



دانشکده فیزیک
گروه فیزیک

پایان نامه

برای دریافت درجه کارشناسی ارشد در رشته
فیزیک، گرایش ذرات بنیادی

عنوان

الگوریتم جستجوی کوانتومی گراور با
استفاده از فرمالیزم جبر هندسی
کلیفورد

استاد راهنما

دکتر حسین موحدیان

دانشجو

کوثر السادات تفلخ

۱۳۹۳

سید

ماحصل آموختہ ہایم را تقدیم می کنم بہ آنان کہ مہر آسمانی شان آرام بخش آلام
زمینی ام است

تقدیم بہ پدر و مادر عزیز تر از جانم

و استاد بزرگوارم دکتر حسین موحدیان

بوسہ بردستان پر مہرمان

پروردگارا...۱

پروردگارا به درگاه تو پناه می‌آورم و تو نیز پناهم بخش تا موجودی آزمند و خویشتن دوست نباشم.

مگذار که صولت خشم حصار بردباری مرا درهم بشکند و حمله‌ی حسد مناعت فطرت مرا به خفت و مذلت فرو کشاند.

پروردگارا از بدخویی که دل دوستان بشکند و به دشمنان نشاط و نیرو بخشد، از لجاج شهوت که همت‌های بلند را پست سازد و پرده‌ی عفاف و عصمت چاک زند به درگاه تو پناه می‌آورم.

پروردگارا روا مدار که سر به دنبال هوس بگذارم و در ظلمات جهل و ضلال از چراغ هدایت به دور افتم و بیغوله را از شاهراه باز نشناسم. روا مدار که به خواب غفلت فرو افتم و کیفر غفلت خویش بینم. آن چنان کن که خاطر زیر دستان ما از دست ما نرنجند و زیر دستان ما که در حق ما محبت و مرحمت روا داشته اند از پاداش سپاس ما خشنود شوند.

آن چنان کن که قدر نعمت بدانیم و شکر نعمت به جای آوریم.

سپاس گزارمی...

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت‌های او ندانند و کوشندگان، حق او را گزاردن نتوانند...

با تقدیر و تشکر شایسته از استاد فرهیخته جناب آقای دکتر حسین موحدیان که با نکته‌های دلاویز و گفته‌های بلند، صحیفه‌های سخن را علم‌پرور نمود و همواره راهنما و راه‌گشای نگارنده در اتمام و اکمال پایان نامه بوده است.

و بعد از مدت‌ها، پس از پیمودن راه‌های فراوان که با حضور شیرین اساتید عزیزم، با راهنمایی‌ها و دغدغه‌های فراوانشان و شیطنت‌های زیبای آن دوران، نگاه‌های دلسوز پدر و مادر عزیزتر از جانم، با چشم‌های پر از برق شوق، و زیبایی حضور خواهرانم و برادر عزیزم محمد مصطفی در کنارم، که خستگی‌های این راه را به امید و روشنی راه تبدیل کرده و امیدوارم بتوانم در آینده‌ای نزدیک جوابگوی این همه محبت آن‌ها باشم ...

- با سپاس بی‌دریغ خدمت دوستان گران‌مایه‌ام خانم‌ها، مریم خان احمدی، مهشید اخوان‌نژاد، مریم برزویی بیدگلی، احمد کاوه و مجید مرادی که مرا صمیمانه و مشفقانه یاری داده‌اند. از استادان شایسته جناب آقایان دکتر علی اکبر رجبی و دکتر مرتضی رفیعی که زحمت داوری این رساله را متقبل شدند، نهایت تشکر و قدردانی را دارم.

- و با تشکر خالصانه خدمت همه کسانی که به نوعی مرا در به انجام رساندن این مهم یاری نموده‌اند.

تعمدنامه

- اینجانب کوثرالسادات تفاخ دانشجوی کارشناسی ارشد رشته فیزیک دانشکده فیزیک دانشگاه شاهرود، نویسنده پایان‌نامه با عنوان الگوریتم جستجوی کوانتومی گراور با استفاده از فرمالیزم جبر هندسی کلیفورد، تحت راهنمایی دکتر حسین موحدیان متعهد می‌شوم:
- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
 - در استفاده از نتایج پژوهش‌های دیگر پژوهش‌گران، به مرجع مورد استفاده استناد شده است.
 - مطالب این پایان‌نامه، تا کنون توسط خود، یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارایه نشده است.
 - حقوق معنوی این اثر، به دانشگاه شاهرود متعلق دارد، و مقالات مستخرج با نام “دانشگاه شاهرود” یا “University of Shahrood” به چاپ خواهد رسید.
 - حقوق معنوی تمام افرادی که در به‌دست آوردن نتایج اصلی پایان‌نامه تاثیرگذار بوده‌اند، در مقالات مستخرج از پایان‌نامه رعایت می‌گردد.
 - در تمام مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافت‌های آنها) استفاده شده است، ضوابط و اصول اخلاقی رعایت شده است.
 - در تمام مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته (یا استفاده) شده است، اصل رازداری و اصول اخلاق انسانی رعایت شده است.

کوثرالسادات تفاخ
۱۳۹۳

مالکیت نتایج و حق نشر

- تمام حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) متعلق به دانشگاه شاهرود می‌باشد. این مطلب باید به نحو مقتضی، در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در این پایان‌نامه بدون ذکر منبع مجاز نمی‌باشد.

چکیده

یکی از مسائلی که توسط الگوریتم‌های کوانتومی با سرعت بیشتر نسبت به الگوریتم‌های کلاسیک حل می‌شود، مربوط به مسئله‌ی جستجو است. الگوریتم جستجوی کوانتومی که اصول اولیه‌ی آن توسط گراور مطرح شد، به عنوان یکی از بهترین روش‌های جستجوی کوانتومی قادر است که با سرعت قابل توجهی $O(N)$ (در کامپیوترهای کلاسیک) را به $O(\sqrt{N})$ (در کامپیوترهای کوانتومی) کاهش دهد که برای N های بزرگ کاهش قابل ملاحظه‌ای دارد.

ما در این پایان‌نامه قصد داریم تا الگوریتم جستجوی گراور را با استفاده از فرمالیزم جبر کلیفورد فرمول‌بندی کنیم.

ابتدا نشان می‌دهیم که جبر هندسی کلیفورد نمایش ساده‌تر و مهم‌تری نسبت به نمادگذاری براکت دیراک دارد و در مرحله‌ی دوم، با استفاده از ضریب وزنی بیشینه و کمینه در فضای جستجوی گراور، پایه‌هایی تعریف می‌کنیم که این امکان را به ما می‌دهد تا تصویر ساده‌ای از جستجوی گراور مشابه با حرکت تقدیمی ذره‌ای با اسپین $\frac{1}{2}$ داشته باشیم. با استفاده از این فرمالیزم جستجوی دقیق و کاملی را حل می‌کنیم.

ما ادعا نمی‌کنیم که الگوریتم بهتری ایجاد می‌کنیم، اما نشان می‌دهیم که جبر هندسی، به‌طور واضح تفسیر زیبایی از الگوریتم جستجوی گراور را بیان می‌کند.

در انتهای پایان‌نامه ابتدا عملگر جدیدی را پیشنهاد می‌دهیم و نشان می‌دهیم که این عملگر یکانی همانند عملگر هادامارد در الگوریتم جستجوی کوانتومی گراور عمل کرده و با احتمال بسیار بالایی با $O(\sqrt{N})$ تکرار الگوریتم به حالت مورد جستجو دسترسی پیدا می‌کند. با این تفاوت که این عملگر مفهوم فیزیکی جالبی دارد و آن این است که عملگر جدید T شبیه به ماتریس پائولی σ_y است.

در مرحله‌ی بعدی، عملگر یکانی دیگری مانند T' را در نظر می‌گیریم. برای ایجاد برهم‌نهی از تمامی حالات پایه، عملگر پیشنهادی T' را بر روی حالت دلخواه اثر می‌دهیم و الگوریتم جستجوی کوانتومی گراور را برای این مسئله حل می‌کنیم. هدف پیدا کردن عملگر پیشنهادی T' و حالت دلخواه اولیه است. همچنین بررسی می‌کنیم به ازای چند مرتبه تکرار عملگر جدید با احتمال بالایی به حالت مورد نظر دست پیدا خواهیم کرد.

پیشگفتار

پردازش ماشینی اطلاعات، در هر شکلی بر مبنای محاسبات کلاسیک انجام می‌شود اما روش بهتر برای پردازش اطلاعات بر اساس مکانیک کوانتومی می‌باشد. این روش جدید با ویژگی‌هایی همراه است که آن را از محاسبات کلاسیک متمایز می‌سازد؛ البته وجود تفاوت بین این دو به معنای حذف یکی و جایگزینی دیگری نیست. در دهه ۱۹۸۰ هنگامی که ایده کامپیوترهای کوانتومی ابتدا توسط ریچارد فاینمن^۲ و سپس به شکل منسجم‌تر توسط دیوید دویچ^۳ مطرح شد توانایی نظری این ماشین‌ها در انجام محاسبات موازی مثل یک تردستی عجیب به نظر می‌رسید اما در سال ۱۹۹۴ اتفاقی افتاد که باعث شد محاسبات کوانتومی به هدف دولت‌ها، نیروهای نظامی و هرکس دیگری که اسرار دیجیتالی داشت تبدیل شود.

در این پایان نامه قصد داریم که با استفاده از جبر کلیفورد عملگرهای الگوریتم گراور را به شکل جدیدی بیان کنیم که باعث ساده شدن محاسبات پیچیده‌تر می‌شود. این مجموعه شامل ۵ فصل و ۱ ضمیمه است. مطالب هر فصل به طور مختصر عبارتست از:

- در فصل ۱، مقدمه، نگاهی بر تاریخچه موضوع مورد بررسی آورده شده است. بنا به ضرورت مقدماتی از مفاهیم اطلاعات کوانتومی و مفاهیم محاسبات کوانتومی ذکر گردیده است. در ادامه در مورد ویژگی‌های یک کامپیوتر کوانتومی صحبت شده است.
- در فصل ۲ نگاهی به جبر کلیفورد می‌اندازیم و در ادامه انعکاس و دوران را در این فضا بررسی می‌کنیم.
- در فصل ۳ الگوریتم جستجوی کوانتومی گراور را با استفاده از فرمالیزم برا-کت دیراک توضیح می‌دهیم.
- در فصل ۴ الگوریتم جستجوی کوانتومی گراور را با استفاده از فرمالیزم جبر کلیفورد فرمول‌بندی می‌کنیم و سپس آن را به دوران کلی تعمیم می‌دهیم.
- در فصل ۵ عملگر جدیدی را پیشنهاد می‌دهیم که در جستجوی کوانتومی گراور همانند عملگر هادامارد عمل کرده و بعد از $O(\sqrt{N})$ با احتمال بالایی به جواب مورد نظر دسترسی پیدا می‌کنیم.
- در ضمیمه، به اثبات روابط مندرج در پایان‌نامه پرداخته‌ایم.

^۲Richard Feynman

^۳David Deutsch

لیست مقالات مستخرج از پایان نامه

۱. تفاق کوثرالسادات، موحدیان حسین، استفاده از جبر کلیفورد در الگوریتم جستجوی کوانتومی گراور، همایش ملی علوم و مهندسی کامپیوتر زیرمجموعه نهمین سمپوزیوم پیشرفتهای علوم و تکنولوژی، موسسه آموزش عالی خاوران مشهد، پذیرش برای سخنرانی، چاپ در سیویلیکا، ۱۳ آذرماه ۱۳۹۳.
۲. تفاق کوثرالسادات، موحدیان حسین، الگوریتم جستجوی کوانتومی گراور دقیق تعمیم یافته در جبر کلیفورد، دومین همایش ملی پژوهش‌های کاربردی در ریاضی و فیزیک، دانشگاه جامع علمی کاربردی تهران، پذیرش برای سخنرانی، چاپ در سیویلیکا، ۲ بهمن ۱۳۹۳.
۳. تفاق کوثرالسادات، موحدیان حسین، الگوریتم جستجوی کوانتومی گراور، دومین همایش ملی پژوهش‌های کاربردی در علوم کامپیوتر و فناوری اطلاعات، دانشگاه جامع علمی کاربردی تهران، پذیرش برای پوستر، چاپ در سیویلیکا، ۷ اسفند ۱۳۹۳.

فهرست مطالب

۱	مقدمه	۱
۲	مقدمه	۱.۱
۳	مفاهیم مقدماتی محاسبات کوانتومی	۱.۱.۱
۵	اطلاعات کوانتومی و محاسبات کوانتومی	۲.۱.۱
۷	منطق کوانتومی و برهم‌نهی	۳.۱.۱
۹	کامپیوتر کوانتومی	۲.۱
۹	کامپیوتر کوانتومی چیست؟	۱.۲.۱
۱۰	بیت و کیوبیت	۲.۲.۱
۱۲	تداخل کوانتومی	۳.۲.۱
۱۳	ارزیابی تابع و توازی کوانتومی	۴.۲.۱
۱۵	گیت کوانتومی و گیت کلاسیکی	۵.۲.۱
۲۲	مدارهای کوانتومی	۶.۲.۱
۲۵	جبر کلیفورد	۲
۲۶	مقدمه	۱.۲
۲۹	تبدیلات هندسی	۲.۲
۲۹	انعکاس	۱.۲.۲
۳۱	دوران	۲.۲.۲
۳۳	الگوریتم‌های کوانتومی	۳
۳۴	الگوریتم دویچ	۱.۳
۳۵	الگوریتم دویچ-جوزا	۲.۳
۳۶	الگوریتم گراور استاندارد	۳.۳
۴۹	کاربرد جبر کلیفورد در الگوریتم جستجوی کوانتومی	۴
۵۰	مقدمه	۱.۴

۵۳	بردارهای پایه اصلاح شده برای فضای جستجو	۲.۴
۵۶	عملگر جستجوی گراور در جبر هندسی	۳.۴
۵۸	جستجوی گراور کامل و دقیق	۴.۴
۵۹	شرایط فازی	۱.۴.۴
۶۲	جستجوی گراور دقیق تعمیم یافته	۵.۴
۶۵	عملگر پیشنهادی جدید برای الگوریتم جستجوی کوانتومی گراور	۵
۶۶	مقدمه	۱.۵
۶۶	روش محاسبات عملگر پیشنهادی T	۲.۵
۷۰	روش محاسبات T'	۳.۵
۷۵	اثبات روابط مندرج در پایان نامه	آ
۷۶	اثبات روابط فصل ۴	۱.آ
۹۰		مراجع
۹۲		نمایه

فصل ١

مقدمه

۱.۱ مقدمه

نظریه کامپیوترکوانتومی از سال ۱۹۸۲ مطرح بوده است از زمانی که فیزیکدان مشهور و برنده جایزه نوبل «ریچارد فاینمن» برای نخستین بار، پیشنهاد کرد که باید محاسبات از دنیای دیجیتال وارد دنیای کوانتومی شود، همچنین بیان کرد کامپیوتر کوانتومی چگونه ممکن است کار کند. این پیشنهاد تا اوایل سال ۱۹۹۰ مورد توجه جدی قرار نگرفت و به صورت آکادمیک باقی ماند، البته در سال ۱۹۸۵، دویچ متوجه شد که اظهارات فاینمن، می‌تواند تدریجاً به ساخت کامپیوتر کوانتومی منجر شود و مقاله‌ای را منتشر کرد مبنی بر اینکه اصولاً هر فرآیند فیزیکی را می‌توان به خوبی با کامپیوترهای کوانتومی مدل سازی کرد.

بالاخره در ۱۹۹۴ «پیترو شور» نخستین گام را برای محقق کردن این آرزو برداشت. وقتی که بعضی از مشکلات کلیدی کامپیوترهای معمولی نشان داده شد، کامپیوترهای کوانتومی در اصل می‌توانستند خارج از رونوشت‌های کلاسیکی خود محاسبات را انجام دهند و اجرا نمایند یعنی کارایی بسیار بالاتری را نسبت به کامپیوترهای معمولی از خود نشان می‌دادند. وی مقاله‌ای را منتشر نمود که حاوی روشی برای استفاده از کامپیوترهای کوانتومی در حل مشکل پیچیده‌ای در نظریه اعداد، به نام فاکتورگیری بود.

او نشان داد که چگونه یک مجموعه از عملیات ریاضی که منحصراً برای کامپیوترهای کوانتومی طراحی شده‌اند، می‌توانند چنین دستگاهی را به انجام فاکتورگیری از اعداد بیشماری با سرعت بالاتر از کامپیوترهای کلاسیک، قادر سازد. با این اختراع، محاسبات کوانتومی از یک کنجکاوی به یک توجه جهانی تبدیل شد.

از آن موقع به بعد، گروه‌های تحقیقاتی در سرتاسر دنیا مسابقه‌ای را برای پیش قدم شدن در ساخت یک سیستم عملی آغاز نمودند. به این ترتیب ارتباط نوینی بین نظریه‌ی اطلاعات و فیزیک کوانتومی شروع به شکل‌گیری کرد که امروزه آن را محاسبات کوانتومی یا محاسبات نانو متری^۱ می‌نامیم. محاسبات کوانتومی مشکلات گذشته را برطرف می‌سازد و افق جدیدی را ایجاد می‌کند.

قدرت خارق‌العاده کامپیوتر کوانتومی در نتیجه وقوع پدیده‌ای موسوم به توازی کوانتومی، مکانیزمی که انجام و اجرای محاسبات حجیم، زیاد و مکرر را به طور هم‌زمان مقدور می‌سازد. این یک مقابله سخت و نیرومند و فرق نمایان و بزرگ با کامپیوترهای کلاسیک

^۱ Nano Computing

است که قادرند تنها هر عملیات را فقط به صورت یک عمل در هر دفعه و البته خیلی سریع انجام دهند.

اغلب کامپیوترهای دیجیتال امروزی بر مبنای بیت‌ها یا بایتهایی کار می‌کنند که محدود به 0 و 1 هستند. اما کامپیوتر کوانتومی وسیله‌ای محاسباتی است که به جای بیت‌ها دارای کیوبیت‌ها است. کیوبیت مخفف کوانتوم-بیت است که در هر زمان نمایانگر بیش از یک عدد است. یک کامپیوتر مبتنی بر بیت‌های کوانتومی، تعداد حالات پایه بیشتری نسبت به کامپیوترهای معمولی دارد و به طور هم‌زمان می‌تواند دستورات بیشتری اجرا کند. یکی از قابلیت‌های کامپیوترهای کوانتومی که موجب تفاوت آنها با کامپیوترهای کلاسیک می‌شود بحث موازی بودن ذاتی پردازش در آنها است.

کامپیوتر کوانتومی به عنوان یک ماشین محاسبه‌گر، از گیت‌های منطقی برای پردازش اطلاعات بهره می‌برد. تفاوت عمده میان گیت‌های منطقی کلاسیک و کوانتومی آن است که ورودی و خروجی گیت‌های کوانتومی می‌تواند حالت برهم‌نهی یک کیوبیت نیز باشد. یکی از گیت‌های منطقی کوانتومی، گیت $CNOT$ است. در بخش‌های بعدی همراه با چندین نمونه به توضیح بیشتر گیت‌های کوانتومی و کلاسیکی خواهیم پرداخت.

۱.۱.۱ مفاهیم مقدماتی محاسبات کوانتومی

در محاسبات کوانتومی به جای مقادیر 0 و 1 بیت، از مقادیر 0 و 1 کیوبیت استفاده می‌شود. یک کیوبیت علاوه بر 0 و 1 می‌تواند در برهم‌نهی از 0 و 1 نیز قرار بگیرد (که نمادگذاری برا-کت دیراک در مکانیک کوانتومی است). به عبارتی برای حالت‌های $|0\rangle$ و $|1\rangle$ کیوبیت کلی می‌تواند به صورت ترکیب خطی زیر باشد

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1.1)$$

که α و β اعداد مختلط هستند و دامنه‌های حالات نامیده می‌شوند. $|\psi\rangle$ برداری در فضای برداری دوبعدی مختلط است که $\{|0\rangle, |1\rangle\}$ پایه‌های متعامد را تشکیل می‌دهند و پایه‌های محاسباتی نامیده می‌شوند. نمایش ماتریسی $|0\rangle$ و $|1\rangle$ به صورت زیر داده می‌شود:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

تفسیر فیزیکی در معادله‌ی (۱.۱) این است که حالت $|\psi\rangle$ می‌تواند به‌طور هم‌زمان در حالت $|0\rangle$ و $|1\rangle$ باشد. حالت $|\psi\rangle$ می‌تواند کوله‌باری از اطلاعات باشد اما این اطلاعات در سطح کوانتومی باقی می‌ماند. در سطح کوانتومی باید اندازه‌گیری روی کیوبیت انجام شود. مکانیک کوانتومی به ما می‌گوید که فرآیند اندازه‌گیری، حالت کیوبیت را آشفته می‌کند و در نهایت حالت $|\psi\rangle$ به یکی از پایه‌های $|0\rangle$ یا $|1\rangle$ فروریزش می‌کند. با احتمال $|\alpha|^2$ حالت $|0\rangle$ و با احتمال $|\beta|^2$ حالت $|1\rangle$ را پیدا می‌کنیم که:

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2.1)$$

برای توصیف حالات بیشتر از یک کیوبیت، مفهوم کلی ضرب تانسوری باید اعمال شود.

در مکانیک کوانتومی معمولاً با سیستم‌های چند ذره‌ای سروکار داریم. برای بررسی یک سیستم چند ذره‌ای به یک فضای هیلبرت کلی برای این سیستم نیاز داریم. برای تشکیل این فضای هیلبرت از ضرب تانسوری فضای هیلبرت هر یک از ذرات استفاده می‌کنیم. برای این منظور از تعریف زیر استفاده می‌کنیم. ضرب تانسوری $|v\rangle \otimes |w\rangle$ به‌صورت زیر داده می‌شود:

$$|v\rangle \otimes |w\rangle = \begin{pmatrix} v_1 |w\rangle \\ \vdots \\ v_m |w\rangle \end{pmatrix}$$

کت حالت توصیف‌کننده‌ی این سیستم دو ذره‌ای به‌صورت زیر حاصل می‌شود:

$$|\psi\rangle = \sum_{i,j} \alpha_{i,j} |v_i\rangle \otimes |w_j\rangle$$

که $|v\rangle \in C^n$ و $|w\rangle \in C^m$ و v_1, \dots, v_n مختصات بردار $|v\rangle$ هستند. نمادگذاری دیگری از ضرب تانسوری می‌تواند به‌صورت $|v, w\rangle$ و $|v\rangle |w\rangle$ نیز باشد. چند خاصیت از ضرب تانسوری:

۱.

$$|v\rangle \in C^n, \quad |w\rangle \in C^m \rightarrow |v\rangle \otimes |w\rangle \in C^n \otimes C^m \quad (3.1)$$

بعد فضای هیلبرت بزرگتر، برابر ضرب اعداد فضاهای هیلبرت کوچکتر است.

۲. اگر $|v\rangle$ و $|w\rangle$ هرمیتی باشند، آنگاه $|v\rangle \otimes |w\rangle$ نیز هرمیتی است.

۳. اگر $|v\rangle$ و $|w\rangle$ یکانی باشند، آنگاه $|v\rangle \otimes |w\rangle$ نیز یکانی است.

در حالت کلی، حالت $|\psi\rangle$ شامل n کیوبیت در یک کامپیوتر کوانتومی، برهم‌نهی از 2^n حالت $\{|0\rangle, |1\rangle, \dots, |2^n - 1\rangle\}$ است:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \quad (4.1)$$

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1 \quad (5.1)$$

نتیجه‌ی حاصل از اندازه‌گیری حالت $|\psi\rangle$ ، یافتن حالت $|i_0\rangle$ با احتمال $|\alpha_{i_0}|^2$ است که $0 \leq i_0 < 2^n$.

دو بردار $|\psi\rangle$ و $|\varphi\rangle$ در فضای برداری V داده شده‌اند. ضرب داخلی این دو بردار به صورت $\langle\psi|\varphi\rangle$ و ضرب خارجی آنها به صورت $|\psi\rangle\langle\varphi|$ داده می‌شود. اعمال ضرب خارجی بر روی بردار $|v\rangle$ به صورت زیر تعریف می‌شود:

$$(|\psi\rangle\langle\varphi|)|v\rangle = \langle\varphi|v\rangle|\psi\rangle, \forall |v\rangle \in V \quad (6.1)$$

۲.۱.۱ اطلاعات کوانتومی و محاسبات کوانتومی

در دنیای امروز کامپیوترهای کوانتومی را در دو حیطة مجزا یاد می‌کنند: حیطة اول رمزنگاری کوانتومی است. یعنی شما بتوانید پیامی را به صورت رمز درآورده و برای گیرنده بفرستید، بدون آنکه شخص دیگری متوجه محتوی آن شود و اگر این اتفاق افتاد شخص گیرنده متوجه شود. حیطة دوم حل مسئله کوانتومی است، مسائلی نظیر شبیه سازی پدیده‌های مختلف فیزیکی توسط کامپیوتر و کار کردن با اعداد بسیار بزرگ و جستجوی پایگاه داده‌ها.

اما واقعا پردازش از جنس کامپیوتر کوانتومی چه تفاوتی با پردازش از جنس کامپیوتر کلاسیک دارد؟ پاسخ به این سوال را در بخش‌های بعدی خواهیم یافت.

رویای محاسبات ماشینی یا ماشینی که بتواند مسائل را در اشکال گوناگون حل کند کمتر از دو قرن است که زندگی بشر را به‌طور جدی دربر گرفته است. اگر از ابزارهایی نظیر چرتکه و برخی تلاش‌های پراکنده دیگر در این زمینه بگذریم، شاید بهترین شروع را بتوان به تلاش‌های «چارلز بابیج» و «بلز پاسکال» با ماشین محاسبه مکانیکی‌شان نسبت داد. با گذشت زمان و تا ابتدای قرن بیستم تلاش‌های زیادی جهت بهبود ماشین محاسب مکانیکی صورت گرفت که همه آن‌ها بر پایه ریاضیات دهدهی^۲ بود، یعنی این ماشین‌ها محاسبات را همان‌طور که ما روی کاغذ انجام می‌دهیم انجام می‌دادند. اما تحول بزرگ در محاسبات ماشینی در ابتدای قرن بیستم شروع شد. این زمانی است که الگوریتم و مفهوم فرایندهای الگوریتمی^۳ به سرعت در ریاضیات و به تدریج در سایر علوم رشد کرد. ریاضیدانان شروع به معرفی سیستم‌های جدیدی برای پیاده‌سازی الگوریتمی کلی کردند

^۲ decimal

^۳ algorithmic processes

که در نتیجه‌ی آن، سیستم‌های انتزاعی محاسباتی به وجود آمدند. در این میان سهم برخی بیشتر از سایرین بود. آنچه امروزه آنرا دانش کامپیوتر و یا الکترونیک دیجیتال می‌نامیم مرهون و مدیون کار ریاضیدان برجسته انگلیسی به نام «آلن تورینگ»^۴ است. وی مدلی ریاضی را ابداع کرد که آنرا ماشین تورینگ می‌نامیم و اساس تکنولوژی دیجیتال در تمام سطوح آن است. وی با پیشنهاد استفاده از سیستم دودویی برای محاسبات به جای سیستم عدد نویسی دهدهی که تا آن زمان در ماشین‌های مکانیکی مرسوم بود، انقلابی عظیم را در این زمینه بوجود آورد. پس از نظریه طلایی تورینگ، دیری نپایید که «جان فون نویمان»^۵ یکی دیگر از نظریه پردازان بزرگ قرن بیستم موفق شد ماشین محاسبه‌گری را بر پایه طرح تورینگ و با استفاده از قطعات و مدارات الکترونیکی ابتدایی بسازد. به این ترتیب دانش کامپیوتر بتدریج از ریاضیات جدا شد و امروزه خود زمینه‌ای مستقل و در تعامل با سایر علوم به شمار می‌رود. گیت‌های پیشرفته، مدارات ابر مجتمع، منابع ذخیره و بازیابی بسیار حجیم و کوچک، افزایش تعداد عمل در واحد زمان و غیره از مهم‌ترین این پیشرفت‌ها در بخش سخت‌افزاری محسوب می‌شوند. در ۱۹۶۵ «گوردون مور»^۶ اظهار کرد که توان کامپیوترها هر دو سال دو برابر خواهد شد. در تمام این سال‌ها، تلاش عمده در جهت افزایش قدرت و سرعت عملیاتی در کنار کوچک سازی زیر ساخت‌ها و اجزای بنیادی بوده است. نظریه مور در دهه‌های ۶۰ و ۷۰ میلادی تقریباً درست بود. اما از ابتدای دهه ۸۰ میلادی و با سرعت گرفتن این پیشرفت‌ها، شبهات و پرسش‌هایی در محافل علمی مطرح شد که این کوچک سازی‌ها تا کجا می‌توانند ادامه پیدا کنند؟ کوچک کردن ترازیستورها و مجتمع کردن آنها در فضای کمتر نمی‌تواند تا ابد ادامه داشته باشد زیرا در حدود ابعاد نانومتری اثرات کوانتومی از قبیل تونل‌زنی الکترونی بروز می‌کنند.

