**دانشگاه یزد**

**دانشکده‌ی ریاضی**

**گروه علوم کامپیوتر**

**پایان‌نامه جهت دریافت درجه کارشناسی ارشد علوم کامپیوتر**

# کاربرد روش‌های جستجوی کوانتومی برای پیدا کردن نقطه تعادلی نش

**استاد راهنما:**

**دکتر محمدرضا هوشمنداصل**

**استاد مشاور:**

**دکتر علی دلاور خلفی**

**پژوهش‌گر:**

**زهره محسنی**

**شهریور ۱۳۹۰**

# سپاس‌گزاری

سپاس خدا را که مرا به راه دانش رهنمون شد و هموست که فرصت شاگردی اساتید گرامی را بر من ارزانی داشت تا چراغی بر تاریکی جهلم باشند.

از استاد بزرگوارم، جناب آقای دکتر محمدرضا هوشمند اصل، استاد راهنمای این پژوهش، که افق‌های جدیدی بر پنجره‌ی ذهنم گشودند، سپاس‌گزارم و رهنمودهای ایشان را ارج می‌نهم.

همراهی و راهنمایی‌های جناب آقای دکتر علی دلاور خلفی به عنوان استاد مشاور این پژوهش درخور تقدیر و تشکر است.

## تقدیم به

همسر عزیزم و پدر و مادر مهربانم که همواره در طول تحصیل از حمایت بی‌دریغ آنها بهره برده‌ام.

# چکیده

یکی از ویژگی‌های مهم کامپیوترهای کوانتومی، که پایه بسیاری از الگوریتم‌های کوانتومی بر آن استوار است، امکان پردازش بیش از یک حالت به صورت هم‌زمان می‌باشد به این ویژگی توازی کوانتومی گویند. همین ویژگی توازی کوانتومی است که کامپیوترهای کوانتومی را قادر می‌سازد تا چندین ورودی را در قالب یک حالت دریافت کنند و در یک واحد زمانی همه‌ی آن‌ها را پردازش کنند. از الگوریتم‌های مهم جستجوی کوانتومی می‌توان به الگوریتم گروور اشاره نمود که جستجو را روی یک پایگاه داده نامرتب با تعداد $N$ داده انجام می‌دهد و نقطه‌ی هدف را در زمان $O(\sqrt{N})$ پیدا می‌کند. بویر الگوریتم جستجوی گروور را در سال ۱۹۹۸ بهبود بخشید و دوور-هویر با استفاده از الگوریتم بویر الگوریتمی برای حل مسئله‌ی بهینه‌سازی ارائه داده است.

الگوریتم جستجوی کوانتومی را می‌توان برای پیدا کردن نقطه‌ی تعادلی نش بکار بست. در این پایان‌نامه با استفاده از ایده‌ی تبدیل مسئله‌ی جستجوی نقطه‌ی تعادلی نش بازی‌های دونفره با توابع پرداخت درجه دو-دوخطی به مسئله‌ی بهینه‌سازی که توسط دکتر دلاور ارائه شده، یک روش برای یافتن جستجوی کوانتومی مبتنی بر الگوریتم دوور-هویر نقطه تعادلی نش این نوع مسائل ارائه خواهد شد. در حالت کلاسیک حل این مسئله‌ی بهینه‌سازی با تعداد داده‌های $N$ به زمان $O(N)$ نیاز دارد. در این پایان نامه روشی برای جستجوی نقطه‌ی تعادلی نش با استفاده از الگوریتم کوانتومی بهینه‌سازی دوور-هویر ارائه شده است که در این روش زمان جستجوی نقطه‌ی تعادلی نش به $O(\sqrt{N})$ کاهش یافته است.

