> شیوه یافتن مولدهای  $H$  با استفاده از  $H^\perp$  در حالت کلی خارج از این مقال است  
<sup>۱۰</sup> 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.

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

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  $\{0, r, 2r, \dots, Q-r\}$  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 نبودن این نسبت، با قیدهایی، این الگوریتم با احتمال خوبی همچنان به درستی عمل می‌کند. [۲]

### الگوریتم‌های جست‌وجو، شمارش و تقویت

یک تابع به شکل  $D \rightarrow \mathbb{Z}_2$  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

## الگوریتم ۳ جست و جو

```

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 / THETA / 4) {
        Apply mirrorT on x, y
        Apply mirrorD on x, y
    }

    result: D = Measure x
    return result
}

```

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

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

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  $\Delta'_{e_1} = \Delta_{e_1}(I_x \otimes Z_y)\Delta_{e_1}$

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

نکته قابل توجه این است که مقدار  $y$  در طی همهٔ این عملیات‌های  $F'$  و  $\Delta'_{e_1}$  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  $\beta$  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. از این رو، مرتبه این الگوریتم  $\mathcal{O}(\sqrt{T/D})$  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

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

نزدیک شد. به این بیان، الگوریتم تقویت دامنه می‌گویند. [۳]

### الگوریتم‌های جبرخطی

یکی دیگر از الگوریتم‌های پایه‌ای و مشهور در رایانش کوانتومی، الگوریتم‌های جبرخطی برای داده‌های نهان‌شده دامنه‌ای<sup>۱۱</sup> هستند که مشهورترین الگوریتم آن‌ها الگوریتم اچ‌اچ‌ال برای حل معادلات خطی است [۲۱]. علی‌رغم تسریع فراچندجمله‌ای این الگوریتم‌ها، شیوه دریافت ورودی و بازگشت خروجی از آن‌ها محل بحث است و هنوز مقیاس‌پذیر بودن آن و به‌صرفه بودن آن برای کاربردهای مختلف پذیرفته‌شده نیست. از این رو از بحث جزئیات آن پرهیز می‌کنیم.

### الگوریتم‌های ولگشت

همچنان که در الگوریتم‌های تصادفی کلاسیک از ولگشت استفاده‌های فراوانی می‌شود، در الگوریتم‌های کوانتومی نیز ولگشت می‌تواند ابزار مهمی باشد که حتی در شرایطی منجر به تسریع‌های فراچندجمله‌ای بشود. [۲۲] برای پرهیز از پیچیدگی و اطناب بررسی الگوریتم‌های مبتنی بر ولگشت، به تشریح ایده آن‌ها بسنده می‌کنیم. البته این ایده در همه الگوریتم‌ها به شکل یکسان دیده نمی‌شود. در نظر بگیرید حالت<sup>۱۱</sup> نهان‌سازی دامنه‌ای به فرایندی می‌گویند که در طی آن، داده‌ای به شکل  $(x_1, \dots, x_n)$  را در حالتی کوانتومی به شکلی ذخیره کنیم که داده‌ها، در دامنه حالت‌ها قرار بگیرند.

$$|\psi\rangle = \gamma \sum x_i |i\rangle \quad (۲-۱۰۱)$$

طبیعتاً نیاز به بهنجارش وجود دارد که در این صورت  $\gamma$  ضریب بهنجارش است.

کوانتومی ای داریم که بر روی پایه‌ای به بزرگی اعداد صحیح تعریف شده است

$$|\phi, \bullet\rangle := |\bullet\rangle \in W := \text{Hilbert}(\mathbb{Z}) \quad (102-2)$$

حالا تصور کنید یک کیوبیت به نام  $C$  (سکه) در کنار این حالت قرار می‌دهیم

$$|\phi, \bullet\rangle |C\rangle = \frac{1}{\sqrt{2}} |\bullet\rangle_W \otimes (|\bullet\rangle_C + |\uparrow\rangle_C) \quad (103-2)$$

اگر تحولی به شکل زیر در نظر بگیریم

$$S = \sum_i |i + \uparrow\rangle\langle i|_W |\uparrow\rangle\langle \uparrow|_C + \sum_i |i - \uparrow\rangle\langle i|_W |\bullet\rangle\langle \bullet|_C \quad (104-2)$$

می‌بینیم که این تحول و این حالت‌ها، شبیه به یک ولگشت عمل می‌کنند. هرچند این ولگشت تفاوتی با ولگشت‌های کلاسیک ندارد اما با تغییر  $|C\rangle$  به  $(|\bullet\rangle - |\uparrow\rangle)/\sqrt{2}$  شاهد تفاوت‌ها خواهیم بود. [۲۳]

## ۳-۲-۲ 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.

## 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.

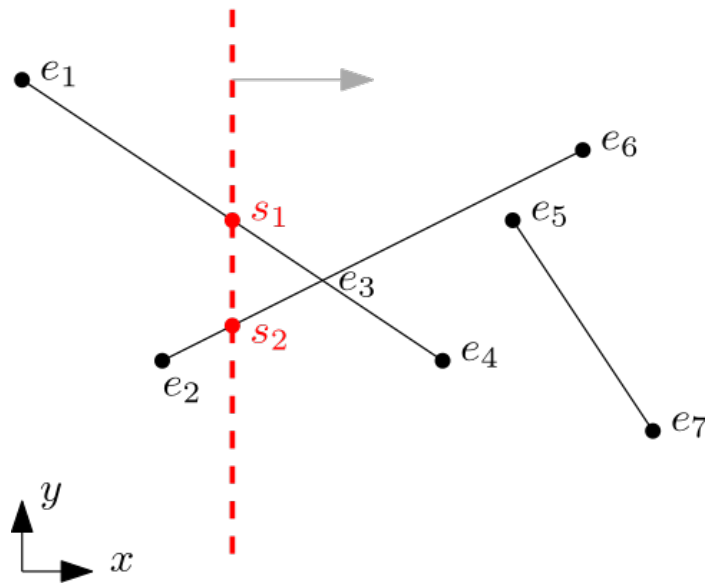
برای مطالعه‌ای مروری بر هندسه محاسباتی، ابتدا چند الگوریتم پایه‌ای و پرکاربرد را مرور می‌کنیم.



