



دانشکده فیزیک
گروه ذرات بنیادی

پایان نامه

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

عنوان

الگوریتم جستجوی گراور با استفاده از درهمتنیدگی چندطرفه

استاد راهنما

دکتر حسین موحدیان

دانشجو

صفورا محمودی کوره کایجاری

۱۳۹۴

تقدیم به پدر بزرگوار و مادر مهربانم
آن دو فرشته ای که از خواسته هایشان گذشتند، سختی ها را به جان خریدند و خود را سپر
بلای مشکلات و ناملایمات کردند تا من به جایگاهی که اکنون در آن ایستاده ام برسم

و
تقدیم به استاد بزرگوارم
که اگر راهنمایی های بی دریغ ایشان نبود این مهم به نتیجه نمی رسید
بوسه بردستان این عزیزان

سپاس گزارى...^۴

ضمن سپاس و ستايش به درگاه ايزد منان كه به من توانايى داد كه با استعانت از او بتوانم اين پژوهش را انجام دهم، بر خود لازم مى بينم از دلگر مى و تشويق اساتيد و دوستان كه در نگارش اين مجموعه مرا يارى نمودند، قدردانى نمايم:

از جناب آقاى دكتر حسين موحديان، استاد راهنماى عزيزم، كه در طول نگارش اين مجموعه با راهنمايى هاى عالمانه و بجايشان، سكاندار شايسته اى در هدايت اين پايان نامه بوده اند.

از يك يك اعضاى خانواده ام كه مشوق من بودند تا به اين جايگاه دست يابم.
از جناب آقاى تيمور انديك همكلاسى گرامى ام كه در تدوين و پژوهش و نگارش اين مهم مرا يارى رساندند.

و در خاتمه از دوستان عزيزم خانم شيما ابراهيمى و خانم معصومه گل آرا و ديگر دوستانى كه مرا در انجام اين تحقيق يارى نمودند، قدردانى و تشكر مى نمايم.

صفورا محمودى كوره كايجارى
۱۳۹۴

تعمدنامه

اینجانب صفورا محمودی دانشجوی کارشناسی ارشد رشته فیزیک دانشگاه شاهرود، نویسنده پایان نامه با عنوان الگوریتم جستجوی گراور با استفاده از دره‌متنیدگی چندطرفه، تحت راهنمایی دکتر حسین موحدیان متعهد می‌شوم:

- تحقیقات در این پایان نامه 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 پایان نامه، تاکنون توسط خود، یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارایه نشده است.
- حقوق معنوی این اثر، به دانشگاه صنعتی شاهرود متعلق دارد، و مقالات مستخرج با نام “بررسی الگوریتم جستجوی گراور با استفاده از دره‌متنیدگی چندطرفه در دانشگاه صنعتی شاهرود” یا “Shahrood University of technology به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به دست آوردن نتایج اصلی پایان نامه تاثیرگذار بوده‌اند، در مقالات مستخرج از پایان نامه رعایت می‌گردد.
- در تمام مراحل انجام این پایان نامه، در مواردی که از موجود زنده (یا بافت‌های آنها) استفاده شده است، ضوابط و اصول اخلاقی رعایت شده است.
- در تمام مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته (یا استفاده) شده است، اصل رازداری و اصول اخلاق انسانی رعایت شده است.

صفورا محمودی کوره کابجاری
۱۳۹۴

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 صنعتی شاهرود می‌باشد. این مطلب باید به نحو مقتضی، در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در این پایان نامه بدون ذکر منبع مجاز نمی‌باشد.

چکیده

در این پایان نامه ویژگی‌های درهمتنیدگی چند طرفه را برای حالت‌های کوانتومی بررسی می‌کنیم. اخیراً معلوم شده است که در همتنیدگی‌های چند طرفه در بعضی از الگوریتم‌های کوانتومی مثل الگوریتم جستجوی گراور نقش مهمی دارند. مسئله الگوریتم‌های کوانتومی عبارت است از این که یک حالت پایه‌ی خاص را در بین کل حالت‌های موجود پیدا کنیم. این حالت خاص همان جواب مسئله است. در الگوریتم جستجوی گراور اولین مرحله تشکیل یک کت حالت است که حاصل برهم‌نهی تمامی پایه‌های فضای n بعدی می‌باشد. این کت باید با تمام این پایه‌ها هم‌پوشانی برابری داشته باشد. ایده کلی در روش الگوریتم گراور افزایش تدریجی دامنه جواب و کاهش دامنه غیر جواب می‌باشد، تا جایی که اندازه دامنه جواب بسیار زیاد و اندازه دامنه‌های دیگر بسیار کم شود. در این صورت با اندازه‌گیری حالت سیستم، جواب مسئله جستجو با احتمال بالایی بدست می‌آید. این موضوع با مطالعه خواص در همتنیدگی حالت‌های وزنی یکسان معلوم شده است که آن را نیز بررسی می‌کنیم. سپس حالت‌های بیشتری را که با کاربرد تکراری چرخه گراور یا عملگر اوراکل که یک عملگر یکانی است به وجود می‌آیند را در نظر می‌گیریم و خواص در همتنیدگی چند طرفه آنها را تجزیه و تحلیل می‌کنیم و نهایتاً توصیفی کیفی و کمی از دینامیک در همتنیدگی در الگوریتم جستجوی گراور ارائه می‌دهیم.

لیست مقالات مستخرج از پایان نامه

۱. محمودی. ص. موحدیان. ح. ”بررسی الگوریتم جستجوی گراور با استفاده از دره‌متنیدگی
چندطرفه”. سومین کنفرانس بین المللی پژوهش‌های کاربردی در مهندسی کامپیوتر و فناوری
اطلاعات. دانشگاه تربیت مدرس. ۱۵ بهمن ماه ۹۴

فهرست مطالب

لیست تصاویر خ

لیست جداول د

۱	مقدمه	۱
۲	۱.۱ مقدمه	۲
۲	۲.۱ کامپیوترهای کوانتومی	۲
۳	۳.۱ تاریخچه کامپیوترهای کوانتومی	۳
۴	۴.۱ تفاوت‌های میان یک کامپیوتر کوانتومی و یک کامپیوتر کلاسیکی	۴
۴	۵.۱ محاسبات کوانتومی	۴
۴	۶.۱ کت‌ها و براها و عملگرها	۴
۵	۷.۱ بیت و کیوبیت	۵
۷	۸.۱ ماتریس چگالی	۷
۸	۹.۱ کره بلاخ	۸
۱۰	۱۰.۱ درهم‌تنیدگی کوانتومی	۱۰
۱۱	۱۰.۱.۱ سیستم‌های دو قسمتی و پایه‌های بل	۱۱
۱۳	۲ گیت‌های کلاسیکی و کوانتومی و الگوریتم‌های کوانتومی	۱۳
۱۴	۱.۲ گیت‌های کلاسیکی و کوانتومی	۱۴
۱۴	۲.۲ تفاوت گیت‌های کلاسیکی و کوانتومی	۱۴
۱۴	۳.۲ انواع گیت‌های کوانتومی و کلاسیکی	۱۴
۲۲	۴.۲ الگوریتم‌های کوانتومی	۲۲
۲۲	۱.۴.۲ الگوریتم دویچ	۲۲
۲۳	۲.۴.۲ الگوریتم دویچ-جوزا	۲۳

۲۵	۳	الگوریتم جستجوی گراور
۲۶	۱.۳	جستجوی کوانتومی
۲۶	۲.۳	الگوریتم جستجوی گراور
۲۷	۱.۲.۳	ایده کلی الگوریتم گراور
۲۷	۲.۲.۳	شکل کلی یک مدار گراور
۲۷	۳.۲.۳	ساختار کلی مدار گراور
۳۰	۳.۳	تغییر عملگر گراور به عملگر دوران
۳۳	۴	الگوریتم جستجوی گراور با استفاده از درهم‌تنیدگی چندطرفه
۳۴	۱.۰.۴	حالت‌های وزنی یکسان حقیقی (REWS)
۳۵	۲.۰.۴	درجه جدایی‌پذیری
۳۶	۳.۰.۴	تجزیه و تحلیل کیفی حالت‌های دو مقداری با استفاده از درجه جدایی‌پذیری
۴۱	۴.۰.۴	تجزیه و تحلیل کمی حالت‌های دو مقداری با استفاده از اندازه‌ی درهم‌تنیدگی
۴۱	۵.۰.۴	عدد اشمیت
۴۲	۶.۰.۴	رنک یا رتبه یک ماتریس
۴۵	۱.۴	دینامیک درهم‌تنیدگی الگوریتم جستجوی گراور
۴۶	۱.۱.۴	تجزیه و تحلیل کیفی دینامیک الگوریتم جستجوی گراور
۴۸	۲.۱.۴	تجزیه و تحلیل کمی دینامیک الگوریتم جستجوی گراور
۴۹	۲.۴	نتایج
۵۲	۱.۲.۴	اثبات فرمول ۱ فصل ۴
۵۳	۲.۲.۴	اثبات فرمول ۲ فصل ۴
۵۶		مراجع
۵۸		نمایه

لیست تصاویر

۱۰.۱	کره بلاخ. نقاط روی کره متناظر با حالت‌های خالص و نقاط درون کره متناظر با حالت‌های آمیخته هستند.	۹
۱.۲	شکل هندسی گیت $Controlled - U$	۱۸
۲.۲	شکل هندسی گیت $CNOT$	۱۸
۳.۲	شکل هندسی گیت Z, Y, X	۲۰
۴.۲	شکل هندسی گیت $f - gate$	۲۱
۱.۳	مدار الگوریتم گراور	۲۷
۲.۳	ساختار مدار گراور	۲۷
۳.۳	شکل هندسی گیت $f - gate$	۲۸
۴.۳	بردار حالت ورودی که ترکیب خطی از همه‌ی داده‌های ممکن با ضرایب مساوی است	۲۹
۵.۳	بردار حالت ورودی بعد از آن که تابع یک‌بار آن را خوانده است	۲۹
۶.۳	بردار حالت بعد از انعکاس حول متوسط	۲۹
۷.۳	تغییر عملگر گراور به عملگر دوران	۳۲

لیست جداول

۱۵	گیت کلاسیکی <i>NOT</i>	۱.۲
۱۵	گیت کلاسیکی <i>AND</i>	۲.۲
۱۶	گیت کلاسیکی <i>OR</i>	۳.۲
۱۶	گیت کلاسیکی <i>XOR</i>	۴.۲
۱۷	گیت کلاسیکی <i>NAND</i>	۵.۲
۱۹	گیت کلاسیکی <i>Toffoli</i>	۶.۲

فصل ۱

مقدمه

۱.۱ مقدمه

کامپیوترهای کلاسیکی که امروزه با آن‌ها سروکار داریم، با بکارگیری بیتها^۱ که در دو حالت خاص می‌توانند وجود داشته باشند کار می‌کنند. اما کامپیوترهای کوانتومی به دو حالت خاص محدود نمی‌شوند. آنها اطلاعات را به وسیله بیتهای کوانتومی (کیوبیتها)^۲ کدگذاری می‌کنند که می‌توانند بی‌نهایت حالت را به خود بگیرد. این کامپیوترها برای پردازش اطلاعات از پدیده‌های کوانتومی همچون درهم‌نهمش^۳ و درهم‌تنیدگی^۴ استفاده می‌کنند.

۲.۱ کامپیوترهای کوانتومی

کامپیوتری که امروزه ما با آن سروکار داریم، برای کارکردن باید تعدادی صفر و یک را بفهمد و پردازش کند. همه اطلاعات اعم از حروف و اعداد یا وضعیت مودم و موس ما با مجموعه‌ای از بیت‌های متشکل از صفرها و یک‌ها به کامپیوتر داده می‌شود.

در کامپیوترهای معمولی قوانین فیزیک کلاسیک حاکم است، بیت‌های اطلاعات، خیلی ساده تعریف می‌شوند، سوئیچ‌های الکتریکی می‌توانند روشن یا خاموش باشند، اشیا می‌توانند اینجا باشند، می‌توانند هم نباشند! ولی کامپیوترهای کوانتومی با طبیعت دودویی‌های فیزیک کلاسیک محدود نمی‌شود، کامپیوتر کوانتومی دستگاهی است که یک پدیده‌ی فیزیکی را بر اساس قوانین فیزیک کوانتومی به صورت منحصر به فردی در می‌آورد تا به صورت اساسی یک حالت جدید از پردازش اطلاعات را تشخیص دهد. در واقع روش بهتر و قدرتمندتر برای پردازش اطلاعات پیش رویمان بر اساس فیزیک کوانتومی می‌باشد. در این بخش به بیان تاریخچه و تفاوت‌های کامپیوترهای کوانتومی و کلاسیک می‌پردازیم و نحوه برقراری ارتباط را در کامپیوترهای کوانتومی شرح می‌دهیم.

کامپیوتر تنها بخشی از دنیایی است که ما آنرا دنیای دیجیتال^۵ می‌نامیم. پردازش ماشینی اطلاعات، در هر شکلی، بر مبنای دیجیتال و محاسبات کلاسیک انجام می‌شود. اما روش بهتر برای پردازش اطلاعات بر اساس مکانیک کوانتومی می‌باشد. این روش جدید با ویژگی‌هایی همراه است که آنرا از محاسبات کلاسیک بسیار متمایز می‌سازد. گرچه محاسبات دانشی است که اساس تولد آن در ریاضیات بود، اما کامپیوترها سیستم‌هایی فیزیکی هستند و فیزیک در آینده این دانش نقش تعیین‌کننده‌ای خواهد داشت. البته وجود تفاوت بین این دو به معنای حذف یکی و جایگزینی دیگری نیست. به قول «نیلز بور» گاهی

^۱ Bit

^۲ Qubit

^۳ Superposition

^۴ Entanglement

^۵ Digital

ممکن است خلاف یک حقیقت انکارناپذیر منجر به حقیقت انکارناپذیر دیگری شود. بنابراین محاسبات کوانتومی را به عنوان یک زمینه و روش جدید و بسیار کارآمد مطرح می‌کنیم. وجود چند پدیده مهم که مختص فیزیک کوانتومی است، آن را از دنیای کلاسیک جدا می‌سازد. هر سیستم محاسباتی دارای یک پایه اطلاعاتی است که نماینده کوچکترین میزان اطلاعات قابل نمایش، چه پردازش شده و چه خام است. در محاسبات کلاسیک این واحد ساختاری را بیت می‌نامیم که گزیده‌ی واژه‌ی «عدد دودویی» است زیرا می‌تواند تنها یکی از دو رقم مجاز صفر و یک را در خود نگه دارد. به عبارت دیگر هر یک از ارقام یاد شده در محاسبات کلاسیک، کوچک‌ترین میزان اطلاعات قابل نمایش محسوب میشوند.