گرچه همیشه تکنولوژی چندین گام بزرگ از نظریه عقب است، بسیاری از دانشمندان در زمینه‌های مختلف به فکر رفع این مشکل تا زمان رشد فناوری به حد مورد نظر افتادند. به این ترتیب بود که برای نخستین بار در سال ۱۹۸۲ «ریچارد فاینمن» معلم بزرگ فیزیک و برنده جایزه نوبل، پیشنهاد کرد که باید محاسبات را از دنیای دیجیتال وارد دنیای جدیدی به نام کوانتوم کرد که بسیار متفاوت از قبلی است و نه تنها مشکلات گذشته و محدودیت‌های موجود را بر طرف می‌سازد، بلکه افق‌های جدیدی را نیز به این مجموعه اضافه می‌کند. این پیشنهاد تا اوایل دهه ۹۰ میلادی مورد توجه جدی قرار

^۴Alan Turing

^۵John von Neumann

^۶Gordon E. Moore

نگرفت تا بالاخره در ۱۹۹۴ «پیتر شور»^۷ از آزمایشگاه *ATandT* در آمریکا نخستین گام را برای محقق کردن این آرزو برداشت. به این ترتیب ارتباط نوینی بین نظریه اطلاعات و مکانیک کوانتومی شروع به شکل‌گیری کرد که امروز آنرا محاسبات کوانتومی یا محاسبات نانومتری^۸ می‌نامیم. در واقع هدف محاسبات کوانتومی یافتن روش‌هایی برای طراحی مجدد ادوات شناخته شده محاسبات (مانند گیت‌ها و ترانزیستورها) به گونه‌ایست که بتوانند تحت اثرات کوانتومی، که در محدوده ابعاد نانومتری و کوچک‌تر بروز می‌کنند، کار کنند.

۳.۱.۱ منطق کوانتومی و برهم‌نهی

منطق دودویی یعنی کوچکترین واحد اطلاعات یا همان بیت می‌تواند دارای مقداری برابر یک یا صفر باشد. اما هر بیت در کامپیوترهای کوانتومی را کیوبیت^۹ می‌نامند. کیوبیت‌ها در کامپیوترهای کوانتومی علاوه بر دو وضعیت بالا و پایین از وضعیت سومی نیز بهره می‌گیرند. می‌توان این وضعیت را به اصطلاح حالت برهم‌نهی^{۱۰} نامید.

مهمترین خصلت پدیده‌های کوانتومی برهم‌نهی است ولی درک آن به‌عنوان پدیده‌ای که مشابهی در دنیای محسوس اطراف ما ندارد دشوار است. برهم‌نهی کوانتومی یکی از مهمترین مزیت‌هایی است که پژوهشگران حوزه کوانتومی در صدد به‌کارگیری آن برای انجام دادن محاسبات هستند. از دید فیزیکی، بیت، سیستم فیزیکی است با حداقل دو حالت متمایز که بتواند در یک لحظه در یکی از این دو حالت باشد. در ضمن فاصله انرژی میان این دو حالت باید به قدری باشد که بتوان آن‌ها را از میان این دو تمیز داد. اگر به‌جای ترانزیستور، یک الکترون یا هر ذره کوانتومی دیگری را به‌عنوان نماینده یک بیت در نظر بگیریم نخستین نکته آن است که تعداد حالات ممکن برای این کیوبیت خیلی بیشتر از دو حالت صفر و یک است.

اسپین یک ذره را در نظر بگیرید. اسپین یک الکترون را فقط می‌توان در دو حالت مخالف هم یافت. بیشترین اطلاعاتی که با اندازه‌گیری از حالت کوانتومی یک ذره به دست می‌آید این است که جهت اسپین یا در جهت میدان مغناطیسی یا در خلاف جهت آن

^۷Peter Shor

^۸nano computing

^۹Qubit

^{۱۰}Super position

است. پیش از اندازه‌گیری، اسپین این الکترون می‌توانسته در هر ترکیبی از حالت‌های بالا و پایین باشد و این همان مفهوم برهم‌نهی است. براساس حالت قبلی الکترون، می‌توان فهمید که الکترون با چه احتمالی در حالت اسپین بالا و با چه احتمالی در حالت اسپین پایین خواهد بود. مثلاً الکترون با احتمال سی درصد در حالت اسپین بالا و با احتمال هفتاد درصد در حالت اسپین پایین است. توجه داریم که جمع احتمال‌های یافتن الکترون در دو حالت ممکن برابر یک است.

خواندن حالت نهایی یک حالت کوانتومی به‌نحوی که بتوان از حالت‌های برهم‌نهی استفاده کرد دشوار و غیرمستقیم است. برای خواندن اطلاعات نهایی از خصلت تداخل حالت‌های کوانتومی استفاده می‌شود. در طی این مراحل احتمال بروز خطا وجود دارد. یعنی کوچکترین اختلال خارجی می‌تواند مقادیر برهم‌نهی یا دقیق کوانتوم‌ها را تغییر دهد. برای غلبه بر انواع اختلال‌های خارجی و احتمال‌های ذاتی به‌دست آمدن جواب‌های نادرست، از الگوریتم‌های تصحیح خطای کوانتومی استفاده می‌شود. اما این الگوریتم‌ها با الگوریتم‌های تصحیح خطا در کامپیوترهای کلاسیک کاملاً متفاوت است. الگوریتم‌های تصحیح خطای کوانتومی بر پایه یک خصوصیت کوانتومی به نام درهم‌تنیدگی^{۱۱} طراحی شده‌اند.

چگونه یک کامپیوتر کوانتومی می‌تواند در برخی مسائل و نه برای مسائل دیگر، افزایش سرعت داشته باشد؟ برای متخصصان علوم کامپیوتر نکته اساسی درباره یک مسئله آن است که زمان مورد نیاز برای حل کردن آن چگونه با افزایش اندازه مسئله زیاد می‌شود.

حال فرض کنید که چند جعبه با ابعاد مختلف دارید و به دنبال راهی هستید تا آن را در صندوق خود بگنجانید یا فرض کنید که یک نقشه به شما داده شده و می‌خواهید هر کشور را با رنگ قرمز، آبی یا سبز رنگ آمیزی کنید به شکلی که هیچ دو کشور همسایه‌ای به یک رنگ درنیایند یا اینکه فهرست جزیره‌هایی به شما داده شده که با پل‌هایی به هم مرتبط شده‌اند و می‌خواهید سفری سیاحتی ترتیب دهید که از هر جزیره تنها یک بار دیدن کنید. برای این مسائل الگوریتم‌هایی می‌شناسیم که تا حدی بهتر از آزمودن هر جواب ممکن هستند اما هیچ الگوریتمی را نمی‌شناسیم که اساساً بهتر از بقیه باشد. هر کدام از الگوریتم‌های شناخته شده نیاز به مدت زمانی دارد که به طور نمایی با اندازه مسئله بزرگ می‌شود.

^{۱۱} Entanglement

در دهه ۱۹۸۰ هنگامی که ایده کامپیوترهای کوانتومی ابتدا توسط ریچارد فاینمن و سپس به شکل منسجم‌تر توسط دیوید دویچ مطرح شد توانایی نظری این ماشین‌ها در انجام محاسبات موازی مثل یک تردستی عجیب به نظر می‌رسید اما در سال ۱۹۹۴ اتفاقی افتاد که باعث شد محاسبات کوانتومی به هدف دولت‌ها، نیروهای نظامی و هرکس دیگری که اسرار دیجیتالی داشت تبدیل شود.

پیتر شور یک ریاضیدان نظری که آن زمان در آزمایشگاه‌های بل مشغول به کار بود الگوریتمی برای کامپیوتر کوانتومی کشف کرد که می‌توانست بسیار موثرتر از روش‌های موجود عوامل اول یک عدد صحیح بزرگ را تعیین کند. تجزیه یک عدد به عوامل اول آن از جمله مسائلی است که کامپیوترهای معمولی را به بن‌بست می‌کشاند. در واقع کامپیوترها آنقدر در این کار ناتوانند که بیشتر سیستم‌های رمزگذاری امروزی متکی بر حاصل ضرب اعداد اول بسیار بزرگ هستند؛ یافتن این عوامل اول چند دهه وقت یک کامپیوتر را می‌گیرد. الگوریتم پیتر شور این وضعیت را تغییر داد و تصور اینکه حجم انبوهی از اطلاعات ممکن است چنین آسیب‌پذیر شود، جرقه آغازین مسابقه‌ای جهانی برای ساختن ماشینی شد که توانایی کافی برای شکستن کدها را داشته باشد.

۲.۱ کامپیوتر کوانتومی

۱.۲.۱ کامپیوتر کوانتومی چیست؟

کامپیوتر کوانتومی ماشینی است که از پدیده‌ها و اصول مکانیک کوانتومی مثل برهم‌نهی و درهم‌تنیدگی برای انجام محاسباتش استفاده می‌کند. کامپیوترهای کوانتومی با کامپیوترهای فعلی که با ترانزیستورها کار می‌کنند تفاوت اساسی دارند؛ ایده‌ی اصلی که در پس کامپیوترهای کوانتومی نهفته است این است که می‌توان از اصول مکانیک کوانتومی برای ذخیره‌سازی و انجام عملیات روی داده‌ها استفاده کرد.

اگرچه محاسبات کوانتومی تازه در ابتدای راه قرار دارد، اما آزمایش‌هایی انجام شده است که در طی آنها عملیات محاسبات کوانتومی روی تعداد کمی از کیوبیت‌ها اجرا شده است. تحقیقات نظری و عملی در این زمینه ادامه دارد و بسیاری از مؤسسات دولتی و نظامی از تحقیقات در زمینه‌ی کامپیوترهای کوانتومی چه برای اهداف غیر نظامی و چه برای اهداف امنیتی مثل تجزیه و تحلیل رمز حمایت می‌کنند.

توابعی که توسط کامپیوترهای کلاسیک قابل محاسبه نیستند، توسط کامپیوترهای کوانتومی نیز محاسبه نمی‌شوند. کامپیوترهای کوانتومی برای ما علاوه بر سرعت بیشتر امنیت را نیز را به ارمغان می‌آورند.

۲.۲.۱ بیت و کیوبیت

در کامپیوترهای کلاسیک هر نوع داده‌ای در بیت‌های کلاسیکی ذخیره می‌شود. یک بیت کلاسیک، صرفنظر از نوع سخت‌افزاری که بر آن به‌کار رفته است، یک سیستم فیزیکی است که می‌تواند در دو حالت ۰ و ۱ قرار بگیرد. هر نوع پردازشی در نهایت به این معناست که ما بتوانیم توابع دلخواهی را برای داده‌هایی که در این حافظه ذخیره شده‌اند محاسبه کنیم.

مفهوم اصلی در کامپیوتر کوانتومی بیت کوانتومی یا کیوبیت است که معادل با حالت کوانتومی $|\psi\rangle$ است. یک کیوبیت به یک سیستم کوانتومی گفته می‌شود که فضای هیلبرت آن دو بعدی است. این فضای هیلبرت را به صورت:

$$c^2 := \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \alpha, \beta \in c \right\}$$

نشان می‌دهیم. معمول است که بردارهای پایه‌ی این فضا را با:

$$\begin{cases} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{cases} \quad (7.1)$$

نشان می‌دهند. یک کیوبیت بر خلاف بیت کلاسیکی می‌تواند همچنین در ترکیبی از حالت‌های فوق قرار بگیرد:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (8.1)$$

که α و β اعداد مختلط هستند با شرط اینکه:

$$|\alpha|^2 + |\beta|^2 = 1$$

اگر اندازه گیری بر روی کیوبیت انجام شود، با احتمال $|\alpha|^2$ در حالت $|0\rangle$ و با احتمال $|\beta|^2$ در حالت $|1\rangle$ پیدا می شود. علاوه بر اینکه کیوبیت بر خلاف بیت کلاسیکی می تواند برهم نهی از حالات پایه قرار بگیرد، تفاوت دیگر بین بیت کلاسیکی و کیوبیت در این است که بیت را می توان به راحتی و بدون آشفته کردن حالت آن اندازه گیری کرد و به اطلاعات آن دست یافت، اما یک کیوبیت بعد از اندازه گیری حالت آن در یکی از حالت های پایه تبدیل می شود و دیگر نمی توان اطلاعات اضافی را از آن به دست آورد.

پردازش ماشینی اطلاعات، در هر شکلی بر مبنای محاسبات کلاسیک انجام می شود اما روش بهتر برای پردازش اطلاعات بر اساس مکانیک کوانتومی است، این روش جدید با ویژگی هایی همراه است که آن را از محاسبات کلاسیک متمایز می سازد؛ البته وجود تفاوت بین این دو به معنای حذف یکی و جایگزینی دیگری نیست، به قول "نیلزبور" گاهی ممکن است خلاف یک حقیقت انکارناپذیر منجر به حقیقت انکارناپذیر دیگری شود. وجود چند پدیده ی مهم که مختص فیزیک کوانتومی است آن را از دنیای کلاسیک جدا می سازد. این پدیده ها عبارتند از: برهم نهی، تداخل، درهم تنیدگی، ناموضعیّت. یک کیوبیت ممکن است در حالت های کلاسیک 0 یا 1 وجود داشته باشد، یا ترکیبی از این دو (یعنی به طور هم زمان مقادیر 0 و 1 را داشته باشیم "حالت برهم نهی"). با توجه به مکانیک کوانتومی نمی توان دقیقا وجود یا عدم وجود یک ذره را مشخص کرد. البته آنچه که در کامپیوترهای کوانتومی اهمیت ویژه دارد همین احتمالات است.

در یک رایانه ی کوانتومی به جای استفاده از ترانزیستورها و مدارهای رایانه ای معمولی، از اتم و سایر ذرات ریز برای پردازش اطلاعات استفاده می شود. یک اتم می تواند به عنوان بیت حافظه در رایانه عمل کند. یک زوج از کیوبیت ها می توانند در هر برهم نهی از 4 حالت قرار بگیرند و همین طور برای 3 کیوبیت برهم نهی از 8 حالت وجود دارد.

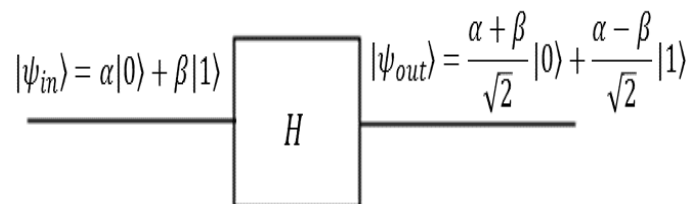
یک سیستم n کیوبیتی 2^n شیء را اندیس گذاری می کند مثلا $2^3 = 8$ شیء، فضای سیستم 3 کیوبیتی، 8 تا پایه. در کل یک کامپیوتر کوانتومی با n کیوبیت می تواند در هر برهم نهی از 2^n حالت به طور هم زمان قرار بگیرد، برخلاف کامپیوترهای کلاسیکی که در هر لحظه فقط در یکی از حالات می توانند قرار بگیرند. یک مثال برای نحوه ی پیاده سازی کیوبیت ها در کامپیوترهای کوانتومی، استفاده از ذراتی با اسپین $|\uparrow\rangle$ و $|\downarrow\rangle$ یا $|0\rangle$ و $|1\rangle$ است. اطلاعات روی حالت های فیزیکی سیستم ذخیره می شود و با عملیات روی سیستم، اطلاعات تحول می یابند.

۳.۲.۱ تداخل کوانتومی

گیت هادامارد یکی از مهمترین گیت‌های کوانتومی است. عمل یکانی هادامارد بر روی حالت $|\psi\rangle$ به صورت زیر است:

$$H|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \frac{\alpha + \beta}{\sqrt{2}} \\ \frac{\alpha - \beta}{\sqrt{2}} \end{pmatrix} \quad (9.1)$$

یکی از کاربرهای جالب این گیت این است که می‌توان بوسیله‌ی آن کت پایه‌ی n بعدی $|0\rangle^{\otimes n}$ را به یک برهم‌نهی مساوی از کت‌های پایه فضای n بعدی تبدیل کرد. اثر گیت



شکل ۱.۱: شکل هندسی گیت H

هادامارد بر روی کیوبیت اختیاری، مثالی از تداخل کوانتومی است^{۱۲}. زمانی که $H|\psi\rangle$ اثر می‌کند چه اتفاقی می‌افتد؟

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (10.1)$$

$$\Rightarrow H|\psi\rangle = \left(\frac{\alpha + \beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha - \beta}{\sqrt{2}}\right)|1\rangle \quad (11.1)$$

احتمال دستیابی به حالت $|0\rangle$ و $|1\rangle$ به صورت زیر تغییر می‌کند:

$$\alpha \rightarrow \frac{\alpha + \beta}{\sqrt{2}} \quad (12.1)$$

$$\beta \rightarrow \frac{\alpha - \beta}{\sqrt{2}} \quad (13.1)$$

$$\alpha = \beta \Rightarrow |\psi\rangle \rightarrow |0\rangle$$

$$\alpha \neq \beta \Rightarrow |\psi\rangle \rightarrow |1\rangle$$

که در اینجا تداخل کوانتومی نمایان می‌شود. دو نوع تداخل کوانتومی داریم: تداخل مثبت و تداخل منفی. در تداخل مثبت دامنه‌ها تقویت می‌شوند و دامنه‌ی احتمال افزایش می‌یابد. در تداخل منفی، دامنه‌ها تضعیف شده و در نتیجه دامنه‌ی احتمال کاهش می‌یابد. تداخل کوانتومی نقش مهمی در الگوریتم‌های کوانتومی دارد. با استفاده از تداخل کوانتومی این امکان برای ما وجود دارد که اطلاعاتی از $f(x)$ برای مقادیر مختلف x را بیابیم.

۴.۲.۱ ارزیابی تابع و توازی کوانتومی

اگر تابع $f(x)$ به ازای تمام x ها یکی باشد تابع ثابت است:

$$f(x) = 0 \quad \text{or} \quad f(x) = 1 \quad (\text{for all } x's)$$

اگر برای نیمی از x ها ۰، و برای نیمی دیگر ۱ باشد تابع متوازن نامیده می‌شود:

$$f(x) = \begin{cases} 1 & \text{for half of } x's \\ 0 & \text{for half of } x's \end{cases} \quad (14.1)$$

تابع همانی:^{۱۳}

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x = 1 \end{cases} \quad (15.1)$$

در تابع همانی ورودی و خروجی یکی است.

تابع وارونی بیت:^{۱۴}

$$f(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x = 1 \end{cases} \quad (16.1)$$

تابع همانی و وارونی بیت هر دو تابع متوازن نامیده می‌شوند، زیرا خروجی‌ها به ازای نیمی از ورودی‌ها برابر صفر و به ازای نیمی دیگر برابر یک می‌باشند.

^{۱۳}Identity function

^{۱۴}Bit flip function

پردازش کوانتومی، پردازشی ذاتا موازی

یکی از قابلیت‌های کامپیوترهای کوانتومی که موجب تفاوت آن‌ها با کامپیوترهای کلاسیک می‌شود بحث موازی بودن ذاتی کامپیوتر کوانتومی است.

فرض کنید یک رجیستر^{۱۵} سه کیوبیتی داریم که می‌تواند در حالت‌های برهم‌نهم این سه کیوبیت قرار گیرد در حالی که رجیستر کلاسیک که سه بیت معمولی دارد در هر لحظه می‌تواند در یکی از هشت حالت ممکن باشد، اما رجیستر کوانتومی هر یک از این هشت حالت را با احتمال معینی خواهد داشت و می‌تواند از طریق برهم‌کنش‌های فیزیکی، مقدار این ضرایب احتمال را تغییر داد که این اتفاق در واقع به طور هم‌زمان روی مقادیری از هشت حالت ممکن می‌افتد. در کامپیوترهای کوانتومی پردازش تمامی حالت‌ها فقط در یک لحظه و به‌طور هم‌زمان صورت می‌گیرد، این نوع پردازش توازی کوانتومی نامیده می‌شود. توازی کوانتومی یکی از ویژگی‌های مهم در الگوریتم‌های کوانتومی است که به کامپیوتر کوانتومی این امکان را می‌دهد که یک تابع $f(x)$ را برای مقادیر مختلف x به‌طور هم‌زمان ارزیابی کند. اگر U_f یک تبدیل خطی باشد، روی یک ورودی که برهم‌نهی خطی از حالات مختلف است به‌طور هم‌زمان اثر می‌کند و برهم‌نهی از نتایج به‌دست می‌آورد. با استفاده از این روش توازی کوانتومی محاسبه‌ی $f(x)$ برای N مقدار از x در به‌کارگیری یک‌بار عملگر U_f امکان‌پذیر است.

برای مثال فرض می‌کنیم $f: \{0, 1\} \rightarrow \{0, 1\}$ و کیوبیتی با حالت اولیه $|x, y\rangle$ در نظر می‌گیریم که $|x\rangle$ بیت کنترل و $|y\rangle$ بیت هدف است. با به‌کاربردن یک گیت منطقی مناسب f -گیت داریم:

$$|x, y\rangle \longrightarrow |x, y \oplus f(x)\rangle \quad (17.1)$$

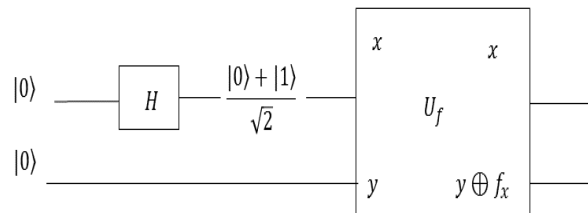
$|x\rangle$ ، n کیوبیتی است که به‌صورت برهم‌نهی از 0 و 1 است که در اثر گیت هادامارد روی صفر به‌دست آمده است و U_f آن را به شکل زیر درمی‌آورد [۲]:

$$U_f |x, y\rangle = U_f \left| \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}, |0\rangle \right) \right\rangle = \frac{|0, f(0) \oplus 0\rangle + |1, f(1) \oplus 0\rangle}{\sqrt{2}} \quad (18.1)$$

بعد از اندازه‌گیری نمی‌توانیم بگوییم که تابع ثابت بوده یا متوازن. دویچ^{۱۶} برای حل این مشکل الگوریتمی طراحی می‌کند که در فصل ۳ این الگوریتم را توضیح خواهیم داد.

^{۱۵}Register

^{۱۶}Deutsch

شکل ۲.۱: $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$

۵.۲.۱ گیت کوانتومی و گیت کلاسیکی

گیت‌ها که اجزای اصلی یک مدار منطقی را تشکیل می‌دهند عملیات پردازش اطلاعات روی بیت‌ها در کامپیوترهای کلاسیکی و کیوبیت‌ها در کامپیوترهای کوانتومی را برعهده دارند. در ادامه با انواع این گیت‌ها و نحوه‌ی عملشان آشنا خواهیم شد.

یک تفاوت عمده میان گیت‌های منطقی کلاسیک و کوانتومی آن است که ورودی و خروجی گیت‌های کوانتومی می‌تواند حالت برهم‌نهمش یک کیوبیت هم باشد در صورتی که در دنیای کلاسیک حالت برهم‌نهمش وجود ندارد. اگر اطلاعات را در کیوبیت‌ها یعنی حالت‌های کوانتومی ذخیره کنیم، به ناچار پردازش اطلاعات می‌بایستی یا با عملگرهای یکانی که تحول را نشان می‌دهند و یا با اندازه‌گیری‌ها انجام بگیرند. معمولاً اصطلاح گیت کوانتومی برای عملگر یکانی به‌کار برده می‌شود. گیت کوانتومی هرگاه روی یک کیوبیت اثر کند آن را گیت تک کیوبیتی و هرگاه روی n تا کیوبیت اثر کند آن را گیت n کیوبیتی می‌گویند. از جمله این گیت‌ها گیت کوانتومی هادامارد و گیت کوانتومی f -گیت است.

در زیر چند نمونه از گیت‌های کوانتومی و کلاسیکی را نشان داده ایم [۱]:

گیت NOT

مثال ساده‌ای از گیت کلاسیکی گیت NOT است که در واقع عمل انعکاس بیت را انجام می‌دهد:

$$0 \mapsto 1$$

$$1 \mapsto 0$$

<i>Inpute</i>	<i>Not</i>
0	1
1	0

شکل ۳.۱: گیت کلاسیکی *NOT*

گیت *OR*

گیت کلاسیکی *OR* به این صورت است که اگر *A* یا *B* ۱ باشند خروجی برابر ۱ و در غیر این صورت خروجی صفر است.

<i>A</i>	<i>B</i>	<i>A OR B</i>
0	0	0
0	1	1
1	0	1
1	1	1

شکل ۴.۱: گیت کلاسیکی *OR*

گیت *AND*

گیت کلاسیکی *AND* تنها زمانی ۱ است که هر دو ورودی ۱ باشند.

گیت *XOR*

گیت کلاسیکی *XOR* به این صورت عمل می‌کند اگر فقط یکی از ورودی‌ها ۱ باشد خروجی ۱، اما اگر هر دو ورودی ۱ باشند خروجی ۰ است.

A	B	$A \text{ AND } B$
0	0	0
0	1	0
1	0	0
1	1	1

شکل ۵.۱: گیت کلاسیکی AND

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

شکل ۶.۱: گیت کلاسیکی XOR گیت $NAND$

گیت کلاسیکی بعدی که در محاسبات کلاسیکی دارای اهمیت است، گیت $NAND$ است و به این صورت عمل می‌کند که ابتدا با دو بیت رودی همچون گیت AND عمل می‌کند و سپس حاصل را NOT می‌کند. این گیت برگشت‌ناپذیر است.

گیت $Toffoli$

گیت بعدی گیت $Toffoli$ است که دارای دو بیت کنترل و یک بیت هدف است و به این صورت عمل می‌کند که ابتدا دو بیت کنترل AND می‌شوند و سپس نتیجه با بیت هدف XOR می‌شود.