## ۲-۳-۱ 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 ۲-۳-۷) دارند. بدون در نظر گرفتن جزئیات، این الگوریتم با استفاده از یک صف رخداد و یک درخت (یا هر داده‌ساختار 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 داده‌ساختار وضعیت را به‌روز 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 آن‌جا جلو می‌بریم و تغییر وضعیت را اعمال می‌کنیم.

برای مثال، در مسئله برخورد پاره‌خط‌ها (تعریف شده در ۲-۳-۱)، 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» می‌گویند. [۲۴]



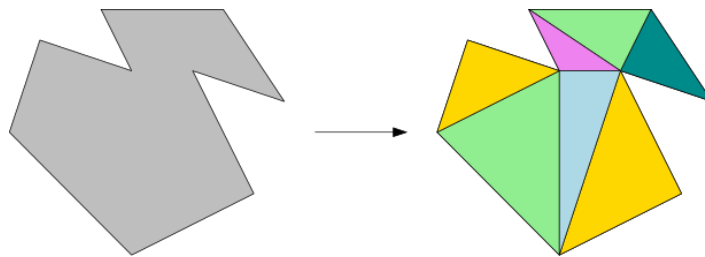
شکل ۲-۱: نمایشی از الگوریتم جاروب خطی برای مسئله تلاقی پاره‌خط‌ها که رخدادها با  $e_i$  و داده‌های وضعیت با  $s_i$  مشخص شده‌اند

### 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 خواهند بود. برای مثال، هر پاره‌خط نظیر یک سه‌قید خطی است و به سادگی می‌توان متصور شد که مسئله وجود تلاقی پاره‌خط‌ها (تعریف‌شده در ۲-۱-۳) 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 ۱-۱-۳) است که به شکل برنامه‌ریزی خطی تعمیم‌یافته قابل بیان است. [۲۴]

### ۲-۳-۳ 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.



شکل ۲-۲: مثالی از مسئله مثلث‌بندی و پاسخ آن

جواب این مسئله یکتا نیست و هرچندضلعی ممکن است به شیوه‌های گوناگونی مثلث‌بندی شود. از این رو مسائلی سخت‌تر از مثلث‌بندی وجود دارند که جواب مشخصی دارند، نظیر مثلث‌بندی‌ای که مجموع طول اضلاع مثلث‌ها کمینه شود که آن را مثلث‌بندی کمینه‌وزن می‌نامند. [۲۵]

یک الگوریتم برای این مسئله، تقسیم چندضلعی به چندضلعی‌های یکنوا و پس از آن مثلث‌بندی است که پیچیدگی زمانی  $O(N \log N)$  خواهد داشت.

مسئله مثلث‌بندی به عنوان یک پیش‌پردازش کاربردی برای حل مسئله وجود نقطه در چندضلعی (تعریف شده در ۲-۳) یا دیگر مسائل برخورد نظیر دنبال کردن پرتو استفاده می‌شود و از این رو اهمیت فراوانی در هندسه محاسباتی و گرافیک کامپیوتری دارد. [۲۴]

## ۲-۳-۴ ساختمان داده لیست یال‌های دوسویه متصل

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

این افراز صفحه را می‌توان به شکل یک گراف مسطح دید که بر روی آن گره‌ها، یال‌ها و ناحیه‌ها همان نقاط، پاره‌خط‌ها و چندضلعی‌ها هستند که افرازهای صفحه را تشکیل می‌دهند. این گراف غیرجهت‌دار خواهد بود اما می‌توانیم هر یال آن را با دو یال جهت‌دار که در جهت عکس یکدیگر قرار گرفته‌اند جایگزین کنیم و به هر یال این گراف جدید «نیم‌یال» می‌گوییم. دلیل این تعریف آن است که آن‌گاه ناحیه چپ هر نیم‌یال را می‌توانیم به شکل دقیقی تعریف کنیم.

این داده‌ساختار متشکل از سه لیست است:

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

- تابع  $\text{Coordinates}(v)$  که مختصات نقطه  $v$  را بازمی‌گرداند.
  - تابع  $\text{IncidentEdge}(v)$  که نیم‌یالی دلخواه را بازمی‌گرداند که نقطه شروعش  $v$  باشد.
۲. لیستی از نیم‌یال‌ها که برای هر نیم‌یال توابع زیر تعریف شده‌اند
- تابع  $\text{Origin}(e)$  که نقطه شروع نیم‌یال را مشخص می‌کند.
  - تابع  $\text{Twin}(e)$  که نیم‌یالی را بازمی‌گرداند که دقیقاً برعکس  $e$  است.
  - تابع  $\text{IncidentFace}(e)$  ناحیه‌ای که در چپ نیم‌یال قرار گرفته‌است را بازمی‌گرداند.
  - تابع  $\text{Next}(e)$  نیم‌یالی را بازمی‌گرداند که شروعش نقطه پایان  $e$  باشد و ناحیه سمت چپ این دو نیم‌یال با هم یکی باشد.
  - تابع  $\text{Prev}(e)$  نیم‌یالی را بازمی‌گرداند که پایانش نقطه شروع  $e$  باشد و ناحیه سمت چپ این دو نیم‌یال با هم یکی باشد.
۳. لیستی از ناحیه‌ها که برای هر ناحیه توابع زیر تعریف شده‌اند
- تابع  $\text{OuterComponent}(f)$  اگر ناحیه‌ای وجود دارد که این ناحیه را به طور کامل دربر گرفته‌است آن را بازمی‌گرداند.
  - تابع  $\text{InnerComponents}(v)$  لیستی از ناحیه‌هایی که به طور کامل در این ناحیه قرار گرفته‌اند (و با یکدیگر و با ناحیه بیرونی برخورد ندارند) بازمی‌گرداند.
- مقادیر این توابع محاسبه می‌شوند و در لیست یا دیکشنری نگهداری می‌شوند. با استفاده از این داده‌ساختار می‌توان با آغاز کردن از هر عنصری به همه عناصر دیگر دست یافت. [۲۴]

## ۲-۳-۵ ساختمان داده درخت کی‌دی

یکی دیگر از ساختارهای پرکاربرد در هندسه محاسباتی، درخت کی‌دی است. اگر فرض کنیم نقاطی در فضای  $k$ -بعدی داریم، درخت کی‌دی، درختی دودویی و متقارن است که در هر گره با عمق  $d$  برحسب بعد  $d \bmod k$  ام جداسازی اتفاق می‌افتد. یعنی به این شکل که در گره ریشه، نقاط برحسب مقدار جدا می‌شوند و از مقداری کمتر، در زیردرخت چپ و از مقداری بیشتر در زیردرخت راست قرار خواهند گرفت، و به شکل مشابهی برای گره‌های ریشه برحسب مؤلفه‌های دیگر.