# فهرست مطالب


**پیش‌گفتار** **۱**

**۱ مقدمات** **۵**

۱.۰.۱ مقدمه‌ای بر جبر خطی . . . . . ۵

۱.۱ محاسبات کوانتومی . . . . . ۱۱

۱.۱.۱ کیوبیت . . . . . ۱۱

۲.۱.۱ عملگر اندازه‌گیری کوانتومی . . . . . ۱۳

۲.۱ عملگرهای کوانتومی . . . . . ۱۳

۱.۲.۱ چند عملگر کوانتومی . . . . . ۱۵

۳.۱ توازی کوانتومی . . . . . ۱۸

**۲ بهینه‌سازی کوانتومی** **۲۱**

۱.۲ الگوریتم دویچ . . . . . ۲۱

۲.۲ الگوریتم دویچ–جوزا . . . . . ۲۳

۳.۲ الگوریتم جستجوی کوانتومی گروور . . . . . ۲۵

۱.۳.۲ مراحل الگوریتم جستجوی گروور . . . . . ۲۵

۲.۳.۲ تشریح عملگر الگوریتم جستجوی کوانتومی گروور $(G_n)$ . . . . . ۲۶

۳.۳.۲ تحلیل پیچیدگی زمانی الگوریتم جستجوی گروور . . . . . ۲۹

۴.۳.۲ تعبیرهندسی الگوریتم جستجوی گروور . . . . . ۳۳

۴.۲ الگوریتم جستجوی کوانتومی بویر . . . . . ۳۵

۱.۴.۲ مراحل الگوریتم جستجوی بویر . . . . . ۳۷
۲.۴.۲ محاسبه‌ی پیچیدگی زمانی الگوریتم بویر . . . . . ۳۷
۵.۲ مسئله‌ی بهینه‌سازی . . . . . ۴۱
۱.۵.۲ بهینه‌سازی کوانتومی با استفاده از الگوریتم جستجوی گروور . . . . . ۴۱
۲.۵.۲ الگوریتم بهینه‌سازی کوانتومی سراسری دوور-هویر . . . . . ۴۲

**۳ نظریه بازی‌ها ۴۹**

۱.۳ بازی و ارکان آن . . . . . ۴۹
۲.۳ دسته‌بندی بازی‌ها . . . . . ۵۰
۳.۳ فرم‌های مختلف نمایش بازی‌ها . . . . . ۵۱
۴.۳ نقطه‌ی تعادلی نش . . . . . ۵۲
۱.۴.۳ محاسبه‌ی پیچیدگی زمانی جستجوی نقطه‌ی تعادلی نش بازی دونفره . . . . . ۵۶
۵.۳ کوانتومی‌سازی بازی‌ها . . . . . ۵۶

**۴ کاربرد روش‌های جستجوی کوانتومی برای جستجوی نقطه‌ی تعادلی نش ۶۱**

۱.۴ کاربرد روش‌های جستجوی کوانتومی در جستجوی نقطه‌ی تعادلی نش در بازی‌های با توابع پرداخت درجه دو-دوخطی . . . . . ۶۱
۱.۱.۴ تبدیل مسئله‌ی جستجوی نقطه‌ی تعادلی نش به مسئله‌ی بهینه‌سازی . . . . . ۶۲
۲.۱.۴ جستجوی نقطه‌ی تعادلی نش با استفاده از بهینه‌سازی کوانتومی . . . . . ۶۴
۲.۴ الگوریتم جستجوی کوانتومی نقطه‌ی تعادلی نش بازی‌های دو نفره با فرم نمایش ماتریسی ۷۰

**نتیجه‌گیری ۷۲**

**مراجع ۷۳**

**واژه‌نامه فارسی به انگلیسی ۷۸**

**واژه‌نامه انگلیسی به فارسی ۸۰**

# لیست تصاویر


۱.۱ گیت $NAND$ کلاسیک . . . . . ۱۵

۲.۱ گیت تافولی . . . . . ۱۶

۳.۱ گیت $NAND$ کوانتومی . . . . . ۱۷

۴.۱ گیت $BUFFER$ کوانتومی . . . . . ۱۷

۱.۲ جعبه سیاه عملکرد الگوریتم دویچ . . . . . ۲۲

۲.۲ جعبه سیاه عملکرد الگوریتم دویچ-جوزا . . . . . ۲۴

۳.۲ جعبه سیاه عملگر $V_f$ . . . . . ۲۶

۴.۲ شکل هندسی عملکرد الگوریتم جستجوی گروور . . . . . ۳۴

۵.۲ نمودار $\frac{S}{\sqrt{\frac{N}{k}}}$ برحسب $\frac{k}{N}$ به ازای $\lambda = ۱/۳۴$ . . . . . ۳۹