گیت‌های کوانتومی تقریباً مشابه گیت‌های کلاسیکی هستند. یکی از تفاوت‌های مهم بین این دو گیت، برگشت‌پذیر بودن گیت‌های کوانتومی است. به این معنا که می‌توان با استفاده از خروجی گیت‌های کوانتومی، ورودی آنها را دوباره بازسازی کرد. در مورد

A	B	$A \text{ NAND } B$
0	0	1
0	1	1
1	0	1
1	1	0

شکل ۷.۱: گیت کلاسیکی NAND

$C1$	$C2$	T	T'
0	0	1	1
1	1	0	1
1	1	1	0
0	1	0	0

شکل ۸.۱: گیت کلاسیکی Toffoli

گیت‌های کلاسیکی مانند XOR ، AND ، $NAND$ و ... ورودی دوبیتی به خروجی تک بیتی تبدیل می‌شود و به‌وضوح برگشت‌ناپذیرند. اما اگر یک گیت کوانتومی با عملگر U ، حالت ورودی $|\psi\rangle_{in}$ را به $|\psi\rangle_{out}$ تبدیل کند، می‌توان گیتی با عملگر U^\dagger تشکیل داد تا $|\psi\rangle_{out}$ را مجدداً به $|\psi\rangle_{in}$ تبدیل کند. گیت‌های کوانتومی، عملگرهای یکانی هستند و در نتیجه برگشت‌پذیرند:

$$UU^\dagger = U^\dagger U = I \quad (۱۹.۱)$$

اگر H عملگر هرمیتی باشد، e^{iHt} نیز هرمیتی است.

عملگرهای کوانتومی را می‌توان با ماتریس نمایش داد. یک گیت کوانتومی با n ورودی و خروجی را می‌توان با ماتریس 2^n بعدی نشان داد. مثلاً نمایش ماتریسی گیت دوکیوبیتی 4×4 است.

گیت X

گیت کوانتومی NOT با ماتریس پائولی X انجام می‌شود:

$$X = U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (20.1)$$

$$U_{NOT}|0\rangle = |1\rangle \quad (21.1)$$

$$U_{NOT}|1\rangle = |0\rangle \quad (22.1)$$

اثر گیت کوانتومی NOT بر روی هر حالت دلخواه $|j\rangle$ به صورت زیر نوشته می‌شود:

$$X|j\rangle = |j \oplus 1\rangle \quad (23.1)$$

گیت Z

یکی دیگر از گیت‌های کوانتومی تک کیوبیتی مربوط به ماتریس پائولی Z است که *Phaseflip* نامیده می‌شود زیرا:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi'\rangle = \alpha|0\rangle - \beta|1\rangle \quad (24.1)$$

$$Z|\psi\rangle = (|0\rangle\langle 0| - |1\rangle\langle 1|)\alpha|0\rangle + \beta|1\rangle \quad (25.1)$$

$$= \alpha|0\rangle - \beta|1\rangle \quad (26.1)$$

و در حالت کلی اثر گیت Z بر روی هر حالت دلخواهی مثل $|j\rangle$ به صورت زیر است:

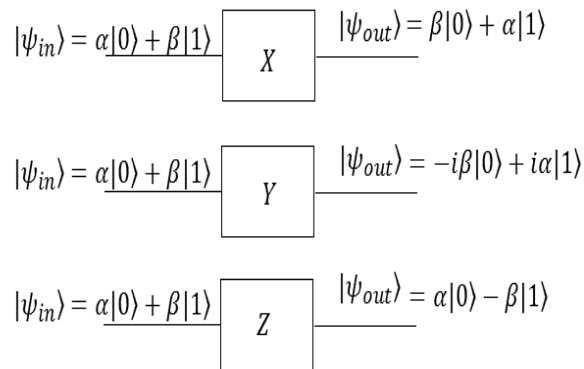
$$Z|j\rangle = (-1)^j|j\rangle \quad (27.1)$$

گیت $Phase - shift$

گیت کلی $Phase - shift$ را در نظر می‌گیریم. این گیت فاز کت پایه‌ی $|1\rangle$ را به اندازه‌ی θ تغییر می‌دهد. بنابراین قادر است فاز نسبی یک برهم‌نهمش از $|0\rangle$ و $|1\rangle$ را تغییر دهد:

$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad (28.1)$$

واضح است اثر این گیت بر روی حالت $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ، وقتی $\theta = \pi$ باشد، گیت Z را نتیجه می‌دهد.

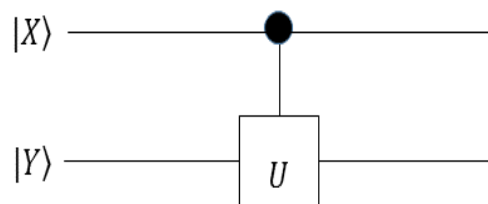


شکل ۹.۱: شکل هندسی گیت X, Y, Z

گیت‌های *Controlled - U*

گیت‌های *Controlled - U* مهم‌ترین گیت‌های دو یا چند کیوبیتی هستند. ورودی این گیت‌ها شامل یک کیوبیت کنترل $|X\rangle$ و یک کیوبیت هدف $|Y\rangle$ است. کیوبیت کنترل تعیین می‌کند که آیا یک عمل یکانی مشخص روی کیوبیت هدف انجام شود یا خیر.

عملکرد این گیت‌ها به این صورت است که اگر کیوبیت کنترل در حالت $|0\rangle$ باشد، گیت هیچ عملی روی کیوبیت هدف انجام نمی‌دهد و در صورتی که کیوبیت کنترل در حالت $|1\rangle$ باشد، گیت عملگر یکانی U را بر روی کیوبیت هدف اثر می‌دهد.

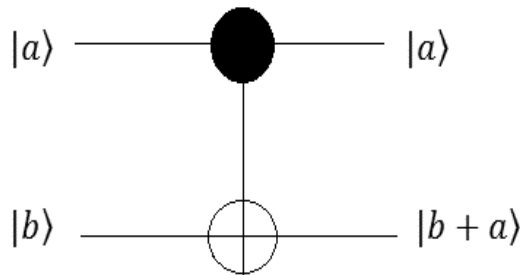


شکل ۱۰.۱: شکل هندسی گیت *Controlled - U*

گیت *CNOT*

یکی از معروفترین گیت‌های *Controlled - U* گیت *CNOT* است. گیت کنترل شده *NOT* یا به اختصار *CNOT*، دو کیوبیت را به عنوان حالت ورودی دریافت می‌کند که یکی

کیوبیت کنترل و دیگری کیوبیت هدف است. کاری که این گیت انجام می‌دهد این است که کیوبیت کنترل را با کیوبیت هدف جمع کرده و باقیمانده‌ی تقسیم این جمع بر ۲ را به عنوان خروجی هدف بیرون می‌دهد. در واقع اگر ارزش کیوبیت کنترل صفر باشد، کیوبیت هدف را تغییر نمی‌دهد اما اگر ارزش کیوبیت کنترل یک باشد گیت $CNOT$ روی کیوبیت هدف مانند یک گیت NOT عمل می‌کند.



شکل ۱۱.۱: شکل هندسی گیت $CNOT$

که در آن \oplus به معنای باقیمانده‌ی تقسیم جمع بر مبنای ۲ است.

$$|X\rangle|Y\rangle \xrightarrow{CNOT} |X\rangle|X \oplus Y\rangle \quad (29.1)$$

در حالتی که کیوبیت کنترل به صورت یک برهم‌نهی از کیوبیت‌های $|0\rangle$ و $|1\rangle$ باشد، خروجی گیت $CNOT$ به صورت زیر خواهد بود:

$$|X\rangle = \alpha|0\rangle + \beta|1\rangle \quad : \quad |X\rangle|Y\rangle \longrightarrow |X\rangle(\alpha|0 \oplus Y\rangle + \beta|1 \oplus Y\rangle) \quad (30.1)$$

گیت f - gate (function - gate)

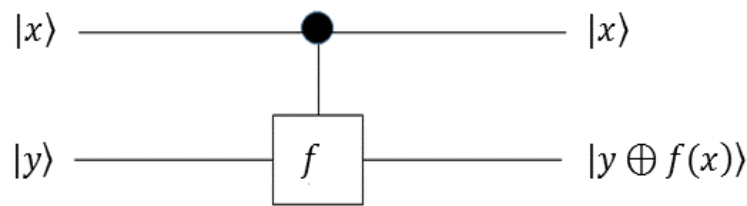
یکی دیگر از مهم‌ترین گیت‌های $Controlled - U$ گیت‌های f - gate هستند. این گیت، ورودی کنترل را (که یک رجیستر به اندازه‌ی n کیوبیت است: $x \in \{0, 1\}^n$) به صورت تابعی از f ، بر کیوبیت هدف (که یک رجیستر به اندازه‌ی m کیوبیت است: $y \in \{0, 1\}^m$) می‌نگارد.

$$f : \{0, 1\}^n \rightarrow \{0, 1\}^m$$

$$|x\rangle|y\rangle \xrightarrow{f\text{-gate}} |x\rangle|(y \oplus f(x))\rangle \quad (31.1)$$

به ازای $|y\rangle = |0\rangle$ خواهیم داشت:

$$|x\rangle|0\rangle \xrightarrow{f\text{-gate}} |x\rangle|f(x)\rangle \quad (32.1)$$



شکل ۱۲.۱: شکل هندسی گیت f - gate

درحالتی که ورودی کنترل به صورت یک برهم‌نهی از کت‌های پایه‌ی $|x\rangle$ باشد، آنگاه:

$$\sum_x |x\rangle |0\rangle \xrightarrow{f\text{-gate}} \sum_x |x\rangle |f(x)\rangle \quad (۳۳.۱)$$

این نشان می‌دهد که حتی اگر تعداد زیادی ورودی داشته باشیم، کامپیوتر کوانتومی تنها با یک بار استفاده از f - gate می‌تواند تابع تمام ورودی‌ها را یک جا و به‌طور موازی محاسبه کند این یکی از بزرگترین مزایای کامپیوترهای کوانتومی نسبت به کامپیوترهای کلاسیکی است.

۶.۲.۱ مدارهای کوانتومی

طرز عمل یک کامپیوتر کلاسیکی توسط بیت‌ها است که مجهز به مجموعه‌ای از گیت‌هاست که می‌توانند روی مجموعه‌ای از بیت‌ها اثر کنند. اما طرز عمل یک کامپیوتر کوانتومی کیوبیت‌ها است. تصور می‌کنیم که این نیز به یک مجموعه‌ی مجزا از اجزای اساسی مجهز شده است که گیت‌های کوانتومی نامیده می‌شود. هر گیت کوانتومی یک تبدیل یکانی است که روی تعداد ثابتی از کیوبیت‌ها اثر می‌گذارد. در محاسبات کوانتومی n تعداد محدودی از کیوبیت‌ها، مجموعه‌ای با مقادیر $|0\rangle, |1\rangle, \dots, |n-1\rangle$ هستند. مدار کوانتومی نمایش ساختاری است که از تعداد محدودی گیت‌های کوانتومی که روی این کیوبیت‌ها اثر می‌گذارند تشکیل شده است. در نهایت یک اندازه‌گیری از همه‌ی کیوبیت‌ها انجام می‌شود و تصویر هر کدام روی پایه‌های $\{|0\rangle, |1\rangle\}$ است. خروجی این اندازه‌گیری نتیجه‌ی محاسبات است.

الگوریتم‌های کوانتومی روی یک حالت اولیه معین اثر می‌کنند و چنان تنظیم شده‌اند که حالت نهایی چنان باشد که اندازه‌گیری روی آن جواب یک مسئله‌ی معین را با احتمال بسیار خوبی به دست آورد. یکی از مؤثرترین الگوریتم‌های کوانتومی جستجوی

گراور است که کاربرد آسان آن استفاده از برهم‌نهی حالات کوانتومی است.

فصل ۲

جبر کلیفورد

۱.۲ مقدمه

فرمالیزم جبر هندسی^۱ دارای نمایشی برای توصیف معادل فرمالیزم ضرب تانسوری در مکانیک کوانتومی است. برای برپایی چارچوب GA در نمایش حالت‌های کوانتومی با مجموعه‌ی راستگرد بردارهای پایه‌ی متعامد (e_1, e_2, e_3) شروع می‌کنیم که دارای خاصیت زیر هستند $[5], [6]$:

$$e_i \cdot e_j = \delta(i, j)$$

و

$$(e_1)^2 = (e_2)^2 = (e_3)^2 = 1$$

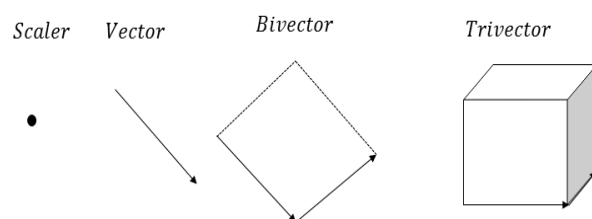
و برای i, j متفاوت خاصیت پادجابجایی داریم:

$$e_i e_j = -e_j e_i \quad (1.2)$$

$e_i e_j$ نمایانگر مساحت جهت‌دار در فضای R^2 است و بردار دو بعدی^۲ نامیده می‌شود.

قبل از هرچیز در این بخش قصد داریم که بحث ساده‌ای از جبر کلیفورد و یا به‌طور شناخته شده، جبرهندسی (GA) بیان کنیم.

علاوه بر اسکالرها^۳ و بردارها^۴، اشیاء و عناصر کلی‌تر شامل بردارهای دو بعدی^۵ و بردارهای سه بعدی^۶ را خواهیم یافت که هر کدام از این اشیاء توصیف هندسی واضحی از اشکال زیر دارند:



^۱ Geometric Algebra (GA)

^۲ bivector

^۳ scaler

^۴ vector

^۵ Bivector

^۶ trivector

که در واقع اسکالر تصویر یک نقطه در فضا است و بسط هندسی ندارد. بردار تصویر یک قطعه خط است که هم طول و هم جهت دارد. بردار دوبعدی تصویر رویه‌ی یک مسیر است که مساحت و جهت دارد و به همین ترتیب بردار سه بعدی تصویر یک قطعه از فضای سه بعدی است که حجم و جهت دارد. هر شیء یک درجه^۷ دارد که متناسب با تعداد ابعادی است که در بسط هندسی دارد و در جدول زیر برای اشیاء مختلف آمده است [۵]، [۶].

object	visualized	geometric extent	grade
scaler	point	no geometric extent	۰
vector	line segment	extent in ۱ direction	۱
bivector	patch of surface	extent in ۲ directions	۲
trivector	piece of apace	extent in ۳ directions	۳
ect.			

قسمت $grad - N$ از هر $cliff$ به صورت $\langle c \rangle_N$ نشان داده می‌شود.

هر عنصر از جبر کلیفورد^۸ را می‌توان با دیگری جمع کرد که این یکی از خاصیت‌های مهم جبر کلیفورد است که آنرا از بقیه جبرها متمایز می‌سازد:

$$C = s + V + B \quad (۲.۲)$$

که s : اسکالر، B : بردار دو بعدی و V : بردار سه بعدی است.

عملگر ضرب هندسی به صورت AB نوشته می‌شود و دارای خاصیت شرکت‌پذیری و توزیع‌پذیری است:

$$(AB)C = A(BC) = ABCA(B + C) = AB + AC \quad (۳.۲)$$

در حالت کلی می‌توان گفت که ضرب هر $cliff$ با اسکالر جابه‌جا پذیر است:

$$Cs = sC$$

ضرب داخلی و ضرب خارجی را به صورت زیر تعریف می‌کنیم:

$$P.Q := \frac{PQ + QP}{۲} \quad (۴.۲)$$

^۷grade

^۸clifford algebra

که P و Q هر دو درجه‌ای برابر ۱ دارند دارند. (هر دو بردار هستند)

$$P \wedge Q := \frac{PQ - QP}{2} \quad (5.2)$$

که P و Q هر دو $grade \leq 1$ دارند (اسکالر یا بردار هستند).

نتیجه

نتیجه‌ی اول از معادلات فوق این است که ضرب هندسی^۹ از دو بردار را می‌توان به صورت زیر نوشت:

$$PQ = P \cdot Q + P \wedge Q \quad (6.2)$$

که:

$$P \cdot Q = \langle PQ \rangle_0$$

$$P \wedge Q = \langle PQ \rangle_2$$

که P و Q درجه‌ای برابر یک دارند اما برای هر درجه بالاتر یا پایین‌تر از ۱ غلط است. برای مثال:

$$sC = s \cdot C = s \wedge C \neq s \cdot C + s \wedge C \quad (7.2)$$

نتیجه‌ی دوم از معادلات فوق این است که ضرب داخلی دو بردار جابه‌جاپذیر است اما ضرب خارجی دو بردار جابه‌جا پذیر نیست:

$$P \cdot Q = Q \cdot P$$

$$P \wedge Q = -Q \wedge P \quad (8.2)$$

نتیجه‌ی ضرب خارجی یک بردار دو بعدی است که مساحت یک متوازی‌الاضلاع جهت‌دار را نشان می‌دهد. $P \wedge Q$ به ازای هر دو بردار پادمتقارن است نه برای هر دو $cliff$. برای مثال:

$$C = C \wedge s \quad (\text{پادمتقارن نیست})$$

ضرب داخلی دو بردار متقارن است در حالی که ضرب داخلی یک بردار و بردار دو بعدی پادمتقارن است:

$$V \cdot X = X \cdot V$$

$$V \cdot B = -B \cdot V \quad (9.2)$$

^۹geometric product

دو بردار P و Q را در یک فضای سه بعدی به صورت زیر تعریف می‌کنیم و سپس ضرب هندسی بین این دو بردار را می‌یابیم:

$$P = P_1 e_1 + P_2 e_2 + P_3 e_3$$

$$Q = Q_1 e_1 + Q_2 e_2 + Q_3 e_3$$

$$\begin{aligned} PQ &= (P_1 e_1 + P_2 e_2 + P_3 e_3)(Q_1 e_1 + Q_2 e_2 + Q_3 e_3) \\ &= P_1 Q_1 + P_2 Q_2 + P_3 Q_3 + (P_2 Q_3 - Q_2 P_3) e_2 e_3 + (P_1 Q_3 - P_3 Q_1) e_1 e_3 \\ &\quad + (P_1 Q_2 - Q_1 P_2) e_1 e_2 \\ &= P \cdot Q + \iota P \times Q = P \cdot Q + P \wedge Q \end{aligned}$$

که از قبل ضرب داخلی و ضرب خارجی دو بردار را معرفی کرده‌ایم و ι یک بردار سه بعدی است که آنرا به صورت $e_1 e_2 e_3$ تعریف می‌کنیم که نمایانگر حجم واحد است $P \wedge Q = \iota P \times Q$. با استفاده از ضرب معادله‌ی فوق برای پایه‌های متعامد می‌توان نوشت:

$$e_i e_j = e_i \cdot e_j + e_i \wedge e_j = \delta_{i,j} + \iota \epsilon_{i,j,k} e_k \quad (10.2)$$

که e_1, e_2, e_3 تداعی کننده‌ی ماتریس‌های پائولی هستند و $\iota^2 = e_1 e_2 e_3 e_1 e_2 e_3 = -1$ که ι مانسته‌ی $i = \sqrt{-1}$ واحد موهومی است و توان دوم بردار دوبعدی دارای علامت منفی است:

$$(e_i e_j)^2 = e_i e_j e_i e_j = -1$$

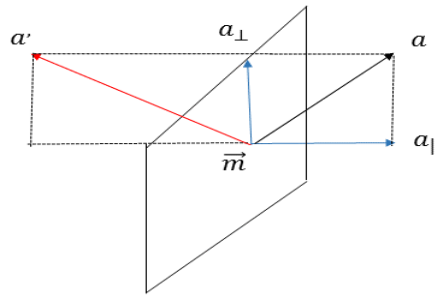
۲.۲ تبدیلات هندسی

تبدیلات هندسی در فضای سه بعدی شامل انعکاس و دوران می‌توانند توسط عملگرهای هندسی (ضرب خارجی، ضرب هندسی و ... توصیف شوند [۶][۵].

۱.۲.۲ انعکاس

قصد داریم که انعکاس^۱ بردار a در صفحه‌ای با بردار نرمال واحد (m) را به دست آوریم که انعکاس بردار a را با a' نشان می‌دهیم. با ضرب m در دو طرف بردار a و

^۱ Reflection

شکل ۱۰.۲: انعکاس بردار a

علامت معکوس، a' به صورت زیر به دست می آید:

$$a' = -mam \quad (۱۱.۲)$$

a می تواند ترکیبی از یک قسمت عمود بر m (a_{\perp}) و یک قسمتی که موازی با m (a_{\parallel}) است باشد:

$$a = a_{\perp} + a_{\parallel}$$

در نتیجه معادله (۱۱.۲) به صورت زیر حاصل می شود:

$$-mam = -m(a_{\perp} + a_{\parallel})m$$

$$\Rightarrow -mam = -ma_{\perp}m - ma_{\parallel}m \quad (۱۲.۲)$$

از آنجایی که m و a_{\perp} بردارهای متعامد هستند، ضرب آنها پادجابه جایی است:

$$a_{\perp}m = -ma_{\perp}$$

اما a_{\parallel} و m بردارهای واقع شده در یک خط هستند، در نتیجه ضرب آنها جابه جاپذیر است:

$$a_{\parallel}m = ma_{\parallel}$$

در نهایت معادله (۱۲.۲) به صورت زیر است:

$$-mam = m^2 a_{\perp} - m^2 a_{\parallel} \quad (۱۳.۲)$$

و از آنجایی که m بردار واحد است پس $m^2 = ۱$ ،

$$\Rightarrow -mam = a_{\perp} - a_{\parallel} \quad (۱۴.۲)$$

می توان مشاهده کرد که انعکاس بردار a در صفحه ای با بردار نرمال واحد m ، توسط ضرب هندسی به دست می آید [۵]، [۶]:

$$a' = -mam \quad (۱۵.۲)$$

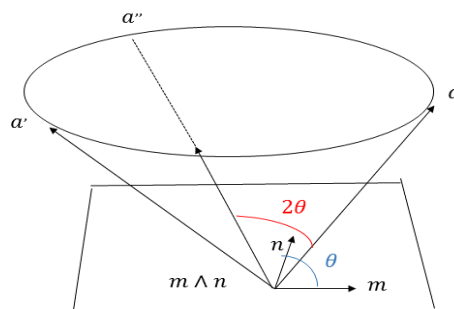
۲.۲.۲ دوران

دوران بردار a را در صفحه‌ای که شامل دو بردار واحد m و n است انجام می‌دهیم. a'' (دوران بردار a) از دو انعکاس متوالی به دست می‌آید. اولین انعکاس در صفحه‌ای با بردار m بهنجار به یک و دومین انعکاس در صفحه‌ای با بردار n بهنجار به یک است:

$$a' = -mam$$

$$a'' = -na'n = -n(-mam)n = (nm)a(mn) \quad (۱۶.۲)$$

اگر θ زاویه بین m و n باشد، زاویه‌ی بین بردار a و بردار دوران یافته a'' 2θ خواهد



شکل ۲.۲: دوران بردار a

بود و مولد دوران را می‌توان به صورت زیر تعریف کرد:

$$R = nm, \quad R^\dagger = mn \quad (۱۷.۲)$$

در نتیجه داریم:

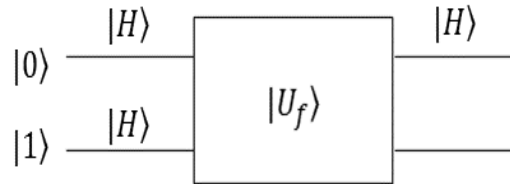
$$a'' = RaR^\dagger \quad (۱۸.۲)$$

فصل ۳

الگوریتم‌های کوانتومی

۱.۳ الگوریتم دویچ

همان‌طور که در فصل ۱ گفتیم، این الگوریتم برای شناسایی نوع تابع به‌کار می‌رود [۱]. این الگوریتم شامل ۳ مرحله است:



شکل ۱.۳: الگوریتم دویچ

۱. اعمال اپراتور هادامارد بر روی حالت ورودی $|0\rangle|1\rangle$

۲. اعمال اپراتور U_f

۳. اعمال اپراتور هادامارد بر روی کیوبیت اول

$$(H \otimes H)|0\rangle|1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) \quad (1.3)$$

$$U_f|00\rangle = |0, 0 \oplus f(0)\rangle = (1 - f(0))|00\rangle + f(0)|01\rangle$$

$$U_f|01\rangle = |0, 1 \oplus f(0)\rangle = (1 - f(0))|01\rangle + f(0)|00\rangle$$

$$U_f|10\rangle = |1, 0 \oplus f(1)\rangle = (1 - f(1))|10\rangle + f(1)|11\rangle$$

$$U_f|11\rangle = |1, 1 \oplus f(1)\rangle = (1 - f(1))|11\rangle + f(1)|10\rangle$$

$$\begin{aligned} |\psi'\rangle &= U_f(H \otimes H) \\ &= (1 - f(0))|00\rangle + f(0)|01\rangle + (1 - f(0))|01\rangle + f(0)|00\rangle \\ &\quad + (1 - f(1))|10\rangle + f(1)|11\rangle + (1 - f(1))|11\rangle + f(1)|10\rangle \end{aligned}$$

$$|\psi_{out}\rangle = (H \otimes I)|\psi'\rangle = (1 - f(0) - f(1))|0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) + (f(1) - f(0))|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

اگر تابع ثابت باشد، خروجی زیر را داریم:

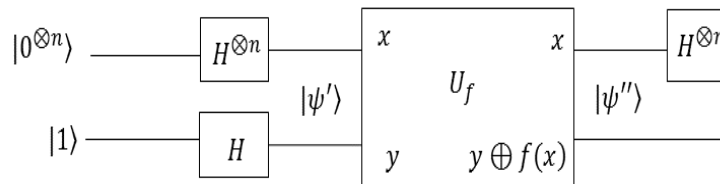
$$|\psi_{out}\rangle = \pm|0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (۲.۳)$$

و اگر تابع متوازن باشد، خروجی به صورت زیر حاصل می شود:

$$|\psi_{out}\rangle = \pm|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (۳.۳)$$

۲.۳ الگوریتم دوپیچ-جوزا

الگوریتم دوپیچ-جوزا^۱ تعمیم یافته‌ی الگوریتم دوپیچ است با این تفاوت که $x \in \{0, 1\}^n$ [۱].



شکل ۲.۳: الگوریتم دوپیچ-جوزا

$$|\psi'\rangle = (|H^{\otimes n} \otimes H|0^{\otimes n}\rangle|1\rangle) \quad (۴.۳)$$

$$|\psi'\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (۵.۳)$$

$$U_f|\psi'\rangle = |\psi''\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (۶.۳)$$

اعمال اپراتور هادامارد بر روی n کیوبیت حالت $|x\rangle$ به صورت زیر است:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_x \sum_y (-1)^{x \cdot y} |y\rangle \quad (۷.۳)$$

در نتیجه خروجی به صورت زیر حاصل می شود:

$$|\psi_{out}\rangle = \frac{1}{2^n} \sum_x \sum_y (-1)^{x \cdot y + f(x)} |y\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (۸.۳)$$

^۱Deutsch-Jozsa

از اندازه‌گیری n کیوبیت ورودی در حالت $|\psi_{out}\rangle$ دو نتیجه‌ی احتمالی زیر وجود دارد:

- اگر تمام کیوبیت‌ها در $|y\rangle$ صفر باشند، تابع ثابت است.
- اگر حداقل یکی از کیوبیت‌ها در $|y\rangle$ یک باشد، تابع متوازن است.

۳.۳ الگوریتم گراور استاندارد

اغلب ما به دنبال پیدا کردن یک حالت بین N حالت نامنظم هستیم، این معادل است با پیدا کردن یک موضوع برای یک هدف خاص در سیستم نرم‌افزاری که قابلیت ذخیره‌سازی، بازیافت و اصلاح اطلاعات را دارد که در یک موقعیت مشخص قرار دارد. زیرا هر حالت ممکن از این سیستم دارای یک شیء ثبت شده‌ی مشخص است.