یک بیت کوانتومی (که به آن کیوبیت اطلاق می‌گردد) ممکن است درحالت‌های کلاسیک صفر یا یک وجود داشته باشد، یا ترکیبی از این دو (یعنی در آن واحد، مقادیر صفر و یک را به طور همزمان داشته باشیم حالت برهم نهی) یا حتی معرف عددی باشند که حالت آنها را جایی بین صفر و یک تعیین می‌کند. با توجه به مکانیک کوانتومی، نمی‌توان دقیقاً وجود یا عدم وجود یک ذره ریز را مشخص کرد. می‌توان به وسیله آمار و احتمال، امکان وجود این ذره‌های ریز را در مکان و زمان مشخصی تعیین کرد، اما هیچ راهی برای دانستن قطعی این که آیا این ذره آنجا هست یا نه وجود ندارد. البته آنچه که در کامپیوترهای کوانتومی با ارزش است همین احتمالات است.

۳.۱ تاریخچه کامپیوترهای کوانتومی

نظریه کامپیوترهای کوانتومی از سال ۱۹۸۲ مطرح بوده است. از زمانی که ریچارد فاینمن برای نخستین بار پیشنهاد کرد که باید محاسبات از دنیای دیجیتال وارد دنیای جدیدی به نام کوانتوم شود. همچنین بیان کرد که کامپیوترهای کوانتومی چگونه ممکن است کار کنند. در سال ۱۹۸۵ دویچ متوجه شد که اظهارات فاینمن می‌تواند تدریجاً به ساخت کامپیوترهای کوانتومی منجر شود. بالاخره در سال ۱۹۹۴ (پیت شور) نخستین گام را در جهت ساخت کامپیوترهای کوانتومی برداشت. در این زمان کامپیوترهای کوانتومی 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 منحصر برای کامپیوترهای کوانتومی طراحی شده‌اند می‌توانند چنین دستگاهی را به انجام فاکتورگیری از اعداد بیشماری با سرعت بالاتر از کامپیوترهای کلاسیکی قادر سازد. از آن موقع به بعد گروه‌های تحقیقاتی در سراسر دنیا مسابقه‌ای برای پیش‌قدم شدن در ساخت یک سیستم عملی آغاز نمودند به این ترتیب ارتباط نوینی بین نظریه اطلاعات و فیزیک کوانتومی شروع به شکل‌گیری کرد که امروزه آن را محاسبات کوانتومی^۶ می‌نامند.

^۶Quantum computation

۴.۱ تفاوت‌های میان یک کامپیوتر کوانتومی و یک کامپیوتر کلاسیکی

در مقایسه این دو نوع کامپیوتر می‌توان گفت مسائلی که زمانی تصور می‌شد در کامپیوترهای کلاسیکی غیر قابل حل است در کامپیوترهای کوانتومی حل خواهد شد و شبیه سازی های صورت گرفته به واقعیت نزدیکتر می‌شود. تفاوت دیگر کامپیوترهای کوانتومی و کلاسیک این است که اندازه ترانزیستورها هر سال کوچکتر می‌شود. وقتی اندازه ترانزیستورها به ابعاد اتمی نزدیکتر می‌شود دیگر قوانین حاکم بر فیزیک کلاسیک بر رفتار اتمها حاکم نیست به طور مثال کسی نمی‌داند یک الکترون، در زمان مشخصی، دقیقاً در کجا قرار دارد یا کسی نمی‌تواند به درستی تشخیص دهد که الکترون در یک سیم به کجا می‌رود. یعنی وقتی به ابعاد اتمی نزدیک می‌شویم فیزیک کوانتومی رفتار اتمی را توضیح می‌دهد و دیگر قوانین فیزیک کلاسیک کاربرد ندارد. در واقع این نوع از کامپیوترها با استفاده از رفتارهای میکروسکوپی ذره‌ها کار می‌کنند.

۵.۱ محاسبات کوانتومی

هدف محاسبات کوانتومی یافتن روش‌هایی برای طراحی مجدد ادوات شناخته شده محاسبات مانند : (گیت‌ها) به گونه‌ای است که بتوانند تحت اثرات کوانتومی که در محدوده ابعاد نانومتری و کوچکتر بروز می‌کنند کار کنند. ورود به دنیای محاسبات کوانتومی نیازمند دو پیش زمینه مهم است : نخست باید اصول اساسی و برخی تعابیر مهم مکانیک کوانتومی را به طور دقیق بررسی کرد سپس مفهوم اطلاعات در فیزیک، چه به صورت کلاسیک و چه در معنای جدید کوانتومی آن باید درک شود. بنابراین محاسبات کوانتومی را به عنوان یک زمینه و روش جدید و بسیار کارآمد مطرح می‌کنند.

۶.۱ کت‌ها و براها و عملگرها

در مکانیک کوانتومی یک حالت فیزیکی برای مثال اتم نقره با جهت اسپین تعریف شده، با یک بردار حالت در یک فضای برداری مختلط نمایش داده می‌شود. به تبعیت از دیراک این بردار را کت می‌نامیم و آن را با کت $|\alpha\rangle$ نشان می‌دهیم.

به عنوان یک اصل موضوعی، این کت دارای تمام اطلاعات یک حالت فیزیکی است، هر چیزی را که در مورد حالت بخواهیم در کت وجود دارد. دو کت می‌توانند با هم جمع شوند :

$$|\alpha\rangle + |\beta\rangle = |\gamma\rangle \quad (1.1)$$

و حاصل جمع کت $|\gamma\rangle$ همچنان یک کت است. اگر $|\alpha\rangle$ را در یک عدد مختلط c ضرب کنیم نتیجه حاصل ضرب $c|\alpha\rangle$ نیز کت دیگری است. عدد c می‌تواند در سمت راست یا چپ قرار گیرد، این دو تفاوتی ندارند :

$$c|\alpha\rangle = |\alpha\rangle c \quad (2.1)$$

در حالت ویژه‌ای که c صفر باشد، کت نتیجه را کت پوچ می‌نامند. در فضای برداری مورد نظر یک مشاهده پذیر نظیر مولفه‌های تکانه یا اسپین، می‌تواند با یک عملگر، مانند A نمایش داده شود. در حالت عمومی، یک عملگر از سمت چپ روی یک کت عمل می‌کند و نتیجه همچنان یک کت است :

$$A(|\alpha\rangle) = A|\alpha\rangle \quad (3.1)$$

به طور کلی $A|\alpha\rangle$ برابر حاصل ضرب یک ثابت در $|\alpha\rangle$ نیست. با این وجود، کتهای خاصی که آنها را به عنوان ویژه‌کت عملگر A می‌شناسیم و به صورت زیر نشان داده می‌شوند مهم هستند :

$$|\alpha'\rangle, |\alpha''\rangle, |\alpha'''\rangle, \dots$$

با خاصیت :

$$\begin{aligned} A|\alpha'\rangle &= \alpha' |\alpha'\rangle \\ A|\alpha''\rangle &= \alpha'' |\alpha''\rangle \end{aligned} \quad (4.1)$$

که $\alpha', \alpha'', \alpha'''$ دقیقاً عدد هستند [۱].

۷.۱ بیت و کیوبیت

در کامپیوترهای کلاسیکی هر نوع داده‌ای در بیت‌های کلاسیکی ذخیره می‌شود. یک بیت کلاسیک، صرف نظر از نوع سخت افزاری که در آن به کار رفته است، یک سیستم فیزیکی است که می‌تواند، در دو حالت ۰، 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. یک کیوبیت به یک سیستم کوانتومی گفته می‌شود که فضای هیلبرت $^{\vee}$ آن دو بعدی است این فضای هیلبرت را به صورت زیر نمایش می‌دهیم :

$$C^{\vee} = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \alpha, \beta \in c \right\} \quad (5.1)$$

^{\vee}D. Hilbert

معمول است که بردارهای پایه‌ی این فضا را با :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (6.1)$$

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

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

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (7.1)$$

که α, β اعداد مختلط هستند، با این شرط که :

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

اگر اندازه‌گیری بر روی کیوبیت انجام شود با احتمال $|\alpha|^2$ در حالت $|0\rangle$ و با احتمال $|\beta|^2$ در حالت $|1\rangle$ پیدا می‌شود.

تفاوت دیگر بین بیت کلاسیکی و کیوبیت در این است که بیت را می‌توان به راحتی و بدون آشفته کردن حالت آن اندازه‌گیری کرد و به اطلاعات آن دست یافت، اما یک کیوبیت بعد از اندازه‌گیری حالت آن به یکی از حالت‌های پایه تبدیل می‌شود و دیگر نمی‌توان اطلاعات اضافی را از آن بدست آورد.

وجود چند پدیده مهم که مختص فیزیک کوانتومی است آن را از دنیای کلاسیک جدا می‌سازد، این پدیده‌ها عبارتند از : برهمه‌نی، تداخل، درهم‌تنیدگی، ناموضعیّت.

یک کیوبیت ممکن است در حالت‌های کلاسیک 0 یا 1 وجود داشته باشد، یا ترکیبی از این دو (یعنی به طور همزمان مقادیر 0 و 1 را داشته باشیم، حالت برهمه‌نی)).

یک سیستم n کیوبیتی 2^n شیء را شماره‌گذاری می‌کند مثلاً اگر یک سیستم 3 کیوبیتی داشته باشیم، این سیستم می‌تواند $2^3 = 8$ شیء را اندیس گذاری کند. در کل یک کامپیوتر کوانتومی با n کیوبیت می‌تواند در هر برهمه‌نی از 2^n حالت به طور همزمان قرار بگیرد، برخلاف کامپیوترهای کلاسیکی که در هر لحظه فقط در یکی از حالات می‌توانند قرار بگیرند.

یک مثال برای نحوه‌ی پیاده‌سازی کیوبیت‌ها در کامپیوترهای کوانتومی، استفاده از ذراتی با اسپین $|\uparrow\rangle$ و $|\downarrow\rangle$ یا $|0\rangle$ و $|1\rangle$ است. اطلاعات روی حالت‌های فیزیکی سیستم ذخیره می‌شود و با عملیات روی سیستم، اطلاعات تحویل می‌یابند.

۸.۱ ماتریس چگالی

برای هر بردار واحد $|\psi\rangle \in H$ ماتریس چگالی متناظر آن به صورت زیر تعریف می‌شود: [۲]

$$\rho = |\psi\rangle \langle \psi| \quad (۸.۱)$$

این ماتریس دو خاصیت دارد:

$$\rho \geq 0 \quad ۱.$$

$$\text{tr} \rho = 1 \quad ۲.$$

برای هر $|v\rangle \in H$ واضح است که:

$$\langle v | \rho | v \rangle = |\langle v | \psi \rangle|^2 \geq 0 \quad (۹.۱)$$

$$\text{tr} \rho = \text{tr} |\psi\rangle \langle \psi| = \langle \psi | \psi \rangle = 1 \quad (۱۰.۱)$$

در حالت کلی ρ یک ماتریس چگالی نامیده می‌شود اگر خواص ۱ و ۲ را داشته باشد. مثلاً ماتریس $\frac{1}{d}I$ که در آن I ماتریس همانی در یک فضای d بعدی است، این دو خاصیت را دارد و ماتریس چگالی است. ولی این ماتریس چگالی، « خالص » نیست ($\text{tr}(\rho^2) \neq 1$) یعنی برای هر $|v\rangle$ ،

$$\frac{1}{d}I \neq |v\rangle \langle v| \quad (۱۱.۱)$$

اگر سیستم در حالت $|\psi\rangle$ باشد و اندازه‌گیری $\{M_i\}$ را روی آن اعمال کنیم، احتمال این که حاصل اندازه‌گیری i باشد برابر است با :

$$p_i = \langle \psi | M_i^\dagger M_i | \psi \rangle = \text{tr}(M_i^\dagger M_i |\psi\rangle \langle \psi|) = \text{tr}(M_i^\dagger M_i \rho) \quad (۱۲.۱)$$

همچنین تغییر حالت سیستم از این رابطه به دست می‌آید :

$$|\psi\rangle \rightarrow |\psi'\rangle = \frac{1}{\sqrt{p(i)}} M_i |\psi\rangle \quad (۱۳.۱)$$

$$\rho \rightarrow \rho' = |\psi'\rangle \langle \psi'| = \frac{1}{p(i)} M_i |\psi\rangle \langle \psi| M_i^\dagger = \frac{1}{p(i)} M_i \rho M_i^\dagger \quad (۱۴.۱)$$

بنابراین اندازه‌گیری را می‌توان بر حسب ماتریس‌های چگالی نوشت. تحول زمانی هم به همین صورت قابل بیان است :

$$|\psi\rangle \rightarrow U |\psi\rangle \quad (۱۵.۱)$$

$$\rho \rightarrow U \rho U^\dagger$$

اگر $X \geq 0$ آنگاه $M X M^\dagger$ نیز مثبت نیمه معین است (ماتریس A مثبت نیمه معین است اگر و تنها اگر همه ویژه مقادیر آن بزرگتر یا مساوی صفر باشد). پس $U \rho U^\dagger$ مثبت نیمه معین است و داریم :

$$\text{tr}(U \rho U^\dagger) = \text{tr}(\rho U^\dagger U) = \text{tr}(\rho) = 1$$

یعنی $U\rho U^\dagger$ نیز یک ماتریس چگالی است. لذا اصول مکانیک کوانتم را می‌توان برحسب این فرمول بندی جدید نوشت.

مثال :

اگر $|\psi\rangle = \frac{1}{\sqrt{4}}(|00\rangle + |11\rangle)$ باشد ماتریس چگالی متناظر با آن برابر است با :

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{4}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$$

$$= \frac{1}{4} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad (16.1)$$

۹.۱ کره بلاخ

کلی‌ترین حالت یک کیوبیت با یک ماتریس چگالی دو در دو داده می‌شود، این ماتریس را با ρ نشان می‌دهیم. از آنجا که ماتریس یک و ماتریس‌های پائولی یک پایه برای فضای ماتریس‌های دو در دو یکانی تشکیل می‌دهند می‌توان این ماتریس را به شکل زیر نوشت:

$$\rho = \frac{1}{4}(r_0 I + \vec{r} \cdot \vec{\sigma}) = \frac{1}{4} \begin{pmatrix} r_0 + z & x - iy \\ x + iy & r_0 - z \end{pmatrix} \quad (17.1)$$

که در آن $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ ماتریس‌های پائولی هستند. حال دقت می‌کنیم که:

الف : ρ هرمیتی است. بنابراین ضرایب $r_0, \vec{r}$ حقیقی هستند.

ب : $tr(\rho) = 1$ بنابراین $r_0 = 1$.