به همین منظور می‌توانیم برای ساختِ درختِ کی‌دی از الگوریتم زیر بهره بگیریم.

### الگوریتم ۴ شیوه ساختِ درختِ کی‌دی

```
function BuildKdTree(ps : Set(Point), depth : integer = 0) {
  if (size(ps) == 1)
    return Leaf(point = ps[1])
  else
    i = (depth mod k) + 1
    mid = median(Set(p[i] for p in ps))
    leftPs = Set(p for p in ps if p[i] < mid)
    rightPs = Set(p for p in ps if p[i] >= mid)
    leftSubtree = BuildKdTree(leftPs, depth + 1)
    rightSubtree = subBuildKdTree(rightPs, depth + 1)
    return Node(value = mid,
                 dimension = i,
                 left = leftSubtree,
                 right = rightSubtree)
}
```

با ساختن این درخت می‌توانیم به پرسش لیست نقطه‌های درون یک ابرمکعب در مرتبه  $\mathcal{O}(\sqrt{N} + r)$  پاسخ دهیم که در آن  $r$  تعداد نتایج این پرسش است. به این ترتیب که اگر بازه به شکل  $[a_1, b_1] \times \dots \times [a_n, b_n]$  باشد، آن‌گاه اگر در مواجهه با گره‌ای که مقدار آن  $x$  و بعد مربوط به آن  $i$  باشد، اگر  $a_i > x$  از جست‌وجوی زیردرختِ راست صرف‌نظر می‌کنیم و به شکل مشابهی اگر  $b_i < x$  از زیر درختِ چپ صرف‌نظر می‌کنیم. [۲۴] همچنین قابل حدس است که کوثری وجود یا عدم وجود هر نقطه نیز از مرتبه  $\mathcal{O}(\log N)$  باشد.

## ۲-۳-۶ دوگانگی

دوگانگی به شیوه‌ای در طراحی الگوریتم‌های هندسی گفته می‌شود که از این واقعیت استفاده می‌کند که تحت تبدیل  $*$  که بر روی نقاط و خطوط مانند زیر عمل می‌کند

$$*: \begin{cases} \text{خط } y = ax - b \mapsto \text{نقطه } (a, b) \\ \text{نقطه } (m, -b) \mapsto \text{خط } y = mx + b \end{cases} \quad (2-105)$$

قوانین برقرار است که می‌تواند منجر به حل مسئله شود. ساده‌ترین قائده به این صورت است که اگر نقطه  $p$  بر روی خط  $l$  جای دارد،  $l^*$  بر روی  $p^*$  قرار می‌گیرد.

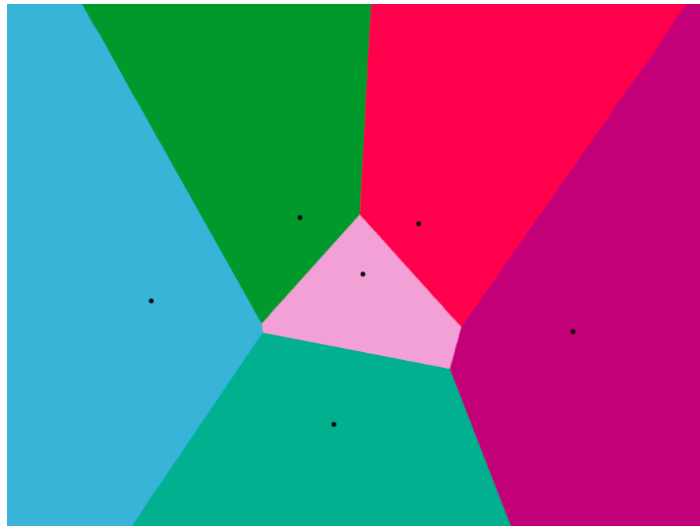
به عنوان مثال مشخص است که مسئله سه نقطه هم‌خط (۳-۱-۲) با دوگانگی به مسئله سه نقطه

هم خط (۲-۱-۳) تبدیل می‌شود. [۲۴، فصل هشتم]

## ۲-۳-۷ پیش‌پردازش‌های کاربردی، مثال دیاگرام ورونی

به عنوان یکی دیگر از پیش‌پردازش‌های کاربردی در هندسه محاسباتی می‌توان به دیاگرام ورونی اشاره کرد. برای یک مجموعه‌ای از نقاط مانند  $S$ ، می‌توانیم دیاگرامی رسم کنیم که صفحه را به ناحیه‌ها افراز می‌کند که هر کدام مجموعه نقاطی است که نزدیک‌ترین نقطه به آن‌ها در  $S$  یک نقطه خاص مانند  $s \in S$  است.

این دیاگرام را می‌توان به شکل گرافی مسطح دید که در آن خطوط مرز ناحیه‌ها، یال‌های گراف و نقاط تلاقی خطوط، گره‌های گراف هستند.



شکل ۲-۳: مثالی از دیاگرام ورونی برای شش نقطه در صفحه

ساده‌ترین کاربردی که می‌توان برای دیاگرام ورونی متصور شد که با استفاده از آن می‌توان به پرسش‌هایی به شکل پیدا کردن نزدیک‌ترین نقطه همسایه در  $S$  به نقطه دلخواه  $p$  پاسخ داد، اما کاربردهای پیچیده‌تری نیز برای آن وجود دارد. برای مثال برای پیدا کردن بزرگ‌ترین دایره خالی از نقاط  $S$  در صفحه، می‌توان از همین دیاگرام کمک گرفت. [۲۴، فصل هفتم]

## فصل ۳

# کارهای پیشین

### ۳-۱ 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 [۲۶][۲۷] 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 باشد. و به نظر می‌رسد هنوز از الگوریتم‌هایی که بهبود سرعتِ توانی دارند در این حوزه استفاده‌ای نشده‌است. [۲۸][۲۹][۳۰][۳۱]

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.