گراور^۲ پی برد که یک الگوریتم کوانتومی برای سیستم ذخیره‌سازی اطلاعات دارای کارایی مؤثرتری نسبت به الگوریتم کلاسیکی دارد که سرعت الگوریتم کوانتومی بیشتر است. در الگوریتم‌های کلاسیکی $O(N)$ می‌تواند نقش $O(\sqrt{N})$ در الگوریتم‌های کوانتومی را ایفا کند که این پیشرفت در الگوریتم‌های کوانتومی بسیار مهم است. در این الگوریتم از نمایش باینری تابع f استفاده می‌کنیم که برای حالت مشخص مقدار یک و برای بقیه حالات مقدار صفر را دارد. اپراتور متناظر با الگوریتم گراور می‌تواند حالت هدف را مشخص کند.

جستجوی کوانتومی چیست؟

فرض می‌کنیم که در فضای جستجو N شیء داریم که روی شاخص‌های این اشیاء متمرکز می‌شویم که شماره‌ای بین 0 تا $N-1$ دارند. برای راحتی فرض می‌کنیم $N = 2^n$. بنابراین شاخص می‌تواند به صورت n بیتی منظم شود و مسئله‌ی جستجو M جواب دارد که $1 \leq M \leq N$. برای پیدا کردن یک شیء خاص کفایت تا فقط اندیس مربوط به آن را پیدا کنیم. در جستجوی کوانتومی اشیاء با کت‌های n کیوبیتی که هر کدام از این کت‌ها پایه‌هایی از فضای 2^n بعدی است، مشخص می‌شوند. در مسئله‌ی جستجوی کوانتومی ما به دنبال پیدا کردن یک حالت پایه‌ی خاص میان 2^n حالت موجود هستیم. $S = x_0, x_1, \dots, x_{N-1}$ را برای یک مسئله‌ی جستجو بیان می‌کنیم. در الگوریتم گراور یک تابع $f(x)$ با n ورودی داریم که $x \in \{0, 1\}^n$ می‌باشد. $f := S\{0, 1\}^n$ روی این

^۲ LovGrover

مجموعه تعریف شده است. خروجی تابع در یکی از عناصر S برابر یک است (w) و در بقیه عناصر برابر صفر است. نمی دانیم که w کدام یکی از x_i های مجموعه S است.

در کامپیوترهای کلاسیکی برای یافتن w باید تک تک x_i ها را به تابع بدهیم و یک به یک خروجی را نگاه کنیم اگر $f(x) = 1$ یعنی x همان w مورد نظر است و در غیر این صورت اگر $f(x) = 0$ یعنی x جواب نیست:

$$f(x) = \begin{cases} 1 & \text{if } x = w \\ 0 & \text{if } x \neq w \end{cases} \quad (9.3)$$

درواقع در کامپیوترهای کلاسیک به طور متوسط به $O(\frac{N}{2})$ فراخوانی تابع نیاز داریم زیرا ممکن است جواب در اولین گزینه یا در آخرین گزینه باشد که متوسط آن $\frac{N}{2}$ می شود.

در الگوریتم جستجوی کوانتومی با استفاده هوشمندانه ای از اصل برهم نهی و توازی کوانتومی می توان این مقدار را به $O(\sqrt{N})$ کاهش داد که برای N های بزرگ کاهش قابل ملاحظه ای دارد. ابتدا یک برهم نهی^۳ از حالات ورودی را تشکیل می دهیم و آن را به w گرایش می دهیم. اولین کاری که می کنیم ساختن کت حالتی است که حاصل برهم نهش تمامی پایه های فضای n بعدی است. این کت باید با تمامی پایه ها هم پوشانی برابر داشته باشد. این برهم نهی را می توان با استفاده از $H^{\otimes n} |0^{\otimes n}\rangle$ ایجاد کرد.

ساختن ترکیب خطی از بردارهای پایه ی محاسباتی با استفاده از اپراتور هادامارد است. در نتیجه:

$$|S\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle \quad (N = 2^n)$$

که این کت شامل w که جواب مورد نظر است نیز می باشد، به طوری که:

$$\langle w|S\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} \langle w|x\rangle = \frac{1}{\sqrt{N}} \quad (10.3)$$

دو اپراتور در الگوریتم گراور استفاده می شود:

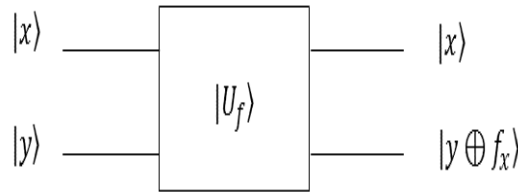
اپراتور اول (U_f):

تابع f را در یک مدار کوانتومی^۴ به صورت اپراتور کوانتومی زیر تعریف می کنیم [۴]:

$$U_f|x, y\rangle = |x_i, f(x_i) \oplus y\rangle \quad (11.3)$$

^۳superposition

^۴Quantum circuits



هرگاه این عملگر را روی ورودی $|x_i\rangle \otimes |-\rangle$ اثر دهیم که در آن $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ ، آنگاه به راحتی دیده می‌شود که:

$$U_f|w\rangle \otimes |-\rangle = -|w\rangle \otimes |-\rangle \quad (12.3)$$

$$U_f|x_i\rangle \otimes |-\rangle = |x_i\rangle \otimes |-\rangle \quad x_i \neq w$$

بنابراین روی زیرفضای اول اثر این عملگر به شکل یک انعکاس ظاهر می‌شود. یعنی این عملگر حالت $|w\rangle$ را به حالت $-|w\rangle$ برمی‌گرداند و بقیه حالات را بدون تغییر باقی می‌گذارد. از این به بعد در بحث خود فضای دوم یعنی $|-\rangle$ را برای سادگی حذف می‌کنیم. در نتیجه می‌توان عملگر U_f را به شکل زیرنوشت:

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle \quad (13.3)$$

که تبدیل U_f برابر اپراتور یکانی I_w است:

$$I_w = I - 2|w\rangle\langle w| \quad (14.3)$$

اپراتور U_f بدون دانستن حالت $|w\rangle$ این انعکاس را انجام می‌دهد. در واقع این اپراتور روی زیرفضای جواب‌ها یک انعکاس ایجاد می‌کند و بقیه حالات بدون تغییر باقی می‌مانند.

U_f یک اپراتور یکانی است

$$|x, (y \oplus f(x))\rangle \xrightarrow{U_f} |x, (y \oplus f(x) \oplus f(x))\rangle \quad (15.3)$$

برای هر $f(x)$ ، $f(x) \oplus f(x) = 0$.
 $|S\rangle$ را به صورت زیر تشکیل می‌دهیم:

$$|S\rangle = H^{\otimes n}|0^{\otimes n}\rangle \otimes H|1\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |x_i\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (16.3)$$

که اثر U_f روی این حالت نتیجه‌ی زیر را به دنبال دارد:

$$if \quad f(x) = 0 \Rightarrow |0\rangle - |1\rangle \rightarrow |0\rangle - |1\rangle$$

$$if \quad f(x) = 1 \Rightarrow |0\rangle - |1\rangle \rightarrow -(|0\rangle - |1\rangle) \quad (17.3)$$

$$\Rightarrow |0\rangle - |1\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle) \quad (18.3)$$

در نتیجه در حالت کلی می‌توان گفت:

$$U_f|S\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (19.3)$$

می‌بینیم که با اثر U_f ، کیوبیت هدف تغییری نکرده است و در ادامه نیز تغییر نمی‌کند پس می‌توان آن را در محاسبات نادیده گرفت.

بحث‌های فوق را می‌توان برای n کیوبیت (رجیستر^۵ ورودی) و m کیوبیت (رجیستر خروجی) عمومیت بخشید.

اپراتور دوم (I_S):

دومین اپراتور مورد استفاده در الگوریتم گراور اپراتور I_S است که آن را به صورت زیر نشان

می‌دهیم:

$$I_S = 2|S\rangle\langle S| - I \quad (20.3)$$

همان‌طور که قبلاً گفتیم:

$$|S\rangle = \frac{1}{\sqrt{N}}(x_0, x_1, \dots, x_{N-1}) = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |x_i\rangle \quad (21.3)$$

می‌توان نشان داد که این انعکاس حول متوسط نیز یک عملگر یکانی است که آن را با I_S نشان می‌دهیم. خواننده می‌تواند به راحتی تصدیق کند که بعد از چندبار خواندن تابع و انعکاس حول متوسط، یعنی بعد از چند بار اعمال عملگر $G = I_S I_w$ شکل حالت به صورتی درخواهد آمد که در آن دامنه مربوط به $|w\rangle$ نسبت به بقیه دامنه‌ها افزایش قابل ملاحظه‌ای پیدا کرده است و در نتیجه اندازه‌گیری چنین حالتی به احتمال زیاد، نتیجه‌اش $|w\rangle$ خواهد بود. البته پس از هر دفعه اندازه‌گیری با احتمال ضعیفی ممکن است که عنصری غیر از $|w\rangle$ یافت شود که در این صورت با خواندن آن به تابع f و به دست آمدن مقدار صفر الگوریتم دوباره از اول طی می‌شود.

حال نشان می‌دهیم که I_S انعکاس حول متوسط دامنه‌ها است [۱]، [۲]، [۳]:

حالت سیستم قبل از اعمال I_S به صورت:

$$|\psi\rangle = \sum_{i=0}^{N-1} a_i |x_i\rangle \quad (22.3)$$

است.

I_S را روی کت $|\psi\rangle$ اثر می‌دهیم:

$$\langle S|x_i\rangle = \frac{1}{\sqrt{N}} \quad (23.3)$$

^۵Register

$$\begin{aligned}
 I_S|\psi\rangle &= (\mathcal{Y}|S\rangle\langle S| - I) \left(\sum_{i=0}^{N-1} a_i|x_i\rangle \right) = \sum_{i=0}^{N-1} a_i (\mathcal{Y}|S\rangle\langle S|x_i\rangle - |x_i\rangle) \\
 &= \sum_i (\mathcal{Y}\bar{a} - a_i)|x_i\rangle \quad (24.3)
 \end{aligned}$$

که

$$\begin{aligned}
 \sum_i a_i \frac{|S\rangle}{\sqrt{N}} &= \sum_i \frac{1}{N} (a_1 + a_2 + \dots + a_N)|x_i\rangle \\
 &= \sum_i \bar{a}|x_i\rangle \quad (25.3)
 \end{aligned}$$

و

$$\frac{1}{N} (a_1 + a_2 + \dots + a_N) = \bar{a} \quad (26.3)$$

که متوسط دامنه‌های حالت $|\psi\rangle$ است. پس $I_S|\psi\rangle$ یعنی دامنه‌ی a_i حول مقدار متوسط دامنه‌ها یعنی \bar{a} انعکاس یافته است [۲]، [۳]، [۱].

از طرفی:

$$I_S = \mathcal{Y}|S\rangle\langle S| - I \quad (27.3)$$

و

$$|S\rangle = H^{\otimes n}|\circ^{\otimes n}\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |x_i\rangle \quad (28.3)$$

$$\Rightarrow I_S = H^{\otimes n} I_o H^{\otimes n} \quad (29.3)$$

که I_o عامل تغییر فاز است:

$$I_o = \mathcal{Y}|\circ^{\otimes n}\rangle\langle\circ^{\otimes n}| - I \quad (30.3)$$

که به صورت زیر نیز نوشته می‌شود:

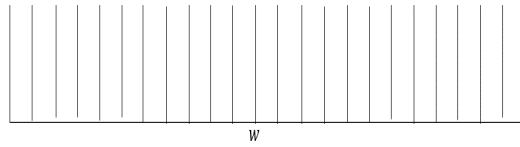
$$|x\rangle \longrightarrow -(-1)^{\delta_{x,\circ}} |x\rangle \quad (31.3)$$

یعنی هر حالت در پایه‌های محاسباتی به جز حالت $|\circ\rangle$ فاز (-1) می‌گیرد [۲]، [۳]، [۱]:

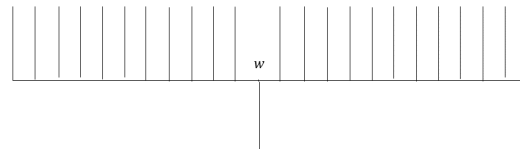
$$I_o|x\rangle = (\mathcal{Y}|\circ\rangle\langle\circ| - I)|x\rangle = \begin{cases} |x\rangle = |\circ\rangle \Rightarrow I_o|x\rangle = |\circ\rangle \\ |x\rangle \neq |\circ\rangle \Rightarrow I_o|x\rangle = -|x\rangle \end{cases} \quad (32.3)$$

بیان شماتیک از الگوریتم گراور در اشکال زیر آمده است: اپراتور گراور به صورت زیر تعریف می‌شود [۱۰]:

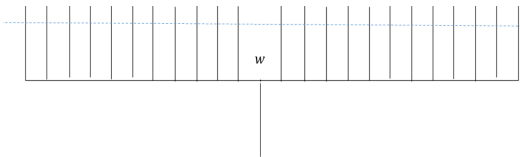
$$G = H^{\otimes n} I_o H^{\otimes n} I_w = H^{\otimes n} (\mathcal{Y}|\circ\rangle\langle\circ| - I) H^{\otimes n} U_f = I_S I_w$$



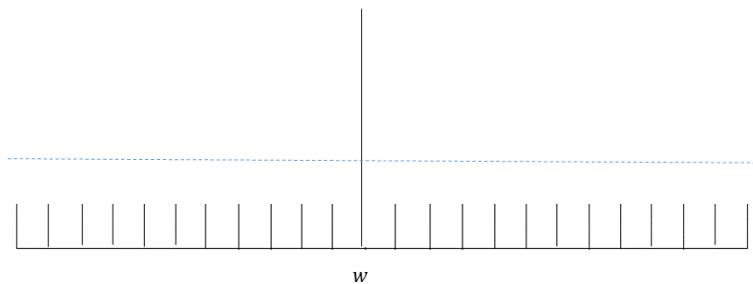
شکل ۳.۳: بردار حالت ورودی که ترکیب خطی از همه داده‌های ممکن با ضرایب مساوی است



شکل ۴.۳: بردار حالت ورودی بعد از آن که تابع آن را یک‌بار خوانده است



شکل ۵.۳: بردار حالت قبل از انعکاس حول متوسط



شکل ۶.۳: بردار حالت بعد از انعکاس حول متوسط

$$G = I_S I_w \quad (۳۳.۳)$$

در این قسمت می‌خواهیم نشان دهیم که با اثر عملگر گراور به تعداد $O(\sqrt{N})$ مرتبه روی حالت اولیه $|S\rangle$ می‌توانیم به حالتی برسیم که دامنه $|w\rangle$ در آن بسیار افزایش یافته است.

برای این کار در فضای حالت‌ها، حالت زیر را تعریف می‌کنیم:

$$|r\rangle = \frac{1}{\sqrt{N-1}} \left(\sum_{x_i \neq w} |x_i\rangle \right) \quad (34.3)$$

حال دقت می‌کنیم که هر دو عملگر I_S و I_w را می‌توان تنها برحسب بردارهای $|w\rangle$ و $|r\rangle$ نوشت. در واقع تمام دینامیک از اول تا به آخر در زیرفضایی طی می‌شود که توسط این دو بردار جاروب می‌شوند. از آنجا که این دو بردار بر هم عمودند می‌توانیم نمایش زیر را برای آن‌ها انتخاب کنیم:

$$|w\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |r\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (35.3)$$

و

$$|S\rangle = \frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} |r\rangle = \begin{pmatrix} \frac{1}{\sqrt{N}} \\ \sqrt{\frac{N-1}{N}} \end{pmatrix} \quad (36.3)$$

در نتیجه خواهیم داشت :

$$I_w = I - 2|w\rangle\langle w| = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad (37.3)$$

و

$$I_S = 2|S\rangle\langle S| - I = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N}\sqrt{N-1} \\ \frac{2}{N}\sqrt{N-1} & 1 - \frac{2}{N} \end{pmatrix} \quad (38.3)$$

در نتیجه عملگر گراور به شکل زیر درخواهد آمد:

$$G = \begin{pmatrix} 1 - \frac{2}{N} & \frac{2}{N}\sqrt{N-1} \\ -\frac{2}{N}\sqrt{N-1} & 1 - \frac{2}{N} \end{pmatrix} \quad (39.3)$$

به راحتی می‌توان تحقیق کرد که این عملگر یک عملگر متعامد است یعنی $I = G^\dagger G$ و در نتیجه چیزی جز یک دوران در صفحه جاروب شده توسط $|r\rangle$ و $|w\rangle$ نیست.

پارامتر دوران θ را به شکل زیر تعریف می‌کنیم:

$$\cos \theta = 1 - \frac{2}{N}, \quad \sin \theta = \frac{2}{N}\sqrt{N-1} \quad (40.3)$$

و به این ترتیب عملگر گراور به شکل زیر درخواهد آمد:

$$\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \quad (41.3)$$

هرگاه روی حالت اولیه $|S\rangle$ عملگر گراور را k بار اثر دهیم یعنی اینکه آن حالت را به اندازه زاویه $k\theta$ چرخانده ایم. برای اینکه ببینیم این حالت چه مقدار به حالت مطلوب یعنی $|w\rangle$ نزدیک شده است می بایست عنصر ماتریسی $\langle w|G^k|S\rangle$ را حساب کنیم که برابر خواهد شد با:

$$\langle w|G^k|S\rangle = \frac{1}{\sqrt{N}} \cos k\theta + \sqrt{\frac{N-1}{N}} \sin k\theta \quad (42.3)$$

اگر قرار دهیم

$$\cos \alpha = \frac{1}{\sqrt{N}} \quad (43.3)$$

$$\sin \alpha = \sqrt{\frac{N-1}{N}} \quad (44.3)$$

آنگاه خواهیم داشت :

$$\langle w|G^k|S\rangle = \cos(k\theta - \alpha) \quad (45.3)$$

برای این که این هم پوشانی به حداکثر خود برسد تقاضا می کنیم که $k \approx \frac{\alpha}{\theta}$.

یک نتیجه خیلی جالب که زود می توان دریافت مربوط به حالتی است که $N = 4$ باشد. در این حالت داریم $\cos \theta = \frac{1}{2}$ و $\cos \alpha = \frac{1}{2}$ و یا:

$$\alpha = \frac{\pi}{3}, \quad \theta = \frac{\pi}{3} \rightarrow k = 1 \quad (46.3)$$

یعنی می توان در این حالت تنها با یک بار خواندن تابع به w آنهم با احتمال یک دست یافت.

برای وقتی که N خیلی بزرگ است داریم:

$$\begin{aligned} \alpha &\approx \frac{\pi}{4}, \quad \cos \theta \approx 1 - \frac{\theta^2}{2} = 1 - \frac{2}{N} \\ \rightarrow \theta &= \frac{2}{\sqrt{N}} \end{aligned} \quad (47.3)$$

و در نتیجه $k \approx (\frac{\pi}{4}\sqrt{N})$. به این ترتیب پس از $O(\sqrt{N})$ مرتبه می توانیم با احتمال خیلی خوب شیء مورد نظر را در درون داده ها پیدا کنیم یعنی می توان در این حالت تنها با

یک بار خواندن تابع به w آن‌هم با احتمال یک دست یافت.

می‌توان این دوران را به شکل هندسی دیگری نیز توصیف کرد [۱]، [۲]، [۳]. اگر M جواب بین N گزینه داشته باشیم می‌توان بردار $|S\rangle$ را به صورت ترکیبی از جواب‌ها و بقیه حالات که جواب‌ها نیستند نوشت:

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \neq w} |x\rangle \quad (48.3)$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x=w} |x\rangle \quad (49.3)$$

$$\Rightarrow |S\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle \quad (50.3)$$

I_w یک انعکاس حول بردار $|\alpha\rangle$ روی صفحه‌ای که شامل $|\alpha\rangle$ و $|\beta\rangle$ است انجام می‌دهد:

$$I_w (a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle \quad (51.3)$$

به‌طور مشابه I_w انعکاس در صفحه‌ی تعریف شده توسط $|\alpha\rangle$ و $|\beta\rangle$ حول بردار $|S\rangle$ است و حاصل دو انعکاس متوالی یک دوران در صفحه‌ی تعریف شده است، بنابراین اگر:

$$\sqrt{\frac{N-M}{N}} = \cos \frac{\theta}{2} \quad (52.3)$$

$$\sqrt{\frac{M}{N}} = \sin \frac{\theta}{2} \quad (53.3)$$

$$|S\rangle \xrightarrow{I_w} |\psi_1\rangle = \cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle \quad (54.3)$$

یعنی I_w ، $|\psi_1\rangle$ را حول $|\alpha\rangle$ انعکاس می‌دهد و بعد از اعمال اپراتور I_S داریم:

$$I_S |\psi_1\rangle = |\psi_2\rangle = (2|S\rangle\langle S| - I) |\psi_1\rangle = 2|S\rangle\langle S|\psi_1\rangle - |\psi_1\rangle \quad (55.3)$$

که $|\psi_2\rangle$ همان انعکاس $|\psi_1\rangle$ حول $|S\rangle$ است و $|S\rangle$ را به اندازه θ می‌چرخاند:

$$\Rightarrow G|S\rangle = \cos \frac{3\theta}{2} |\alpha\rangle + \sin \frac{3\theta}{2} |\beta\rangle \quad (56.3)$$

کت حالت با اثر اپراتور G همواره در این صفحه‌ی دو بعدی باقی می‌ماند و از آن خارج نمی‌شود. نتیجه‌ی حاصل از این دو انعکاس متوالی معادل است با یک دوران به اندازه θ به سمت پایه‌ی $|\beta\rangle$.

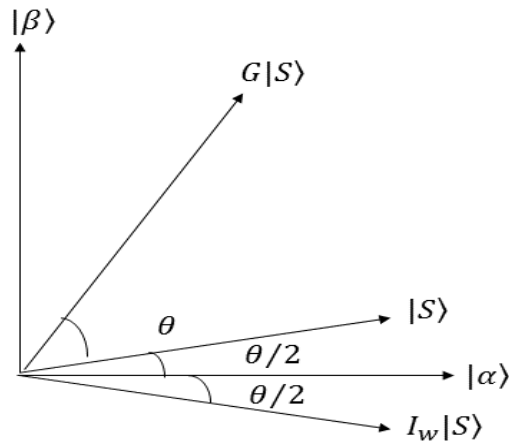
پس اپراتور گراور معادل با یک ماتریس دوران است:

$$\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \quad (57.3)$$

و در حالت کلی برای k بار اثر دادن اپراتور گراور روی $|S\rangle$:

$$G^k |S\rangle = \cos\left(\frac{2k+1}{2}\theta\right) |\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right) |\beta\rangle \quad (58.3)$$

یعنی $G^k |S\rangle$ بردار $|S\rangle$ را به اندازه $k\theta$ می چرخاند. به طور خلاصه اپراتور گراور یک



شکل ۷.۳: دوران بردار ورودی بر روی حالت جواب

دوران در فضای دو بعدی جاروب شده توسط دو بردار $|\alpha\rangle$ و $|\beta\rangle$ است. می توان نشان داد که اعمال اپراتور گراور روی $|S\rangle$ برای یافتن جواب از $O(\sqrt{N})$ مرحله است.

فرض می کنیم که $N \gg M$:

$$\sin\left(\frac{\theta}{2}\right) \simeq \frac{\theta}{2} = \sqrt{\frac{M}{N}} \quad (59.3)$$

برای اینکه بعد از k بار دوران، جواب $|\beta\rangle$ باشد، باید $G |S\rangle$ دورانی به اندازه $\frac{\pi}{4}$ باشد، یعنی:

$$\begin{aligned} G^k |S\rangle = |\beta\rangle &\implies \frac{2k+1}{2}\theta = \frac{\pi}{4} \\ &\implies \frac{2k+1}{2} \cdot 2\sqrt{\frac{M}{N}} = \frac{\pi}{4} \\ &\implies k = \frac{\pi}{4}\sqrt{\frac{N}{M}} - \frac{1}{2} \end{aligned}$$

که برای $N \gg M$:

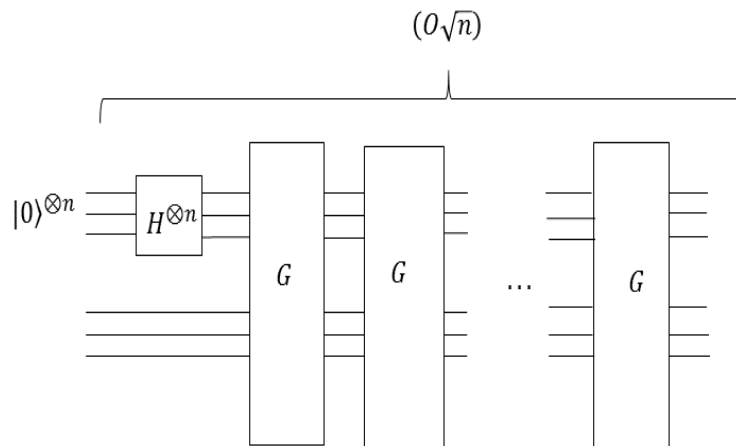
$$k \approx \frac{\pi}{4} \sqrt{\frac{N}{M}} \quad (۶۰.۳)$$

که از $O(\sqrt{N})$ است.

احتمال نزدیک شدن به جواب $(|\beta\rangle)$ بعد از k بار اثر دادن اپراتور گراور:

$$|\langle \beta | G^k | S \rangle|^2 = \sin^2\left(\frac{\sqrt{k+1}}{2}\theta\right) \quad (۶۱.۳)$$

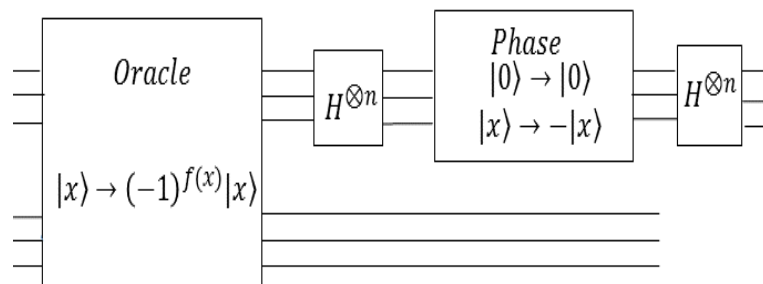
نمودار الگوریتم گراور در شکل زیر نشان داده شده است:



که اپراتور گراور:

$$G = H^{\otimes n} I \cdot H^{\otimes n} U_f \quad (۶۲.۳)$$

و ساختار داخلی هر جعبه‌ی گراور به صورت زیر است:



- می‌توان دریافت که الگوریتم گراور با تغییر حالت اولیه تغییر نخواهد کرد. یعنی اگر به جای حالت اولیه $|S\rangle$ حالت $|\bar{S}\rangle$ را در دسترس داشته باشیم، الگوریتم گراور همچنان بهینه خواهد بود. (برای اثبات بهینه بودن الگوریتم گراور به [۲] مراجعه شود).
- این الگوریتم در هر بار تکرار دامنه‌ی جواب را منفی سپس تمام دامنه‌ها را نسبت به میانگین معکوس می‌کند که سبب افزایش دامنه‌ی جواب و کاهش دامنه‌های دیگر می‌شود.

- افزایش بزرگی دامنه‌ی حالت مورد نظر در هر مرحله نسبت به بقیه حالات سیستم آن را از بقیه حالات متمایز می‌سازد.
- هرگاه تعداد عناصر مطلوب بیش از یکی مثلاً l تا باشد، اصلاح کوچکی در استدلال بالا نشان می‌دهد که می‌توان در زمانی از مرتبه $O\left(\frac{\sqrt{N}}{l}\right)$ به یکی از عناصر مطلوب دست یافت.