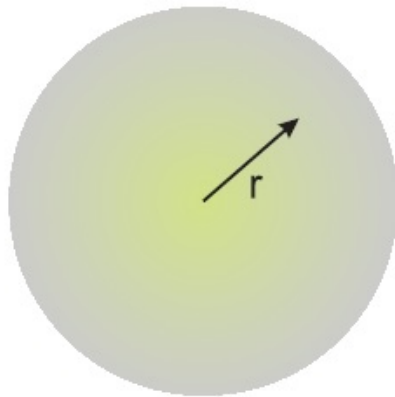
ج : $\rho \geq 0$ برای تامین این شرط می‌بایست ویژه مقدارهای ρ را حساب کنیم. یک محاسبه ساده نشان می‌دهد که ویژه مقدارهای ρ عبارتند از :

$$\lambda_{1,2} = \frac{1}{4}(1 \pm r) \quad (18.1)$$

که در آن r اندازه بردار $\vec{r}$ است.

بنابراین برای مثبت بودن کافی است که طول بردار $\vec{r}$ از یک کمتر باشد: یعنی $\vec{r} \leq 1$.

به این ترتیب بین هر ماتریس چگالی و یک نقطه از یک کره به شعاع واحد یک تناظر یک به یک برقرار



شکل ۱.۱: کره بلاخ. نقاط روی کره متناظر با حالت‌های خالص و نقاط درون کره متناظر با حالت‌های آمیخته هستند.

می‌شود، این کره را کره بلاخ^۸ می‌نامند. که در شکل بالا نشان داده شده است. نقاط روی سطح کره بلاخ نقاطی هستند که در آنها $r = 1$ و بنابراین ویژه مقادیر ρ برابر با یک و صفر هستند. در نتیجه این نقاط متناظر با حالت‌های خالص هستند. در واقع به راحتی می‌توان نشان داد که هرگاه $r = 1$ باشد یعنی r برابر با یک بردار یکه n باشد آنگاه:

$$\rho \equiv \frac{1}{2}(I + n \cdot \sigma) = |n\rangle \langle n| \quad (19.1)$$

که در آن $|n\rangle$ حالت یک ذره با اسپین درجهت بردار یکه n است. از طرف دیگر مرکز کره یعنی $r = 0$ متناظر با حالت کاملاً مخلوط $\rho = \frac{1}{2}I$ است. هرچه از مرکز کره به طرف مرز پیش برویم به درجه خلوص حالت‌ها اضافه می‌شود.

تحول زمانی

تحول زمانی یک سیستم فیزیکی با یک عملگر یکانی مشخص می‌شود. اگر حالت سیستم در زمان t_0 ، ρ و در زمان t_1 ، σ باشد عملگر یکانی U وجود دارد که $\sigma = U\rho U^\dagger$.

سیستمهای ترکیبی

فضای هیلبرت یک سیستم ترکیبی، از ضرب تانسوری فضاهای کوچک‌تر بدست می‌آید. توجه کنید که اگر ρ و σ ماتریس چگالی باشند $\rho \otimes \sigma$ نیز ماتریس چگالی است.

^۸Bloch sphere

فضای هیلبرت

یک فضای ریاضی که در آن حالت‌ها و بردارها را تعریف می‌کنیم فضای هیلبرت می‌گویند. به هر سیستم کوانتومی یک فضای هیلبرت نسبت داده می‌شود. حداکثر تعداد بردارهای مستقل در یک فضای هیلبرت H را بعد آن می‌نامند و با $\dim H$ نشان می‌دهند. در هر فضای هیلبرت می‌توان به تعداد بعد آن بردار پایه معرفی کرد که هر بردار دلخواه بر حسب بردارهای پایه به طور کامل تعیین می‌شود.

۱۰.۱ درهم‌تنیدگی کوانتومی

وقتی از درهم‌تنیدگی کوانتومی سخن می‌گوییم شاید شگفتی‌های دنیای فیزیک برایمان نمایان می‌شود. درهم‌تنیدگی کوانتومی یک پدیده قدیمی با این معنا است که برخی ذرات، مثل فوتون‌ها و الکترون‌ها، می‌توانند “یک بار” بر یکدیگر اثر متقابل بگذارند ولی همچنان حتی پس از جدایی، کیفیت‌هایی نظیر چرخش یا قطبی‌شدگی‌شان مشترک باشد و “با تغییر حالت یکی، دیگری نیز تغییر کند.” در مکانیک کوانتومی، درهم‌تنیدگی یکی از رفتارهای عجیب ذرات است که در آن قوانین فیزیک کلاسیک شکسته می‌شوند و رویدادهای ناممکن به وقوع می‌پیوندند. درهم‌تنیدگی که انیشتین از آن با عنوان “عمل شبح‌وار در یک فاصله” یاد می‌کند، پدیده‌ای است که در آن دو ذره به عنوان یک سیستم عمل می‌کنند حتی هنگامی که توسط فواصل عظیم از هم جدا شده باشند.

اما داستان درهم‌تنیدگی در سال ۱۹۳۵ میلادی شروع شد، زمانی که نکته فوق العاده عجیبی در مورد نظریه کوانتومی توجه آلبرت انیشتین را جلب کرد، نکته ای که چند سالی از فرمول بندی نوین نظریه کوانتومی می‌گذشت همچنان از نگاه تیزبین فیزیکدان‌ها پوشیده مانده بود. انیشتین دریافت که براساس نظریه کوانتومی باید مابین ذراتی که حداقل یکبار با یکدیگر برهم کنش داشته‌اند، نوعی ارتباط اسرارآمیز درونی برقرار شود، به گونه‌ای که اگر ویژگی‌های کوانتومی یکی از این ذرات را تغییر دهیم، مابقی آنها صرف نظر از اینکه در چه فاصله‌ای از ذره اول قرار گرفته‌اند مثلاً یک متر یا یک میلیارد سال نوری فاصله دارند بلافاصله و بطور آنی از این تغییر، تاثیر می‌پذیرد.

انیشتین مقاله مشترکی با دو فیزیکدان دیگر به نام‌های بوریس پودولسکی و ناتان روزن منتشر کرد و در آن مقاله ضمن اعلام نظر خود مبنی بر وجود مشکل در نظریه کوانتومی، نظریه دیگری بنام «نظریه متغیرهای نهانی موضعی» بعنوان جایگزین نظریه کوانتومی ارائه داد. این نظریه به گونه‌ای گردآوری شده بود که تمامی پیش‌بینی‌های نظریه کوانتومی را عیناً البته بدون در نظر گرفتن رابطه آنی و لحظه‌ای بین ذرات، نتیجه می‌داد.

در این مطالعه، پارادوکس EPR نمایان شد، آزمایشی فکری که در تلاش بود ناکامل بودن تئوری مکانیک کوانتومی را نشان دهد. در این مقاله آمده بود: “بنابراین ما مجبوریم چنین نتیجه‌گیری کنیم که توصیف مکانیک کوانتومی از واقعیت فیزیکی توابع موج، غیرکامل می‌باشد.”

با این حال نه تنها واژه درهم‌تنیدگی توسط این سه دانشمند ساخته و پیشنهاد نشده بود بلکه ایشان خواص ویژه این وضعیت را نیز تعمیم نداده بودند. پس از انتشار مقاله EPR ، اروین شرودینگر برای

نخستین بار در نامه‌ای که برای انیشتین می‌نویسد از واژه درهمتنیدگی برای توصیف بستگی دو ذره که موقتاً با یکدیگر در اندرکنش بوده و سپس جدا شده‌اند استفاده کرد. شرودینگر اهمیت EPR را در آن می‌دید که انحراف مکانیک کوانتومی از موازین ذهن کلاسیک نشان می‌داد. وی همچون انیشتین با مفهوم درهمتنیدگی مخالف بود چرا که آشکارا نظریه نسبیت را که در آن سرعت نور، بیشینه سرعت انتقال اطلاعات بود را به چالش می‌کشید. انیشتین بعدها درهمتنیدگی را تاثیر از فاصله شیخ وار نامید و به این ترتیب آن را به سخره گرفت.

کلید پاسخ این سوال مهم را یک فیزیکدان ایرلندی به نام جان بل در سال ۱۹۶۴ میلادی پیدا کرد. جان بل توانست رابطه‌ای ریاضی را که بعدها به نام «نامساوی بل» شهرت یافت، پیدا کند. که می‌توانست مابین پیش‌بینی‌های این دو نظریه رقیب یعنی نظریه کوانتومی و نظریه متغیرهای نهانی موضعی را در آزمایشات خاصی نشان دهد. بر این اساس اگر فیزیکدان‌ها موفق می‌شدند در آزمایشات خود، نقض نامساوی بل را مشاهده کنند، این به معنای صحت نظریه کوانتومی و وجود پدید اسرارآمیز درهمتنیدگی کوانتومی بود و در غیر این صورت، حق با انیشتین بود و هیچ ارتباطی با سرعتی فراتر از سرعت نور مابین ذرات وجود نداشت.

۱.۱۰.۱ سیستم‌های دو قسمتی و پایه‌های بل

سیستم دو قسمتی سیستمی است که شامل دو زیر سیستم می‌باشد. یک مثال از این سیستم، زمانی است که دو مشاهده‌گر آلیس و باب، هر کدام بخشی از یک جفت ذره درهمتنیده شده را در اختیار دارند. فضای هیلبرت چنین سیستمی به صورت حاصلضرب تانسوری از دو فضای هیلبرتی است که سیستم آلیس و باب را توصیف می‌کند. چنانچه فضاها ی هیلبرت آنها را به ترتیب به صورت H_A و H_B تعریف کنیم، فضای هیلبرت سیستم مرکب به صورت زیر خواهد شد :

$$H = H_A \otimes H_B \quad (20.1)$$

اگر حالت‌های پایه را برای آلیس و باب به صورت $|a_i\rangle$ و $|b_j\rangle$ در نظر بگیریم آنگاه حالتها برای سیستم مرکب، به صورت حاصلضرب تانسوری از حالت‌های پایه می‌شود.

$$|a_{ij}\rangle = |a_i\rangle \otimes |b_j\rangle = |a_i\rangle |b_j\rangle = |a_i b_j\rangle \quad (21.1)$$

به دلیل اینکه پایه‌های آلیس و باب هر دو راست بهنجار هستند، بنابراین برای سیستم‌های مرکب خواهیم داشت :

$$\langle \alpha_{ij} | \alpha_{kl} \rangle = \langle a_i b_j | a_k b_l \rangle = \langle a_i | a_k \rangle \langle b_j | b_l \rangle = \delta_{ik} \delta_{jl} \quad (22.1)$$

حال حالت کوانتومی $|\psi\rangle$ از سیستم مرکبی را در نظر می‌گیریم که می‌تواند بر حسب حالت‌های پایه به صورت زیر بسط داده شود :

$$|\psi\rangle = \sum_{i,j} C_{ij} |a_{ij}\rangle = \sum_{i,j} |a_i b_j\rangle \langle a_i b_j | \psi \rangle \quad (23.1)$$

ضرایب بسط $\langle a_i b_j | \psi \rangle$ دامنه‌های احتمال برای پیدا کردن سیستم در حالت $|a_i b_j\rangle$ می‌باشد. از این رو احتمال پیدا کردن سیستم در این حالت به صورت زیر داده می‌شود:

$$\Pr(a_i b_j) = |\langle a_i b_j | \psi \rangle|^2 \quad (24.1)$$

یک نمونه از حالت‌های پایه راست بهنجار برای سیستم دو قسمتی، حالت‌های پایه‌ای بل هستند. مجموعه‌ی پایه‌های بل که گاهی اوقات حالت‌های بل یا حالات EPR نامیده می‌شوند. به صورت زیر می‌باشند:

$$\begin{aligned} |B_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ |B_{01}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\ |B_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\ |B_{11}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}} \end{aligned} \quad (25.1)$$

حالت $|B_{01}\rangle$ به عنوان حالت سه‌تایه (سه‌تایی) شناخته می‌شود. علاوه بر حالت $|B_{01}\rangle$ دو حالت سه‌گانه دیگر $|11\rangle$ و $|00\rangle$ نیز وجود دارد. در حالی که $|B_{11}\rangle$ تک‌تایه است. حالت‌های سه‌تایه، حالتی با اسپین یک هستند ولی در مورد حالات تک‌تایه اسپین حالت برابر با صفر است. حالت‌های بل را می‌توان به صورت خلاصه با عبارت زیر بیان کرد: [۳]

$$|B_{xy}\rangle = \frac{|0y\rangle + (-1)^x |1\bar{y}\rangle}{\sqrt{2}} \quad (26.1)$$

فصل ۲

گیت‌های کلاسیکی و کوانتومی و الگوریتم‌های

کوانتومی

۱.۲ گیت‌های کلاسیکی و کوانتومی

گیت‌ها اجزای اصلی یک مدار منطقی را تشکیل می‌دهند و عملیات پردازش اطلاعات روی بیت‌ها در کامپیوترهای کلاسیکی و کیوبیت‌ها در کامپیوترهای کوانتومی را بر عهده دارند. در ادامه با انواع گیت‌ها و نحوه‌ی عملیاتشان آشنا می‌شویم.

در مقابل گیت‌های کلاسیکی^۱ می‌توان به گیت‌های کوانتومی^۲ به عنوان یکی از اجزای تشکیل دهنده رایانه‌های کوانتومی اشاره کرد. اصطلاح گیت کوانتومی برای عملگر یکانی^۳ بکار می‌رود، هر گیت کوانتومی تبدیل خطی^۴ است. (فضاهای برداری w و v روی هر میدان f در نظر می‌گیریم تابع $T : f \rightarrow w$ یک تبدیل خطی نامیده می‌شود. هرگاه $T(v_1 + v_2) = T(v_1) + T(v_2)$ به ازای $v_1, v_2 \in V$ که می‌توان آن را با ماتریس یکانی توصیف کرد و می‌توان نتیجه گرفت که به دلیل معکوس‌پذیر بودن هر عملگر یکانی، هر گیت کوانتومی نیز معکوس‌پذیر است. به طور کلی اگر گیت کوانتومی بر روی یک کیوبیت اثر کند آن را گیت تک کیوبیتی و هرگاه روی n کیوبیت اثر کند آن را گیت n کیوبیتی می‌نامند.

۲.۲ تفاوت گیت‌های کلاسیکی و کوانتومی

یک تفاوت عمده میان گیت‌های کلاسیکی و کوانتومی در آن است که ورودی و خروجی گیت‌های کوانتومی می‌تواند حالت برهم‌نesh یک کیوبیت هم باشد در صورتی که در دنیای کلاسیک حالت برهم‌نesh وجود ندارد. اگر اطلاعات را در کیوبیت‌ها یعنی حالت‌های کوانتومی ذخیره کنیم، به‌ناچار پردازش اطلاعات یا با عملگرهای یکانی که تحول را نشان می‌دهند یا با اندازه‌گیری‌ها انجام می‌گیرد. در ادامه چند نمونه از گیت‌های کلاسیکی و کوانتومی را نشان داده‌ایم.