۶.۲ تابع بولی $h(w)$ . . . . . ۴۱

۱.۳ نمایش بازی کوانتومی . . . . . ۵۸

۲.۳ نسخه‌ی کوانتومی بازی $PQ$ . . . . . ۵۹

# پیش‌گفتار

در سال ۱۹۳۶ آلن تورینگ نشان داد یک ماشین تورینگ جهانی وجود دارد که هر ماشین تورینگ را می‌توان با آن شبیه‌سازی کرد و ویژگی‌های یک ماشین محاسبه‌گر را تبیین کرد. در سال ۱۹۴۱، کمی پس از مقاله‌ی تورینگ، اولین کامپیوتر شامل اجزای الکترونیکی توسط کونارد زوس[۱] آلمانی اختراع شد. جان‌ون‌نیومن [۲] یک مدل ساده تئوری ارائه داد که چگونه می‌توان اجزای لازم برای یک کامپیوتر را کنار هم گذاشت به‌طوری‌که توانایی ماشین تورینگ جهانی را داشته باشد. کامپیوترهای مدرن و پرسرعت امروزی چیزی به جز یک ماشین تورینگ نیستند و از نظر اساس کار تفاوت بنیادی با اولین کامپیوترها ندارد. پیشرفت بخش سخت افزار با جایگزین شدن لامپ خلأ با ترانزیستور در سال ۱۹۴۷ به بعد انجام شد و در واقع این پیشرفت تکنولوژی تنها باعث تغییر در سرعت و اندازه‌ی کامپیوترها شده است و کاری که اساساً انجام می‌دهند محاسبه روی رشته‌ای از بیت‌ها است که تغییر نکرده است.

پیشرفت و رشد سخت‌افزار هنوز هم با سرعت ادامه دارد، این امر باعث افزایش سرعت پردازش‌ها و میزان حافظه‌ی کامپیوترها خواهد شد. سوالی که پیش روی دانشمندان است این است که آیا با این روند کوچک‌ترشدن کامپیوتر به همراه بالا رفتن سرعت انجام محاسبات آن در دهه‌های آینده می‌توان تمام مسائل سخت[۲-۵] علوم مختلف از جمله علم فیزیک، ریاضی و ... را به‌وسیله‌ی کامپیوترهای قدرتمند حل کرد؟

جواب این سوال منوط بر معیاری است که مسائل سخت و آسان را تعریف می‌کند[۶، ۷]. این معیار در بیان دانشمندان کامپیوتر به نام پیچیدگی زمانی معروف است. آن دسته از مسائل که زمان حل آن‌ها نسبت به اندازه‌ی مسئله چند جمله‌ای باشد، مسائل آسان یا نوع $P$ [۳] نامیده می‌شوند. در مقابل مسائلی که زمان حل آن‌ها نسبت به اندازه‌ی مسئله به صورت نمایی رشد کند مسائل سخت یا نوع $NP$ نامیده می‌شود.

با ادامه‌ی روند کوچک‌ترشدن کامپیوترها پیش‌بینی می‌شود که فاصله‌ی بین دو سلول آن‌قدر کوچک خواهد شد که برای توصیف رفتار این دو سلول باید از قوانین مکانیک کوانتومی استفاده شود[۸-۱۱]. بنابراین بعد از اعمال قوانین مکانیک کوانتومی باید ثبت اطلاعات، خواندن اطلاعات، نحوه‌ی محاسبه و الگوریتم‌ها [۱۲-۱۵] با نحوه‌ی رفتار مکانیک کوانتومی سازگار شود[۱۶، ۱۷]. که نتیجه‌ی این کار، جایگزین شدن کامپیوترهای کوانتومی [۴]

---

[۱] Konard Zuse

[۲] John Von Newman

[۳] Polynomial

[۴] Quantum Computer

$(Q.C)$ به‌جای کامپیوترهای کلاسیک می‌باشد[۱۸، ۱۹].

در کامپیوترهای کلاسیک، عنصر اصلی حافظه بیت$(bit)$، و در کامپیوترهای کوانتومی عنصر اصلی حافظه کیوبیت$(qubit)$، است که در فصل بعد مورد بحث قرار می‌گیرد.

کیوبیت یک حالت کوانتومی است و برای تغییر آن دروازه‌های کوانتومی [۵] مورد نیاز است. بنابر قوانین مکانیک کوانتومی تغییر کیوبیت‌ها توسط عملگرهای یکانی انجام می‌شود. بنابراین باید دروازه‌های یکانی برای انجام تغییرات روی کیوبیت طراحی شود[۲۰-۲۳]. شگفتی کامپیوترهای کوانتومی در این است که یک کیوبیت ترکیب خطی حالت‌های پایه است. بنابراین کامپیوتر کوانتومی قادر است حالت‌های موجود در کیوبیت را به صورت هم‌زمان تغییر دهد که این ویژگی توازی کوانتومی[۶] نامیده می‌شود[۲۲، ۲۳]. توازی کوانتومی نقش اساسی در طراحی الگوریتم‌های کوانتومی ایفا می‌کند و عامل اساسی در کاهش پیچیدگی زمانی الگوریتم‌های کوانتومی نسبت به الگوریتم‌های کلاسیک می‌باشد. بنابراین کامپیوترهای کوانتومی با سرعت و قابلیت‌های فوق‌العاده‌ی خود چشم‌اندازهای جدیدی بر روی دانشمندان می‌گشایند.