فصل ۴

کاربرد جبر کلیفورد در الگوریتم
جستجوی کوانتومی

۱.۴ مقدمه

جستجوی گراور نموی از دوران بردارهای حالت است. در جبر هندسی برای دوران بردار a با زاویه $|a|$ مولد دوران به صورت زیر تعریف می‌شود:

$$R = e^{-ia/2} = \cos(|a|/2) - i \frac{a}{|a|} \sin(|a|/2) \quad (1.4)$$

در واقع هر مولد دوران را می‌توان به صورت زیر نوشت:

$$R = \exp(\beta/2) \quad (2.4)$$

که β یک بردار دو بعدی است. دوران بردار $V = v_1e_1 + v_2e_2 + v_3e_3$ به صورت زیر است:

$$V' = RVR^\dagger = e^{-ia/2}Ve^{ia/2} \quad (3.4)$$

ساده‌ترین مثال از یک سیستم دو حالت، اسپین کوانتومی است. حالت‌های اسپین می‌تواند نمایشی از بردارهای دو مؤلفه‌ای مختلط شناخته شده‌ی اسپینورها باشد که می‌تواند با یک کدگذاری کلی‌تر در فضای D_3 با نگاشت یک‌به‌یک خطی بین حالت (بردار مختلط) و ساختار بردار چندبعدی^۱ از ترم‌هایی با درجه‌ی زوج (مثل اسکالر و بردار دوبعدی) تعریف شود.

ساده‌ترین نگاشت به صورت زیر تعریف می‌شود [۷]، [۸]:

$$\begin{aligned} |\psi\rangle = Z_1|\uparrow\rangle + Z_2|\downarrow\rangle &= \begin{pmatrix} a_0 + ia_3 \\ -a_2 + ia_1 \end{pmatrix} \longleftrightarrow \psi = a_0 + a_k i e_k \\ &= a_0 + a_1 i e_1 + a_2 i e_2 + a_3 i e_3 \end{aligned} \quad (4.4)$$

برای یک سیستم تک ذره‌ای بردارهای پایه به صورت زیر نگاشت می‌شوند [۷]، [۸]:

$$\begin{aligned} |0\rangle &\longleftrightarrow 1 \\ |1\rangle &\longleftrightarrow -i e_2 \end{aligned} \quad (5.4)$$

اثر عملگرهای کوانتومی σ_k و واحد موهومی i روی حالت $|\psi\rangle$ به صورت زیر نگاشت می‌شوند:

$$\begin{aligned} \hat{\sigma}_k |\psi\rangle &\longleftrightarrow e_k \psi e_3 = -i e_k \psi i e_3 \\ \hat{\sigma}_1 \hat{\sigma}_2 \hat{\sigma}_3 &= i |\psi\rangle \longleftrightarrow \psi i e_3 \end{aligned} \quad (6.4)$$

^۱multivector

ψ را می‌توان به یک ترم چگالی و یک ترم مولد دوران تجزیه کرد که بردار ثابت چرخان است:

$$\begin{aligned}\rho &= \psi^\dagger \psi = (a_0 + a_k \iota e_k)(a_0 - a_k \iota e_k) \\ &= a_0^2 + a_1^2 + a_2^2 + a_3^2 \\ &= \psi^\dagger \psi = \rho^{-1}\end{aligned}\quad (7.4)$$

ρ بزرگی بردار حالت ψ است. پس می‌توان بردار چند بعدی ψ را به صورت زیر بازنویسی کرد:

$$\psi = \rho^{1/2} R \quad (8.4)$$

که همانطور که از قبل می‌دانیم:

$$RR^\dagger = R^\dagger R = 1$$

$$a \xrightarrow{R} a' = RaR^\dagger \quad (9.4)$$

مؤلفه‌های بردار اسپینی S به صورت زیر است:

$$S_k = \langle \psi | \sigma_k | \psi \rangle \quad (10.4)$$

اگر بردار $|\psi\rangle$ را به صورت زیر در نظر بگیریم:

$$\psi = \begin{pmatrix} a_0 + ia_3 \\ -a_2 + ia_1 \end{pmatrix} \quad (11.4)$$

که همانطور که می‌بینیم:

$$|0\rangle \leftrightarrow 1$$

$$|1\rangle \leftrightarrow -\iota e_2$$

$$i|\psi\rangle \leftrightarrow \psi \iota e_3 \quad (12.4)$$

در نتیجه رابطه‌ی (۱۰.۴) به صورت زیر حاصل می‌شود [۱۳]:

$$\begin{aligned}& (a_0 - ia_3, -a_2 - ia_1) (\sigma_x \hat{i} + \sigma_y \hat{j} + \sigma_z \hat{k}) \begin{pmatrix} a_0 + ia_3 \\ -a_2 + ia_1 \end{pmatrix} \\ &= \begin{bmatrix} 2a_0 a_2 + 2a_1 a_3 \\ -2a_2 a_3 + 2a_0 a_1 \\ a_0^2 + a_3^2 - a_1^2 - a_2^2 \end{bmatrix} \quad (13.4)\end{aligned}$$

و در جبر هندسی به صورت زیر است:

$$S_k = \langle \tilde{\psi} e_k \psi e_3 \rangle = e_k \cdot (\psi e_3 \tilde{\psi}) \quad (14.4)$$

می‌توان از معادله‌ی (۱۴.۴) دریافت که تمام مؤلفه‌های بردار اسپین می‌توانند در یک بسط به صورت زیر خلاصه شوند [۷]، [۸]:

$$S = \psi e_3 \tilde{\psi} = \rho^{1/2} Re_3 \rho^{1/2} \tilde{R} = \rho Re_3 \tilde{R} \quad (15.4)$$

از اینرو R در فضای سه بعدی یک دستور برای دوران بردار e_3 روی مشاهده‌پذیر بردار اسپینی است.

نرمالیزه کردن مشاهده‌پذیر تعریف شده بردار اسپینی واحد به صورت زیر است:

$$S_k = \frac{\psi e_3 \tilde{\psi}}{\rho} = Re_3 \tilde{R} \quad (16.4)$$

که تعریف بردار واحد است که نمایش کلی یک نقطه روی کره‌ی بلاخ است.

با استفاده از حالت‌های بیشینه و کمینه ما می‌توانیم یک تصویر هندسی از مراحل جستجو را پیدا کنیم.

در این فصل ابتدا در یک فضای دو بعدی مختلط و با استفاده از حالت‌های خوش تعریف $|m\rangle$ و $|\sigma\rangle$ ، چهار عملگر ممکن را تعریف می‌کنیم. در بخش اول سعی شده است نشان دهیم که با استفاده از این ۴ عملگر می‌توان بردارهای پایه را برای فضای جستجو به دست آورد و خواهیم دید که شکل ماتریسی عملگر گراور همان عملگر دوران است.

در بخش دوم عملگر جستجوی گراور را با استفاده از جبر هندسی به دست می‌آوریم و نشان می‌دهیم که تعداد تکرار عملگر گراور برای رسیدن به جواب از مرتبه‌ی \sqrt{N} است.

در بخش سوم این فصل جستجوی گراور دقیق‌تری را مطرح می‌کنیم و در بخش چهارم جستجوی گراور تعمیم یافته از بخش سوم را بیان می‌کنیم.

الگوریتم جستجوی کوانتومی گراور به دنبال چگونگی تغییرات تابع موج حالت اولیه $|\sigma\rangle$ به حالت مورد نظر $|m\rangle$ است. $|m\rangle$ نمایشگر مجموعه‌ای از جواب‌هاست که با انجام عمل اندازه‌گیری یکی از اعضای این مجموعه به دست می‌آید و برای آنالیز کردن این تغییرات پایه‌های متعامد $|m\rangle$ و $|m^\perp\rangle$ تعریف می‌شوند. با این وجود در این پایان‌نامه ما از پایه‌های دیگری که بر اساس ضرب وزنی بیشینه و کمینه تعریف شده‌اند استفاده می‌کنیم. این تعریف جدید به ما اجازه می‌دهد که حالت اولیه $|\sigma\rangle$ و حالت مورد نظر $|m\rangle$ به طور متقارن در این فضا نشان داده شوند. در واقع اجازه به ایده‌سازی فرآیند جستجوی گراور متناظر با حرکت تقدیمی ذره‌ای با اسپین $\frac{1}{2}$ در یک میدان مغناطیسی.

در روش جستجوی کوانتومی گراور، ذره از راستای حالت اولیه $|\sigma\rangle$ به حالت نهایی $|m\rangle$ دوران می‌کند. جبر کلیفورد قبلاً در روش جستجوی گراور به کار گرفته شده است با این وجود رهیافت اتخاذ شده در این جا نمایش کارآمد مؤثر را درست به همان خوبی تجسم می‌کند. هم‌چنین ضرب هندسی می‌تواند به‌عنوان نمایش دیگری از ضرب تانسوری استفاده شود. بنابراین توصیف دیگری از محاسبات کوانتومی و الگوریتم‌های کوانتومی بدون فرمالیزم مکانیک کوانتومی را می‌دهد. جبر هندسی کلیفورد هم‌چنین یک چارچوب غالب برای برهم‌کنش n ذره‌ی کیوبیت ارائه می‌دهد که n بزرگ است.

۲.۴ بردارهای پایه اصلاح شده برای فضای جستجو

با استفاده از حالت‌های بیشینه و کمینه ما می‌توانیم یک تصویر هندسی از مراحل جستجو را پیدا کنیم. در یک فضای دو بعدی مختلط و با استفاده از حالت‌های خوش تعریف $|m\rangle$ و $|\sigma\rangle$ ، چهار عملگر ممکن داریم:

$$|\sigma\rangle\langle\sigma|, |m\rangle\langle m|, |m\rangle\langle\sigma|, |\sigma\rangle\langle m|$$

با استفاده از این چهار عملگر، عملگرهای زیر را تعریف می‌کنیم [۹]:

$$J_1 = \frac{P - |\sigma\rangle\langle\sigma| - |m\rangle\langle m|}{2|\alpha|} \quad (17.4)$$

$$J_2 = \frac{-i(\alpha^*|m\rangle\langle\sigma| - \alpha|\sigma\rangle\langle m|)}{2|\alpha|\beta}$$

$$J_3 = \frac{|\sigma\rangle\langle\sigma| - |m\rangle\langle m|}{2\beta}$$

که $\alpha = \langle\sigma|m\rangle$ (می‌تواند مختلط باشد) و $\beta = \sqrt{1 - |\alpha|^2}$ و $i = \sqrt{-1}$ و

$$P = \frac{(|\sigma\rangle\langle\sigma| - |m\rangle\langle m|)^2}{\beta^2}$$

روابط زیر بین عملگرهای فوق برقرار است:

$$[J_i, J_j] = i\epsilon_{ijk}J_k \quad (18.4)$$

$$[J_i, J_j]_+ = \delta_{ij} \frac{P}{4} \quad (\text{که } \delta_{ij} \text{ علامت دلتای کرونیکر و } \epsilon \text{ علامت لوی چی وی تا است})$$

$$[P, J_i] = 0 \quad (19.4)$$

توان دوم مولدهای معادلات قبل به‌صورت زیر هستند:

$$J_1^2 = J_2^2 = J_3^2 = \frac{1}{4\beta^2} (|\sigma\rangle\langle\sigma| - |m\rangle\langle m|)^2 = \frac{1}{4}P \quad (20.4)$$

به راحتی می‌توان دریافت که:

$$P|\sigma\rangle = |\sigma\rangle$$

$$P|m\rangle = |m\rangle$$

$$P^2 = P \quad (21.4)$$

$$C = J_1^2 + J_2^2 + J_3^2 = \frac{3}{4}P \quad (22.4)$$

که این روابط متناظر با سیستم اسپین $\frac{1}{2}$ است. عملگرهای بالا برنده و پایین آورنده به صورت زیر هستند:

$$J_{\pm} = J_1 \pm iJ_2$$

با توجه به اینکه:

$$J_-|\downarrow\rangle = 0$$

$$J_+|\uparrow\rangle = 0 \quad (23.4)$$

حالت‌های با ضریب وزنی بالا و پایین را پیدا می‌کنیم:

$$|\uparrow\rangle = \sec \frac{\theta}{4} \left(\cos \frac{\theta}{4} |m\rangle - e^{-i\delta} \sin \frac{\theta}{4} |\sigma\rangle \right) \quad (24.4)$$

$$|\downarrow\rangle = \sec \frac{\theta}{4} \left(\sin \frac{\theta}{4} |m\rangle - e^{-i\delta} \cos \frac{\theta}{4} |\sigma\rangle \right) \quad (25.4)$$

که $\alpha = |\alpha|e^{i\delta}$ و $\sin \frac{\theta}{4} = |\alpha|$

در می‌یابیم که: $J_3|\downarrow\rangle = -\frac{1}{4}|\downarrow\rangle$ و $J_3|\uparrow\rangle = \frac{1}{4}|\uparrow\rangle$ که برای سیستم اسپین $\frac{1}{2}$ انتظار می‌روند. حال می‌توان با استفاده از روابط فوق حالت‌های $|m\rangle$ و $|\sigma\rangle$ را در پایه‌های جدید به دست آورد:

$$|\sigma\rangle = \cos \frac{\theta}{4} |\uparrow\rangle - \sin \frac{\theta}{4} |\downarrow\rangle$$

$$|m\rangle = e^{i\delta} \left(\sin \frac{\theta}{4} |\uparrow\rangle - \cos \frac{\theta}{4} |\downarrow\rangle \right) \quad (26.4)$$

$$|m^\perp\rangle = e^{i\delta} \left(-\cos \frac{\theta}{4} |\uparrow\rangle + \sin \frac{\theta}{4} |\downarrow\rangle \right)$$

عملگر گراور با استفاده از این نتایج به صورت زیر به دست می‌آید:

$$G = -(I - 2|\sigma\rangle\langle\sigma|)(I - 2|m\rangle\langle m|) \quad (27.4)$$

$$\Rightarrow G = -I + 2 \cos^2 \frac{\theta}{4} |\uparrow\rangle\langle\uparrow| + \sin \theta |\uparrow\rangle\langle\downarrow| - \sin \theta |\downarrow\rangle\langle\uparrow| + 2 \cos^2 \frac{\theta}{4} |\downarrow\rangle\langle\downarrow| \quad (28.4)$$

فرم ماتریسی عملگر گراور و بردار حالت اولیه به صورت زیر است:

$$G = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \quad (29.4)$$

$$|\sigma\rangle = \begin{pmatrix} \cos \frac{\theta}{4} \\ -\sin \frac{\theta}{4} \end{pmatrix} \quad (30.4)$$

حال یک نگاهت به فضای جبر کلیفورد انجام می‌دهیم. با توجه به روابط (۱۲.۴) اسپینورهای معادله (۲۶.۴) به صورت زیر تبدیل می‌شوند:

$$|\sigma\rangle \mapsto \cos \frac{\theta}{4} + \sin \frac{\theta}{4} \iota e_2 = +e^{\iota e_2 \theta / 4}$$

$$|m\rangle \mapsto \left(\sin \frac{\theta}{4} + \cos \frac{\theta}{4} \iota e_2 \right) e^{\delta e_3} = e^{\iota e_2 (\pi/2 - \theta/4)} \delta e_3 = \iota e_2 e^{-\iota e_2 \theta / 4} e^{\delta e_3} \quad (31.4)$$

$$|m^\perp\rangle \mapsto \left(-\cos \frac{\theta}{4} + \sin \frac{\theta}{4} \iota e_2 \right) e^{\delta e_3} = e^{-\iota e_2 \theta / 4}$$

حال می‌توان تبدیل زیر را در فضای جبر هندسی در نظر گرفت و تحت این تبدیل اسپینورهای فوق را در فضای حقیقی به دست آورد:

$$S = \psi e_3 \psi^\dagger \quad (32.4)$$

با توجه به تبدیل فوق، معادلات (۳۱.۴) به صورت زیر تبدیل می‌شوند:

$$\sigma = e^{\iota e_2 \theta / 4} e_3 e^{-\iota e_2 \theta / 4} = e^{\iota e_2 \theta / 2} e_3 = -\sin \frac{\theta}{4} e_1 + \cos \frac{\theta}{4} e_3$$

$$m = e^{\iota e_2 (\pi/2 - \theta/4)} e^{\delta e_3} e_3 e^{-\delta e_3} e^{-\iota e_2 (\pi/2 - \theta/4)} = e_3 e^{-\iota e_2 (\pi - \theta/4)} \quad (33.4)$$

$$= -e^{-\iota e_2 \theta / 2} e_3 = -\sin \frac{\theta}{4} e_1 - \cos \frac{\theta}{4} e_3$$

$$m^\perp = e^{-\iota e_2 \theta / 4} e_3 e^{\iota e_2 \theta / 4} = e_3 e^{\iota e_2 \theta / 2} = \sin \frac{\theta}{4} e_1 + \cos \frac{\theta}{4} e_3$$

که از $e_3 e_2 = -e_2 e_3$ استفاده شده است.

۳.۴ عملگر جستجوی گراور در جبر هندسی

در بخش قبل توانستیم بردارهای پایه را برحسب بردارهای بالابرنده و پایین آورنده به دست آوریم و با استفاده از این بردارهای جدید عملگر گراور را محاسبه کنیم و دیدیم که شکل ماتریسی عملگر گراور همان ماتریس دوران است. حال می‌خواهیم عملگر گراور را در فضای جبر هندسی به دست آوریم.

همان‌طور که می‌دانیم عملگر گراور اثر دو اوراکل^۲ اوراکل است. ابتدا اثر این دو اوراکل را در جبر هندسی توضیح می‌دهیم و سپس عملگر گراور را با استفاده از این دو اوراکل در فضای جبر هندسی تشکیل می‌دهیم.

اثر اوراکل اول G_m روی $|m\rangle$ نتیجه‌ای به صورت زیر دارد:

$$(I - 2|m\rangle\langle m|)|m\rangle = -|m\rangle$$

که در واقع انعکاس m حول محور $|m^\perp\rangle$ است. همان‌طور که در فصل دوم توضیح دادیم، انعکاس را در جبر هندسی می‌توان به صورت زیر نمایش داد:

$$m^\perp \sigma m^\perp = m \sigma m \quad (34.4)$$

که بردار m و σ در معادلات (۳۳.۴) تعریف شده‌اند. اثر اوراکل اول روی بردار اولیه σ به صورت:

$$m \sigma m = e^{-ie_2\theta/2} e_3 e_3 e^{-ie_2\theta/2} e^{-ie_2\theta/2} e_3 = e^{-ie_2 3\theta/2} e_3 = \cos \frac{3\theta}{4} e_3 + \sin \frac{3\theta}{4} e_1 \quad (35.4)$$

است که در شکل ۱.۴ نشان داده شده است. حال می‌توان بردارهای m ، σ و m^\perp را مطابق شکل زیر در یک فضای کارتزین حقیقی رسم کرد. اثر اوراکل دوم در عملگر گراور به صورت:

$$G_\sigma = I - 2|\sigma\rangle\langle\sigma|$$

است که انعکاس جدیدی حول بردار σ ایجاد می‌کند:

$$\sigma(m\sigma m)\sigma = e^{ie_1\theta/2} e_3 e^{-ie_2 3\theta/2} e_3 e^{ie_1\theta/2} e_3 = -e_3 e^{ie_1\theta/2} \quad (36.4)$$

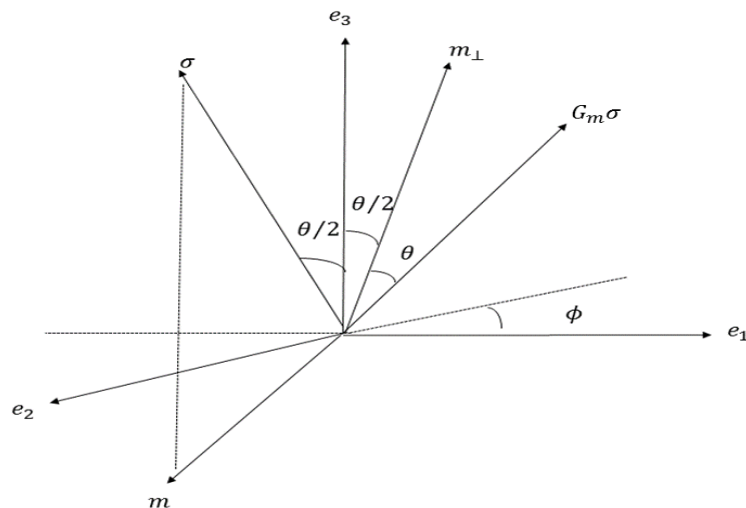
می‌توان دریافت در جبر کلیفورد اعمال عملگر گراور بر روی حالت اولیه به صورت زیر است:

$$\sigma(m\sigma m)\sigma = (\sigma m)\sigma(m\sigma) = G\sigma G^\dagger$$

عملگر گراور حاصل از این دو انعکاس به صورت زیر است:

$$G = -\sigma m = e^{ie_2\theta/2} e_3 e_3 e^{ie_2\theta/2} = e^{ie_2\theta} \quad (37.4)$$

^۲Oracel



شکل ۱.۴: جستجوی گراور در یک فضای سه بعدی با استفاده از حالت‌های بالا برنده و پایین آورنده

با مقایسه‌ی معادله (۳۷.۴) و (۳۳.۳) درمی‌یابیم که نتیجه‌ی فوق از عملگر گراور استاندارد، مهم و پرمعنی است. همان‌طور که در معادله‌ی (۳۷.۴) می‌بینیم، عملگر گراور در واقع دوران به اندازه‌ی 2θ حول محور e_2 است. مطابق با شکل ۱.۴، پرواضح است بعد از k بار اعمال عملگر گراور، دوران بردار σ روی بردار m اتفاق می‌افتد (که بردار σ و m در معادله‌ی (۳۳.۴) تعریف شده‌اند).

اکنون به دنبال یافتن تعداد عملکرد عملگر گراور برای یافتن جواب خاص هستیم. در جبر کلیفورده، k بار اثر عملگر گراور روی بردار اولیه σ را به صورت زیر نمایش می‌دهیم:

$$G^k \sigma G^k = e^{ike_2\theta} e^{ike_2\theta/2} e_3 e^{-ike_2\theta} = e^{ie_2(2k\theta + \theta/2)} e_3 = m \quad (38.4)$$

با توجه به m به دست آمده در (۳۳.۴) تساوی زیر برقرار است:

$$e^{ie_2(2k\theta + \theta/2)} e_3 = e^{ie_2(\pi - \theta/2)} e_3 \quad (39.4)$$

با مساوی قرار دادن طرفین معادله‌ی فوق:

$$2k\theta + \frac{\theta}{2} = \pi - \frac{\theta}{2} \quad (40.4)$$

داریم:

$$k = \frac{\pi}{2\theta} - \frac{1}{2} \quad (41.4)$$

از طرفی در فصل سوم، با توجه به تعریف معادله‌ی (۵۳.۳) برای پایگاه داده‌ای با N

عضو و M جواب، $\theta = \arcsin \sqrt{\frac{M}{N}}$ است، در نتیجه خواهیم داشت:

$$k = \frac{\pi}{4 \arcsin \sqrt{\frac{M}{N}}} - \frac{1}{2} \approx \frac{\pi}{4} \sqrt{\frac{N}{M}} \quad (42.4)$$

که نتیجه شناخته شده‌ای برای جستجوی گراور استاندارد است اگرچه این نتیجه تضمین نمی‌کند که k عدد صحیحی باشد. بنابراین نیازمندیم تا تعداد تکرار الگوریتم جستجوی گراور را رندسازی کنیم. از طرفی ما می‌توانیم جستجو را کمی بهتر انجام دهیم، به عبارت بهتر برای تضمین اینکه k عدد صحیحی است و بنابراین با اطمینان کامل به حالت جواب $|m\rangle$ خواهیم رسید.

۴.۴ جستجوی گراور کامل و دقیق

در این بخش سعی داریم تا نمایش کلی‌تری از جستجوی گراور را فرمولبندی کنیم. برای این کار عملگر گراور تعریف شده در معادله (۳۳.۳) را می‌توان به این صورت اصلاح کرد که بردار اولیه $|\sigma\rangle$ روی بردار $|m\rangle$ واقع شود. ابتدا حالت کلی از عملگر گراور را می‌سازیم، برای این کار ابتدا عملگرهای G_σ و G_m را به صورت زیر تعریف می‌کنیم [۱۲]، [۱۱]:

$$G_\sigma = I - (\mathbb{1} - e^{i\phi_1})|\sigma\rangle\langle\sigma| \quad (43.4)$$

$$G_m = I - (\mathbb{1} - e^{i\phi_2})|m\rangle\langle m| \quad (44.4)$$

$$\Rightarrow G = -(I - (\mathbb{1} - e^{i\phi_1})|\sigma\rangle\langle\sigma|)(I - (\mathbb{1} - e^{i\phi_2})|m\rangle\langle m|) \quad (45.4)$$

که برای $\phi_1 = \phi_2 = \pi$ می‌بینیم که به همان نتیجه‌ی عملگر گراور در معادله‌ی (۳۳.۳) می‌رسیم.

دوران به اندازه‌ی ϕ_2 حول محور m را به صورت زیر نمایش دهیم:

$$G_m = e^{i\frac{\phi_2}{2}(\sin(\frac{\theta}{2})e_1 + \cos(\frac{\theta}{2})e_3)} \quad (46.4)$$

واضح است اگر قرار دهیم $\phi_2 = \pi$ خواهیم داشت:

$$G_m = e^{i\frac{\pi}{2}(\sin(\frac{\theta}{2})e_1 + \cos(\frac{\theta}{2})e_3)} \quad (47.4)$$

$$= \cos \frac{\pi}{4} + i \sin \frac{\pi}{4} (\sin(\frac{\theta}{2})e_1 + \cos(\frac{\theta}{2})e_3) \quad (48.4)$$

$$= \iota m \quad (49.4)$$

بنابراین اثر اوراکل G_m بر حالت اولیه σ به صورت زیر خواهد بود:

$$G_m \sigma G_m^\dagger = \iota m \sigma (-\iota m) = m \sigma m \quad (50.4)$$

همانطور که می بینیم نتیجه‌ای مشابه اوراکل در معادله (۳۴.۴) است.

به طور مشابه دوران به اندازه ϕ_1 حول محور σ به صورت زیر است:

$$G_\sigma = e^{-\iota \frac{\phi_1}{2} (-\sin(\theta/2)e_1 + \cos(\theta/2)e_3)} \quad (51.4)$$

بنابراین برای جستجوی گراور دقیق و کامل، عملگر گراور به صورت زیر حاصل می‌شود:

$$G = -G_\sigma G_m \quad (52.4)$$

$$= e^{-\iota \frac{\phi_1}{2} (-\sin(\theta/2)e_1 + \cos(\theta/2)e_3)} e^{\iota \frac{\phi_2}{2} (\sin(\theta/2)e_1 + \cos(\theta/2)e_3)}$$

$$= -e^{\iota \beta \hat{v}} \quad (53.4)$$

که با حل معادله‌ی فوق داریم:

$$G = -\left[\cos \frac{\phi_1}{2} \cos \frac{\phi_2}{2} + \cos \theta \sin \frac{\phi_1}{2} \sin \frac{\phi_2}{2} + \sin \frac{\phi_1 + \phi_2}{2} \sin \frac{\theta}{2} \iota e_1 \right] \quad (54.4)$$

$$+ \left[\sin \frac{\phi_1}{2} \sin \frac{\phi_2}{2} \sin \theta \iota e_2 - \cos \frac{\theta}{2} \sin \frac{\phi_1 - \phi_2}{2} \iota e_3 \right]$$

که فرم کلی عملگر گراور است و تفسیری از دوران حول محور کلی است.