۳.۲ انواع گیت‌های کوانتومی و کلاسیکی

در زیر چند نمونه از گیت‌های کوانتومی و کلاسیکی را نشان می‌دهیم: [۳]

^۱Classical gates

^۲Quantum gates

^۳Unitary operator

^۴Linear transformation

گیت NOT

گیت NOT یک گیت کلاسیکی می‌باشد که عمل انعکاس بیت‌ها را انجام می‌دهد:

جدول ۱.۲: گیت کلاسیکی NOT

x	$NOT\ x$
۰	۱
۱	۰

گیت AND

گیت AND یک گیت کلاسیکی می‌باشد و تنها زمانی ۱ است که هر دو ورودی ۱ باشند در غیر این صورت صفر است.

جدول ۲.۲: گیت کلاسیکی AND

x	y	$x\ AND\ y$
۰	۰	۰
۰	۱	۰
۱	۰	۰
۱	۱	۱

گیت OR

گیت OR یک گیت کلاسیکی می‌باشد به این صورت که اگر x یا y یک باشند، خروجی برابر با یک می‌شود در غیر این صورت خروجی صفر می‌شود.

جدول ۳.۲: گیت کلاسیکی OR

x	y	$x OR y$
۰	۰	۰
۰	۱	۱
۱	۰	۱
۱	۱	۱

گیت XOR

گیت XOR یک گیت کلاسیکی می‌باشد به این صورت که اگر فقط یکی از ورودی‌ها ۱ باشد، خروجی ۱ است اما اگر هر دو ورودی ۱ باشد خروجی صفر می‌شود.

جدول ۴.۲: گیت کلاسیکی XOR

x	y	$x XOR y$
۰	۰	۰
۰	۱	۱
۱	۰	۱
۱	۱	۰

گیت $NAND$

گیت $NAND$ یک گیت کلاسیکی می‌باشد که در محاسبات کلاسیکی^۵ دارای اهمیت است، به این صورت که در ابتدا با دو بیت ورودی مثل گیت AND عمل می‌کند و سپس حاصل را NOT می‌کند، این گیت برگشت‌ناپذیر است. گیت‌های کلاسیکی مانند AND ، XOR ، $NAND$ ، ...، ورودی

^۵Classical computing

جدول ۵.۲: گیت کلاسیکی NAND

x	y	$x \text{ NAND } y$
۰	۰	۱
۰	۱	۱
۱	۰	۱
۱	۱	۰

دو بیتی به خروجی تک بیتی تبدیل می‌شود و به وضوح برگشت‌ناپذیرند، اما اگر یک گیت کوانتومی با عملگر U ، حالت ورودی $|\psi\rangle_{in}$ را به حالت $|\psi\rangle_{out}$ تبدیل کند می‌توان گیتی با عملگر $U^\dagger$ تشکیل داد تا کت $|\psi\rangle_{out}$ را مجدداً به $|\psi\rangle_{in}$ تبدیل کند یعنی گیت‌های کوانتومی یکانی و برگشت‌پذیرند. عملگرهای کوانتومی را می‌توان با ماتریس نمایش داد. یک گیت کوانتومی با n ورودی و خروجی را می‌توان با ماتریس 2^n بعدی نمایش داد، به عنوان مثال نمایش ماتریسی گیت دو کیوبیتی، 4×4 است. گیت X گیت کوانتومی NOT است که با ماتریس پائولی X انجام می‌شود:

$$X = U_{not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (1.2)$$

$$\begin{cases} U_{not} |0\rangle = |1\rangle \\ U_{not} |1\rangle = |0\rangle \end{cases} \quad (2.2)$$

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

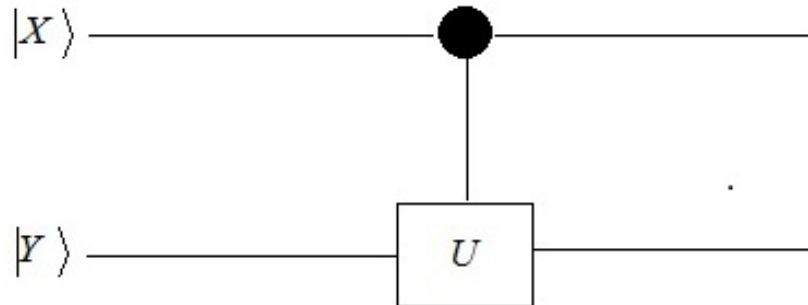
$$X |i\rangle = |i \oplus 1\rangle \quad (3.2)$$

که در این جا علامت $\oplus$ به معنای باقیمانده، تقسیم جمع بر ۲ می‌باشد.

گیت $Controlled - U$

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 می‌شود یا خیر. عملگر این گیت به این صورت است که اگر

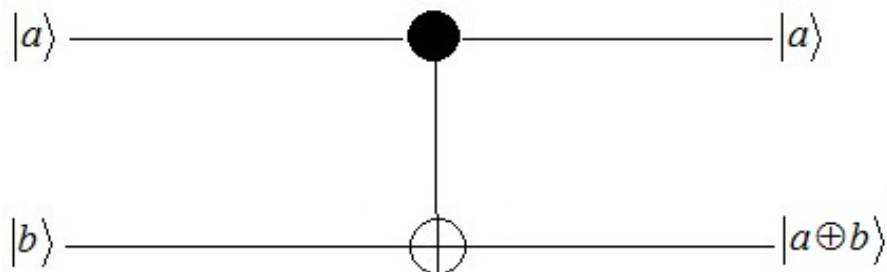
کیوبیت کنترل در حالت $|0\rangle$ باشد گیت هیچ عملی روی کیوبیت هدف انجام نمی‌دهد و در صورتی که کیوبیت کنترل در حالت $|1\rangle$ باشد گیت، عملگر یکانی را بر روی کیوبیت هدف اثر می‌دهد.



شکل ۱.۲: شکل هندسی گیت $Controlled - U$

گیت $CNOT$

یکی از مهم‌ترین گیت‌های $Controlled - U$ گیت $CNOT$ است. گیت کنترل شده $CNOT$ دو کیوبیت را به عنوان حالت ورودی دریافت می‌کند که یکی کیوبیت کنترل و دیگری کیوبیت هدف است. کاری که این کیوبیت انجام می‌دهد این است که کیوبیت کنترل را با کیوبیت هدف جمع کرده و حاصل را بر دو تقسیم می‌کند و باقیمانده را به عنوان خروجی هدف بیرون می‌دهد. 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 ۲.۲: شکل هندسی گیت $CNOT$

$$|X\rangle |Y\rangle \xrightarrow{CNOT} |X\rangle |X \oplus Y\rangle \quad (۴.۲)$$

گیت هادامارد (H)

بی‌شک این گیت یکی از مهم‌ترین گیت‌های کوانتومی است. عمل یکانی هادامارد روی کت‌های پایه‌ی محاسباتی به صورت زیر تعریف می‌شود:

$$H|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (5.2)$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} \langle 0|H|0\rangle & \langle 0|H|1\rangle \\ \langle 1|H|0\rangle & \langle 1|H|1\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (6.2)$$

یکی از کاربردهای این گیت این است که می‌توان به وسیله‌ی آن کت پایه‌ی n بعدی $|0^{\otimes n}\rangle$ را به یک برهم‌نیش مساوی از کت‌های پایه‌ی فضای n بعدی تبدیل کرد. برای مثال به‌ازای $n = 3$

$$\begin{aligned} H^{\otimes 3}|0^{\otimes 3}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \end{aligned} \quad (7.2)$$

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.

جدول ۶.۲: گیت کلاسیکی *Toffoli*

C_1	C_2	T	T'
۰	۰	۰	۰
۰	۱	۰	۱
۱	۰	۱	۱
۱	۱	۱	۰

گیت Z

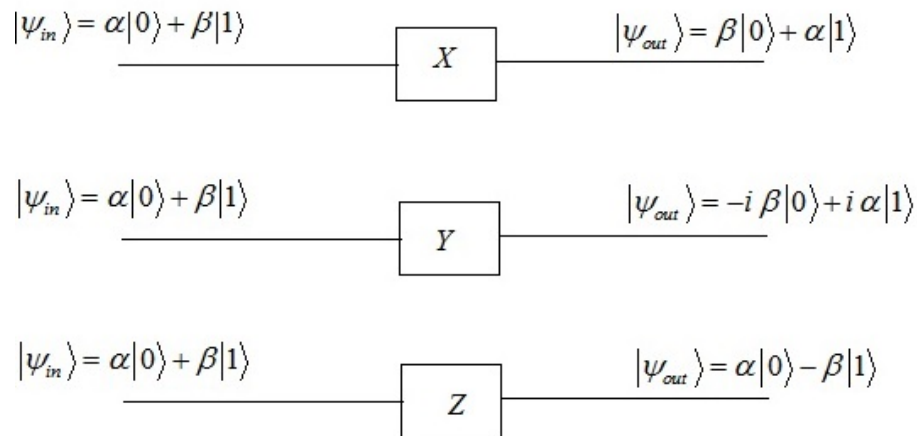
یکی دیگر از گیت‌های کوانتومی تک کیوبیتی مربوط به ماتریس پائولی Z است که فاز برگردان^۶ می‌شود زیرا :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi'\rangle = \alpha|0\rangle - \beta|1\rangle \quad (۸.۲)$$

$$\begin{aligned} Z|\psi\rangle &= (|0\rangle\langle 0| - |1\rangle\langle 1|)\alpha|0\rangle + \beta|1\rangle \\ &= \alpha|0\rangle - \beta|1\rangle \end{aligned} \quad (۹.۲)$$

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

$$Z|i\rangle = (-1)^i|i\rangle \quad (۱۰.۲)$$



شکل ۳.۲: شکل هندسی گیت Z, Y, X

گیت f - gate

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

^۶Phase flip

هدف (که یک ریجستر به اندازه m کیوبیت است : $y \in \{0, 1\}^m$) می‌نگارد.

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

$$|x\rangle |y\rangle \xrightarrow{f\text{-gate}} |x\rangle |(y \oplus f(x))\rangle \quad (11.2)$$

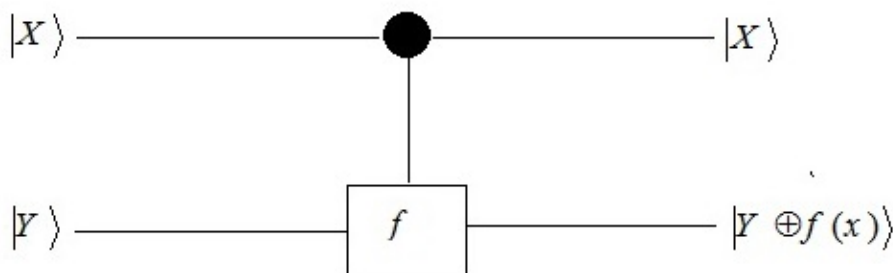
به ازای $|y\rangle = |0\rangle$ خواهیم داشت :

$$|x\rangle |0\rangle \xrightarrow{f\text{-gate}} |x\rangle |f(x)\rangle \quad (12.2)$$

در حالی که ورودی کنترل به صورت یک برهم‌نهی از کتهای پایه‌ی $|x\rangle$ باشد آنگاه رابطه زیر را داریم:

$$\sum_x |x\rangle |0\rangle \xrightarrow{f\text{-gate}} \sum_x |x\rangle |f(x)\rangle \quad (13.2)$$

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



شکل ۴.۲: شکل هندسی گیت $f\text{-gate}$

گیت $Phase - shift$

گیت کلی $Phase - shift$ را در نظر می‌گیریم. این گیت، فازکت پایه‌ی $|1\rangle$ را به اندازه θ تغییر می‌دهد.

$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad (14.2)$$

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.

۴.۲ الگوریتم‌های کوانتومی

۱.۴.۲ الگوریتم دویچ

الگوریتم دویچ^۷ برای شناسایی نوع تابع (ثابت یا متوازن) به کار می‌رود که شامل سه مرحله است:

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

$$(H \otimes H) |0\rangle |1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) \quad (15.2)$$

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

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

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

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

$$|\psi'\rangle = U_f(H \otimes H)$$

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

$$+ (1 - f(1)) |10\rangle + f(1) |11\rangle + (1 - f(1)) |11\rangle + f(1) |10\rangle$$

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

اگر تابع ثابت باشد خروجی به صورت زیر حاصل می‌شود:

$$|\psi_{out}\rangle = \pm |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \quad (16.2)$$

و اگر تابع متوازن باشد خروجی به صورت زیر به دست خواهد آمد:

$$|\psi_{out}\rangle = \pm |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \quad (17.2)$$

^۷Deutsch algorithm

تابع متوازن

یک تابع همانی^۸ (تابعی که ورودی و خروجی آن یک عدد می‌باشد، یعنی اگر ورودی صفر باشد خروجی نیز صفر خواهد شد و اگر ورودی یک باشد خروجی نیز یک می‌باشد) و بیت برگردان^۹ (تابعی که یک را به صفر و صفر را به یک تبدیل می‌کند) را تابع متوازن^{۱۰} می‌گویند زیرا به ازای نیمی از ورودی‌ها، خروجی یک و به ازای نیمی دیگر از ورودی‌ها، خروجی صفر را می‌دهد.

$$f(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x = 1 \end{cases} \quad (18.2)$$

تابع ثابت

تابع ثابت^{۱۱} تابعی است که به ازای هر ورودی یک خروجی را می‌دهد.

$$f(x) = \begin{cases} 1 & \text{if } x = 0 \text{ or } 1 \\ 0 & \text{if } x = 0 \text{ or } 1 \end{cases} \quad (19.2)$$

۲.۴.۲ الگوریتم دویچ-جوزا

الگوریتم دویچ جوزا^{۱۲} حالت تعمیم یافته‌ای از الگوریتم دویچ است با این تفاوت که $x \in \{0, 1\}^n$ است. این الگوریتم به ما اجازه می‌دهد که مشخص کنیم که یک تابع $f(x)$ ، تابعی ثابت است یا تابعی متوازن.

$$|\psi'\rangle = (H^{\otimes n} \otimes H) |0^{\otimes n}\rangle |1\rangle \quad (20.2)$$

$$|\psi'\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (21.2)$$

$$U_f |\psi'\rangle = |\psi''\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (22.2)$$

^۸Identity^۹Bit flip^{۱۰}Balanced^{۱۱}Constant^{۱۲}Deutsch-Jozsa algorithm

با اعمال اپراتور هادامارد بر روی حالت $|x\rangle$ داریم :

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_x \sum_y (-1)^{x \cdot y} |y\rangle \quad (23.2)$$

در نتیجه خروجی به صورت زیر بدست می‌آید :

$$|\psi_{out}\rangle = \frac{1}{2^n} \sum_x \sum_y (-1)^{x \cdot y + f(x)} |y\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (24.2)$$

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

۱. اگر تمام کیوبیت‌ها در $|y\rangle$ صفر باشند تابع ثابت است.