دو تا از مهمترین الگوریتم‌های کوانتومی عبارت‌اند از: الگوریتم کوانتومی شور[۷] و الگوریتم جستجوی کوانتومی گروور [۸].

الگوریتم شور در سال ۱۹۹۴ ارائه شد و یک الگوریتم کوانتومی نوع $P$ برای تجزیه‌ی اعداد صحیح و پیدا کردن لگاریتم روی یک میدان متناهی می‌باشد [۲۴، ۲۵]. برای این دو مسئله بهترین الگوریتم‌های کلاسیک شناخته شده از نوع $NP$ هستند. نتایج الگوریتم کوانتومی شور توجه فوق‌العاده‌ای را در میان دانشمندان نظری و تجربی برانگیخت. چرا که مسئله‌ی تجزیه‌ی اعداد بزرگ تا آن روز در شمار مسائل $NP$ بوده و به همین دلیل قلب سیستم رمزنگاری همچون $RSA$ به شمار می‌رفته است [۲۶، ۲۷].

گروور که در سال ۱۹۹۵ یک الگوریتم جستجوی کوانتومی ارائه داد قادر بود یک داده را در میان پایگاه داده‌ای نامرتب به طول $N$( که $N$ خیلی بزرگ است) با پیچیدگی زمانی $O(\sqrt{N})$ پیدا کند[۲۲-۲۴]، در حالی‌که این جستجو با بهترین الگوریتم‌های کلاسیک از مرتبه‌ی $O(N)$ می‌باشد.

سپس بویر الگوریتم جستجوی گروور را بهبود داد و دوور-هویر از الگوریتم بویر برای ارائه‌ی الگوریتم بهینه‌سازی

---

[۵] Quantum gate

[۶] Quantum paralleism

[۷] Shor's Algorithm

[۸] Grover's Algorithm

استفاده کرد.

نقطه‌ی تعادلی نش نقطه‌ای است با این ویژگی که هیچ بازیکنی نمی‌تواند با تغییر استراتژی خود نتیجه‌ی بهتری به‌دست آورد. اساس جستجوی نقطه‌ی تعادلی نش عمل بهینه‌سازی است. پیچیدگی زمانی الگوریتم جستجوی نقطه‌ی تعادلی نش در حالت کلاسیک که اندازه‌ی مجموعه استراتژی آن $N$ می‌باشد برابر $O(N^2)$ است.

در این پایان‌نامه هدف کاهش پیچیدگی زمانی جستجوی نقطه‌ی تعادلی نش در بازی‌های دو نفره است. این مسئله در این پایان‌نامه به دو حالت مورد بحث قرار گرفته است. حالت اول که بازی‌های دو نفره تابع پرداخت درجه دو -دوخطی دارند و حالت دوم بازی‌هایی که توابع پرداخت آن‌ها با فرم نمایش ماتریسی است. دکتر دلاور مسئله‌ی جستجوی نقطه‌ی تعادلی نش در بازی‌های دو نفره با توابع پرداخت درجه دو-دوخطی را به مسئله‌ی بهینه‌سازی تبدیل کردند که در حالت کلاسیک حل این مسئله به زمان $O(N^2)$ نیاز دارد ولی این زمان را با استفاده از الگوریتم بهینه‌سازی کوانتومی دوور-هویر به $O(N)$ کاهش داده‌ایم. و در بازی‌های دونفره که توابع پرداخت آن‌ها با فرم نمایش ماتریسی است با استفاده از الگوریتم بهینه‌سازی کوانتومی دوور-هویر زمان به $O(N\sqrt{N})$ کاهش یافت.

این پایان‌نامه به صورت زیر تنظیم شده است:

در فصل اول مباحثی از جبر خطی که در محاسبات کوانتومی بکار می‌آید، آورده شده است و سپس مقدمه‌ای از محاسبات کوانتومی و ویژگی‌های آن مورد بحث قرار می‌گیرد.

در فصل دوم در ابتدا به تشریح الگوریتم جستجوی گروور پرداخته شده است و بهبود سرعت عمل جستجو با استفاده از الگوریتم جستجوی کوانتومی گروور به نسبت الگوریتم‌های کلاسیک نشان داده شده است. سپس الگوریتم جستجوی بویر تشریح می‌شود و در نهایت الگوریتم بهینه‌سازی کوا.نتومی دوور-هویر ارائه گردیده است که این الگوریتم با استفاده از الگوریتم بویر نقطه‌ی بهینه را پیدا می‌کند.