۱.۴.۴ شرایط فازی

همان‌طور که در شکل ۱.۴ دیدیم، با استفاده از بردارهای پایه متعامد و بهنجار $|\uparrow\rangle$ و $|\downarrow\rangle$ ، σ و m در صفحه‌ی e_1 و e_3 واقع‌اند. بنابراین با استفاده از استدلال هندسی، برای اینکه بردار σ بتواند روی بردار m واقع شود باید عملگر گراور در صفحه‌ی e_1 و e_2 قرار بگیرد. در نتیجه در رابطه‌ی (۵۴.۴) باید مؤلفه‌ی e_3 را حذف کرد، برای این‌کار در معادله‌ی (۵۲.۴) باید شرایط فازی $\phi_1 = \phi_2$ را برقرار کنیم [۱۴]، [۱۲]. بنابراین یک جستجوی کامل و دقیق به فرم زیر خواهد بود:

$$G = -e^{\iota \beta (\sin \alpha e_1 + \cos \alpha e_2)} \quad (55.4)$$

با مساوی قرار دادن رابطه‌ی فوق و (۵۴.۴) همراه با اعمال شرایط فازی خواهیم داشت:

$$\sin \frac{\beta}{2} = \sin \frac{\theta}{2} \sin \frac{\phi}{2}$$

$$\cot \alpha = \cos \frac{\theta}{2} \tan \frac{\phi}{2} \quad (56.4)$$

به طور واضح می بینیم که اگر $\phi_1 = \phi_2 = \pi$ در معادله‌ی (۵۴.۴)، دقیقاً به عملکرد جستجوی گراور استاندارد می‌رسیم.

حال باید به دنبال محاسبه ϕ برای جستجوی کامل و دقیق مطرح شده در بخش ۴.۴ باشیم. با استفاده از رابطه‌ی (۳۳.۴) و رابطه‌ی (۵۵.۴) و قرار دادن آن در رابطه‌ی (۳۸.۴) داریم:

$$e^{\iota k\beta(\sin \alpha e_1 + \cos \alpha e_2)} e^{\iota e_2 \frac{\theta}{\varphi}} e_{\varphi} e^{-\iota k\beta(\sin \alpha e_1 + \cos \alpha e_2)} = -e^{-\iota e_2 \frac{\theta}{\varphi}} e_{\varphi}$$

با بازنویسی دوباره‌ی آن داریم:

$$e^{\iota k\beta(\sin \alpha e_1 + \cos \alpha e_2)} e^{\iota e_2 \frac{\theta}{\varphi}} e^{\iota k\beta(\sin \alpha e_1 + \cos \alpha e_2)} e^{\iota e_2 \frac{\theta}{\varphi}} = -1$$

$$(e^{\iota k\beta(\sin \alpha e_1 + \cos \alpha e_2)} e^{\iota e_2 \frac{\theta}{\varphi}})^2 = -1 \quad (57.4)$$

حال بخاطر اینکه دو مرحله عمل متوالی را می‌توان با یک عملکرد جابجا کرد می‌توان نوشت:

$$(e^{\iota k\beta(\sin \alpha e_1 + \cos \alpha e_2)} e^{\iota e_2 \frac{\theta}{\varphi}}) = e^{\iota \kappa \hat{v}} = \cos \kappa + \iota \hat{v} \sin \kappa \quad (58.4)$$

که بردار \hat{v} یکانی است.

برای حل معادله‌ی (۵۷.۴) نیاز به حل معادله‌ی زیر داریم:

$$(e^{\iota \kappa \hat{v}})^2 = \cos 2\kappa + \iota \hat{v} \sin 2\kappa = -1 \quad (59.4)$$

واضح است که $\kappa = \frac{\pi}{2}$.

توجه کنیم از آنجایی که طرف راست معادله‌ی (۵۸.۴) برابر با $\iota \hat{v}$ است، باید قسمت اسکالر صفر شود. در نتیجه معادله‌ی (۵۸.۴) را به صورت زیر بازنویسی می‌کنیم:

$$\left\langle \left(\cos k\beta + \iota \sin k\beta(\sin \alpha e_1 + \cos \alpha e_2) \right) \left(\cos \frac{\theta}{\varphi} + \iota \sin \frac{\theta}{\varphi} e_2 \right) \right\rangle.$$

$$\cos k\beta \cos \frac{\theta}{\varphi} - \sin k\beta \sin \frac{\theta}{\varphi} \cos \alpha = 0$$

$$\begin{aligned} \cot k\beta &= \tan \frac{\theta}{\varphi} \cos \alpha \\ &= \frac{\sin \frac{\theta}{\varphi}}{\sqrt{\cos \frac{\theta}{\varphi} + \cot^2 \frac{\theta}{\varphi}}} \end{aligned} \quad (60.4)$$

به راحتی می توان از معادله ی (۶۰.۴) و (۵۶.۴) تعداد تکرار الگوریتم گراور را به دست آورد:

$$\Rightarrow \cot k\beta = \frac{\sin \frac{\theta}{2}}{\sqrt{\left(\cos^2 \frac{\theta}{2} + \cot^2 \frac{\phi}{2}\right)}} \quad (۶۱.۴)$$

$$\Rightarrow k\beta = \operatorname{arccot} \frac{\sin \frac{\theta}{2}}{\sqrt{\left(\cos^2 \frac{\theta}{2} + \cot^2 \frac{\phi}{2}\right)}}$$

$$\Rightarrow k = \frac{\operatorname{arccot} \frac{\sin \frac{\theta}{2}}{\sqrt{\left(\cos^2 \frac{\theta}{2} + \cot^2 \frac{\phi}{2}\right)}}}{\beta}$$

$$\Rightarrow k = \frac{\operatorname{arccot} \frac{\sin \frac{\theta}{2}}{\sqrt{\left(\cos^2 \frac{\theta}{2} + \cot^2 \frac{\phi}{2}\right)}}}{2 \arcsin\left(\sin \frac{\theta}{2} \sin \frac{\phi}{2}\right)} \quad (۶۲.۴)$$

با توجه به محاسبات فوق درمی یابیم اگر $\phi = \pi$ باشد آنگاه کمینه تعداد تکرار الگوریتم گراور به صورت زیر است:

$$k_m = \frac{\operatorname{arccot} \tan \frac{\theta}{2}}{\theta} = \frac{\frac{\pi}{2} - \frac{\theta}{2}}{\theta} = \frac{\pi}{2\theta} - \frac{1}{2} \quad (۶۳.۴)$$

$$\Rightarrow k_m = \frac{\pi}{2\theta} - \frac{1}{2} \quad (۶۴.۴)$$

که از روابط مثلثاتی زیر استفاده کرده ایم:

$$\sin\left(\frac{\theta}{2} - \frac{\pi}{2}\right) = -\cos \frac{\theta}{2}$$

$$\cos\left(\frac{\theta}{2} - \frac{\pi}{2}\right) = \sin \frac{\theta}{2}$$

همان طور که می بینیم معادله ی (۶۴.۴) دقیقاً همان تعداد تکرار الگوریتم معادله ی (۴۱.۴) را به ما می دهد. اما می بینیم که سرعت الگوریتم گراور به همان اندازه است و دقیق کردن الگوریتم برای ما سرعت بالاتری را به ارمغان نمی آورد. حال می خواهیم به دنبال قسمت اصلی موضوع که همان تعداد تکرار الگوریتم است برگردیم. همانطور که در معادله ی (۶۴.۴) دیدیم ما با یک عدد اعشاری مواجه شده ایم در صورتی که تعداد تکرار الگوریتم نمی تواند اعشاری باشد برای این کار از رندسازی استفاده می کنیم:

$$k_m = \left\lceil \frac{\pi}{2\theta} - \frac{1}{2} \right\rceil \quad (۶۵.۴)$$

حال به معادله ی (۶۲.۴) برمی گردیم و ϕ را محاسبه می کنیم:

$$2k_m \arcsin \left(\sin \frac{\theta}{2} \sin \frac{\phi}{2} \right) = \operatorname{arccot} \left(\frac{\sin \frac{\theta}{2}}{\sqrt{\cos^2 \frac{\theta}{2} + \cot^2 \frac{\phi}{2}}} \right)$$

به سادگی می توان دریافت:

$$\sin \frac{\phi}{2} = \sin \frac{\pi}{2k_m + 2} \sec \frac{\theta}{2} \quad (۶۶.۴)$$

که θ و k_m به ترتیب در معادله ی (۵۳.۳) و (۶۴.۴) مشخص شده اند. و جستجوی دقیق با استفاده از عملگر گراور در معادله ی (۵۵.۴) انجام می شود.

۵.۴ جستجوی گراور دقیق تعمیم یافته

برای یک حالت کلی تر می توانیم عملگر گراور را به صورت کلی تر زیر در نظر بگیریم
[۱۵]، [۱۷]، [۱۶]:

$$G = -UI_\gamma U^{-1} G_m = -G'_\sigma G_m \quad (۶۷.۴)$$

که:

$$G'_\sigma = UI_\gamma U^{-1}$$

و

$$I_\gamma = I + (e^{i\phi_\gamma} - 1)|\gamma\rangle\langle\gamma|$$

و با انتخاب بردار دلخواه $|\gamma\rangle = |0\rangle = |000\dots 0\rangle$ و $U = H$ داریم:

$$G'_\sigma = UI_\gamma U^{-1} = I + (e^{i\phi_\sigma} - 1)H|\gamma\rangle\langle\gamma|H = I + (e^{i\phi_\sigma} - 1)|\sigma\rangle\langle\sigma| = G_\sigma$$

همانطور که می دانیم الگوریتم گراور به حالت اولیه حساسیت ندارد، بنابراین می توانیم بردار حالت اولیه $|\sigma\rangle$ را به صورت زیر تغییر دهیم:

$$|\gamma'\rangle = -e^{-i\phi/2} \cos \frac{\theta_0}{4} |\uparrow\rangle + e^{i\phi/2} \sin \frac{\theta_0}{4} |\downarrow\rangle \quad (۶۸.۴)$$

با توجه به معادله‌ی (۳۲.۴) بردار متناظر با بردار حالت اولیه $|\gamma'\rangle$ در جبر کلیفورد به صورت زیر است:

$$\gamma' = -\sin \frac{\theta_0}{\gamma} \cos \phi_0 e_1 - \sin \frac{\theta_0}{\gamma} \sin \phi_0 e_2 + \cos \frac{\theta_0}{\gamma} e_3 \quad (۶۹.۴)$$

با مقایسه‌ی معادله‌ی (۶۹.۴) و بردار قطبش در معادله‌ی (۳۳.۴) می‌بینیم که θ به θ_0 تغییر کرده است و چرخش در صفحه‌ی $e_{1,2}$ به اندازه‌ی ϕ_0 است. اگر $\phi_0 = 0$ قرار دهیم، ما توانسته‌ایم جستجوی گراور دقیق استاندارد (با توجه به بردار σ در معادله‌ی (۳۳.۴)) را پوشش دهیم. بردار قطبش حالت اولیه در معادله‌ی (۶۹.۴) یک بردار واحد است. حال دوران حول این بردار جدید را می‌یابیم:

$$G_\gamma = e^{-i\gamma \frac{\phi_1}{\gamma}} = e^{-i\frac{\phi_1}{\gamma}} (-\sin \frac{\theta_0}{\gamma} \cos \phi_0 e_1 - \sin \frac{\theta_0}{\gamma} \sin \phi_0 e_2 + \cos \frac{\theta_0}{\gamma} e_3) \quad (۷۰.۴)$$

و بنابراین جستجوی گراور تعمیم یافته توسط

$$G = -G_\gamma G_m \quad (۷۱.۴)$$

داده می‌شود:

$$\Rightarrow G = e^{-i\gamma \frac{\phi_1}{\gamma}} e^{im \frac{\phi_2}{\gamma}} = e^{-i\frac{\phi_1}{\gamma}} (-\sin \frac{\theta_0}{\gamma} \cos \phi_0 e_1 - \sin \frac{\theta_0}{\gamma} \sin \phi_0 e_2 + \cos \frac{\theta_0}{\gamma} e_3) e^{i\frac{\phi_2}{\gamma}} (\sin(\frac{\theta}{\gamma}) e_1 + \cos(\frac{\theta}{\gamma}) e_3) \quad (۷۲.۴)$$

این معادله به‌طور واضح نسبتاً سنگین و طاقت فرسا است. به‌عنوان گزینه‌ی زیباتر و مناسب‌تر می‌توانیم حالت‌های پایه در معادله‌ی (۲۴.۴) و (۲۵.۴) را تنظیم کنیم و حل دقیق داده شده در معادله‌ی (۵۵.۴) ضرورتاً اعمال خواهد شد.

فصل ۵

عملگر پیشنهادی جدید برای الگوریتم
جستجوی کوانتومی گراور

۱.۵ مقدمه

عملگر هادامارد در الگوریتم جستجوی کوانتومی گراور، برهم‌نهمی از تمامی حالات ورودی با دامنه‌های یکسان می‌سازد. برای یافتن حالت مورد نظر با احتمال بسیار بالا، دو عملگر در این الگوریتم نقش بسیار مهمی دارند: عملگر اول عمل انعکاس دامنه‌ی تمامی حالات مورد جستجو را برعهده دارد و عملگر دوم انعکاس حول متوسط دامنه‌ها است. همان‌طور که در فصل ۳ دیدیم، بعد از $O(\sqrt{N})$ تکرار الگوریتم جستجوی کوانتومی گراور، با احتمال بسیار بالایی به حالت مورد نظر دسترسی پیدا می‌کنیم.

در قسمت اول این فصل، عملگر جدیدی مانند T را می‌یابیم که همانند عملگر هادامارد برهم‌نهمی از تمامی حالات ورودی با دامنه‌های یکسان ایجاد می‌کند با این تفاوت که این عملگر جدید دارای مفهوم فیزیکی جالبی است و آن این است که عملگر پیشنهادی T شبیه به ماتریس پائولی σ_y است. خواهیم دید تعداد تکرار الگوریتم گراور برای یافتن حالت مورد نظر با احتمال بسیار بالا با اعمال عملگر T بر روی حالت اولیه $|0\rangle$ ، از مرتبه \sqrt{N} است.

در قسمت دوم قصد داریم با اثر عملگر دیگری مانند T' بر روی حالت اولیه دلخواه $|1\rangle + f|0\rangle$ ، برهم‌نهمی از تمامی حالات پایه بسازیم. هدف یافتن عملگر جدید T' و حالت اولیه سیستم است و بررسی می‌کنیم تعداد تکرار الگوریتم گراور برای یافتن حالت مورد نظر با احتمال بسیار بالا از چه مرتبه‌ای است.

۲.۵ روش محاسبات عملگر پیشنهادی T

یک سیستم 4 کیوبیتی را در نظر می‌گیریم و الگوریتم گراور را با اعمال عملگری دلخواه و یکانی مثل $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ مورد بررسی قرار می‌هیم. می‌خواهیم بررسی کنیم با اعمال چند بار تکرار الگوریتم به بیشینه‌ی دامنه‌ی احتمال حالت مورد نظر می‌رسیم و به ازای این بیشینه مؤلفه‌های ماتریس دلخواه چه اعدادی هستند. عملگر دلخواه T را به صورت زیر در نظر می‌گیریم:

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

شرط یکانی بودن را بر روی عملگر T اعمال می‌کنیم:

$$TT^\dagger = I \implies$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = I \implies \begin{cases} a^2 + b^2 = 1 \\ c^2 + d^2 = 1 \\ ac + bd = 0 \end{cases} \quad (1.5)$$

اعمال عملگر T بر روی حالت ورودی $|0\rangle$ و ساختن برهم‌نهی از تمامی حالات ورودی:

$$T|0\rangle = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = a|0\rangle + c|1\rangle.$$

سیستم ۴ کیوبیتی را در نظر می‌گیریم:

$$\begin{aligned} |\Psi_0\rangle = T^{\otimes 4}|0\rangle^{\otimes 4} &= a^4|0000\rangle + a^3c|0001\rangle + a^3c|0010\rangle + a^3c|0100\rangle \\ &+ a^3c|1000\rangle + a^2c^2|0011\rangle + a^2c^2|0110\rangle + a^2c^2|1001\rangle \\ &+ a^2c^2|1010\rangle + a^2c^2|1100\rangle + ac^3|1011\rangle + ac^3|1101\rangle \\ &+ ac^3|1110\rangle + ac^3|0111\rangle + a^2c^2|0101\rangle + c^4|1111\rangle \end{aligned}$$

همان‌طور که می‌دانیم در الگوریتم جستجوی کوانتومی گراور از دو عملگر انعکاس دامنه‌ی حالت مورد نظر و سپس انعکاس حول متوسط دامنه‌ها استفاده می‌کنیم. تکرار اول

۱. اعمال عملگر انعکاس فاز حالت مورد نظر که در این مورد، حالت مورد نظر $|6\rangle = |0110\rangle$ مورد بررسی قرار می‌گیرد.

$$\begin{aligned} |\Psi_1\rangle &= a^4|0\rangle + a^3c|1\rangle + a^3c|2\rangle + a^3c|3\rangle \\ &+ a^3c|4\rangle + a^2c^2|5\rangle - a^2c^2|6\rangle \\ &+ a^2c^2|7\rangle + a^2c^2|8\rangle + a^2c^2|9\rangle \\ &+ a^2c^2|10\rangle + ac^3|11\rangle + ac^3|12\rangle \\ &+ a^3c|13\rangle + ac^3|14\rangle + c^4|15\rangle. \end{aligned}$$

۲. اعمال عملگر انعکاس حول متوسط دامنه‌ها:

$$|\Psi_2\rangle = (T - 2|\Psi_0\rangle\langle\Psi_0|)|\Psi_1\rangle = \sum_i (a - 2\bar{a})|x_i\rangle,$$

که در این جا نیز همانند عملگر هادامارد، باید متوسط دامنه‌ها به صورت

$$\bar{a} = \frac{\sum_i a_i}{N}, \quad (2.5)$$

$$\bar{a} = \frac{a^4 + 4a^3c + 4a^2c^2 + 4ac^3 + c^4}{16} \Rightarrow 2\bar{a} = \frac{a^4 + 4a^3c + 4ac^3 + c^4 + 4a^2c^2}{8}.$$

$$\begin{aligned} |\Psi_2\rangle &= \frac{1}{8}a^4 - \frac{1}{8}(c^4 + 4a^2c^2 + 4a^3c + 4ac^3)|0\rangle \\ &+ \sum_{i=1}^4 \frac{4}{8}a^3c - \frac{1}{8}(a^4 + 4a^2c^2 + 4ac^3 + c^4)|i\rangle \\ &+ \sum_{i=5, i \neq 6}^{10} \frac{4}{8}a^2c^2 - \frac{1}{8}(a^4 + 4ac^3 + 4a^3c + c^4)|i\rangle \\ &+ \left(\frac{-12}{8}\right)a^2c^2 - \frac{1}{8}(a^4 + 4a^3c + 4ac^3 + c^4)|6\rangle \\ &+ \sum_{i=11}^{14} \frac{4}{8}ac^3 - \frac{1}{8}(a^4 + 4a^3c + 4a^2c^2 + c^4)|i\rangle \\ &+ \frac{1}{8}c^4 - \frac{1}{8}(a^4 + 4a^2c^2 + 4a^3c + 4ac^3)|15\rangle. \end{aligned}$$

با توجه به معادلات (۱.۵) و رابطه (۲.۵) ما کسیم مقدار دامنه حالت $|6\rangle$ را به دست می‌آوریم. به ازای این ما کسیم مقادیر a, c, b و d به صورت زیر خواهند بود:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

عملگر جدید یکانی است:

$$TT^\dagger = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$T^2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (-i)(\sigma_y)$$

$$\Rightarrow T = (-i)^{\frac{1}{4}} (\sigma_y)^{\frac{1}{4}} \quad (۳.۵)$$

$$= e^{\frac{i\pi}{4}} (\sigma_y)^{\frac{1}{4}} \quad (۴.۵)$$

نتیجه‌ی جالب این است که عملگر T شبیه به عملگر پائولی σ_y است. از این به بعد مقادیر a و c به دست آمده را جایگذاری می‌کنیم.

می‌خواهیم بررسی کنیم با چند مرتبه تکرار الگوریتم گراور با اعمال عملگر جدید T به بیشترین احتمال دامنه حالت $|۶\rangle$ خواهیم رسید. در الگوریتم گراور با اعمال عملگر هادامارد روی حالت ۴ کیوبیتی بیشینه مقدار دامنه حالت $|۶\rangle$ به ازای سه مرتبه تکرار الگوریتم است.

$$|\Psi_2\rangle = \frac{-۶}{۳۲}|۰\rangle + \sum_{i=1}^4 \frac{-۶}{۳۲}|i\rangle + \sum_{i=۵, i \neq ۶}^{۱۰} \frac{-۶}{۳۲}|i\rangle + \frac{-۲۲}{۳۲}|۶\rangle + \sum_{i=۱۱}^{۱۴} \frac{-۶}{۳۲}|i\rangle + \frac{-۶}{۳۲}|۱۵\rangle.$$

$$A_0 = -۰/۱۸۷۵ \Rightarrow P_0 = ۰/۰۳۵$$

$$A_{i=1}^4 = -۰/۱۸۷۵ \Rightarrow P_{i=1}^5 = ۰/۰۳۵$$

$$A_{i=۶} = -۰/۶۸۷۵ \Rightarrow P_{i=۶} = ۰/۴۷$$

$$A_{i=۱۱}^{۱۴} = -۰/۱۸۷۵ \Rightarrow P_{i=۱۱}^{۱۴} = ۰/۰۳۵$$

$$A_{۱۵} = -۰/۱۸۷۵ \Rightarrow P_{i=۱۵} = ۰/۳۵$$

$$\sum P_i = ۱$$

تکرار دوم:

۱. اعمال عملگر انعکاس فاز حالت مورد نظر $|۶\rangle$:

$$|\Psi_3\rangle = \sum_{i=۰, i \neq ۶}^{۱۵} \frac{-۶}{۳۲}|i\rangle + \frac{۲۲}{۳۲}|۶\rangle$$

$$\bar{a} = \frac{-۶ \times ۱۵ + ۲۲}{۳۲ \times ۱۶} \Rightarrow ۲\bar{a} = \frac{-۶۸}{۱۶ \times ۱۶}$$

۲. اعمال عملگر انعکاس حول متوسط دامنه‌ها:

$$|\Psi_4\rangle = \sum_{i=۰, i \neq ۶}^{۱۵} \frac{-۶}{۳۲} + \frac{۶۸}{۱۶ \times ۱۶}|i\rangle + \frac{۲۲}{۳۲} + \frac{۶۸}{۱۶ \times ۱۶}|۶\rangle$$

$$A_{i=۰, i \neq ۶}^{۱۵} = ۰/۰۷۸ \Rightarrow P_{i=۰, i \neq ۶}^{۱۵} = ۰/۰۰۶$$

$$A_{i=6} = 0.95 \Rightarrow P_{i=6} = 0.90$$

تکرار سوم:

۱. اعمال عملگر انعکاس فاز حالت موردنظر $|6\rangle$:

$$|\Psi_5\rangle = \sum_{i=0, i \neq 6}^{15} \frac{640}{256} |i\rangle - \frac{244}{256} |6\rangle$$

۲. اعمال عملگر انعکاس حول متوسط دامنه‌ها

$$\bar{a} = \frac{56}{40.96} \Rightarrow 2\bar{a} = \frac{56}{20.48}$$

$$|\Psi_6\rangle = \sum_{i=0, i \neq 6}^{15} \frac{104}{20.48} |i\rangle + \frac{2008}{20.48} |6\rangle$$

$$A_{i=0, i \neq 6}^{15} = 0.05 \Rightarrow P_{i=0, i \neq 6}^{15} = 0.002$$

$$A_{i=6} = 0.98 \Rightarrow P_{i=6} = 0.96$$

همان‌طور که دیدیم با اعمال سه مرتبه از عملگر جدید همانند اعمال عملگر هادامارد با احتمال بسیار بالایی به جواب موردنظر دسترسی پیدا کردیم.

۳.۵ روش محاسبات T'

در قسمت قبلی عملگر T را به گونه‌ای یافتیم که علاوه بر ایجاد برهم‌نهی از تمامی حالات پایه و با دامنه‌های یکسان، شبیه به ماتریس پائولی σ_y بود. هم‌چنین دیدیم که برای یک سیستم ۴ کیوبیتی بعد از ۳ مرتبه الگوریتم جستجوی کوانتومی گراور با احتمال بسیار بالایی به جواب رسیدیم. در این قسمت قصد داریم عملگر دیگری را مورد بررسی قرار دهیم. عملگر جدیدی مانند T' را بر روی حالت اولیه دلخواهی مثل $|e|0\rangle + f|1\rangle$ اثر می‌دهیم و برهم‌نهی از تمامی حالات پایه می‌سازیم. الگوریتم گراور را همانند قبل تکرار می‌کنیم. هدف یافتن عملگر جدید T' و حالت دلخواه اولیه است. سپس بررسی می‌کنیم با چند مرتبه تکرار الگوریتم جستجوی گراور بر روی یک سیستم ۴ کیوبیتی به حالت مورد نظر با احتمال بسیار بالایی دسترسی پیدا خواهیم کرد.

$$T' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} (|e|0\rangle + f|1\rangle) \quad (5.5)$$

با این شرط که:

$$|e|^2 + |f|^2 = 1 \quad (6.5)$$

که مولفه‌های عملگر دلخواه را موهومی در نظر می‌گیریم:

$$a = a_x + ia_y \quad (۷.۵)$$

$$b = b_x + ib_y \quad (۸.۵)$$

$$c = c_x + ic_y \quad (۹.۵)$$

$$d = d_x + id_y \quad (۱۰.۵)$$

$$(۱۱.۵)$$

شرط یکانی بودن عملگر جدید ایجاب می‌کند که شرط‌های زیر برقرار باشند:

$$a_x^2 + a_y^2 + b_x^2 + b_y^2 = 1 \quad (۱۲.۵)$$

$$c_x^2 + c_y^2 + d_x^2 + d_y^2 = 1 \quad (۱۳.۵)$$

$$a_x c_x + a_y c_y + d_x b_x + d_y b_y = 0 \quad (۱۴.۵)$$

$$a_y c_x - a_x c_y + d_y b_x - b_y d_x = 0 \quad (۱۵.۵)$$

$$a_y c_x - a_x c_y + d_y b_x - b_y d_x = 0 \quad (۱۶.۵)$$

$$c_y a_x + b_y d_x - c_x a_y - d_y b_x = 0 \quad (۱۷.۵)$$

$$\begin{aligned} |\Psi_0\rangle &= T^{\otimes 4} |0\rangle^{\otimes 4} \\ &= (af + be) |0000\rangle + (af + be)^2 (cf + de) |0001\rangle \\ &\quad + (af + be)^2 (cf + de) |0010\rangle + (af + be)^2 (cf + de) |0100\rangle \\ &\quad + (af + be)^2 (cf + de) |1000\rangle + (af + be)^2 (cf + de)^2 |0011\rangle \\ &\quad + (af + be)^2 (cf + de)^2 |0110\rangle + (af + be)^2 (cf + de)^2 |1001\rangle \\ &\quad + (af + be)^2 (cf + de)^2 |1010\rangle + (af + be)^2 (cf + de)^2 |1100\rangle \\ &\quad + (af + be)(cf + de)^2 |1011\rangle + (af + be)c^2 |1101\rangle \\ &\quad + (af + be)(cf + de)^2 |1110\rangle + (af + be)(cf + de)^2 |0111\rangle \\ &\quad + (af + be)^2 (cf + de)^2 |0101\rangle + (cf + de)^4 |1111\rangle \end{aligned} \quad (۱۸.۵)$$

به دنبال پیشنهادی کردن حالت مورد نظر زیر هستیم:

$$\begin{aligned}
 & -\frac{1}{\lambda}(af+be)^2(cf+de)^2 - \frac{1}{\lambda}(af+be)^4 + (cf+de)^4 + 4(af+be)^3(cf+de) \\
 & + 4(cf+de)^3(af+be)] \\
 F = & -\frac{1}{\lambda}(af+be)^2(cf+de)^2 - \frac{1}{\lambda}(af+be)^4 + (cf+de)^4 + 4(af+be)^3(cf+de) \\
 & + 4(cf+de)^3(af+be) + \lambda(ax^2 + ay)^2 + bx^2 + by^2 - 1) \\
 & + \gamma(c_x^2 + c_y^2 + d_x^2 + d_y^2 - 1) \\
 & + \xi(a_x c_x + a_y c_y + b_x d_x + b_y d_y) + \chi(a_y c_x - a_x c_y - b_y d_x + b_x d_y) \\
 & + \eta(a_y c_x + a_x c_y + b_x d_x + b_y d_y) \\
 & + \kappa(c_y a_x + b_y d_x - c_x a_y - d_y b_x) \tag{۱۹.۵}
 \end{aligned}$$

با مشتق‌گیری از معادله‌ی (۱۹.۵) بر حسب تمام متغیرها داریم:

$$D[F[a, b, c, d, e, f], a] = 0, \tag{۲۰.۵}$$

$$D[F[a, b, c, d, e, f], b] = 0, \tag{۲۱.۵}$$

$$D[F[a, b, c, d, e, f], c] = 0, \tag{۲۲.۵}$$

$$D[F[a, b, c, d, e, f], d] = 0, \tag{۲۳.۵}$$

$$D[F[a, b, c, d, e, f], e] = 0, \tag{۲۴.۵}$$

$$D[F[a, b, c, d, e, f], f] = 0, \tag{۲۵.۵}$$

$$D[F[a, b, c, d, e, f], \lambda] = 0, \tag{۲۶.۵}$$

$$D[F[a, b, c, d, e, f], \gamma] = 0, \tag{۲۷.۵}$$

$$D[F[a, b, c, d, e, f], \chi] = 0, \tag{۲۸.۵}$$

$$D[F[a, b, c, d, e, f], \kappa] = 0, \tag{۲۹.۵}$$

$$D[F[a, b, c, d, e, f], \eta] = 0, \tag{۳۰.۵}$$

$$D[F[a, b, c, d, e, f], \zeta] = 0; \tag{۳۱.۵}$$

باحل دستگاه معادلات فوق مؤلفه‌های ماتریس جدید و یک حالت دلخواه به دست می‌آید که در دست اقدام است.