## ۳-۱-۱ مسائل مربوط به تحدب

**مسئله پوش محدب:** در فضای  $d$ -بعدی  $N$  نقطه داریم، مطلوب است پوش محدب آنها، یعنی چندضلعی‌ای که برابر مجموعه همه ترکیب‌های محدب این نقاط است. یا به عبارتی دیگر، مطلوب است مجموعه‌ای از نقاط که به شکل ترکیب محدبی از نقاط دیگر قابل نوشتن نیستند. بگیریم این پوش محدب  $M$  رویه داشته باشد [۲۷][۲۹][۲۵، فصل بیست و ششم]

- الگوریتم کلاسیک: با استفاده از برنامه‌ریزی خطی الگوریتم حساس به خروجی‌ای وجود دارد که در حالت غیرتبهگن<sup>۱</sup> در زمان  $O(N^2 + M \log N)$  مسئله را حل می‌کند. در کلی‌ترین حالت، بهترین الگوریتم حساس به خروجی  $O(NM)$  و برای حالت دوبعدی  $O(N \log M)$  است
- حد کلاسیک: طبیعتاً الگوریتم مذکور، نیاز به زمان  $\Omega(M)$  دارد و حدی نیز برای مقدار رویه‌ها وجود دارد که  $M \leq \kappa N^{\lfloor d/2 \rfloor}$  که  $\kappa$  عددی ثابت است.
- الگوریتم کوانتومی: با استفاده از تسریع در زیرروال برنامه‌ریزی خطی، در زمان  $O(M\sqrt{N} \log N)$  قابل حل است که یعنی در حد  $M$ ‌های کوچک، تسریع خواهد داشت. همچنین، برای حالت دوبعدی، با تسریع‌های مبتنی بر جست‌وجوی کوانتومی، می‌توان در زمان  $O(\sqrt{NM})$  این مسئله را حل کرد.

**مسئله محاسبه فاصله هاسدورف:** فاصله هاسدورف بر روی دو مجموعه متراکم از نقاط به شکل زیر تعریف می‌شود

$$d_H(X, Y) := \max\left\{\max_{x \in X} \min_{y \in Y} \|x - y\|, \max_{y \in Y} \min_{x \in X} \|x - y\|\right\} \quad (۳-۱)$$

اگر یک  $N$ -ضلعی محدب و یک  $M$ -ضلعی محدب داشته باشیم، مطلوب است محاسبه هاسدورف این دو. [۲۶][۳۲]

- الگوریتم کلاسیک: در زمان  $O(M + N)$  قابل حل است.
- الگوریتم کوانتومی: در زمان  $O((N + M)^{\frac{3}{2}} \log^2(N + M))$  قابل حل است.

<sup>۱</sup> هیچ  $d + 1$  نقطه‌ای وجود نداشته باشد که بر ابرصفحه‌ای  $d - 1$  بعدی قرار بگیرند.



**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. [۲۴، فصل چهارم] [۲۸]

- الگوریتم کلاسیک: در فضای دوبعدی با اضافه کردن تدریجی نقاط، با امیدریاضی 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 تعداد پرسش  $\Omega(\sqrt{N})$  اثبات می‌شود.

**مسئله پوشش جعبه با نوارها:** در فضای دوبعدی یک جعبه به شکل  $R = [a, b] \times [c, d]$  داده شده، هر نوار، به فضای بین دو خط موازی در فضا می‌گوییم. تعداد  $N$  نوار داده شده‌اند، مطلوب است جواب این سؤال که آیا این نوارها جعبه را پوشش می‌دهند.

**پوشش مثلث‌ها یک مثلث و  $N$  مثلث داده شده‌اند، سؤال این است که آیا اجتماع  $N$  مثلث، مثلث اولی را می‌پوشاند.**

**حفره در پوشش  $N$  مثلث داده شده‌اند، مسئله این است که آیا اشتراک این‌ها دارای حفره است یا خیر.**

**پوشش چندباره نقاط یک نقطه، یک عدد  $t$  و  $N$  نیم صفحه داده شده‌اند، مطلوب است این که آیا نقطه با حداقل  $t$  نیم صفحه پوشیده شده است یا خیر.**

چهار مسئله فوق، قابل کاهش به سه جمع هستند و اصطلاحاً سه جمع-سخت هستند، پس حد  $\Omega(N^{2-o(1)})$  برای زمان کلاسیک و حد  $\Omega(N^{1-o(1)})$  برای زمان کوانتومی آن‌ها معتبر است [۳۱] و همگی با استفاده از الگوریتمی مشابه سه نقطه هم خط، به نام پوشش کلی (تعریف شده در ۳-۱-۲) در زمان  $\mathcal{O}(N^{1+o(1)})$  حل می‌شوند. این الگوریتم از افزایش صفحات در روش تقسیم و حل و از تسریع جست و جوی کوانتومی استفاده می‌کند. [۳۰]

### ۳-۱-۲ مسائل مربوط به برخورد و اشتراک

**مسئله وجود تلاقی پاره خط‌ها:** در فضای دوبعدی،  $N$  پاره خط داریم، مطلوب است این که وجود دارند دو پاره خطی که با هم تلاقی داشته باشند. [۲۴، فصل دوم] [۲۸]

- الگوریتم کلاسیک: با تکنیک‌های نظیر جاروب خطی (در بخش ۲-۳-۱) متعددی می‌توان در زمان  $O(N \log N)$  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 وجود اشتراک اجسام محدب: در فضای  $d$ -بعدی در نظر بگیرید که  $N$  شکل محدب داریم، هدف فهمیدن این است که آیا نقطه‌ای وجود دارد که در همه این‌ها مشترک باشد. [۲۷] [۲۵]، فصل چهل و دوم
- الگوریتم کلاسیک: می‌دانیم برای فضای دوبعدی و با فرض یکی بودن تعداد اضلاع اشکال محدب، الگوریتمی با پیچیدگی  $O(N)$  وجود دارد.
- حد کلاسیک: حداقل نیاز به بررسی همه  $N$  شکل داریم پس تعداد پرسش از چندضلعی‌ها  $\Omega(N)$  خواهد بود.
- الگوریتم کوانتومی: با استفاده از کاهش مسئله به ارضاپذیری برنامه‌ریزی خطی در  $O(\sqrt{N} \log N)$  پرسش فاصله و مقایسه مربوط به چندضلعی‌ها قابل حل است.
- مسئله برخورد اجسام در حالت کلی: در فضای  $d$ -بعدی در نظر بگیرید که  $N$  شکل داریم، هدف فهمیدن همه برخوردهای این اجسام است. فرض کنید این اجسام  $M$  برخورد دارند. [۲۹]
- الگوریتم کلاسیک: می‌دانیم که بدون استفاده از خواص هندسی فضا، این کار در  $O(N^2)$  امکان‌پذیر است.
- الگوریتم کوانتومی: با استفاده از جست‌وجوی کوانتومی و همچنان بدون استفاده از خواص هندسی فضا، زمان این کار به  $O(N\sqrt{M})$  کاهش می‌یابد.
- مسئله سه نقطه هم خط: تعداد  $N$  نقطه در صفحه داده شده‌اند، مطلوب است این که آیا خطی وجود دارد که از سه نقطه عبور کند یا خیر. [۳۰] [۳۱] [۲۵]، فصل بیست و هشتم
- الگوریتم کلاسیک: با بیان این مسئله به عنوان وجود مثلث با مساحت صفر، در زمان  $\Theta(N^2)$  قابل انجام است.