در فصل سوم به بحث درباره‌ی نظریه‌ی بازی‌ها پرداخته شده است. در این فصل ابتدا تعریف بازی و انواع آن آورده شده و در ادامه نقطه‌ی تعادلی نش در بازی‌ها معرفی گردیده است. در پایان نحوه‌ی کوانتومی‌سازی بازی‌ها مورد بحث قرار گرفته است.

در فصل چهارم روشی برای جستجوی نقطه‌ی تعادلی نش با استفاده از الگوریتم‌های جستجوی کوانتومی ارائه گردیده است. در این روش، ابتدا مسئله‌ی جستجوی نقطه‌ی تعادلی نش به مسئله‌ی بهینه‌سازی تبدیل می‌شود و سپس از الگوریتم دوور-هویر برای جستجوی نقطه‌ی بهینه استفاده می‌گردد.

# فصل ۱

# مقدمات

در این فصل به مطالب مقدماتی مورد نیاز در فصول بعدی پرداخته می شود. برای تکمیل جزییات می تون به منابع [۲۴-۲۲] مراجعه نمود.

### ۱.۰.۱ مقدمه‌ای بر جبر خطی

در این بخش جبر خطی مورد نیاز در محاسبات کوانتومی مطرح خواهد شد.

### فضای برداری

فضای برداری مورد استفاده در مکانیک کوانتومی، فضای برداری $\mathbb{C}^n$، یعنی فضای برداری‌ای متشکل از همه‌ی $n$تایی‌های مرتب از اعداد مختلط، $(z_۱, z_۲, ..., z_n)$ می‌باشد. عناصر فضای برداری را بردار گویند و به شکل یک ماتریس ستونی نمایش داده می‌شود:

$$\begin{pmatrix} z_۱, z_۲, \dots, z_n \end{pmatrix}^T$$

یک عمل جمع در این فضا به صورت زیر تعریف می‌شود:

$$\begin{pmatrix} z_۱, \dots, z_n \end{pmatrix}^T + \begin{pmatrix} z'_۱, \dots, z'_n \end{pmatrix}^T = \begin{pmatrix} z_۱ + z'_۱, \dots, z_n + z'_n \end{pmatrix}^T$$

که عمل‌های جمع در ماتریس سمت راست، عمل‌های جمع معمولی روی اعداد مختلط هستند. همچنین عمل ضرب اسکالر در فضای برداری $\mathbb{C}^n$ به صورت زیر تعریف می‌شود:

$$k \begin{pmatrix} z_۱, \dots, z_n \end{pmatrix}^T = \begin{pmatrix} kz_۱, \dots, kz_n \end{pmatrix}^T$$

که $k$ یک عدد مختلط و عمل‌های ضرب در ماتریس سمت راست، عمل‌های ضرب معمولی روی اعداد مختلط هستند.

در مکانیک کوانتومی علامت استاندار زیر را برای نمایش بردارها به کار می‌برند:

$$|\psi\rangle$$

$\psi$ نامی برای بردار است و $|.\rangle$ علامتی است که نشان می‌دهد شی مورد نظر یک بردار است.

همچنین در هر فضای برداری یک بردار صفر که با علامت $\circ$ نشان داده می‌شود، تعریف می‌شود به طوری که به ازای هر بردار $|v\rangle$ عضو این فضای برداری خاصیت زیر برقرار باشد:

$$|v\rangle + \circ = |v\rangle$$

توجه کنید که علیرغم اینکه بردار صفر، یک بردار است آن را با علامت کت نشان نمی‌دهند، این یک استثنا به شمار می‌رود زیرا در مکانیک کوانتومی $|\circ\rangle$ را به معنای دیگری به کار می‌برند. در فضای برداری $\mathbb{C}^n$، بردار صفر برابر $(\circ, ..., \circ)$ می‌باشد.

## فضای ضرب داخلی

به فضای برداری $\mathcal{H}$ یک فضای ضرب داخلی می‌گویند اگر ضرب داخلی $\langle .,. \rangle$، به نحوی که $\mathcal{H} \times \mathcal{H} \to \mathbb{C}$، تعریف شده باشد و در روابط زیر صدق کند:

۱) $\langle x, x\rangle \geq \circ$، $\langle x, x\rangle = \circ \Leftrightarrow x = \circ$.

۲) $\langle x, y\rangle = \overline{\langle x, y\rangle}$.