پیوست آ

اثبات روابط مندرج در پایان نامه

۱.آ اثبات روابط فصل ۴

$$\begin{aligned}
 P &= \frac{(|\sigma\rangle\langle\sigma| - |m\rangle\langle m|)^\nu}{\beta^\nu} \\
 &= \frac{1}{\beta^\nu} \left[|\sigma\rangle\langle\sigma| + |m\rangle\langle m| - |\sigma\rangle\langle m| \langle\sigma|m\rangle - |m\rangle\langle\sigma| \langle m|\sigma\rangle \right] \\
 &= \frac{1}{\beta^\nu} \left[|\sigma\rangle\langle\sigma| + |m\rangle\langle m| - \alpha|\sigma\rangle\langle m| - \alpha^*|m\rangle\langle\sigma| \right]
 \end{aligned}$$

$$\begin{aligned}
 \Rightarrow P^\nu &= \frac{1}{\beta^\nu} \left[|\sigma\rangle\langle\sigma| + |m\rangle\langle m| + \alpha^\nu |\sigma\rangle\langle m| + \alpha^{*\nu} |m\rangle\langle\sigma| \langle\sigma|m\rangle \right. \\
 &\quad \left. + |\sigma\rangle\langle m| \langle\sigma|m\rangle - \alpha|\sigma\rangle\langle m| \langle\sigma|\sigma\rangle - \alpha^*|m\rangle\langle\sigma| \langle\sigma|m\rangle \right. \\
 &\quad \left. - \alpha^*|m\rangle\langle\sigma| \langle\sigma|\sigma\rangle - \alpha^*\alpha|m\rangle\langle m| \langle\sigma|m\rangle + \alpha\alpha^*|m\rangle\langle m| \langle\sigma|\sigma\rangle \right]
 \end{aligned}$$

$$\begin{aligned}
 \Rightarrow P^\nu &= \frac{1}{\beta^\nu} \left[|\sigma\rangle\langle\sigma| + |m\rangle\langle m| + \alpha^\nu \alpha^* |\sigma\rangle\langle m| + \alpha^{*\nu} \alpha |m\rangle\langle\sigma| + \alpha|\sigma\rangle\langle m| - \alpha\alpha^* |\sigma\rangle\langle\sigma| - \alpha|\sigma\rangle\langle m| \right. \\
 &\quad \left. + \alpha\alpha^* |\sigma\rangle\langle\sigma| - \alpha^*|m\rangle\langle\sigma| - \alpha\alpha^* |m\rangle\langle m| + \alpha\alpha^* \alpha |m\rangle\langle m| \right]
 \end{aligned}$$

$$\Rightarrow P^\nu = \frac{1}{\beta^\nu} \left[(\nu - |\alpha|^\nu) |\sigma\rangle\langle\sigma| + (\nu - |\alpha|^\nu) |m\rangle\langle m| + \alpha^* (-\nu + |\alpha|^\nu) |m\rangle\langle\sigma| + (-\nu + |\alpha|^\nu) |\sigma\rangle\langle m| \right]$$

$$\Rightarrow P^\nu = P$$

همچنین داریم:

$$P|\sigma\rangle = \frac{1}{\beta^\nu} \left[(|\sigma\rangle\langle\sigma| - |m\rangle\langle m|)^\nu \right] |\sigma\rangle = |\sigma\rangle$$

$$P|m\rangle = \frac{1}{\beta^\nu} \left[(|\sigma\rangle\langle\sigma| - |m\rangle\langle m|)^\nu \right] |m\rangle = |m\rangle$$

$$\begin{aligned}
 P|\sigma\rangle\langle\sigma| &= \frac{1}{\beta^\nu} \left[(|\sigma\rangle\langle\sigma| - |m\rangle\langle m|)^\nu \right] |\sigma\rangle\langle\sigma| \\
 &= \frac{1}{\beta^\nu} \left[|\sigma\rangle\langle\sigma| + |m\rangle\langle m| - \alpha|\sigma\rangle\langle m| - \alpha^*|m\rangle\langle\sigma| \right] |\sigma\rangle\langle\sigma| \\
 &= \frac{1}{\beta^\nu} \left[|\sigma\rangle\langle\sigma| + \alpha^*|m\rangle\langle\sigma| - \alpha\alpha^*|\sigma\rangle\langle\sigma| - \alpha^*|m\rangle\langle\sigma| \right] \\
 &= \frac{1 - |\alpha|^\nu}{\beta^\nu} |\sigma\rangle\langle\sigma| = |\sigma\rangle\langle\sigma|
 \end{aligned}$$

$$\begin{aligned}
P|m\rangle\langle m| &= \frac{1}{\beta^2} \left[(|\sigma\rangle\langle\sigma| - |m\rangle\langle m|)^2 \right] |m\rangle\langle m| \\
&= \frac{1}{\beta^2} \left[|\sigma\rangle\langle\sigma| + |m\rangle\langle m| - \alpha|\sigma\rangle\langle m| - \alpha^*|m\rangle\langle\sigma| \right] |m\rangle\langle m| \\
&= \frac{1}{\beta^2} \left[\alpha|\sigma\rangle\langle m| + |m\rangle\langle m| - \alpha|\sigma\rangle\langle m| - \alpha^*\alpha|m\rangle\langle m| \right] \\
&= \frac{1 - |\alpha|^2}{\beta^2} |\sigma\rangle\langle\sigma| = |m\rangle\langle m|
\end{aligned}$$

$$[J_1, J_2] = J_1 J_2 - J_2 J_1$$

$$J_1 J_2 = -i \left(\frac{P - |\sigma\rangle\langle\sigma|}{\sqrt{|\alpha|}} \right) \left(\frac{\alpha^*|m\rangle\langle\sigma| - \alpha|\sigma\rangle\langle m|}{\sqrt{|\alpha|\beta}} \right)$$

$$\begin{aligned}
J_1 J_2 &= -i \left[\frac{(\lambda - \beta^2)|\sigma\rangle\langle\sigma| + (\lambda - \beta^2)|m\rangle\langle m| - \alpha|\sigma\rangle\langle m| - \alpha^*|m\rangle\langle\sigma|}{\sqrt{|\alpha|\beta^2}} \right. \\
&\quad \left. \times \left(\frac{\alpha^*|m\rangle\langle\sigma| - \alpha|\sigma\rangle\langle m|}{\sqrt{|\alpha|\beta}} \right) \right] \\
&= \frac{-i}{\sqrt{|\alpha|\beta^2}} \left[(\lambda - \beta^2)\alpha^*|\sigma\rangle\langle\sigma||\sigma\rangle\langle m| + (\lambda - \beta^2)\alpha^*|m\rangle\langle\sigma| \right. \\
&\quad \left. - \alpha\alpha^*|\sigma\rangle\langle\sigma| - \alpha^2|m\rangle\langle\sigma|\langle\sigma|m| - (\lambda - \beta^2)\alpha|\sigma\rangle\langle m| \right. \\
&\quad \left. - \alpha(\lambda - \beta^2)|m\rangle\langle m|\sigma\rangle\langle m| + \alpha^2|\sigma\rangle\langle m|\sigma\rangle\langle m| + \alpha\alpha^*|m\rangle\langle m| \right] \\
&= \frac{-i}{\sqrt{|\alpha|\beta^2}} \left[|\alpha|^2\alpha\alpha^*|\sigma\rangle\langle\sigma| - |\alpha|^2|\sigma\rangle\langle\sigma| - |\alpha|^2|\alpha|^2|m\rangle\langle m| + |\alpha|^2|m\rangle\langle m| \right] \\
&= \frac{-i}{\sqrt{\beta^2}} \left[\underbrace{(|\alpha|^2 - \lambda)}_{-\beta^2} |\sigma\rangle\langle\sigma| + \underbrace{(\lambda - |\alpha|^2)}_{\beta^2} |m\rangle\langle m| \right] \Rightarrow \\
J_1 J_2 &= \frac{-i}{\sqrt{\beta}} \left[-|\sigma\rangle\langle\sigma| + |m\rangle\langle m| \right] \\
J_2 J_1 &= -i \left(\frac{\alpha^*|m\rangle\langle\sigma| - \alpha|\sigma\rangle\langle m|}{\sqrt{|\alpha|\beta}} \right) \\
&\quad \times \left(\frac{(\lambda - \beta^2)|\sigma\rangle\langle\sigma| + (\lambda - \beta^2)|m\rangle\langle m| - \alpha|\sigma\rangle\langle m| - \alpha^*|m\rangle\langle\sigma|}{\sqrt{|\alpha|\beta^2}} \right) \\
&\quad \times \frac{-i}{\sqrt{|\alpha|\beta^2}} \left[\alpha^*(\lambda - \beta^2)|m\rangle\langle\sigma| - \alpha(\lambda - \beta^2)|\sigma\rangle\langle\sigma|\langle m|\sigma| \right. \\
&\quad \left. + (\lambda - \beta^2)\alpha^*|m\rangle\langle m|\langle\sigma|m| - \alpha(\lambda - \beta^2)|\sigma\rangle\langle m| \right. \\
&\quad \left. - \alpha\alpha^*|m\rangle\langle m| + \alpha^2|\sigma\rangle\langle m|\langle m|\sigma| - \alpha^2|m\rangle\langle\sigma|\langle\sigma|m| - \alpha\alpha^*|\alpha\rangle\langle\sigma| \right]
\end{aligned}$$

$$\begin{aligned}
 &= \frac{-i}{\sqrt[4]{|\alpha|^2\beta^2}} \left[\alpha^* |\alpha|^2 |m\rangle \langle \sigma| - |\alpha|^2 - |\alpha|^2 |\sigma\rangle \langle \sigma| + |\alpha|^2 |\alpha|^2 |m\rangle \langle m| \right. \\
 &\quad \left. |\alpha|^2 |\sigma\rangle \langle m| - |\alpha|^2 |m\rangle \langle m| + |\alpha|^2 \alpha^* \sigma\rangle \langle m| - \alpha^* |\alpha| m\rangle \langle \sigma| - |\alpha|^2 |\sigma\rangle \langle \sigma| \right] \\
 &= \frac{-i}{\sqrt[4]{\beta^2}} \left[(\mathbb{1} - |\alpha|^2) |\sigma\rangle \langle \sigma| + (|\alpha|^2 - \mathbb{1}) |m\rangle \langle m| \right] \\
 \Rightarrow [J_1, J_2] &= J_1 J_2 - J_2 J_1 = \frac{-i}{\sqrt[4]{\beta}} (-|\sigma\rangle \langle \sigma| + |m\rangle \langle m| - |\sigma\rangle \langle \sigma| + |m\rangle \langle m|) \\
 &= \frac{i}{\sqrt[4]{\beta}} (|\sigma\rangle \langle \sigma| - |m\rangle \langle m|) = iJ_3
 \end{aligned}$$

به همین ترتیب داریم:

$$\begin{aligned}
 J_2 J_3 &= \frac{i(|\alpha|^2 |\sigma\rangle \langle \sigma| + |\alpha|^2 |m\rangle \langle m| - \alpha |\sigma\rangle \langle m| - \alpha^* |m\rangle \langle \sigma|)}{\sqrt[4]{|\alpha|(\mathbb{1} - |\alpha|^2)}} \\
 &= \frac{1}{\sqrt[4]{\beta}} iJ_1
 \end{aligned}$$

$$\begin{aligned}
 J_3 J_2 &= \frac{i(-|\alpha|^2 |\sigma\rangle \langle \sigma| - |\alpha|^2 |m\rangle \langle m| + \alpha |\sigma\rangle \langle m| + \alpha^* |m\rangle \langle \sigma|)}{\sqrt[4]{|\alpha|(\mathbb{1} - |\alpha|^2)}} \\
 &= -\frac{1}{\sqrt[4]{\beta}} iJ_1
 \end{aligned}$$

$$\Rightarrow [J_2, J_3] = iJ_1 \quad (1.\tilde{A})$$

$$\begin{aligned}
 J_3 J_1 &= \frac{\alpha^* |m\rangle \langle \sigma| - \alpha |\sigma\rangle \langle m|}{\sqrt[4]{|\alpha|\beta}} \\
 &= \frac{1}{\sqrt[4]{\beta}} iJ_2
 \end{aligned}$$

$$\begin{aligned}
 J_1 J_3 &= \frac{-\alpha^* |m\rangle \langle \sigma| + \alpha |\sigma\rangle \langle m|}{\sqrt[4]{|\alpha|\beta}} \\
 &= -\frac{1}{\sqrt[4]{\beta}} iJ_2
 \end{aligned}$$

$$\Rightarrow [J_1, J_3] = iJ_2 \quad (2.\tilde{A})$$

در حالت کلی:

$$[J_i, J_j] = i\epsilon_{i,j,k} J_k \quad (3.\tilde{A})$$

به راحتی می‌توان دریافت که P با J_1 ، J_2 و J_3 جابه‌جا می‌شود.

$$[P, J_3] = 0$$

$$PJ_3 = \frac{1}{\beta^2} \left[|\sigma\rangle\langle\sigma| + |m\rangle\langle m| - \alpha|\sigma\rangle\langle m| - \alpha^*|m\rangle\langle\sigma| \right] \frac{1}{\sqrt{2}\beta} \left(|\sigma\rangle\langle\sigma| - |m\rangle\langle m| \right)$$

$$= \frac{2}{\beta^3} \left[(1 - |\alpha|^2)|\sigma\rangle\langle\sigma| + (-1 + |\alpha|^2)|m\rangle\langle m| \right]$$

و

$$J_3P = \frac{2}{\beta^3} \left[(1 - |\alpha|^2)|\sigma\rangle\langle\sigma| + (-1 + |\alpha|^2)|m\rangle\langle m| \right]$$

$$\Rightarrow [p, J_3] = 0 \quad (4.آ)$$

و با توجه به عملگرهای بالا برنده و پایین آورنده $J_{\pm} = J_1 \pm iJ_2$ می توان حالت‌هایی با ضریب وزنی بالا و پایین تعریف کرد به‌طوریکه:

$$J_+(d_1|m\rangle + d_2|\sigma\rangle) = 0 \quad (5.آ)$$

$$J_-(d_3|m\rangle + d_4|\sigma\rangle) = 0$$

می‌دانیم که:

برهان.

$$J_1|\sigma\rangle = \frac{-\alpha^*}{\sqrt{2}|\alpha|}|m\rangle$$

$$J_1|m\rangle = \frac{-\alpha}{\sqrt{2}|\alpha|}|\sigma\rangle$$

$$J_2|\sigma\rangle = \frac{-i\alpha^*}{\sqrt{2}|\alpha|\sqrt{1-|\alpha|^2}}|m\rangle + \frac{i|\alpha|}{\sqrt{2}\sqrt{1-|\alpha|^2}}|\sigma\rangle$$

$$J_2|m\rangle = \frac{-i|\alpha|}{\sqrt{2}\sqrt{1-|\alpha|^2}}|\sigma\rangle + \frac{i\alpha}{\sqrt{2}|\alpha|\sqrt{1-|\alpha|^2}}|\sigma\rangle$$

$$J_3|\sigma\rangle = \frac{1}{\sqrt{2}\sqrt{1-|\alpha|^2}}(|\sigma\rangle - \alpha^*|m\rangle)$$

$$J_3|m\rangle = \frac{1}{\sqrt{2}\sqrt{1-|\alpha|^2}}(\alpha|\sigma\rangle - |m\rangle) \quad (6.آ)$$

با استفاده از معادلات (۶.آ) و حل معادلات (۵.آ)، ضرایب را به‌دست می‌آوریم:

$$(J_1 + iJ_2)(d_1|m\rangle + d_2|\sigma\rangle) = 0$$

$$d_1(J_1|m\rangle) + d_2(J_1|\sigma\rangle) + i[d_1(J_2|m\rangle) + d_2(J_2|\sigma\rangle)] = 0$$

$$\begin{aligned}
 & d_{\downarrow} \frac{-\alpha}{\sqrt{|\alpha|}} |\sigma\rangle + d_{\uparrow} \frac{-\alpha^*}{\sqrt{|\alpha|}} |m\rangle + id_{\downarrow} \left(\frac{-i|\alpha|}{\sqrt{\beta}} |m\rangle + \frac{i\alpha}{\sqrt{|\alpha|\beta}} |\sigma\rangle \right) + d_{\uparrow} \left(\frac{-i|\alpha|^*}{\sqrt{|\alpha|\beta}} |m\rangle + \frac{i|\alpha|}{\sqrt{\beta}} |\sigma\rangle \right) \\
 & \Rightarrow \left[d_{\downarrow} \left(\frac{-\alpha}{\sqrt{|\alpha|}} - \frac{\alpha}{\sqrt{|\alpha|\beta}} \right) - d_{\uparrow} \frac{|\alpha|}{\sqrt{\beta}} \right] |\sigma\rangle + \left[d_{\uparrow} \left(\frac{-\alpha^*}{\sqrt{|\alpha|}} + \frac{\alpha^*}{\sqrt{|\alpha|\beta}} \right) + d_{\downarrow} \frac{|\alpha|}{\sqrt{\beta}} \right] |m\rangle = 0 \\
 & \Rightarrow d_{\downarrow} = -\frac{\alpha^*(1-\beta)}{|\alpha|^2} d_{\uparrow} \tag{۷.آ}
 \end{aligned}$$

به همین ترتیب برای $J_-(d_{\uparrow}|m\rangle + d_{\downarrow}|\sigma\rangle) = 0$ داریم:

$$J_{\downarrow} - iJ_{\uparrow}(d_{\uparrow}|m\rangle + d_{\downarrow}|\sigma\rangle) = 0$$

$$d_{\uparrow}(J_{\downarrow}|m\rangle) + d_{\downarrow}(J_{\downarrow}|\sigma\rangle) - i[d_{\uparrow}(J_{\uparrow}|m\rangle) + d_{\downarrow}(J_{\uparrow}|\sigma\rangle)] = 0$$

$$\begin{aligned}
 & d_{\uparrow} \frac{-\alpha}{\sqrt{|\alpha|}} |\sigma\rangle + d_{\downarrow} \frac{-\alpha^*}{\sqrt{|\alpha|}} |m\rangle - id_{\uparrow} \left(\frac{-i|\alpha|}{\sqrt{\beta}} |m\rangle + \frac{i\alpha}{\sqrt{|\alpha|\beta}} |\sigma\rangle \right) - id_{\downarrow} \left(\frac{-i\alpha^*}{\sqrt{|\alpha|\beta}} |m\rangle + \frac{i|\alpha|}{\sqrt{\beta}} |\sigma\rangle \right) \\
 & \Rightarrow \left[d_{\uparrow} \left(\frac{-\alpha}{\sqrt{|\alpha|}} + \frac{\alpha}{\sqrt{|\alpha|\beta}} \right) \right] |\sigma\rangle - \left[d_{\downarrow} \left(\frac{\alpha^*}{\sqrt{|\alpha|}} + \frac{\alpha^*}{\sqrt{|\alpha|\beta}} \right) + d_{\uparrow} \frac{|\alpha|}{\sqrt{\beta}} \right] |m\rangle = 0 \\
 & \Rightarrow d_{\uparrow} = -\frac{\alpha^*(1+\beta)}{|\alpha|^2} d_{\downarrow} \tag{۸.آ}
 \end{aligned}$$

□

$$\begin{aligned}
 |\uparrow\rangle &= \sec \frac{\theta}{\varphi} \left(\cos \frac{\theta}{\varphi} |\sigma\rangle - e^{-i\delta} \sin \frac{\theta}{\varphi} |m\rangle \right) \\
 |\downarrow\rangle &= \sec \frac{\theta}{\varphi} \left(\sin \frac{\theta}{\varphi} |\sigma\rangle - e^{-i\delta} \cos \frac{\theta}{\varphi} |m\rangle \right)
 \end{aligned}$$

برهان.

$$\begin{aligned}
 |\uparrow\rangle &= -\frac{\alpha^*(1-\beta)}{|\alpha|^2} d_{\uparrow} |m\rangle + d_{\downarrow} |\sigma\rangle \\
 \Rightarrow |\uparrow\rangle &= d_{\downarrow} \left[\frac{-e^{-i\delta} |\alpha| (1 - \cos \frac{\theta}{\varphi})}{\sin \frac{\theta}{\varphi}} |m\rangle + |\sigma\rangle \right] \\
 &= d_{\downarrow} \left[\frac{-e^{-i\delta} \sin^2 \frac{\theta}{\varphi}}{\sin \frac{\theta}{\varphi} \cos \frac{\theta}{\varphi}} |m\rangle + |\sigma\rangle \right] \\
 &= \frac{d_{\downarrow}}{\cos \frac{\theta}{\varphi}} \left[\frac{-e^{-i\delta} \sin \frac{\theta}{\varphi}}{\cos \frac{\theta}{\varphi}} |m\rangle + \cos \frac{\theta}{\varphi} |\sigma\rangle \right]
 \end{aligned}$$

اگر $k_1 = \frac{d_2}{\theta \cos \frac{\theta}{4}}$ و حالت $|\uparrow\rangle$ را به یک نرمالیزه کنیم، خواهیم داشت:

$$|k_1\rangle = \sec \frac{\theta}{4}$$

$$\Rightarrow |\uparrow\rangle = \sec \frac{\theta}{4} \left(\cos \frac{\theta}{4} |\sigma\rangle - e^{-i\delta} \sin \frac{\theta}{4} |m\rangle \right) \quad (9.0)$$

□

$$J_3 |\uparrow\rangle = \frac{1}{2} |\uparrow\rangle$$

برهان.

$$\frac{|\sigma\rangle\langle\sigma| - |m\rangle\langle m|}{2\beta} \sec \frac{\theta}{4} \left(\cos \frac{\theta}{4} |\sigma\rangle - e^{-i\delta} \sin \frac{\theta}{4} |m\rangle \right)$$

$$= \frac{1}{2 \sec \frac{\theta}{4}} \left[\cos \frac{\theta}{4} |\sigma\rangle - \cos \frac{\theta}{4} \alpha^* |m\rangle - e^{-i\delta} \sin \frac{\theta}{4} \alpha |\sigma\rangle + e^{-i\delta} \sin \frac{\theta}{4} |m\rangle \right]$$

$$= \frac{1}{2} \frac{\sec \frac{\theta}{4}}{\cos \frac{\theta}{4}} \left[\left(\cos \frac{\theta}{4} - 2 \sin^2 \frac{\theta}{4} \cos \frac{\theta}{4} \right) |\sigma\rangle + e^{-i\delta} \left(-2 \sin \frac{\theta}{4} \cos^2 \frac{\theta}{4} + \sin \frac{\theta}{4} \right) |m\rangle \right]$$

$$= \frac{1}{2} \frac{\sec \frac{\theta}{4}}{\cos \frac{\theta}{4}} \left[\left(\cos \frac{\theta}{4} (1 - 2 \sin^2 \frac{\theta}{4}) \right) |\sigma\rangle + e^{-i\delta} \sin \frac{\theta}{4} (1 - 2 \cos^2 \frac{\theta}{4}) |m\rangle \right]$$

$$= \frac{1}{2} \sec \frac{\theta}{4} \left(\cos \frac{\theta}{4} |\sigma\rangle - e^{-i\delta} \sin \frac{\theta}{4} |m\rangle \right)$$

$$= \frac{1}{2} |\uparrow\rangle \quad (10.0)$$

برای اثبات از روابط مثلثاتی زیر استفاده شده است:

$$\sin \frac{\theta}{4} \cos \frac{\theta}{4} = \frac{1}{2} \sin \frac{\theta}{2} \quad (11.0)$$

$$\cos^2 \frac{\theta}{4} = \frac{1}{2} (1 + \cos \frac{\theta}{2}) \quad (12.0)$$

$$\sin^2 \frac{\theta}{4} = \frac{1}{2} (1 - \cos \frac{\theta}{2}) \quad (13.0)$$

$$\beta = \sqrt{1 - |\alpha|^2} = \sqrt{1 - \sin^2 \frac{\theta}{4}} = \cos \frac{\theta}{4} \quad (14.0)$$

$$\alpha = \sin \frac{\theta}{4} e^{i\delta} \quad (15.0)$$

□

برهان.

$$\begin{aligned} |\uparrow\rangle &= \sec \frac{\theta}{\varphi} \left(\cos \frac{\theta}{\varphi} |\sigma\rangle - e^{-i\delta} \sin \frac{\theta}{\varphi} |m\rangle \right) \\ |\downarrow\rangle &= \sec \frac{\theta}{\varphi} \left(\sin \frac{\theta}{\varphi} |\sigma\rangle - e^{-i\delta} \cos \frac{\theta}{\varphi} |m\rangle \right) \end{aligned}$$

$$\begin{aligned} \Rightarrow |\uparrow\rangle &= \sec \frac{\theta}{\varphi} \left(\cos \frac{\theta}{\varphi} |\sigma\rangle - e^{-i\delta} \sin \frac{\theta}{\varphi} |m\rangle \right) \times \left(-\cos \frac{\theta}{\varphi} \right) \\ |\downarrow\rangle &= \sec \frac{\theta}{\varphi} \left(\sin \frac{\theta}{\varphi} |\sigma\rangle - e^{-i\delta} \cos \frac{\theta}{\varphi} |m\rangle \right) \times \left(\sin \frac{\theta}{\varphi} \right) \end{aligned}$$

$$\begin{aligned} \Rightarrow -\cos \frac{\theta}{\varphi} |\uparrow\rangle + \sin \frac{\theta}{\varphi} |\downarrow\rangle &= \sec \frac{\theta}{\varphi} \left(-\cos^2 \frac{\theta}{\varphi} - \sin^2 \frac{\theta}{\varphi} \right) |\sigma\rangle \\ &= -\sec \frac{\theta}{\varphi} \cos \frac{\theta}{\varphi} |\sigma\rangle \end{aligned}$$

$$\Rightarrow |\sigma\rangle = \cos \frac{\theta}{\varphi} |\uparrow\rangle - \sin \frac{\theta}{\varphi} |\downarrow\rangle$$