۲. اگر حداقل یکی از کیوبیت‌ها در $|y\rangle$ یک باشد تابع متوازن خواهد بود [۳].

فصل ۳

الگوریتم جستجوی گراور

۱.۳ جستجوی کوانتومی

فرض می‌کنیم N مهره داریم که N نام دانشجو به صورت نامنظم روی آنها ثبت شده است و این نام‌ها به وسیله‌ی اعداد ۰ تا $N - 1$ اندیس گذاری شده‌اند. حال می‌خواهیم از میان این نام‌ها به دنبال یک نام خاص بگردیم. واضح است که برای پیدا کردن این نام کافیهست تا فقط اندیس مربوط به آن را پیدا کنیم.

برای جستجوی کوانتومی، نام‌ها را با کت‌های n کیوبیتی اندیس‌گذاری می‌کنیم. هر کدام از این کت‌ها، پایه‌ای از یک فضای 2^n بعدی است.

یک سیستم n کیوبیتی می‌تواند $N = 2^n$ شماره را اندیس‌گذاری کند. برای مثال فرض می‌کنیم $N = 8$ مهره داریم و می‌خواهیم نام‌ها را روی آنها اندیس‌گذاری کنیم. برای اندیس‌گذاری این هشت نام، نیاز به یک سیستم سه کیوبیتی داریم:

$$(1.3) \quad |i\rangle : |000\rangle \quad |001\rangle \quad |010\rangle \quad |011\rangle \quad |100\rangle \quad |101\rangle \quad |110\rangle \quad |111\rangle$$

بنابراین مسئله جستجوی کوانتومی عبارت است از پیدا کردن یک حالت خاص در میان 2^n حالت موجود.

در الگوریتم‌های کلاسیکی به طور میانگین در $\frac{N}{2}$ بار این جستجو انجام می‌گیرد ولی در الگوریتم‌های کوانتومی این کار بسیار سریعتر انجام می‌گیرد. یعنی به طور کلی در $\sqrt{N}$ مرحله این کار صورت می‌گیرد [۴، ۵].

۲.۳ الگوریتم جستجوی گراور

یکی از الگوریتم‌های کوانتومی الگوریتم جستجوی گراور^۱ است. در الگوریتم جستجوی گراور اولین مرحله تشکیل یک کت حالت مثل $|\psi\rangle$ می‌باشد.

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \quad N = 2^n$$

که $|\psi\rangle$ با اعمال عملگر $H^{\otimes n}$ روی کت $|0\rangle^{\otimes n}$ بدست می‌آید.

$$H = \frac{1}{\sqrt{2}} [|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| - |1\rangle \langle 1|] \quad (2.3)$$

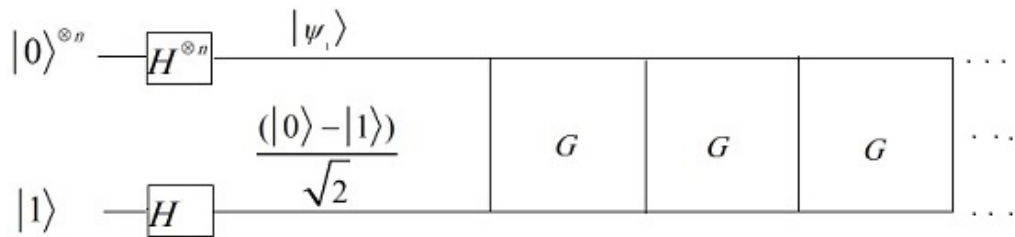
$$H|0\rangle = \frac{1}{\sqrt{2}} [|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| - |1\rangle \langle 1|] |0\rangle = \frac{1}{\sqrt{2}} [|0\rangle + |1\rangle]$$

^۱Grover's search algorithm

۱.۲.۳ ایده کلی الگوریتم گراور

در الگوریتم جستجو گراور ایده اصلی افزایش دامنه جواب و کاهش دامنه غیر جواب است. [۵]

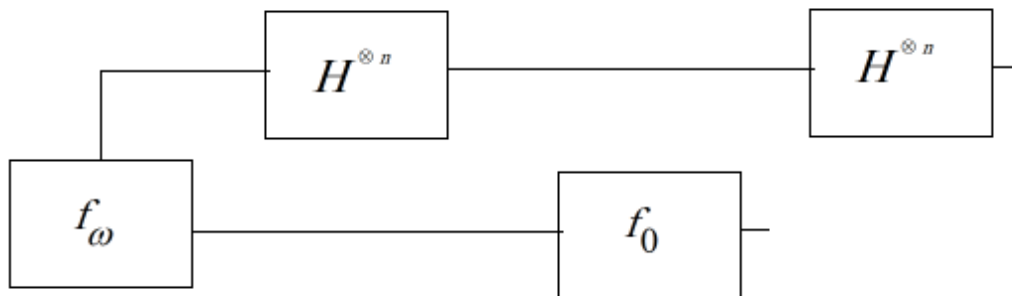
۲.۲.۳ شکل کلی یک مدار گراور



شکل ۱.۳: مدار الگوریتم گراور

که هر مربع که با حرف G نشان داده شده است یک مدار گراور می‌باشد و ساختارش به صورت زیر می‌باشد:

۳.۲.۳ ساختار کلی مدار گراور



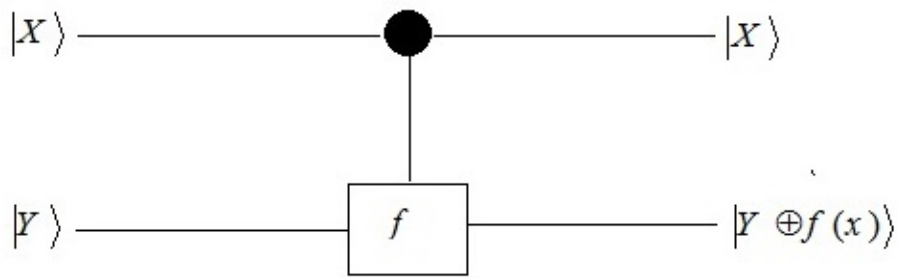
شکل ۲.۳: ساختار مدار گراور

حال به بررسی اجزای مدار گراور می‌پردازیم:

f_{ω} : یک f -gate است که ضریب i هایی که جواب مسئله است را منفی و بقیه را بدون تغییر باقی می‌گذارد.

f -gate:

فرض می‌کنیم به یک سیستم دو داده به صورت زیر می‌دهیم:

شکل ۳.۳: شکل هندسی گیت f - gate

$$|x\rangle |y\rangle \xrightarrow{f\text{-gate}} |x\rangle |y \oplus f(x)\rangle \quad (3.3)$$

اگر فرض کنیم کیوبیت هدف به صورت زیر باشد :

$$|u\rangle = \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{\frac{y\pi i}{2^m}} |y\rangle \quad (4.3)$$

با اعمال f - gate خواهیم داشت :

$$\sum_x |x\rangle |u\rangle \xrightarrow{f\text{-gate}} \sum_x \left(\frac{1}{\sqrt{2^m}} |x\rangle \sum_{y=0}^{2^m-1} e^{\frac{y\pi i}{2^m}} |y \oplus f(x)\rangle \right) \quad (5.3)$$

$$= \sum_x \left(\frac{1}{\sqrt{2^m}} e^{\frac{f(x)\pi i}{2^m}} |x\rangle \sum_{y=0}^{2^m-1} e^{\frac{y\pi i}{2^m}} |y \oplus f(x)\rangle \right)$$

$$\sum_x e^{\frac{f(x)\pi i}{2^m}} |x\rangle |u\rangle \quad (6.3)$$

در الگوریتم گراور $m = 1$ و کیوبیت هدف یعنی $|u\rangle$ برابر است با :

$$|u\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \quad (7.3)$$

یعنی همان اثر عملگر هادامارد روی $|1\rangle$.

$$\sum_x |x\rangle e^{\frac{f(x)\pi i}{2}} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \sum_x |x\rangle e^{(\pi i)f(x)} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

$$e^{\pi i} = \cos \pi + i \sin \pi = -1 \quad (8.3)$$

$$\sum_x (-1)^{f(x)} |x\rangle \left[\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] \xrightarrow{f_w(i)} (-1)^{f_w(i)} |i\rangle \left[\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right]$$

از روابط بالا نتیجه می گیریم که کیوبیت هدف بدون تغییر باقی می ماند و جواب مسئله به اندازه π درجه تغییر فاز می دهد و منفی می شود.

چون کیوبیت هدف تا آخر بدون تغییر باقی می ماند بنابراین در بقیه مسیر از نوشتن آن خودداری می کنیم. شکل عملگری f_w را با I_w نشان می دهیم.

$$I_w = I - 2|w\rangle \langle w| \quad (9.3)$$

که w ها جواب مسئله می‌باشند.

جزء دیگر الگوریتم گراور f است که ضریب همه i ها را به جز $|0\rangle^{\otimes n}$ منفی می‌کند یعنی :

$$|i\rangle \rightarrow (-1)^{1+f_0} |i\rangle$$

شکل عملگر f را با I_0 نشان می‌دهیم که ضریب $|0\rangle^{\otimes n}$ را منفی و بقیه را بدون تغییر می‌گذارد.

$$I_0 = I - 2|0\rangle^{\otimes n}\langle 0|^{\otimes n} \quad (10.3)$$

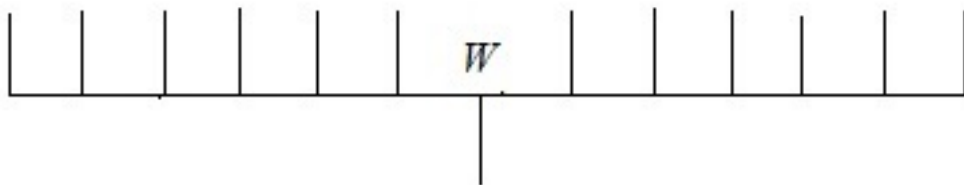
و I_s نیز که جواب را به صورت معکوس درمی‌آورد به صورت زیر می‌باشد :

$$I_s = 2|\psi_1\rangle\langle\psi_1| - I \quad (11.3)$$

در حالت کلی کاربرد عملگر گراور را در اولین حلقه به صورت زیر نمایش می‌دهیم:
با تکرار عملگر گراور دامنه جواب بیشتر و دامنه غیر جواب کمتر می‌شود [۴، ۵].



شکل ۴.۳: بردار حالت ورودی که ترکیب خطی از همه‌ی داده‌های ممکن با ضرایب مساوی است



شکل ۵.۳: بردار حالت ورودی بعد از آن‌که تابع یک‌بار آن را خوانده است



شکل ۶.۳: بردار حالت بعد از انعکاس حول متوسط

توضیح شکل‌های بالا

منظور از W جواب مسئله می‌باشد.

در شکل ۴.۳ در بین چندین حالت مختلف یک حالت را به عنوان جواب مسئله انتخاب می‌کنیم. با تاثیر عملگر I_w بر روی جواب مسئله، جواب منفی می‌شود مانند نشان داده شده در شکل ۵.۳. سپس با تاثیر عملگر I_s روی حالت قبل جواب را معکوس کرده و به اندازه دو برابر دامنه حالت‌های غیر جواب آن را افزایش می‌دهد مانند نشان داده شده در شکل ۶.۳. در نتیجه دامنه جواب رو به افزایش و دامنه غیر جواب رو به کاهش می‌باشد.

۳.۳ تغییر عملگر گراور به عملگر دوران

می‌توان عملگر گراور را در یک نمودار دو بعدی با پایه‌های $|\alpha\rangle$ و $|\beta\rangle$ بنویسیم که $|\alpha\rangle$ کت i ‌هایی است که جزء جواب نیستند و $|\beta\rangle$ کت i ‌هایی است که جزء جواب هستند.

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum'' |i\rangle \quad (12.3)$$

که $\sum''$ یعنی جمع روی i ‌هایی که جواب نیستند و

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum' |i\rangle \quad (13.3)$$

می‌باشد، که $\sum'$ یعنی جمع روی i ‌هایی که جواب هستند.

حال $|\psi_1\rangle$ را می‌توان به این صورت نوشت :

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle = \frac{1}{\sqrt{N}} (\sum'' |i\rangle + \sum' |i\rangle) = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle \quad (14.3)$$

$$= \cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle$$

که در آن عبارات زیر را قرار دادیم :

$$\sin \frac{\theta}{2} = \sqrt{\frac{M}{N}}, \quad \cos \frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$$

بعد از اینکه عملگر I_w اثر می‌کند، دامنه جوابها منفی می‌شود و بنابراین :

$$|\psi_1\rangle \xrightarrow{I_w} |\psi_2\rangle = \cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle \quad (15.3)$$

یعنی $|\psi_1\rangle$ حول $|\alpha\rangle$ انعکاس می‌یابد.