۳) $\langle x, \lambda y + z\rangle = \lambda \langle x, y\rangle + \langle x, z\rangle$.

## بهنجار بردار

به ازای بردار $x \in \mathcal{H}$، بهنجار[۱] بردار $x$ به صورت زیر تعریف می‌شود:

$$\|x\| = \sqrt{\langle x, x\rangle}$$

و به ازای دو بردار دلخواه $x, y \in \mathcal{H}$ و عدد $\lambda \in \mathbb{C}$ روابط زیر برقرار باشد:

۱) $\|x\| \geq \circ$، $\|x\| = \circ \Leftrightarrow x = \circ$.

[۱] Norm

۲) $\|\lambda x\| = |\lambda| \, \|x\|$.

۳) $\|x + y\| \leq \|x\| + \|y\|$.

**تعریف ۱.۰.۱ فضای بهنجار:** یک فضای برداری با بهنجار $\|.\|$ فضای بهنجار است.

## دنباله‌ی کوشی

$\{x_n\}$ یک دنباله‌ی کوشی نامیده می‌شود هرگاه به ازای هر $\varepsilon > ۰$، $N > ۰$ وجود داشته باشد که:

$$\forall m, n > N \qquad |x_m - x_n| < \varepsilon$$

## فضای کامل

در یک فضای بهنجار $\mathcal{H}$ اگر همه‌ی دنباله‌های کوشی $\mathcal{H}$ متناهی باشد، فضا کامل است. به عبارتی اگر بردار $x \in \mathcal{H}$ وجود داشته باشد که $\|x_n - x\| \to ۰$ برقرار باشد.

## فضای هیلبرت

یک فضای ضرب داخلی اگر کامل باشد فضای هیلبرت[۲] نامیده می‌شود.

## عملگرهای خطی

هر عملگر خطی بین فضای برداری $V$ و $W$ به صورت تابع $A : V \to W$ تعریف می‌شود به طوری که نسبت به ورودی‌هایش خطی باشد:

$$A\left(\sum_i a_i \left|v_i\right\rangle\right) = \sum_i a_i A\left(\left|v_i\right\rangle\right) \qquad (۱\text{-}۰.۱\text{-}۱)$$

معمولاً $A\left(\left|v\right\rangle\right)$ به صورت ساده با $A\left|v\right\rangle$ نشان داده می‌شود. هنگامی که گفته می‌شود که عملگر خطی روی فضای $V$ تعریف شده است منظور این است که یک عملگر خطی به صورت $V \to V$ تعریف شده است.

یکی از مهمترین عملگرهای خطی در هر فضای برداری $V$ عملگر همانی $I_v$ می‌باشد که با معادله:

$$I_v \left|v\right\rangle = \left|v\right\rangle$$

تعریف می‌شود. یکی دیگر از عملگرهای خطی در هر فضای برداری عملگر صفر می‌باشد. عملگر صفر هر بردار از فضا را به بردار صفر نگاشت می‌کند: $۰ \left|v\right\rangle = ۰$ از رابطه‌ی ( ۱-۱-۰.۱-۱) به سادگی می‌توان فهمید که اگر عملِ

[۲] Hilbert

عملگر $A$ برای هر بردار پایه از فضای برداری $V$ معلوم باشد آنگاه عمل $A$ روی هر بردار دیگر از این فضا نیز تعریف شده است. فرض کنید $V$ و $W$ و $X$ فضای برداری باشند و $A : V \to W$ و $B : W \to X$ عملگرهای خطی باشند. ترکیب این دو عملگر $B(A(|v\rangle))$ را به صورت ساده با $BA|v\rangle$ نشان می‌دهیم.

راه معمول برای نوشتن عملگرهای خطی، نمایش ماتریسی آن‌ها می‌باشد. پر واضح است که هر ماتریس $A$ با ابعاد $m \times n$ از اعداد مختلط در واقع یک عملگر خطی از $\mathbb{C}^n$ به $\mathbb{C}^m$ می‌باشد. در صورتی که $A|v\rangle$ را به صورت ضرب ماتریس $A$ در بردار $|v\rangle$ تعریف کنیم:

$$A|v\rangle = |w\rangle \quad \Rightarrow \quad \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}_{m\times n} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}_{n\times 1} = \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix}_{m\times 1}$$

فرض کنید $A : V \to W$ یک عملگر خطی از فضای برداری $V$ به $W$ تعریف شده باشد. همچنین فرض کنید $|v_1\rangle, \ldots, |v_n\rangle$ مجموعه پایه برای فضای $V$ و $|w_1\rangle, \ldots, |w_m\rangle$ مجموعه پایه برای فضای $W$ باشد. بنابراین به ازای هر $i$ از محدوده $1, \ldots, m$ اعداد مختلط $A_{i1}, \cdots, A_{in}$ وجود دارد به‌طوری‌که:

$$|w_i\rangle = \sum_{j=1}^{n} a_{ij} |v_j\rangle$$

ماتریسی که درایه‌های آن $a_{ij}$ها باشند را نمایش ماتریسی عملگر خطی $A$ گویند.