به همین ترتیب برای $|m\rangle$ داریم:

$$|m\rangle = e^{i\delta} \left(\sin \frac{\theta}{\varphi} |\uparrow\rangle - \cos \frac{\theta}{\varphi} |\downarrow\rangle \right)$$

و $|m^\perp\rangle$ با توجه به رابطه $|m\rangle$ به صورت:

$$|m^\perp\rangle = e^{i\delta} \left(-\cos \frac{\theta}{\varphi} |\uparrow\rangle + \sin \frac{\theta}{\varphi} |\downarrow\rangle \right)$$

□

و عملگر گراور با استفاده از نتایج فوق به صورت زیر به دست می‌آید:

$$G = -(I - \varphi |\sigma\rangle\langle\sigma|)(I - \varphi |m\rangle\langle m|) \quad (۱۶.آ)$$

برهان.

$$\begin{aligned}
 G &= -I + \gamma|m\rangle\langle m| + \gamma|\sigma\rangle\langle\sigma| - \gamma\alpha|\sigma\rangle\langle m| \\
 &= -I + \gamma\left(\sin\frac{\theta}{\gamma}|\uparrow\rangle - \cos\frac{\theta}{\gamma}|\downarrow\rangle\right)\left(\sin\frac{\theta}{\gamma}\langle\uparrow| - \cos\frac{\theta}{\gamma}\langle\downarrow|\right) \\
 &\quad + \gamma\left(\cos\frac{\theta}{\gamma}|\uparrow\rangle - \sin\frac{\theta}{\gamma}|\downarrow\rangle\right)\left(\cos\frac{\theta}{\gamma}\langle\uparrow| - \sin\frac{\theta}{\gamma}\langle\downarrow|\right) \\
 &\quad - \gamma\alpha e^{-i\delta}\left(\cos\frac{\theta}{\gamma}|\uparrow\rangle - \sin\frac{\theta}{\gamma}|\downarrow\rangle\right)\left(\sin\frac{\theta}{\gamma}\langle\uparrow| - \cos\frac{\theta}{\gamma}\langle\downarrow|\right) \\
 \Rightarrow & -I + \gamma\left(\sin^2\frac{\theta}{\gamma}|\uparrow\rangle\langle\uparrow| - \sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}|\downarrow\rangle\langle\uparrow| - \sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}|\uparrow\rangle\langle\downarrow| + \cos^2\frac{\theta}{\gamma}|\downarrow\rangle\langle\downarrow|\right) \\
 &\quad + \gamma\left(\cos^2\frac{\theta}{\gamma}|\uparrow\rangle\langle\uparrow| - \cos\frac{\theta}{\gamma}\sin\frac{\theta}{\gamma}|\downarrow\rangle\langle\uparrow| - \cos\frac{\theta}{\gamma}\sin\frac{\theta}{\gamma}|\uparrow\rangle\langle\downarrow| + \sin^2\frac{\theta}{\gamma}|\downarrow\rangle\langle\downarrow|\right) \\
 &\quad - \gamma\alpha e^{-i\delta}\left(\cos\frac{\theta}{\gamma}\sin\frac{\theta}{\gamma}|\uparrow\rangle\langle\uparrow| - \sin^2\frac{\theta}{\gamma}|\downarrow\rangle\langle\uparrow| - \cos^2\frac{\theta}{\gamma}|\uparrow\rangle\langle\downarrow| + \sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}|\downarrow\rangle\langle\downarrow|\right) \\
 = & -I + \gamma\left[\cos^2\frac{\theta}{\gamma}|\uparrow\rangle\langle\uparrow| - \sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}|\downarrow\rangle\langle\uparrow| - \sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}|\uparrow\rangle\langle\downarrow| + \sin^2\frac{\theta}{\gamma}|\downarrow\rangle\langle\downarrow|\right] \\
 &\quad + \gamma\left[\sin^2\frac{\theta}{\gamma}|\uparrow\rangle\langle\uparrow| - \sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}|\downarrow\rangle\langle\uparrow| - \sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}|\uparrow\rangle\langle\downarrow| + \cos^2\frac{\theta}{\gamma}|\downarrow\rangle\langle\downarrow|\right] \\
 &\quad - \gamma\sin\frac{\theta}{\gamma}\left[\sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}|\uparrow\rangle\langle\uparrow| - \sin^2\frac{\theta}{\gamma}|\downarrow\rangle\langle\uparrow| - \cos^2\frac{\theta}{\gamma}|\uparrow\rangle\langle\downarrow| + \sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}|\downarrow\rangle\langle\downarrow|\right] \\
 \Rightarrow G &= -I + \gamma\cos^2\frac{\theta}{\gamma}|\uparrow\rangle\langle\uparrow| + \sin\theta|\uparrow\rangle\langle\downarrow| - \sin\theta|\downarrow\rangle\langle\uparrow| + \gamma\cos^2\frac{\theta}{\gamma}|\downarrow\rangle\langle\downarrow| \quad (١٧.٥)
 \end{aligned}$$

□

برهان.

$$\begin{aligned}
 G &= -e^{-i\frac{\phi_1}{\gamma}}(-\sin(\theta/\gamma)e_1 + \cos(\theta/\gamma)e_3)e^{i\frac{\phi_2}{\gamma}}(\sin(\theta/\gamma)e_1 + \cos(\theta/\gamma)e_3) \\
 &= -\left[-\cos\frac{\phi_1}{\gamma}\cos\frac{\phi_2}{\gamma} + \sin\frac{\phi_1}{\gamma}\sin\frac{\theta}{\gamma}\cos\frac{\phi_2}{\gamma}(\iota e_1) - \sin\frac{\phi_1}{\gamma}\cos\frac{\theta}{\gamma}\cos\frac{\phi_2}{\gamma}(\iota e_3) \right. \\
 &\quad + \sin\frac{\phi_1}{\gamma}\sin\frac{\theta}{\gamma}\sin\frac{\phi_2}{\gamma}\sin\frac{\theta}{\gamma}(\iota e_1 \iota e_1) + \cos\frac{\phi_1}{\gamma}\sin\frac{\phi_2}{\gamma}\sin\frac{\theta}{\gamma}(\iota e_1) \quad (١٨.٥) \\
 &\quad - \sin\frac{\phi_1}{\gamma}\cos\frac{\theta}{\gamma}\sin\frac{\phi_2}{\gamma}\sin\frac{\theta}{\gamma}(\iota e_3 \iota e_1) + \cos\frac{\phi_1}{\gamma}\sin\frac{\phi_2}{\gamma}\cos\frac{\theta}{\gamma}(\iota e_3) \\
 &\quad \left. + \sin\frac{\phi_1}{\gamma}\sin\frac{\phi_2}{\gamma}\sin\frac{\theta}{\gamma}\cos\frac{\theta}{\gamma}(\iota e_1 \iota e_3) - \sin\frac{\phi_1}{\gamma}\cos\frac{\theta}{\gamma}\sin\frac{\phi_2}{\gamma}\cos\frac{\theta}{\gamma}(\iota e_3 \iota e_3)\right]
 \end{aligned}$$

با توجه به روابط مثلثاتی زیر:

$$\sin a \cos b = \frac{1}{2} \left[\sin\left(\frac{a+b}{2}\right) + \sin\left(\frac{a-b}{2}\right) \right] \quad (19. \tilde{A})$$

$$\sin a \cos a = \frac{1}{2} \sin(2a) \quad (20. \tilde{A})$$

و ساده سازی معادله‌ی (۱۸.آ) خواهیم داشت:

$$G = - \left[\cos \frac{\phi_1}{2} \cos \frac{\phi_2}{2} + \cos \theta \sin \frac{\phi_1}{2} \sin \frac{\phi_2}{2} + \sin \frac{\phi_1 + \phi_2}{2} \sin \frac{\theta}{2} \iota e_1 \right. \\ \left. + \sin \frac{\phi_1}{2} \sin \frac{\phi_2}{2} \sin \theta \iota e_2 - \cos \frac{\theta}{2} \sin \frac{\phi_1 - \phi_2}{2} \iota e_3 \right] \quad (21. \tilde{A})$$

□

برهان. اثبات روابط (۵۶.۴) با اعمال شرایط فازی $\phi_1 = \phi_2$:

$$- \left[\cos^2 \frac{\phi}{2} + \cos \theta \sin^2 \frac{\phi}{2} + \sin \phi \sin \frac{\theta}{2} (\iota e_1) + \sin^2 \frac{\phi}{2} \sin \theta (\iota e_2) \right] = e^{\iota \beta (\sin \alpha e_1 + \cos \alpha e_2)}$$

$$\Rightarrow - \left[\cos^2 \frac{\phi}{2} + \cos \theta \sin^2 \frac{\phi}{2} + \sin \phi \sin \frac{\theta}{2} (\iota e_1) + \sin^2 \frac{\phi}{2} \sin \theta (\iota e_2) \right]$$

$$= - [\cos \beta + \iota \sin \beta (\sin \alpha e_1 + \cos \alpha e_2)]$$

از مساوی قرار دادن طرفین تساوی داریم:

$$\begin{cases} \cos^2 \frac{\phi}{2} + \cos \theta \sin^2 \frac{\phi}{2} = \cos \beta \\ \sin \phi \sin \frac{\theta}{2} (\iota e_1) = \sin \beta \sin \alpha \iota e_1 \\ \sin^2 \frac{\phi}{2} \sin \theta (\iota e_2) = \sin \beta \cos \alpha \iota e_2 \end{cases} \quad (22. \tilde{A})$$

با تقسیم رابطه‌ی دوم و سوم از معادله‌ی (۲۲.آ) داریم:

$$\cot \alpha = \tan \frac{\phi \sin \frac{\phi}{2} \sin \theta \cos \frac{\phi}{2}}{\sin \phi \sin \frac{\theta}{2}}$$

$$= \tan \frac{\phi \frac{1}{2} \sin \phi \sin \theta}{\sin \phi \sin \frac{\theta}{2}}$$

$$= \tan \frac{\phi}{2} \cos \frac{\theta}{2} \quad (23. \tilde{A})$$

و رابطه‌ی اول از معادله‌ی (۲۲.آ) به صورت زیر ساده می‌شود:

$$\sin^2 \beta = \frac{1}{2}(1 - \cos 2\beta) \Rightarrow \cos 2\beta = 1 - 2 \sin^2 \beta \quad (24.آ)$$

$$\begin{aligned} \frac{1 - (1 - \sin^2 \frac{\phi}{2}) - \cos \theta \sin^2 \frac{\phi}{2}}{2} &= \sin^2 \frac{\beta}{2} \\ \frac{(\sin^2 \frac{\phi}{2})(1 - \cos \theta)}{2} &= \sin^2 \frac{\beta}{2} \\ \Rightarrow \frac{\sin^2 \frac{\phi}{2}}{\sin^2 \frac{\theta}{2}} &= \sin^2 \frac{\beta}{2} \end{aligned} \quad (25.آ)$$

□

برهان. اثبات معادله‌ی (۶۰.۴): روابط مثلثاتی زیر را در نظر می‌گیریم

$$1 + \tan^2 A = \sec^2 \quad (26.آ)$$

$$\sec A = \frac{1}{\cos} \quad (27.آ)$$

$$\sqrt{\cos^2 A} = \frac{1}{\sqrt{1 + \tan^2 A}} \quad (28.آ)$$

حال با استفاده از روابط فوق داریم:

$$\begin{aligned} \cot k\beta &= \tan \frac{\theta}{2} \cos \alpha \\ &= \frac{\sin \frac{\theta}{2}}{\cos \frac{\theta}{2}} \cos \alpha \\ &= \frac{\sin \frac{\theta}{2}}{\sqrt{\cos^2 \frac{\theta}{2} (1 + \tan^2 \alpha)}} \\ &= \frac{\sin \frac{\theta}{2}}{\sqrt{\cos^2 \frac{\theta}{2} (1 + \frac{1}{\cot^2 \alpha})}} \\ &= \frac{\sin \frac{\theta}{2}}{\sqrt{(\cos^2 \frac{\theta}{2} + \cos^2 \frac{\theta}{2} \frac{1}{\cot^2 \alpha})}} \\ &= \frac{\sin \frac{\theta}{2}}{\sqrt{(\cos^2 \frac{\theta}{2} + \frac{1}{\tan^2 \frac{\phi}{2}})}} \\ &= \frac{\sin \frac{\theta}{2}}{\sqrt{(\cos^2 \frac{\theta}{2} + \cot^2 \frac{\phi}{2})}} \end{aligned}$$

□

برهان. اثبات معادله‌ی (۶۶.۴)

$$\begin{aligned}
 2k_m \arcsin \left(\sin \frac{\theta}{\sqrt{2}} \sin \frac{\phi}{\sqrt{2}} \right) + \arctan \left(\frac{\sin \frac{\theta}{\sqrt{2}}}{\sqrt{\cos^2 \frac{\theta}{\sqrt{2}} + \cot^2 \frac{\phi}{\sqrt{2}}}} \right) &= \frac{\pi}{\sqrt{2}} \\
 \arctan x &= \arcsin \frac{x}{\sqrt{1+x^2}} \\
 \Rightarrow \arctan \left(\frac{\sin \frac{\theta}{\sqrt{2}}}{\sqrt{\cos^2 \frac{\theta}{\sqrt{2}} + \cot^2 \frac{\phi}{\sqrt{2}}}} \right) &= \arcsin \left(\sin \frac{\theta}{\sqrt{2}} \sin \frac{\phi}{\sqrt{2}} \right) \\
 \Rightarrow 2k_m \arcsin \left(\sin \frac{\theta}{\sqrt{2}} \sin \frac{\phi}{\sqrt{2}} \right) + \arcsin \left(\sin \frac{\theta}{\sqrt{2}} \sin \frac{\phi}{\sqrt{2}} \right) &= \frac{\pi}{\sqrt{2}} \\
 \Rightarrow \arcsin \left(\sin \frac{\theta}{\sqrt{2}} \sin \frac{\phi}{\sqrt{2}} \right) &= \frac{\pi}{\sqrt{2}(2k_m + 1)} \\
 \sin \frac{\phi}{\sqrt{2}} &= \sin \frac{\pi}{\sqrt{2}k_m + \sqrt{2}} \csc \frac{\theta}{\sqrt{2}} \tag{۲۹.آ}
 \end{aligned}$$

□

اثبات مربوط به معادله‌ی (۶۹.۴) از معادلات (۲۲.۴) و (۲۵.۴) استفاده می‌کنیم.

برهان.

$$\gamma' = \gamma \iota e_3 \gamma^\dagger$$

$$\begin{aligned}
 \gamma' &= (-e^{-\phi \iota e_3 / \sqrt{2}} \cos \frac{\theta_0}{\sqrt{2}} - \iota e_2 e^{\phi \iota e_3 / \sqrt{2}} \sin \frac{\theta_0}{\sqrt{2}}) \iota e_3 \times (-e^{\phi \iota e_3 / \sqrt{2}} \cos \frac{\theta_0}{\sqrt{2}} + \sin \frac{\theta_0}{\sqrt{2}} e^{-\phi \iota e_3 / \sqrt{2}} \iota e_2) \\
 &= (-e^{-\phi \iota e_3 / \sqrt{2}} \cos \frac{\theta_0}{\sqrt{2}} - \iota e_2 e^{\phi \iota e_3 / \sqrt{2}} \sin \frac{\theta_0}{\sqrt{2}}) (-\iota e_3 e^{\phi \iota e_3 / \sqrt{2}} \cos \frac{\theta_0}{\sqrt{2}} + \sin \frac{\theta_0}{\sqrt{2}} e^{-\phi \iota e_3 / \sqrt{2}} \iota e_3 \iota e_2) \\
 &= \iota e_3 (\cos^2 \frac{\theta_0}{\sqrt{2}} - \sin^2 \frac{\theta_0}{\sqrt{2}}) + e^{-\phi \iota e_3 / \sqrt{2}} \cos \frac{\theta_0}{\sqrt{2}} \sin \frac{\theta_0}{\sqrt{2}} e_3 e_2 + e^{-\phi \iota e_3 / \sqrt{2}} \cos \frac{\theta_0}{\sqrt{2}} \sin \frac{\theta_0}{\sqrt{2}} e_3 e_2
 \end{aligned}$$

با توجه به اینکه $e_i e_j = \delta_{i,j} + \iota \varepsilon_{i,j,k} e_k$ خواهیم داشت:

$$\gamma' = -\sin \frac{\theta_0}{\sqrt{2}} \cos \phi_0 e_1 - \sin \frac{\theta_0}{\sqrt{2}} \sin \phi_0 e_2 + \cos \frac{\theta_0}{\sqrt{2}} e_3 \tag{۳۰.آ}$$

□

مثال ۱.۱.۱. مثالی از بخش (۴.۴):

برای جستجوی یک داده‌ی خاص از بین ۱۶ داده، بردار قطبش بعد از k بار اعمال عملگر گراور:

$$\begin{aligned} P &= G^k \sigma G^{\dagger k} \\ &= e^{(ik\beta(\sin \alpha e_1 + \cos \alpha e_2))} e^{ie_2 \frac{\theta}{4}} e_3 e^{-ik\beta(\sin \alpha e_1 + \cos \alpha e_2)} \\ &= -(\sin 2k\beta \cos \alpha \cos \frac{\theta}{4} + \cos^2 k\beta \sin \frac{\theta}{4} - \sin^2 k\beta \sin \frac{\theta}{4} \cos 2\alpha) e_1 \\ &\quad + (\sin k\beta \sin \alpha \cos \frac{\theta}{4} - \sin^2 k\beta \sin 2\alpha \sin \frac{\theta}{4}) e_2 \\ &\quad + (\sin 2k\beta \cos \frac{\theta}{4} + \cos \frac{\theta}{4} \cos 2k\beta) e_3 \end{aligned}$$

با توجه به معادله‌ی (۱.۴.۴) برای ۱۶ داده، $k_m = 3$ ، در معادله‌ی (۵۶.۴) (۵۳.۳)، داریم:

$$\phi = 2,19506$$

$$\alpha = 0,4864$$

$$\beta = 0,4487$$

بعد از k بار اعمال عملگر گراور بردار به صورت زیر حاصل می‌شود:

$$\begin{aligned} G^k \sigma &= -(0,0546434 + 0,195357 \cos 2k\beta + 0,855913 \sin 2k\beta) e_1 \\ &\quad + (-0,10332 + 0,10332 + 0,10332 \cos 2k\beta + 0,452673 \sin 2k\beta) e_2 \\ &\quad + (0,968246 \cos k\beta - 0,220996 \sin 2k\beta) e_3 \end{aligned}$$

بردار اولیه به صورت زیر می‌باشد:

$$\sigma = (-,25, 0, 0,9682)$$

حال به دنبال بردار $m = (-/۲۵, ۰, -/۹۶۸۲)$ هستیم. خواهیم دید که بعد از ۳ بار اعمال عملگر گراور بر روی حالت اولیه به جواب موردنظر دست پیدا خواهیم کرد:

$$k = ۱ \Rightarrow G\sigma = (-/۸۴۵۶, /۳۱۵, /۴۳۰۹) \quad (۳۱.آ)$$

$$k = ۲ \Rightarrow G^2\sigma = (-/۸۴۵۶, /۳۱۵, -/۴۳۰۹)$$

$$k = ۳ \Rightarrow G^3\sigma = (-/۲۵, ۰, -/۹۶۸۲)$$

در مثال زیر پایگاه داده با ۱۶ داده (سیستم ۴ کیوبیتی) را با استفاده از عملگر هادامارد مورد بررسی قرار می‌دهیم:

$$|\psi\rangle = H^{\otimes 4}|0\rangle^{\otimes 4} = \frac{1}{\sqrt{16}} \sum_{i=0}^{15} |i\rangle + |1011\rangle$$

که مجموعه حالات به صورت زیر است:

$$|0000\rangle, |0001\rangle, |0010\rangle, |0011\rangle, |0100\rangle, |0101\rangle, |0110\rangle, |0111\rangle,$$

$$|1000\rangle, |1001\rangle, |1010\rangle, |1011\rangle, |1100\rangle, |1101\rangle, |1110\rangle, |1111\rangle$$

به دنبال جستجوی حالت $|1011\rangle$ هستیم:

$$|\psi\rangle = \frac{1}{\sqrt{16}} \left(\sum_{i=0}^{15} |i\rangle + |1011\rangle \right)$$

$$U_f|\psi\rangle = |\psi_1\rangle = \frac{1}{\sqrt{16}} \left(\sum_{i=0}^{15} |i\rangle - |1011\rangle \right)$$

$$I_S|\psi\rangle = |\psi_2\rangle = \sum_{\substack{i=0 \\ i \neq |1011\rangle}}^{15} (a - 2\bar{a})|i\rangle = \sum_{\substack{i=0 \\ i \neq |1011\rangle}}^{15} \frac{3}{16}|i\rangle + \frac{11}{16}|1011\rangle$$

$$U_f|\psi\rangle_2 = |\psi_3\rangle = \frac{3}{16} \sum_{\substack{i=0 \\ i \neq |1011\rangle}}^{15} |i\rangle - \frac{11}{16}|1011\rangle$$

$$I_S|\psi_3\rangle = |\psi_4\rangle = \sum_{\substack{i=0 \\ i \neq |1011\rangle}}^{15} \frac{5}{64}|i\rangle + \frac{61}{64}|1011\rangle$$

$$U_f|\psi\rangle_4 = |\psi_5\rangle = \frac{5}{64} \sum_{\substack{i=0 \\ i \neq |1011\rangle}}^{15} |i\rangle - \frac{61}{64}|1011\rangle$$

$$I_S|\psi_5\rangle = |\psi_6\rangle = \sum_{i=0}^{15} \frac{-26}{512}|i\rangle + \frac{502}{512}|1011\rangle$$

مراجع

- [1] McMahon, D. *Quantum Computing Explained*. John Wiley & Sons, (2007).
- [2] Nielsen, A., & Chuang, L. *Quantum Information and Quantum Computation*. 1st edn. AddisonWesley, Cambridge, (2002).
- [3] Preskill, J. *Quantum Information and Quantum Computation*, (2009).
- [4] karimipour, V. *QCI, Quantum Search Algorithm Lesson 11*.
- [5] Doran, C. J., & Lasenby, A. N. *Geometric Algebra for Physicists*. Cambridge University Press, (2003).
- [6] Franchini, S., Vassallo, G., & Sorbello, F. *A Brief Introduction to Clifford Algebra*, (1930).
- [7] De Sabbata, V., & Datta, C. *Geometric Algebra and Applications to Physics (Taylor and Francis) Group*, (2007).
- [8] Parker, R., & Doran, C. *Analysis of 1 and 2 Particle Quantum Systems Using Geometric Algebra*. arXiv Preprint Quant-Ph/0106055, (2001).
- [9] Chappell, J. M., Lohe, M. A., Von Smekal, L., Iqbal, A., & Abbot, D. *An Improved Formalism for the Grover Search Algorithm*. arXiv:1201.1707, (2012).
- [10] Grover, L. K. *Quantum Mechanics Helps in Searching for a Needle in a Haystack*. Physical Review Letters, **79**, 325, (1997).

-
- [11] Hsieh, J. Y., & Li, C. M. *General $SU(2)$ Formulation for Quantum Searching with Certainty*. Physical Review A, **65**, 052322, (2002).
- [12] Li, C. M., Hwang, C. C., Hsieh, J. Y., & Wang, K. S. *General Phase-Matching Condition for a Quantum Searching Algorithm*. Physical Review A, **65**, 034305, (2002).
- [13] Long, G. L., Tu, C. C., Li, Y. S., Zhang, W. L., & Yan, H. Y. *An $SO(3)$ Picture for Quantum Searching*. Journal of Physics A: Mathematical and General, **34**, 861, (2001).
- [14] Long, G. L., Li, Y. S., Zhang, W. L., & Niu, L. *Phase Matching in Quantum Searching*. Physics Letters A, **262**, 27-34, (1999).
- [15] Biham, E., Biham, O., Biron, D., Grassl, M., & Lidar, D. A. *Grover's Quantum Search Algorithm for an Arbitrary Initial Amplitude Distribution*. Physical Review A, **60**, 2742, (1999).
- [16] Grover, L. K. *Quantum Computers Can Search Rapidly by Using Almost any Transformation*. Physical Review Letters, **80**, 4329, (1998).
- [17] Imre, S., & Balázs, F. *Generalized Grover Database Search Operator with Arbitrary Initial State*, (2003).

نمایه

- ۵۳، ۲۴،
چگالی، ۴۸
احتمال، ۴۳
اسپین، ۵۱
اسکالر، ۲۴
الگوریتم دویچ-جوزا، ۳۳
الگوریتم گراور، ۳۴
انعکاس، ۲۷
اپراتور کوانتومی، ۳۵
اپراتور یکانی، ۳۶
بردار، ۲۴
بردار اسپینی واحد، ۴۹
بردار ثابت چرخان، ۴۸
بردار سه بعدی، ۲۴
بردارهای پایه متعامد، ۲۴
برهم‌نهی، ۳۵
بیت، ۳۴
تابع، ۳۵
تابع همانی، ۱۳
تابع وارونی بیت، ۱۳
جبر هندسی، ۲۴
جبر کلیفورد، ۲۴
جستجوی کوانتومی، ۳۴
حالت‌های بیشینه و کمینه، ۴۹
دامنه، ۴۴
درجه، ۲۵
دلتا، ۵۰
دوران، ۲۷
رجیستر، ۳۷
ضرب خارجی، ۲۷
ضرب تانسوری، ۲۴
ضرب داخلی، ۲۷
ضرب هندسی، ۲۶
ضریب وزنی بالا و پایین، ۵۱
لوی‌چی‌ویتا، ۵۰
متوسط دامنه، ۳۷، ۳۸
- مدار کوانتومی، ۳۵
مولد، ۴۷
هم‌پوشانی، ۳۵
کامپیوتر کلاسیکی، ۳۵
کت، ۳۴
کره‌ی بلاخ، ۴۹
کیوبیت، ۳۴

Aabstract

One of the problems that is solved by quantum algorithms in a shorter time and higher speed compared to classical algorithms is the search problems. The Grover's quantum search algorithm, as one of the best quantum search methods is able to increase the speed of classical search from $O(N)$ to $O(\sqrt{N})$. For large N this increase in speed is considerable. In this approach using the Clifford algebra we try to formulate Grover's quantum search.

We show firstly, that Clifford's geometric algebra, provides a significantly simpler representation than the conventional bra-ket notation, and secondly, that the basis defined by the states of maximum and minimum weight in the Grover search space, allows a simple visualization of the Grover search analogous to the precession of a spin $\frac{1}{2}$ particle.

We do not claim the development of an improved algorithm, but show in a tutorial paper that geometric algebra provides extremely compact and elegant expressions with improved clarity for the Grover search algorithm .

at the end of the thesis, first we propose a new operator and show that this unray operator acts like the Hadamard algorithm in Grover's quantum search algorithm and with a high probability with $O(\sqrt{N})$ algorithm frequency accesses to the searched mode. the difference is that this operator has an interesting physical concept. the new operator is similar to the Pauli matrix σ_y . next step, we consider another unray operator like T' . to superposition, from all basic modes we influence the proposed operator T' on the desired mode and the Grover's quantum search algorithm for this problem.

the goal is to find the proposed operator T' and first desired mode. we also checked that for how many repeats of new operator we achieve to the desired mode with high probability.



Shahrood University
Faculty Of Physics

Dissertation Submitted in Partial
Fulfillment of The Requirements For The
Degree of Master of Science in
Particle Physics

Using Clifford Algebra in Grover's Quantum Search Algorithm

Supervisor

Dr. Hossein Movahhedian

by

Kosarsadat Taffakh

2015