سپس با عمل عملگر I_s بر $|\psi_2\rangle$ این کت حول کت $|\psi_1\rangle$ انعکاس می‌یابد:

$$I_s |\psi_2\rangle = (2 |\psi_1\rangle \langle \psi_1| - I) |\psi_2\rangle = 2 \langle \psi_1 | \psi_2 \rangle |\psi_1\rangle - |\psi_2\rangle \quad (16.3)$$

$$= 2(\cos^2 \frac{\theta}{2} - \sin^2 \frac{\theta}{2}) [\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle] - [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle]$$

$$\rightarrow I_s |\psi_2\rangle = \cos(\frac{3\theta}{2}) |\alpha\rangle + \sin(\frac{3\theta}{2}) |\beta\rangle = |\psi_3\rangle \quad (17.3)$$

همانطور که از شکل زیر پیداست کت $|\psi_3\rangle$ کت انعکاس یافته‌ی $|\psi_2\rangle$ حول $|\psi_1\rangle$ است. کت حالت با اثر عملگر گراور همواره در این صفحه دو بعدی باقی می‌ماند و از آن خارج نمی‌شود. نتیجه حاصل از این دو انعکاس متوالی معادل است با یک دوران به اندازه θ درجه به سمت پایه‌ی $|\beta\rangle$ بنابراین عملگر گراور معادل است با یک ماتریس دوران :

$$G = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \quad (18.3)$$

هرگاه روی حالت اولیه‌ی $|\psi_1\rangle$ عملگر گراور را k بار اثر دهیم یعنی اینکه آن حالت را به اندازه‌ی زاویه‌ی $k\theta$ چرخانده‌ایم. برای اینکه ببینیم این حالت چه مقدار به حالت مطلوب یعنی جواب‌های مسئله $|w\rangle$ نزدیک شده است می‌بایست عنصر ماتریسی $\langle \beta | G^k | \psi_1 \rangle$ را حساب کنیم که برابر خواهد شد با :

$$\langle \beta | G^k | \psi_1 \rangle = \frac{1}{\sqrt{N}} \cos k\theta + \sqrt{\frac{N-1}{N}} \sin k\theta \quad (19.3)$$

که در آن

$$\cos \alpha = \frac{1}{\sqrt{N}} \quad (20.3)$$

و

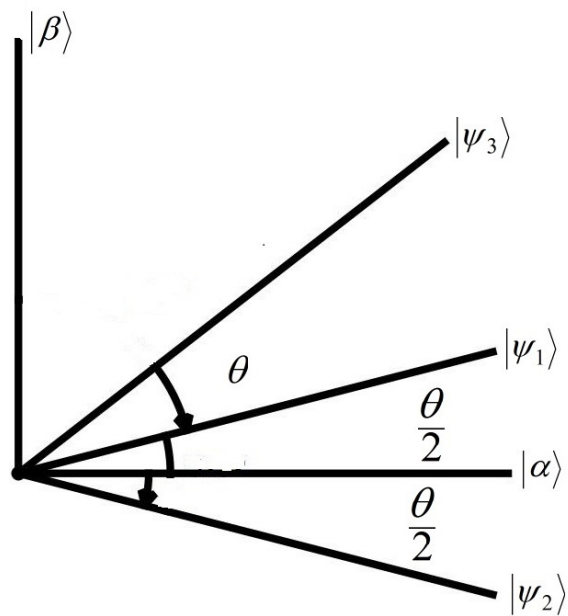
$$\sin \alpha = \sqrt{\frac{N-1}{N}} \quad (21.3)$$

آنگاه خواهیم داشت :

$$\langle \beta | G^k | \psi_1 \rangle = \cos(k\theta - \alpha) \quad (22.3)$$

کت حالت در k امین تکرار عملگر گراور برابر خواهد بود با :

$$G^k |\psi_1\rangle = \cos(\frac{2k+1}{2}\theta) |\alpha\rangle + \sin(\frac{2k+1}{2}\theta) |\beta\rangle \quad (23.3)$$



شکل ۷.۳: تغییر عملگر گراور به عملگر دوران

فصل ۴

الگوریتم جستجوی گراور با استفاده از

دره‌متنیدگی چندطرفه

در این فصل ابتدا ویژگی‌های درهم‌تنیدگی چندطرفه^۱ حالت‌های کوانتومی را بررسی می‌کنیم که شامل حالت‌های تکرار گراور و اوراکل^۲ می‌باشد. بررسی ویژگی‌های درهم‌تنیدگی چندطرفه در الگوریتم گراور با استفاده از درجه جدایی‌پذیری^۳ و اندازه درهم‌تنیدگی^۴ صورت می‌گیرد. سپس توصیفات کمی و کیفی درمورد دینامیک درهم‌تنیدگی^۵ در الگوریتم جستجوی گراور را ارائه می‌دهیم [۵، ۶]. همان طور که در فصل‌های پیشین توضیح دادیم یک نتیجه ویژه در محاسبات کوانتومی کشف بعضی از الگوریتم‌های کوانتومی است که قادر به حل مسائل سریعتر از الگوریتم‌های کلاسیکی می‌باشند. که یکی از این الگوریتم‌های کوانتومی، الگوریتم جستجوی گراور می‌باشد [۱۵].

اخیراً دو فیزیکدان به نام‌های براوس^۶ و ماچیاولو^۷ نقش درهم‌تنیدگی چندطرفه در بعضی از الگوریتم‌های کوانتومی که شامل الگوریتم جستجوی گراور است را کشف کردند. آنها این کار را با مطالعه روی ویژگی‌های درهم‌تنیدگی از حالت‌های وزنی یکسان حقیقی که به آن $REWS$ ^۸ می‌گویند انجام دادند.

۱.۰.۴ حالت‌های وزنی یکسان حقیقی (REWS)

فرض کنیم که $\{|x\rangle | x = 0, \dots, 2^n - 1\}$ پایه‌های محاسباتی n کیوبیتی می‌باشد. آنگاه دو تعریف زیر را خواهیم داشت: [۷]

تعریف ۱. اگر یک حالت n کیوبیتی $|\psi_{REWS}^n\rangle$ به شکل زیر باشد:

$$|\psi_{REWS}^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} a_x |x\rangle$$

که برای هر x داریم: $a_x \in \{1, -1\}$ سپس $|\psi_{REWS}^n\rangle$ یک حالت وزنی یکسان حقیقی n کیوبیتی می‌باشد.

^۱Multipartite entanglement

^۲Oracle

^۳Separable degree

^۴Entanglement measure

^۵Entanglement dynamics

^۶Bruß

^۷Macchiavello

^۸Real equally weighted states

تعریف ۲. اگر یک حالت n کیوبیتی $|\psi_{REWS}^n\rangle$ به صورت زیر باشد :

$$|\psi_{REWS}^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

که در آن $f : \{0, \dots, 2^n - 1\}$ می باشد که یک تابع بولی است. آنگاه $|\psi_{REWS}^n\rangle$ یک حالت وزنی یکسان حقیقی n کیوبیتی می باشد. که $f(x)$ یک تابع وابسته به $|\psi_{REWS}^n\rangle$ می باشد.

در الگوریتم گراور بعد از کاربرد متوالی K بار تکرار گراور حالت زیر بدست می آید: (که در پیوست اثبات شده است)

$$|\psi_K^G\rangle = \frac{\cos[(2k+1)\frac{\theta}{4}]}{\sqrt{2^n} \cos(\frac{\theta}{4})} \sum_{x \in f^{-1}(0)} |x\rangle + \frac{\sin[(2k+1)\frac{\theta}{4}]}{\sqrt{2^n} \sin(\frac{\theta}{4})} \sum_{x \in f^{-1}(1)} |x\rangle \quad (1.4)$$

که $|x\rangle$ پایه‌ی محاسباتی n کیوبیتی را نشان می دهد و $f(x)$ به صورت $\{0, 1\}^n \rightarrow \{0, 1\}$ می باشد. بعد از کاربرد متوالی k بار تکرار اوراکل حالت زیر بدست می آید: (که در پیوست اثبات شده است)

$$|\psi_K^O\rangle = \frac{\cos[2(k-1) + 1)\frac{\theta}{4}]}{\sqrt{2^n} \cos(\frac{\theta}{4})} \sum_{x \in f^{-1}(0)} |x\rangle - \frac{\sin[(2(k-1) + 1)\frac{\theta}{4}]}{\sqrt{2^n} \sin(\frac{\theta}{4})} \sum_{x \in f^{-1}(1)} |x\rangle \quad (2.4)$$

که حالت‌های (۱.۴) و (۲.۴) را می توان به صورت زیر نوشت :

$$|\psi_2\rangle \equiv a \sum_{x \in f^{-1}(0)} |x\rangle + b \sum_{x \in f^{-1}(1)} |x\rangle \quad (3.4)$$

که

$$a, b \in \mathbb{R}$$

و

$$a^2 |f^{-1}(0)| + b^2 |f^{-1}(1)| = 1$$

که حالت‌های بالا را دو مقداری حقیقی^۹ می گویند زیرا $x, x \in f^{-1}(0)$ هایی هستند که متعلق به جواب نمی باشند و $x, x \in f^{-1}(1)$ هایی هستند که متعلق به جواب می باشند و هر دوی آنها دارای مقادیری حقیقی هستند. [۱۱]

۲.۰.۴ درجه جدایی پذیری

فرض می کنیم $|\psi\rangle$ یک حالت خالص از یک سیستم n کیوبیتی باشد. اگر $|\psi\rangle$ را بتوانیم به صورت ضرب تانسوری از حالت‌های خالص از k زیر سیستم منفرد بنویسیم آنگاه به $|\psi\rangle$ جداپذیر مرتبه k ^{۱۰} گفته

^۹Real 2-value states

^{۱۰}K-separable

می‌شود.

با ذکر یک مثال این مطلب را روشن می‌سازیم:

فرض می‌کنیم یک سیستم سه کیوبیتی داریم آنگاه این سیستم دارای هشت عضو می‌باشد. داریم:

$$|\psi\rangle = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |110\rangle, |101\rangle, |111\rangle\}$$

اگر بخواهیم یک حالت خالص از این سیستم سه کیوبیتی را بنویسیم داریم:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \{|001\rangle + |010\rangle\}$$

اکنون می‌خواهیم یک حالت جدایی‌پذیر مرتبه دو برای این حالت خالص بنویسیم آنگاه:

$$|\psi_2\rangle = \frac{1}{\sqrt{4}} \{|0\rangle[|01\rangle + |10\rangle]\}$$

که به صورت ضرب تانسوری از دو حالت خالص می‌باشد. این رابطه جدایی‌پذیر مرتبه دو است.

اگر $\delta(|\psi\rangle) \equiv k$ که در آن $k \in \{1, 2, \dots, n-1\}$ آنگاه به $\delta(|\psi\rangle)$ درجات جدایی‌پذیری از $|\psi\rangle$ می‌گویند.

اگر $\delta(|\psi\rangle) = 1$ باشد آنگاه به $|\psi\rangle$ ، کاملاً درهم‌تنیده^{۱۱} می‌گویند.

و اگر $\delta(|\psi\rangle) = n$ باشد آنگاه به $|\psi\rangle$ کاملاً جدایی‌پذیر^{۱۲} گفته می‌شود.

و اگر $n \geq 3$ و $\delta(|\psi\rangle) \in \{2, 3, \dots, n-1\}$ باشد آنگاه به $|\psi\rangle$ به طور جزئی جدایی‌پذیر^{۱۳} می‌گویند [۷].

۳.۰.۴ تجزیه و تحلیل کیفی حالت‌های دو مقداری با استفاده از درجه جدایی‌پذیری

در این بخش ویژگی‌های درهم‌تنیدگی چند طرفه از حالت‌های دو مقداری که در رابطه (۳.۴) آمده است را با استفاده از درجات جدایی‌پذیری مورد بررسی قرار می‌دهیم: [۱۵]

اگر

$$|f^{-1}(1)| \in \{0, 2^n\}$$

باشد، منظور از عبارت $|f^{-1}(1)|$ با توجه به رابطه (۳.۴) اعدادی هستند که جز جواب می‌باشند. آنگاه:

$$|\psi_2\rangle = \pm \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

که این حالت یک حالت برهم‌نهیده است که کاملاً جدایی‌پذیر می‌باشد.

روابط زیر را در نظر می‌گیریم: [۳]

^{۱۱}Fully entangled

^{۱۲}Fully separable

^{۱۳}Partially separable

$$H = \frac{1}{\sqrt{2}}(|\circ\rangle\langle\circ| + |\circ\rangle\langle 1| + |1\rangle\langle\circ| - |1\rangle\langle 1|)$$

$$\begin{aligned} (H \otimes H)|\circ\rangle|\circ\rangle &= (H|\circ\rangle)(H|\circ\rangle) = \left(\frac{|\circ\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|\circ\rangle+|1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{2}(|\circ\circ\rangle + |\circ 1\rangle + |1\circ\rangle + |11\rangle) \end{aligned} \quad (4.4)$$

ما می‌توانیم $|x\rangle$ را به طور کلی به صورت مقابل نشان دهیم: $x \in \{\circ, 1\}^2$ که از آنجا $|x\rangle$ به صورت یکی از عبارت‌های زیر خواهد شد:

$$|\circ\circ\rangle, |\circ 1\rangle, |1\circ\rangle, |11\rangle$$

و اگر ما بنویسیم $x \in \{\circ, 1\}^3$ آنگاه به این معنی است که $|x\rangle$ به صورت یکی از عبارت‌های زیر می‌باشد:

$$|\circ\circ\circ\rangle, |\circ\circ 1\rangle, |\circ 1\circ\rangle, |1\circ\circ\rangle, |1\circ 1\rangle, |11\circ\rangle, |111\rangle$$

در نتیجه رابطه (4.4) را می‌توانیم به صورت زیر بنویسیم:

$$(H \otimes H)|\circ\rangle|\circ\rangle = H^{\otimes 2}|\circ\rangle^{\otimes 2} = \frac{1}{\sqrt{2^2}} \sum_{x \in \{\circ, 1\}^2} |x\rangle \quad (5.4)$$

در حالت کلی می‌توانیم رابطه (5.4) را به صورت زیر بنویسیم:

$$H^{\otimes n}(|\circ\rangle^{\otimes n}) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{\circ, 1\}^n} |x\rangle \quad (6.4)$$

با توجه به روابط گفته شده، رابطه (6.4) کاملاً جدایی‌پذیر می‌باشد. اگر

$$|f^{-1}(1)| \notin \{\circ, 2^n\}$$

و $a = \circ$ آنگاه:

$$|\psi_2\rangle = \frac{1}{\sqrt{|f^{-1}(1)|}} \sum_{x \in f^{-1}(1)} |x\rangle \quad (7.4)$$

می‌باشد.

رابطه (7.4) در صورتی کاملاً جدایی‌پذیر است اگر و تنها اگر از شروط زیر پیروی کند:

$$|f^{-1}(1)| = 1 \cdot 1$$

$$|f^{-1}(1)| = 2^m \cdot 2 \quad \text{و} \quad |\psi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=\circ}^{2^m-1} |x\rangle \otimes |w\rangle \quad \text{باشد که در آن داریم:}$$

$$m \in \{1, 2, \dots, n-1\}$$

و

$$w \in \{\circ, 1\}^{n-m}$$

واضح است که اگر رابطه (۷.۴) کاملاً جدایی‌پذیر باشد می‌تواند به صورت زیر نوشته شود: [۱۱]

$$\otimes_{i=1}^n (\alpha_i |0\rangle + \beta_i |1\rangle)$$

این رابطه با توجه به شروط ۱ و ۲ و همچنین با توجه به روابط گفته شده در ابتدای این بخش بدست آمده است.

که در آن $\alpha_i, \beta_i \in R$ می‌باشند. عبارت

$$|f^{-1}(1)| \notin \{0, 2^n\}$$

نشان می‌دهد که برای هر i یا

$$\alpha_i = \beta_i$$

یا

$$\alpha_i \cdot \beta_i = 0$$

می‌باشد.

واضح است برای رابطه

$$|f^{-1}(1)| \notin \{0, 2^n\}$$

و $b = 0$ نتایج مشابهی را داریم.

اگر $a = -b$ داریم :

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \quad (8.4)$$

که این حالت بعد از کاربرد اولین مرحله اوراکل بدست می‌آید که برای x هایی که متعلق به جواب هستند $f(x) = 1$ و برای x هایی که متعلق به جواب نیستند $f(x) = 0$ می‌باشد.