- حد کلاسیک: با کاهش این مسئله به سه جمع، حدس زده می‌شود، نیاز به زمان  $\Omega(N^{2-o(1)})$  وجود دارد.
  - الگوریتم کلاسیک: با استفاده از تقسیم و حل با افراز صفحه و استفاده از جست‌وجوی کوانتومی، در زمان  $\mathcal{O}(N^{1+o(1)})$  قابل انجام است.
  - حد کوانتومی: با استفاده از حدس سه جمع کوانتومی، نیاز به زمان  $\Omega(N^{1-o(1)})$  وجود دارد.
- مسئله سه خط هم‌نقطه تعداد  $N$  خط در صفحه داده‌شده‌اند، مطلوب است این که آیا نقطه‌ای وجود دارد که محل برخورد سه خط باشد یا خیر. [۳۰]
- این مسئله دوگان مسئله قبل است و تمامی الگوریتم‌ها و حدود معتبر هستند.
- جدا ساز پاره‌خط‌ها  $N$  پاره‌خط عمودی داده‌شده‌اند، مطلوب است که آیا خط افقی داده‌شده این خاصیت را دارد که با هیچ کدام تلاقی نداشته باشد و در هر سوی خط حداقل یک پاره‌خط باشد. (یعنی همه پاره‌خط‌ها بالای خط یا پایین خط نباشند).
- مشاهده‌پذیری پاره‌خط‌ها  $N$  پاره‌خط و دو پاره‌خط  $s_1$  و  $s_2$  داده‌شده‌اند، هدف این است که بدانیم آیا نقطه‌ای بر روی  $s_1$  وجود دارد که بتواند حداقل یک نقطه از  $s_2$  را ببیند به این معنی که خط واصلشان با هیچ پاره‌خط دیگری تلاقی نکند.
- مشاهده‌پذیری از بی‌نهایت  $N$  پاره‌خط و پاره‌خط  $s$  داده‌شده‌اند، هدف این است که بدانیم آیا نقطه‌ای بر روی  $s$  وجود دارد که از بی‌نهایت دیده‌شود، یعنی از آن بتوان نیم‌خطی تا بی‌نهایت رسم کرد.
- برای سه مسئله فوق نیز، حدها و الگوریتم‌های سه نقطه هم‌خط برقرار است. [۳۰] [۳۱]
- مسئله چیدمان ابرصفحه‌ها:  $N$  ابرصفحه در فضای  $d$  - بعدی داریم، مطلوب است یافتن فضای احاطه‌شده بین پوش این صفحات، اگر  $M$  تعداد رویه‌های آن فضا باشد.
- این مسئله دوگان مسئله پوش محدب (تعریف شده در ۳-۱-۱) است و موارد گفته‌شده در آن‌جا همچنان معتبر است. [۲۷]

## ۳-۱-۳ مسائل مربوط به مجاورت

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. [۳۳، فصل پنجم][۲۸][۳۴]

- الگوریتم کلاسیک: با استفاده از تقسیم و حل، با  $\Theta(N \log N)$  مقایسه (بین فاصله زوج‌نقاط) 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. [۲۸]

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. [۲۸][۳۵، Minimum Geometric Spanning Trees][۳۴]

- 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  $\mathcal{O}((NM \log N \log M)^{\frac{1}{2}} + N \log^2 M + M \log^2 N)$  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  $\mathcal{O}((M+N)^{\frac{1}{2}} \log(M+N))$  حل می‌شود.
- حد کوانتومی: چون این مسئله از مسئله نزدیک‌ترین زوج سخت‌تر است حدهای قبلی برقرار هستند.

### 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. [۳۶]

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.

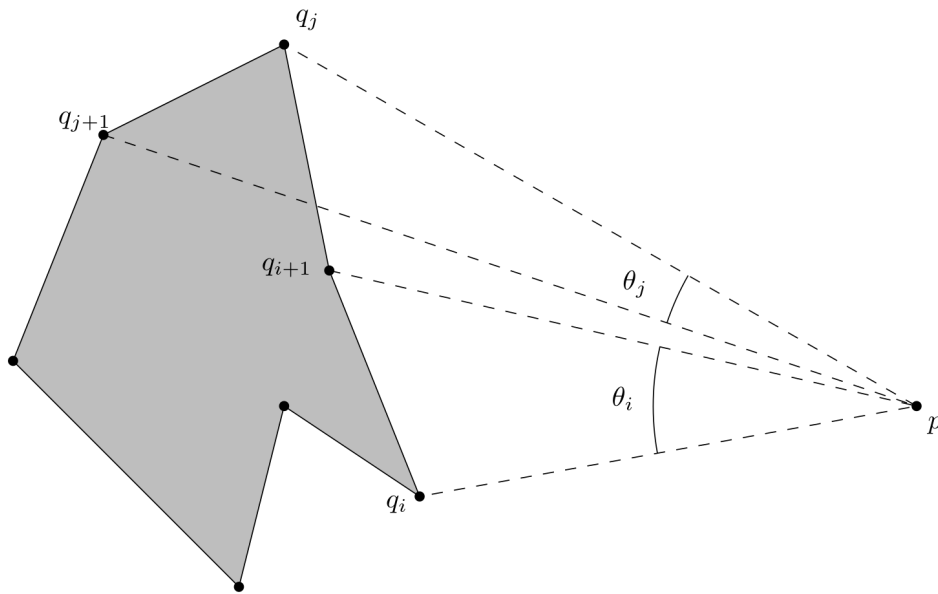
با این ایده می‌توان در مرتبه  $\Theta(N)$  مسئله مذکور را حل کرد.