## ماتریس پاولی

چهار تا از ماتریس‌های پر استفاده در محاسبات کوانتومی، ماتریس‌های پاولی[3] می‌باشد. ماتریس‌های پاولی، ماتریس‌های $2 \times 2$ هستند که در شکل زیر آورده شده است:

$$\sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

[3] pauli

## عملگرهرمیتی[۴]

$A^\dagger$ را مزدوج هرمیتی ماتریس $A$ گویند و به صورت $A^\dagger = (A^*)^T$ تعریف می‌شود که $*$ در آن مزدوج مختلط و $T$ ترانهاده ماتریس می‌باشد.

## عملگر یکانی[۵]

ماتریس $U$ یکانی گفته می‌شود اگر

$$UU^\dagger = U^\dagger U = I$$

که $I$ ماتریس همانی است. به یک عملگر، یکانی گفته می‌شود اگر و فقط اگر هر کدام از نمایش‌های ماتریسی آن یکانی باشد. عملگرهای یکانی از این نظر دارای اهمیت هستند که اندازه‌ی بردارها را حفظ می‌کنند. برای بررسی این گفته فرض کنید $v$ یک بردار دلخواه و $U$ یک عملگر یکانی باشد. بردار $w$ از اعمال عملگر $U$ بر بردار $v$ حاصل شده است و به دلیل یکانی بودن عملگر $U$، اندازه‌ی بردار $v$ و $w$ برابر است:

$$w = Uv$$

$$|w| = w^\dagger w = v^\dagger U^\dagger U v = v^\dagger v = |v|$$

## ضرب تانسوری[۶]

ضرب تانسوری راهی است برای ترکیب فضاهای برداری و ساخت فضای برداری بزرگتر. ضرب تانسوی با علامت $\otimes$ نشان داده می‌شود. فرض کنید $V$ و $W$ دو فضای هیلبرت به ترتیب با ابعاد $m$ و $n$ بعدی باشد آنگاه $V \otimes W$ یک فضای $mn$ بعدی است به طوری که عناصر آن ترکیب خطی‌ای از ضرب تانسوری $|v\rangle \otimes |w\rangle$ می‌باشد که $|v\rangle$ عنصری از $V$ و $|w\rangle$ عنصری از $W$ است. معمولاً ضرب تانسوری $|v\rangle \otimes |w\rangle$ به صورت خلاصه با $|v\rangle|w\rangle$ یا $|v, w\rangle$ یا حتی $|vw\rangle$ نمایش داده می‌شود. برای مثال اگر $V$ فضای برداری دوبعدی با بردارهای پایه $|۰\rangle$ و $|۱\rangle$ باشد، آنگاه $|۱\rangle \otimes |۱\rangle + |۰\rangle \otimes |۰\rangle$ عنصری از $V \otimes V$ به حساب می‌آید.

خواص زیر در ضرب تانسوری برقرار است:

---

[۴] Hermitian operator

[۵] unitary

[۶] tensor product

۱. برای یک مقدار اسکالر داریم:

$$z\left(|v\rangle \otimes |w\rangle\right) = \left(z\,|v\rangle\right) \otimes |w\rangle = |v\rangle \otimes \left(z\,|w\rangle\right)$$

۲. برای هر $|v_۱\rangle$ و $|v_۲\rangle$ عضو $V$ و $|w\rangle$ عضو $W$ داریم:

$$\left(|v_۱\rangle + |v_۲\rangle\right) \otimes |w\rangle = |v_۱\rangle \otimes |w\rangle + |v_۲\rangle \otimes |w\rangle$$

۳. برای هر $|v\rangle$ عضو $V$ و $|w_۱\rangle$ و $|w_۲\rangle$ عضو $W$ داریم:

$$|v\rangle \otimes \left(|w_۱\rangle + |w_۲\rangle\right) = |v\rangle \otimes |w_۱\rangle + |v\rangle \otimes |w_۲\rangle$$