فرض می‌کنیم $|f^{-1}(1)| = 1$ باشد در نتیجه رابطه (۸.۴) مطابق با یک حالت برهم‌نهیده وزنی یکسان حقیقی می‌باشد. که در آن همه داده‌ها با فاز مثبت ظاهر می‌شوند به جز یک داده که همان جواب مسئله است با فاز منفی ظاهر می‌شود. [۱۱] همچنین این حالت یک حالت کاملاً درهم‌تنیده است. زیرا یک حالت جدایی‌پذیر شامل حداقل دو علامت منفی خواهد بود. تعداد حالات ممکن با $|f^{-1}(1)| = 1$ برابر 2^n است. زیرا فاز منفی یک می‌تواند جلوی هر یک از 2^n داده ظاهر شود.

مثال :

$$|\psi\rangle = |00\rangle + |01\rangle - |10\rangle + |11\rangle$$

$$= |0\rangle(|0\rangle + |1\rangle) - |1\rangle(|0\rangle - |1\rangle)$$

رابطه بالا دارای یک جواب می‌باشد یعنی یکی از داده‌ها با فاز منفی ظاهر شده است. بنابراین نمی‌توانیم در حالت کلی به صورت جدایی‌پذیر بنویسیم، در نتیجه کاملاً درهم‌تنیده است.

به طور کلی باید به خاطر داشته باشیم شرط لازم و ضروری برای اینکه رابطه‌ی (۸.۴) کاملاً جدایی‌پذیر باشد این است که خروجی $f(x)$ یا تابعی ثابت باشد یا تابعی متوازن. برای $|f^{-1}(1)|$ های فرد هرگز رابطه (۸.۴) را نمی‌توانیم به صورت ضرب تانسوری از حالت‌ها بنویسیم زیرا منجر به یک تعدادی از فازهای منفی خواهد شد. بنابراین هر وقت تعدادی از جواب‌ها فرد باشند رابطه (۸.۴) کاملاً درهم‌تنیده است. [۱۱]
فرض می‌کنیم:

$$|f^{-1}(1)| \notin \{0, 2^n\}$$

$a \neq -b$ و $\alpha_i \cdot \beta_i \neq 0$ در این صورت اگر $|\psi_2\rangle$ جدایی‌پذیر مرتبه ۲ باشد به صورت زیر می‌باشد:

$$|\psi_2\rangle = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right]^{\otimes k} \otimes \sqrt{2^k} \left[a \sum_{x \in S} |x\rangle + b \sum_{x \in T} |x\rangle \right] \quad (9.4)$$

که در آن $k \in \{1, 2, \dots, n-1\}$ و $S \cap T = \emptyset$ و $S \cup T = \{0, 1\}^{n-k}$ و $|T| = \frac{|f^{-1}(1)|}{2^k}$ می‌باشد.

از آنجایی که $|\psi_2\rangle$ جدایی‌پذیر مرتبه ۲ می‌باشد، بنابراین یک $k \in \{1, 2, \dots, n-1\}$ وجود دارد به طوری که $|\psi_2\rangle$ به صورت زیر باشد:

$$|\psi_2\rangle = \left[\sum_{i=0}^{2^k-1} \alpha_i |i\rangle \right] \otimes \left[\sum_{j=0}^{2^{n-k}-1} \beta_j |j\rangle \right] \quad (10.4)$$

بدون از دست دادن کلیت مسئله فرض می‌کنیم $\alpha_i, \beta_j \in R$ باشد. واضح است برای هر i, j

$$\alpha_i \cdot \beta_j \neq 0$$

می‌باشد زیرا

$$a \cdot b \neq 0$$

است.

فرض می‌کنیم که دو رابطه $\sum_{i=0}^{2^k-1} \alpha_i |i\rangle$ و $\sum_{j=0}^{2^{n-k}-1} \beta_j |j\rangle$ به شکل حالت برهم‌نهی یکنواخت نبوند، که این مورد نشان دهنده این است که

$$i_1, i_2 \in \{0, 1, \dots, 2^k - 1\}$$

و

$$j_1, j_2 \in \{0, 1, \dots, 2^{n-k} - 1\}$$

به طوری که $\alpha_{i_1} \neq \alpha_{i_2}$ و $\beta_{j_1} \neq \beta_{j_2}$ می‌باشد.

از آنجایی که $|\psi_2\rangle$ حالت حقیقی دو مقداری است، آنگاه

$$\alpha_{i_1} \beta_{j_1} = \alpha_{i_2} \beta_{j_2}$$

و

$$\alpha_{i_1} \beta_{j_2} = \alpha_{i_2} \beta_{j_1}$$

که نشان می‌دهد $\beta_{j_1} = -\beta_{j_2}$ است، بنابراین

$$\alpha_{i_1}\beta_{j_1} = -\alpha_{i_1}\beta_{j_2}$$

است که در تضاد با $a \neq -b$ می‌باشد.

بر طبق روابط بالا برای هر

$$|f^{-1}(1)| \notin \{0, 2^n\}$$

تعداد حالتها جدایی‌پذیر مرتبه ۲ به صورت: [۱۱]

$$nB(2^{n-1}, \frac{|f^{-1}(1)|}{2})$$

داده می‌شود. بنابراین اگر

$$|f^{-1}(1)| < 2^{\frac{n}{2}}$$

باشد، مجموعه‌ای از حالتها جدایی‌پذیر مرتبه ۲ با استفاده از رابطه [۱۱]

$$\lim_{n \rightarrow \infty} \frac{nB(2^{n-1}, \frac{|f^{-1}(1)|}{2})}{B(2^n, |f^{-1}(1)|)} \simeq 0 \quad (11.4)$$

بدست می‌آید. که B در رابطه بالا نشان دهنده ضریب دو جمله ای می‌باشد. با توجه به مطالب و

روابط گفته شده نتیجه می‌گیریم که برای هر

$$|f^{-1}(1)| \in (0, 2^{\frac{n}{2}})$$

حالتها در رابطه (۳.۴) در اکثر موارد کاملاً درهمتیده هستند [۱۵].

علاوه بر این، نتایج زیر نیز حاصل می‌گردد:

فرض کنیم:

$$\begin{cases} |f^{-1}(1)| = 2^{n-1} \\ a \neq -b \\ a.b \neq 0 \end{cases} \quad (12.4)$$

آنگاه نتایج زیر بدست می‌آید:

اگر $|f^{-1}(1)| = 2^{n-1}$ و $|\psi_2\rangle$ به فرم یکی از روابط زیر باشد

$$[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]^{\otimes(n-1)} \otimes \sqrt{2^{n-1}}(a|0\rangle + b|1\rangle)$$

و

$$[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]^{\otimes(n-1)} \otimes \sqrt{2^{n-1}}(b|0\rangle + a|1\rangle)$$

آنگاه $|\psi_2\rangle$ کاملاً جداپذیر می‌باشد. اگر $|f^{-1}(1)|$ ، فرد باشد آنگاه $|\psi_2\rangle$ کاملاً درهمتیده

می‌باشد. اگر $|f^{-1}(1)| = 2^q(2p+1)$ باشد که در آن $p \in N$ و $q \in Z^+$ باشد آنگاه

$|\psi_2\rangle$ یا کاملاً درهمتنیده است یا جدایی‌پذیر مرتبه k می‌باشد به شرطی که $k \geq 2$ باشد. اگر $|\psi_2\rangle$ جدایی‌پذیر مرتبه k باشد آنگاه $k \leq q+1$ و $|\psi_2\rangle$ به فرم زیر تبدیل می‌شود:

$$\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes k-1} \otimes \sqrt{2^{k-1}} \left(a \sum_{x \in S} |x\rangle + b \sum_{x \in T} |x\rangle\right)$$

که در آن $S \cup T = \{0, 1\}^{n-k+1}$ و $S \cap T = \Phi$ و $|T| = 2^{q-k+1}(2p+1)$ می‌باشد

۴.۰.۴ تجزیه و تحلیل کمی حالت‌های دو مقداری با استفاده از اندازه‌ی

درهمتنیدگی

در این بخش می‌خواهیم از اندازه درهمتنیدگی برای تعیین درهمتنیدگی چندطرفه حالت‌های حقیقی دو مقداری استفاده کنیم. [۱۵]

۵.۰.۴ عدد اشمیت

یک سیستم مرکب از ضرب $H_A \otimes H_B$ را در نظر می‌گیریم. فرض می‌کنیم $|\psi\rangle \in H_A \otimes H_B$ که یک حالت خالص از این سیستم باشد آنگاه بسط $|\psi\rangle$ به صورت زیر می‌باشد:

$$|\psi\rangle = \sum_i \lambda_i |a_i\rangle |b_i\rangle$$

که $|a_i\rangle$ حالت‌های متعلق به سیستم A هستند و $|b_i\rangle$ حالت‌های متعلق به سیستم B هستند. که این حالت‌ها پایه‌های اشمیت برای سیستم A و سیستم B می‌باشند. [۲] ضریب بسط λ_i که در آن $\lambda_i > 0$ و $\sum_i \lambda_i^2 = 1$ است را ضریب اشمیت^{۱۴} می‌گویند.

ضرایب اشمیت با استفاده از رابطه زیر محاسبه می‌شوند:

$$\rho = |\psi\rangle \langle \psi| \quad (۱۳.۴)$$

$$\rho_A = Tr_B(|\psi\rangle \langle \psi|) \quad (۱۴.۴)$$

این ماتریس دارای ویژه مقادیر برابر λ_i^2 است.

عدد اشمیت تعداد ویژه مقادیر غیر از صفر λ_i می‌باشد [۲].

اگر عدد اشمیت^{۱۵} مساوی یک باشد آنگاه یک حالت جدایی‌پذیر داریم و اگر عدد اشمیت بزرگتر از یک باشد آنگاه یک حالت درهمتنیده خواهیم داشت.

مثال: [۳]

^{۱۴}Schmidt coefficients

^{۱۵}Schmidt number

حالت زیر را در نظر می‌گیریم :

$$|\psi\rangle = \frac{1}{\sqrt{4}}(|\circ\circ\rangle - |\circ 1\rangle - |1\circ\rangle + |11\rangle)$$

می‌خواهیم ببینیم که این حالت جداپذیر است یا درهم‌تنیده.

$$\begin{aligned}\rho &= |\psi\rangle\langle\psi| = \frac{1}{\sqrt{4}}(|\circ\circ\rangle\langle\circ\circ| - |\circ\circ\rangle\langle\circ 1| - |\circ\circ\rangle\langle 1\circ| + |\circ\circ\rangle\langle 11| - |\circ 1\rangle\langle\circ\circ| \\ &+ |\circ 1\rangle\langle\circ 1| + |\circ 1\rangle\langle 1\circ| - |\circ 1\rangle\langle 11| - |1\circ\rangle\langle\circ\circ| + |1\circ\rangle\langle\circ 1| + |1\circ\rangle\langle 1\circ| \\ &- |1\circ\rangle\langle 11| + |11\rangle\langle\circ\circ| - |11\rangle\langle\circ 1| - |11\rangle\langle 1\circ| + |11\rangle\langle 11|) \\ \rho_A &= Tr_B(|\psi\rangle\langle\psi|) = \langle\circ|\psi\rangle\langle\psi|\circ\rangle + \langle 1|\psi\rangle\langle\psi|1\rangle \\ &= \frac{1}{\sqrt{4}}(|\circ\rangle\langle\circ| - |\circ\rangle\langle 1| - |1\rangle\langle\circ| + |1\rangle\langle 1|) + \frac{1}{\sqrt{4}}(|\circ\rangle\langle\circ| - |\circ\rangle\langle 1| - |1\rangle\langle\circ| + |1\rangle\langle 1|) \\ &= \frac{1}{\sqrt{4}}(|\circ\rangle\langle\circ| - |\circ\rangle\langle 1| - |1\rangle\langle\circ| + |1\rangle\langle 1|)\end{aligned}$$

$$\rho_A = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

ویژه مقادیر این ماتریس برابر با : $\lambda_1 = 1$, $\lambda_2 = 0$ عدد اشمیت برابر است با تعداد ویژه مقادیر غیر صفر این ماتریس و از آنجایی که تعداد این ویژه مقادیر غیر صفر یک است بنابراین یک حالت جداپذیر می‌باشد.
فرض کنیم $\chi(|\psi\rangle)$ بیشترین عدد اشمیت از حالت خالص $|\psi\rangle$ باشد، که

$$\chi(|\psi\rangle) \equiv \max_A rank[Tr_B(|\psi\rangle\langle\psi|)] \quad (15.4)$$

۶.۰.۴ رنک یا رتبه یک ماتریس

رنک یا رتبه یک ماتریس A برابر با بیشترین تعداد ستونها (یا سطرها) مستقل خطی در آن ماتریس است.

$$A_{n \times n} \rightarrow |A| \neq 0 \rightarrow Rank(A) = n \rightarrow full Rank$$

$$A_{m \times n} \rightarrow Rank(A) = \min(m, n) \rightarrow full Rank$$

$$A_{m \times n} \rightarrow Rank(A) < \min(m, n) \rightarrow Rank deficiency$$

منظور از $|A|$ دترمینان ماتریس A می‌باشد. برای اینکه رنک یک ماتریس را بدست آوریم باید

ابتدا آن ماتریس را از طریق حل گاوس جردن حل کنیم سپس یک تعداد از سطرها صفر می‌شوند در نتیجه تعداد سطرهایی که صفر نیستند همان رتبه ماتریس می‌باشند.

رابطه (۱۵.۴) دارای ویژگیهای زیر می‌باشد: [۱۵]

۱. $\chi(|\psi\rangle) \in \{1, 2, \dots, 2^{\lfloor \frac{n}{2} \rfloor}\}$ است. اگر $|\psi\rangle$ کاملاً جدایی پذیر باشد، آنگاه $\chi(|\psi\rangle) = 1$ میشود.

۲. $\chi(|\psi\rangle \otimes |\psi'\rangle) = \chi(|\psi\rangle) \cdot \chi(|\psi'\rangle)$

در اینجا به طور کمی ویژگی‌های درهم‌تنیدگی چندطرفه از حالت‌های حقیقی دو مقداری $|\psi_2\rangle$ در فرمول (۳.۴) را مستقیماً با استفاده از بیشترین عدد اشمیت $\chi(|\psi_2\rangle)$ بررسی می‌کنیم.

بر طبق نتایج به دست آمده از قسمت‌های قبلی و ویژگی‌های بیشترین عدد اشمیت می‌توانیم چندین نتیجه زیر را بدست آوریم:

۱. اگر $|f^{-1}(1)| \in \{0, 2^n\}$ باشد آنگاه $\chi = 1$.

۲. فرض کنیم: $|f^{-1}(1)| \notin \{0, 2^n\}$ و $a = 0$ باشد آنگاه:

الف. اگر $\chi = 1$ باشد، آنگاه $m \in \{0, 1, \dots, n\}$ به طوری که $|f^{-1}(1)| = 2^m$ می‌باشد.