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

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

$$\begin{cases} s_i = 0 & \text{اگر } p \text{ در سمت راست خط } q_i q_{i+1} \text{ باشد} \\ s_i = 1 & \text{اگر } p \text{ در سمت چپ خط } q_i q_{i+1} \text{ باشد} \end{cases} \quad (2-3)$$

<sup>۲</sup> 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 به شکل زیر تبدیل می شود.

$$\left| \sum \theta_i s_i \right| = \begin{cases} 2\pi & \text{نقطه داخل چندضلعی است} \\ 0 & \text{نقطه بیرون چندضلعی است} \end{cases} \quad (3-3)$$

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. [۳۷] [۳۸]

## فصل ۴

# بحث و نتایج نو

### ۴-۱ معرفی یک الگوریتم کوانتومی

می بینیم صورت بندی ایده دوم که در فصل پیشین مطرح شد، شباهت زیادی به مسئله مربوط به الگوریتم دویچ-جوزا دارد، اما وجود وزن ها، امکان استفاده از الگوریتم دویچ-جوزا را به ما نمی دهد.

اما می دانیم 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  $\kappa$  یک ضریب برای بهنجارسازی است، آنگاه با استفاده از تبدیل فوریه، می توانیم به حالتی برسیم که دامنه حالت  $|0\rangle$  یا همان عنصر همانی گروه، در آن به شکل زیر باشد

$$\langle 0 | \text{QFT} | \psi \rangle = \frac{1}{N-1} \sum_{q_i q_{i+1} \in \text{segments}} \kappa \theta_i s_i \quad (2-4)$$

که از آن جا که برای هر تبدیل فوریه ای این مهم برقرار است، می توان به جای QFT قرار داد  $H^{\otimes \log(N-1)}$  و فرض بگیریم که  $N-1$  توانی از دو است.

پس برای احتمال اندازه گیری ۰ پس از تبدیل فوریه داریم

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

اما حالا ضریب  $\kappa$  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.<sup>۱</sup>

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 پاره‌خط در مقابل یک نقطه حداکثر به نیم صفحه می‌رسد. در این صورت این احتمال نیز به شکل  $\mathcal{O}(\frac{1}{N^2})$  کوچک خواهد بود.

اما اگر قوی وجود داشته باشد که  $\theta_i \leq \frac{\gamma}{N} \in \mathcal{O}(\frac{1}{N})$  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 ۳-۴ 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.

<sup>۱</sup> ایده تبدیل  $s_i$  به  $(-1)^{s_i}$  دقیقاً مشابه آن چیزی است که در بخش مذکور بحث شد، همچنین برای قسمت  $\theta_i$  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  $\theta_i$  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.



این الگوریتم را می‌توان به شکل 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 x[i]
        if (result)
            is_in = false