ضرب تانسوری روی عملگرها نیز تعریف می‌شود. فرض کنید $|v\rangle$ عنصری از فضای برداری $V$ و $|w\rangle$ عنصری از فضای برداری $W$ باشد و $A$ و $B$ دو عملگر باشند که به ترتیب روی $|v\rangle$ و $|w\rangle$ تعریف شده است. آنگاه می‌توان عملگر خطی $A \otimes B$ را روی فضای به صورت زیر تعریف کرد:

$$\left(A \otimes B\right)\left(|v\rangle \otimes |w\rangle\right) = A\,|v\rangle \otimes B\,|w\rangle$$

به طور کلی ضرب تانسوری عملگرها را می‌توان به این صورت تعریف کرد. اگر دو عملگر به صورت $A : V \to V'$ و $B : W \to W'$ تعریف شده باشد. یک عملگر دلخواه که $V \otimes W$ را به $V' \otimes W'$ نگاشت می‌کند به صورت ترکیب خطی ضرب تانسوری عملگرهایی که $V$ را به $V'$ و $W$را به $W'$ نگاشت می‌کنند، تعریف می‌شود: $C = \sum_i c_i A_i \otimes B_i$ در نمایش ماتریسی فرض کنید که $A$ یک ماتریس $m \times n$ و $B$ یک ماتریس $p \times q$ باشد. آنگاه ضرب تانسوری این دو ماتریس را به صورت زیر نمایش می‌دهیم:

$$A \otimes B = \overbrace{\left.\begin{pmatrix} A_{۱۱}B & A_{۱۲}B & \cdots & A_{۱n}B \\ A_{۲۱}B & A_{۲۲}B & \cdots & A_{۲n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m۱}B & A_{m۲}B & \cdots & A_{mn}B \end{pmatrix}\right\} mp}^{nq}$$

در این نمایش عباراتی همچون $A_{۱۱}B$ نشان دهنده زیرماتریس‌هایی با ابعاد $p \times q$ است به طوری که عناصر آن برابر ماتریس $B$ ضرب در ثابت $A_{۱۱}$ می‌باشد. به عنوان مثال ضرب تانسوری بردارهای $(۱, ۲)$ و $(۲, ۳)$ به

صورت زیر می‌باشد:

$$\begin{pmatrix} ۱ \\ ۲ \end{pmatrix} \otimes \begin{pmatrix} ۲ \\ ۳ \end{pmatrix} = \begin{pmatrix} ۱ \times ۲ \\ ۱ \times ۳ \\ ۲ \times ۲ \\ ۲ \times ۳ \end{pmatrix} = \begin{pmatrix} ۲ \\ ۳ \\ ۴ \\ ۶ \end{pmatrix}$$

و یا ضرب تانسوری ماتریس‌های پاولی $X$ و $Y$ برابر:

$$X \otimes Y = \begin{pmatrix} ۰.Y & ۱.Y \\ ۱.Y & ۰.Y \end{pmatrix} = \begin{pmatrix} ۰ & ۰ & ۰ & -i \\ ۰ & ۰ & i & ۰ \\ ۰ & -i & ۰ & ۰ \\ i & ۰ & ۰ & ۰ \end{pmatrix}$$

می‌باشد. در پایان علامت $|\psi\rangle^{\otimes k}$ را برای $k$ بار ضرب تانسوری بردار $|\psi\rangle$ در هم تعریف می‌کنیم. مثلا $|\psi\rangle^{\otimes ۲} = |\psi\rangle \otimes |\psi\rangle$.

## ۱.۱ محاسبات کوانتومی

### ۱.۱.۱ کیوبیت

در کامپیوترهای کلاسیک یک بیت در یکی از دو وضعیت ۰ یا ۱ قرار دارد ولی در کامپیوترهای کوانتومی یک بیت در وضعیت ترکیب خطی از وضعیت‌های پایه‌ی ۰ و ۱ می‌باشد که وضعیت‌های پایه در کامپیوتر کوانتومی با $|۰\rangle$ و $|۱\rangle$ نشان داده می‌شود. $|.\rangle$ (کت[۷]) در نمادگذاری دیراک نشان‌دهنده بردار ستونی و $\langle.|$ (برا[۸])نشان‌دهنده بردار سطری است:

$$|۰\rangle = \begin{pmatrix} ۱ \\ ۰ \end{pmatrix} \qquad |۱\rangle = \begin{pmatrix} ۰ \\ ۱ \end{pmatrix}$$

$$\langle ۰| = \begin{pmatrix} ۱ & ۰ \end{pmatrix} \qquad \langle ۱| = \begin{pmatrix} ۰ & ۱ \end{pmatrix}$$

[۷] ket

[۸] bra