    return is_in

```

---

## ۲-۴ گسترش الگوریتم برای حالت‌های دیگر

می‌دانیم که برای عملکرد درست الگوریتم لازم است که احتمالی که در معادله ۳-۴ 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 برروی عدد ۰ باشد (که احتمال آن مورد نظر است)، آن را تقویت کرد. تعداد مراحل لازم برای این تقویت از مرتبه  $O(\frac{N}{\kappa})$  خواهد بود که این نشان می‌دهد اگر  $\kappa$  عدد ثابتی باشد، این الگوریتم هیچ تسریعی نمی‌تواند داشته باشد.

## ۳-۴ حد پایین دشمن گونه

این‌طور که پیداست، مسئله نقطه در چندضلعی در حالت کلی نمی‌تواند تسریعی با استفاده از رایانش کوانتومی را تجربه کند. این موضوع به شکل تئوری نیز قابل بررسی است.

تا به این‌جای بحث، محدودیتی برروی سادگی یا غیرسادگی چندضلعی‌ها مشخص نشده و قابل حدس است که تمام بحث‌های گفته‌شده برروی هر دو دسته چندضلعی‌ها برقرار باشند. اما در این بخش، استدلالی برای حد پایین پرسش‌های کلاسیک و کوانتومی لازم برای حل مسئله مذکور بیان می‌شود که تنها برای چندضلعی‌های غیر ساده معتبر است و در صورت محدودیت مسئله به چندضلعی‌های ساده، این حدود غیرمعتبر خواهند بود.

برای بیان این حد از حد پایین دشمن گونه استفاده می‌کنیم که به این ترتیب است که اگر برای مسئله‌ای به شکل  $f: S \rightarrow \mathbb{Z}_2$  دسترسی الگوریتم به ورودی از طریق جعبه سیاه باشد؛ یعنی برای هر ورودی مسئله مانند  $s \in S$  الگوریتم با استفاده از جعبه سیاهی مانند  $O_s$  به جواب مسئله برسد، و همچنین دو زیر مجموعه دلخواه زیر را داشته باشیم

$$X \subseteq \{s | f(s) = 1\} \quad (7-4)$$

$$Y \subseteq \{s | f(s) = 0\} \quad (8-4)$$

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

$$xRy \Leftrightarrow O_x(i) \neq O_y(i) \quad \text{تنها برای یک مقدار } i \quad (۹-۴)$$

از طرف دیگر می‌توانیم رابطه  $R_i$  را نیز به شکلی تعریف کنیم که

$$xR_iy \Leftrightarrow O_x(i) \neq O_y(i) \text{ و } \forall j \neq i \quad O_x(j) = O_y(j) \quad (۱۰-۴)$$

که در این صورت

$$R = \bigcup_i R_i \quad (۱۱-۴)$$

حالا اگر گراف دوبخشی معادل با  $R$  را در نظر بگیریم، کمینه درجه رئوس بخش  $X$  و بخش  $Y$  را به ترتیب  $m$  و  $m'$  بنامیم، از سوی دیگر، برای  $R_i$  ها بیشینه درجه رئوس را به شکل  $l_i$  و  $l'_i$  را تعریف کنیم و بگیریم

$$l := \max_i l_i \quad (۱۲-۴)$$

$$l' := \max_i l'_i \quad (۱۳-۴)$$

آن‌گاه پیچیدگی محاسباتی پرسش‌های این مسئله از مرتبه  $\Omega(\sqrt{\frac{mm'}{ll'}})$  خواهد بود. که بدون اثبات آن را خواهیم پذیرفت [۳۹]

حالا برای استفاده از حد دشمن‌گونه، مسئله زیر را تعریف می‌کنیم

اگر یک  $N$ -ضلعی منتظم  $Q$  را در نظر بگیریم که نقطه  $P$  مرکز آن باشد، حالا چندضلعی  $Q'$  را با مقیاس کردن  $Q$  به مرکز  $P$  و با ضریب  $\frac{1}{4}$  و سپس قرینه نقطه‌ای کردن آن حول  $P$  بسازیم، آن‌گاه به ازای هر رشته  $N$ -بیتی  $s$  یک چندضلعی  $Q^{(s)}$  خواهیم داشت که رئوس آن به این ترتیب به دست می‌آیند

$$q_i^{(s)} = \begin{cases} q_i & s_i = ۱ \\ q'_i & s_i = ۰ \end{cases} \quad (۱۴-۴)$$

حالا مسئله وجود نقطه  $P$  در چندضلعی  $Q^{(s)}$  برابر مسئله زوج بودن وزن همینگ  $s$  خواهد بود. برای اثبات این برابری، می‌توان از استقرای ریاضی استفاده کرد به این ترتیب که به ازای  $s = ۰$  این برابری به

سادگی برقرار است و با تغییر هر بیت از  $s$  می‌توان به سادگی نشان داد که همچنان برابری حفظ می‌شود و در نتیجه برای تمام رشته‌ها برقرار است.

از سوی دیگر، برای مسئله زوج بودن وزن همینگ  $s$ ، می‌توانیم از حد دشمن‌گونه به این ترتیب استفاده کنیم که  $X$  همه رشته‌ها با وزن زوج و  $Y$  همه رشته‌ها با وزن فرد باشند، آن‌گاه  $m$  و  $m'$  هر دو برابر با طول رشته و برابر با  $N$  خواهند بود و مقادیر  $l$  و  $l'$  نیز که مربوط همسایه‌هایی هستند که تنها در پرسش خاص  $i$  (بخوانید بیت  $i$ ام) با هم تفاوت دارند برابر با ۱ خواهند بود، در نتیجه، این مسئله نیاز به  $\Omega(N)$  پرسش خواهد داشت.

از آن‌جا که مسئله زوج بودن وزن همینگ قابل کاهش به وجود نقطه در چندضلعی ست پس حداقل پرسش برای مسئله نقطه در چندضلعی نیز برابر  $\Omega(N)$  خواهد بود.

## فصل ۵

### نتیجه گیری

در این پایان نامه سعی شد که به بررسی راینش کوانتومی و هندسه محاسباتی و تلاقی این دو حیطه پرداخته شود. آنچه به نظر می رسد این است که تلاش های کمی در ترکیب این دو حوزه صورت گرفته است. حال آن که به خاطر ارتباط گسترده هندسه (به خصوص در ابعاد بالا) و راینش کوانتومی پتانسیل خوبی برای تسریع های کوانتومی در مسائل هندسی وجود دارد. همچنین نظیر آنچه در این پایان نامه گفته شد، بسیاری از تسریع های کوانتومی در حضور قیدها و قول ها به دست می آیند که در این حوزه به خاطر ذات هندسی مسائل، همواره قیدهایی بر روی ورودی وجود خواهند داشت و این هم خوانی حتماً قابل استفاده خواهد بود.

آنچه ماحصل این پژوهش بوده است، به طور خاص برای مسئله نقطه در چندضلعی، به این ترتیب است که نشان داده شده هیچ الگوریتم کوانتومی ای نخواهد توانست در حالت کلی، سریع تر از الگوریتم های کلاسیک به پاسخ این مسئله دست پیدا کند. اما با اندکی تغییر مسئله و ایجاد یک قول، مبتنی بر فاصله داشتن نقطه از اضلاع، یا حتی با قدری کاهش حساسیت نسبت به خطا در نزدیکی خطوط چندضلعی، می توان از الگوریتم پیشنهاد شده استفاده کرد که از آنجا که مبتنی بر تبدیل فوری کوانتومی بوده است می تواند باعث تسریع فرا-چند جمله ای بشود و تعداد پرسش ها را تا  $\Theta(1)$  و پیچیدگی زمانی را تا  $\Theta(\log(n))$  کاهش دهد.

نکته حائز اهمیت دیگر این است که از این الگوریتم می تواند به مقدار دلخواهی خطا را کم و به پیچیدگی محاسباتی اضافه کند تا به دقت و سرعت الگوریتم کلاسیک برسد.

از حیث شیوه عملکرد الگوریتم نیز، با توجه به مرور ادبیات، تنها الگوریتمی خواهد بود که بر مبنای جست‌وجو و ولگشت عمل نمی‌کند و از تسریع تبدیل فوریه کوانتومی استفاده می‌کند.

## ۵-۱ کارهای آتی

در این پژوهش جای خالی شبیه‌سازی و نمایش خروجی‌ها برای مشاهده شرایط قول و مقدار خطا وجود دارد. همچنین بررسی الگوریتم‌های تقریبی کلاسیک و طراحی الگوریتم‌های کلاسیک برای همان شرایط قول می‌تواند منجر به مقایسه دقیق‌تری بین راه حل کلاسیک و کوانتومی در این مسئله بشود. از سوی دیگر، بررسی کاربردهای مسئله قولی در هندسه محاسباتی و حوزه‌های دیگری نظیر گرافیک کامپیوتری همچنان مورد سؤال است.

فراتر از این، همچنان بسیاری از مسائل در هندسه محاسباتی هستند که هیچ راه حل کوانتومی‌ای برای آن‌ها پیشنهاد نشده و از سوی دیگر، مسائلی که راه حل یا حد کوانتومی دارند نیز، نیازمند جمع‌بندی و تدوین هستند تا ابزاری یکپارچه شوند. برای مثال، بررسی شیوه ورودی گرفتن اشکال کوانتومی یا پیدا کردن فرایندهای مشترک در الگوریتم‌های کوانتومی این حوزه، از موضوعات ارزشمند برای پژوهش‌های آتی هستند.

## مراجع

- [1] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, 1982.
- [2] 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, 1994.
- [3] L. K. Grover. Quantum computers can search rapidly by using almost any transformation. *Physical Review Letters*, 80(19):4329–4332, 1998.
- [4] I. L. Chuang, N. Gershenfeld, and M. Kubinec. Experimental implementation of fast quantum searching. *Physical Review Letters*, 80(15):3408–3411, 1998.
- [5] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.
- [6] S. Aaronson. *Quantum Computing since Democritus*. Cambridge University Press, 2013.

- [7] C. M. Grinstead and J. L. Snell. *Introduction to Probability*. American Mathematical Society, second edition, 1997.
- [8] V. Karimipour. Lecture notes on quantum computation and information. <http://physics.sharif.edu/~vahid/teachingQC.html>, Fall and Spring 2021. Accessed: 2021-06-25.
- [9] S. Arora and B. Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.
- [10] 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.
- [11] 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.
- [12] J. Watrous. Quantum computational complexity. [arxiv:quant-ph/0804.3401](https://arxiv.org/abs/quant-ph/0804.3401), 2008.
- [13] S. Aaronson. Lecture notes of 6.845 quantum complexity theory. [MIT OpenCourseWare](https://ocw.mit.edu/courses/6-845-quantum-complexity-theory/), Fall 2010. Accessed: 2021-06-25.
- [14] M. Backens. The ZX-calculus is complete for stabilizer quantum mechanics. *New Journal of Physics*, 16(9):093021, 2014.
- [15] 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.
- [16] A. J., A. Adedoyin, J. Ambrosiano, P. Anisimov, A. Bärttschi, 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. [arxiv:cs.ET/1804.03719](https://arxiv.org/abs/cs.ET/1804.03719), 2018.
- [17] A. Montanaro. Quantum algorithms: an overview. *npj Quantum Information*, 2(1):1–8, 2016.
- [18]



- [19] A. Terras. *Fourier Analysis on Finite Groups and Applications*. London Mathematical Society Student Texts. Cambridge University Press, 1999.
- [20] A. Y. Kitaev. Quantum measurements and the abelian stabilizer problem. [arxiv:quant-ph/9511026](#), 1995.
- [21] A. W. Harrow, A. Hassidim, and S. Lloyd. Quantum algorithm for linear systems of equations. *Physical Review Letters*, 103(15):150502, 2009.
- [22] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the thirty-fifth ACM symposium on Theory of computing - STOC '03*, page 59. ACM Press, 2003.
- [23] J. Kempe. Quantum random walks: An introductory overview. *Contemporary Physics*, 44(4):307–327, 2003.
- [24] M. d. Berg. *Computational geometry: algorithms and applications*. Springer, third edition, 2008.
- [25] C. Tóth, J. O'Rourke, and J. E. Goodman, editors. *Handbook of discrete and computational geometry*. CRC Press, third edition, 2017.
- [26] K. Sadakane, N. Sugawara, and T. Tokuyama. Quantum algorithms for intersection and proximity problems. In P. Eades and T. Takaoka, editors, *Algorithms and Computation*, Lecture Notes in Computer Science, pages 148–159. Springer, 2001.
- [27] K. Sadakane, N. Sugawara, and T. Tokuyama. Quantum computation in computational geometry. *Interdisciplinary Information Sciences*, 8(2):129–136, 2002.
- [28] N. Volpato and A. Moura. Bounds for quantum computational geometry problems. 2009.
- [29] M. Lanzagorta and J. Uhlmann. Quantum algorithmic methods for computational geometry. *Mathematical Structures in Computer Science*, 20(6):1117–1125, 2010.
- [30] A. Ambainis and N. Larka. Quantum algorithms for computational geometry problems. 2020.
- [31] H. Buhrman, B. Loff, S. Patro, and F. Speelman. Limits of quantum speed-ups for computational geometry and other problems: Fine-grained complexity via quantum walks. 2021.

- [32] M. J. Atallah. A linear time algorithm for the hausdorff distance between convex polygons. *Information Processing Letters*, 17(4):207–209, 1983.
- [33] F. P. Preparata and M. I. Shamos. *Computational geometry: an introduction*. Texts and monographs in computer science. Springer, 2008.
- [34] S. Aaronson, N.-H. Chia, H.-H. Lin, C. Wang, and R. Zhang. On the Quantum Complexity of Closest Pair and Related Problems. In S. Saraf, editor, *35th Computational Complexity Conference (CCC 2020)*, volume 169 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:43, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.
- [35] M.-Y. Kao, editor. *Encyclopedia of algorithms: with 379 figures and 51 tables*. Springer Reference, second edition, 2016.
- [36] C.-W. Huang and T.-Y. Shih. On the complexity of point-in-polygon algorithms. *Computers & Geosciences*, 23(1):109–118, 1997.
- [37] K. Hormann and A. Agathos. The point in polygon problem for arbitrary polygons. *Computational Geometry*, 20(3):131–144, 2001.
- [38] K. Weiler. An incremental angle point in polygon test, 1994.
- [39] A. Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.

# واژه‌نامه

## الف

ابرصفحه ..... hyperplane

## ب

برنامه‌ریزی خطی تعمیم‌یافته ..... generalized linear programming

## پ

پرسش ..... query

## ت

تقویت دامنه ..... amplitude amplification  
تعینی ..... deterministic

## ج

جعبه‌سیاه ..... oracle

## چ

چیدمان ..... arrangement

## ح

حساس به خروجی ..... output-sensitive  
حد پایین دشمن‌گونه ..... adversarial lower bound

## ر

رایانش ..... computation

## ز

زنجیره مارکوفی ..... markov chain

## ف

فروریزش ..... collapse

## ق

قول ..... promise

## م

و	متغیر تصادفیِ مشترک shared randomness.....
random walk..... ولگشت	مثلث‌بندی triangulation.....
	مدلِ رایانش computational model.....
ه	مربعی quadratic.....
coset..... هم‌دسته	مولد generator.....
ی	ن
unitary..... یکانی	نهمان‌سازیِ دامنه‌ای amplitude encoding.....
	نوفه noise.....

## Abstract

Quantum computing is a computational model based on quantum mechanics principles. After introducing the Grover algorithm and Shor algorithm, quantum computing had become 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 perspectives, 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. The 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, achieves 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