ب. اگر $|f^{-1}(1)| = 1$ باشد آنگاه $\chi = 1$ می‌باشد.

۳. فرض کنیم $a = -b$ آنگاه:

الف. اگر $\chi = 1$ باشد، آنگاه $|f^{-1}(1)| = |f^{-1}(0)| = 2^{n-1}$

ب. اگر $|f^{-1}(1)| = 2^{n-1}$ باشد، آنگاه $\chi \in \{1, 2, \dots, 2^{\lfloor \frac{n}{2} \rfloor}\}$

ج. اگر $|f^{-1}(1)| \neq 2^{n-1}$ باشد، آنگاه $\chi \in \{2, 3, \dots, \min(|f^{-1}(1)| + 1, 2^{\lfloor \frac{n}{2} \rfloor})\}$

د. اگر $|f^{-1}(1)| = 1$ باشد، آنگاه $\chi = 2$.

۴. فرض کنیم $|f^{-1}(1)| \notin \{0, 2^n\}$ و $a \neq -b$ و $a.b \neq 0$ باشد آنگاه:

الف. اگر $\chi = 1$ باشد، آنگاه $|f^{-1}(1)| = |f^{-1}(0)| = 2^{n-1}$.

ب. اگر $|f^{-1}(1)| = 2^{n-1}$ باشد، آنگاه $\chi \in \{1, 2, \dots, 2^{\lfloor \frac{n}{2} \rfloor}\}$.

ج. اگر $|f^{-1}(1)| \neq 2^{n-1}$ باشد، آنگاه $\chi \in \{2, 3, \dots, \min(|f^{-1}(1)| + 1, 2^{\lfloor \frac{n}{2} \rfloor})\}$.

د. اگر $|f^{-1}(1)| = 1$ باشد، آنگاه $\chi = 2$.

اکنون روابط موجود در رابطه (د) قسمت ۳ و رابطه (د) قسمت ۴ را بدست می‌آوریم:

فرض می‌کنیم: $|\psi_2\rangle = a \sum_{x=1}^{2^{n-1}} |x\rangle + b|0\rangle$ باشد و $a.b \neq 0$ آنگاه می‌توانیم حالت

کلی ماتریس چگالی $|\psi_2\rangle\langle\psi_2|$ را به صورت زیر بدست آوریم که ابتدا به ازای مقدار

$n = 2$ ماتریس چگالی را بدست می‌آوریم :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad (16.4)$$

$$|2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |3\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad (17.4)$$

$$a \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + a \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + a \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + b \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} b \\ a \\ a \\ a \end{pmatrix}$$

پس ماتریس چگالی به صورت زیر می‌شود:

$$|\psi_2\rangle \langle \psi_2| = \begin{pmatrix} b \\ a \\ a \\ a \end{pmatrix} \begin{pmatrix} b & a & a & a \end{pmatrix} = \begin{pmatrix} b^2 & ab & ab & ab \\ ab & a^2 & a^2 & a^2 \\ ab & a^2 & a^2 & a^2 \\ ab & a^2 & a^2 & a^2 \end{pmatrix} \quad (18.4)$$

آنگاه حالت کلی به صورت زیر می باشد :

$$|\psi_2\rangle \langle \psi_2| = \begin{pmatrix} b^2 & ab & ab & \dots & ab \\ ab & a^2 & a^2 & \dots & a^2 \\ ab & a^2 & a^2 & \dots & a^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ ab & a^2 & a^2 & \dots & a^2 \end{pmatrix} \quad (۱۹.۴)$$

ماتریس چگالی کاهش یافته $tr_B(|\psi_2\rangle \langle \psi_2|)$ برای هر تقسیم دوقسمتی که m کیوبیت

در A و $n - m$ کیوبیت در B هستند به صورت زیر نوشته می شود:

$$\begin{pmatrix} b^2 + (2^{n-m} - 1)a^2 & ab + (2^{n-m} - 1)a^2 & ab + (2^{n-m} - 1)a^2 & \dots & ab + (2^{n-m} - 1)a^2 \\ ab + (2^{n-m} - 1)a^2 & 2^{n-m}a^2 & 2^{n-m}a^2 & \dots & 2^{n-m}a^2 \\ ab + (2^{n-m} - 1)a^2 & 2^{n-m}a^2 & 2^{n-m}a^2 & \dots & 2^{n-m}a^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ ab + (2^{n-m} - 1)a^2 & 2^{n-m}a^2 & 2^{n-m}a^2 & \dots & 2^{n-m}a^2 \end{pmatrix}_{2^m \times 2^m}$$

که $a, b \neq 0$ و $rank[tr_B(|\psi_2\rangle \langle \psi_2|)] = 2$ [۱۵]

۱.۴ دینامیک درهمتنیدگی الگوریتم جستجوی گراور

در اینجا تنها درهمتنیدگی چندطرفه از اولین n کیوبیت در الگوریتم جستجوی گراور را در نظر می گیریم. [۴] اولین حالت یا $|\circ\rangle^{\otimes n}$ می باشد که کاملاً جداپذیر و با مقدار $\chi = 1$ می باشد. پس از آن حالت $|\psi^G\rangle$ است. این حالت از تاثیر n بار عملگر هادامارد روی حالت اولیه $|\circ\rangle$ بدست می آید.

که شکل ماتریسی عملگر هادامارد به صورت زیر می باشد:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (۲۰.۴)$$

می باشد و شکل عملگری آن نیز به صورت زیر می باشد:

$$H = [|\circ\rangle \langle \circ| + |\circ\rangle \langle 1| + |1\rangle \langle \circ| - |1\rangle \langle 1|] \quad (۲۱.۴)$$

واضح است که $|\psi^G\rangle$ نیز کاملاً جداپذیر و $\chi = 1$ می‌باشد.
 از آنجا $R = [\frac{\pi-\theta}{4} - \frac{1}{4}]$ که حالت تکرار گراور با $G \equiv PO$ بدست آمده است که P معکوسی است که توسط اپراتور $I - |\psi^G\rangle\langle\psi^G|$ بدست می‌آید.
 در نهایت ما می‌توانیم یکی از جوابهای خواسته شده را با احتمال بالا بدست آوریم.
 اگر $|f^{-1}(1)| \geq 2^{n-1}$ باشد آنگاه تصویر دینامیکی الگوریتم جستجوی گراور به صورت زیر می‌باشد:

$$|0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} |\psi^G\rangle \xrightarrow{O} |\psi_1^O\rangle \xrightarrow{P} |\psi_1^G\rangle \xrightarrow{O} \dots \xrightarrow{O} |\psi_R^O\rangle \xrightarrow{P} |\psi_R^G\rangle \quad (22.4)$$

توضیح تصویر دینامیکی بالا

ابتدا کت اولیه را در الگوریتم گراور بدست می‌آوریم که به صورت زیر می‌باشد :

$$|\psi^G\rangle = \cos \frac{\theta}{4} |\alpha\rangle + \sin \frac{\theta}{4} |\beta\rangle \quad (23.4)$$

سپس عمل اوراکل را روی آن اثر می‌دهیم تا کت اولیه اوراکل بدست آید که به صورت زیر می‌شود :

$$|\psi_1^O\rangle = \cos \frac{\theta}{4} |\alpha\rangle - \sin \frac{\theta}{4} |\beta\rangle \quad (24.4)$$

آنگاه با تاثیر P روی آن اولین مرحله تکرار گراور بدست می‌آید که به صورت زیر می‌باشد :

$$|\psi_1^G\rangle = \cos \frac{3\theta}{4} |\alpha\rangle + \sin \frac{3\theta}{4} |\beta\rangle \quad (25.4)$$

برای اینکه به جواب مسئله دست یابیم باید این عمل تکرار گراور را چندین مرحله انجام دهیم که بعد از مرحله اول مراحل بعدی با تاثیر عمل اوراکل روی $|\psi^G\rangle$ بدست می‌آید.

۱.۱.۴ تجزیه و تحلیل کیفی الگوریتم جستجوی گراور

بر طبق نکات و روابط گفته شده ما می‌توانیم به نتایج زیر نیز دست یابیم: [۱۵]

۱. فرض می‌کنیم $|f^{-1}(1)|$ فرد باشد سپس داریم :

الف. کل عبارتهای $|\psi_R^O\rangle, |\psi_{R-1}^G\rangle, |\psi_{R-1}^O\rangle, \dots, |\psi_1^G\rangle, |\psi_1^O\rangle$ کاملاً در همتنیده

می‌باشند.

ب. اگر $\cos[(2R+1)\frac{\theta}{4}] \neq 0$ باشد، آنگاه $|\psi_R^G\rangle$ کاملاً درهمتنیده می‌باشد. در غیر این صورت به طور جزئی جداپذیر می‌باشد ولی کاملاً جداپذیر نخواهد بود.

۲. فرض می‌کنیم $|f^{-1}(1)| = 2^q(2p+1)$ می‌باشد که در آن $p \in N$ و $q \in Z^+$ هستند، آنگاه داریم:

الف. با فرض اینکه $|\psi_1^O\rangle$ کاملاً درهمتنیده باشد عبارات $|\psi_{R-1}^G\rangle, |\psi_{R-1}^O\rangle, \dots, |\psi_1^G\rangle$ و $|\psi_R^O\rangle$ کاملاً درهمتنیده می‌باشند. اگر $\cos[(2R+1)\frac{\theta}{4}] \neq 0$ باشد آنگاه همچنین $|\psi_R^G\rangle$ کاملاً درهمتنیده می‌باشد.

ب. فرض می‌کنیم $|\psi_1^O\rangle$ به شکل زیر باشد:

$$[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]^{\otimes k-1} \otimes \sqrt{2^{k-1}}(\sum_{x \in S} |x\rangle - \sum_{x \in T} |x\rangle)$$

که در آن $k \in \{2, \dots, q+1\}$ و $S \cup T = \{0, 1\}^{n-k+1}$ و $S \cap T = \Phi$ است. آنگاه کل عبارات $|\psi_1^G\rangle, |\psi_2^O\rangle, \dots, |\psi_{R-1}^G\rangle$ و $|\psi_R^O\rangle$ جداپذیر مرتبه k می‌باشند. علاوه بر این $\forall i \in \{1, 2, \dots, R-1\}$ ، و $|\psi_i^G\rangle$ به شکل زیر می‌باشد:

$$[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]^{\otimes k-1} \otimes \sqrt{2^{k-1}}(\frac{\cos[(2i+1)\frac{\theta}{4}]}{\sqrt{2^n} \cos(\frac{\theta}{4})} \sum_{x \in S} |x\rangle + \frac{\sin[(2i+1)\frac{\theta}{4}]}{\sqrt{2^n} \sin(\frac{\theta}{4})} \sum_{x \in T} |x\rangle)$$

و $|\psi_{i+1}^O\rangle$ نیز به شکل زیر می‌باشد:

$$[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]^{\otimes k-1} \otimes \sqrt{2^{k-1}}(\frac{\cos[(2i+1)\frac{\theta}{4}]}{\sqrt{2^n} \cos(\frac{\theta}{4})} \sum_{x \in S} |x\rangle - \frac{\sin[(2i+1)\frac{\theta}{4}]}{\sqrt{2^n} \sin(\frac{\theta}{4})} \sum_{x \in T} |x\rangle)$$

اگر

$$\cos[(2R+1)\frac{\theta}{4}] \neq 0$$

باشد آنگاه $|\psi_R^G\rangle$ جداپذیر مرتبه k می‌باشد. در غیر این صورت جداپذیر مرتبه j است به شرطی که $j \geq k$ باشد.

ج. اگر $\cos[(2R+1)\frac{\theta}{4}] = 0$ باشد آنگاه $|\psi_R^G\rangle$ کاملاً جداپذیر می‌باشد.

اگر $2^{\frac{n}{4}} \leq 2^q(2p+1) = |f^{-1}(1)|$ و $p \geq 1$ باشد ملاحظه می‌کنیم که درهم‌تنیدگی

چندطرفه حالت‌های وزنی یکسان حقیقی خیلی پیچیده می‌شود.

بنابراین $|\psi_1^O\rangle$ با شرط این که $k \geq 2$ $\delta(|\psi_1^O\rangle) = k$ باشد ممکن است فرم متفاوتی

با فرمول (۲۱.۴) داشته باشد به این مفهوم که همه درجات جدایی‌پذیری عبارات

$$|\psi_1^G\rangle, |\psi_2^O\rangle, \dots, |\psi_{R-1}^G\rangle, |\psi_R^O\rangle$$

ممکن است کوچکتر از k باشد به طوری که $|\psi_1^O\rangle$ جدایی‌پذیر مرتبه k می‌باشد.

۲.۱.۴ تجزیه و تحلیل کمی دینامیک الگوریتم جستجوی گراور

بر طبق نتایج بدست آمده در قسمت قبل نتایج زیر به دست می‌آیند :

۱. فرض می‌کنیم $|f^{-1}(1)|$ فرد باشد آنگاه :

$$\chi(|\psi_1^O\rangle), \chi(|\psi_1^G\rangle), \dots, \chi(|\psi_{R-1}^O\rangle), \chi(|\psi_{R-1}^G\rangle), \chi(|\psi_R^O\rangle) \in \text{الف.}$$

$$\{2, 3, \dots, \min(|f^{-1}(1)| + 1, 2^{\lfloor \frac{n}{4} \rfloor})\}$$

در حالت خاص اگر $|f^{-1}(1)| = 1$ باشد آنگاه داریم :

$$\chi(|\psi_1^O\rangle) = \chi(|\psi_1^G\rangle) = \dots = \chi(|\psi_{R-1}^O\rangle) = \chi(|\psi_{R-1}^G\rangle) = \chi(|\psi_R^O\rangle) = 2$$

ب. اگر $\cos[(2R+1)\frac{\theta}{4}] = 0$ و $|f^{-1}(1)| = 1$ باشد آنگاه :

۲. فرض می‌کنیم $2^{\frac{n}{4}} < 2^q(2p+1) = |f^{-1}(1)|$ باشد که در آن $p \in N$ و $q \in Z^+$ باشد آنگاه :

الف. فرض می‌کنیم که $|\psi_1^O\rangle$ کاملاً درهم‌تنیده باشد آنگاه :

$$\chi(|\psi_1^O\rangle), \chi(|\psi_1^G\rangle), \dots, \chi(|\psi_{R-1}^O\rangle), \chi(|\psi_{R-1}^G\rangle), \chi(|\psi_R^O\rangle) \in$$

$$\{2, 3, \dots, \min(|f^{-1}(1)| + 1, 2^{\lfloor \frac{n}{4} \rfloor})\}$$

می‌باشد. اگر $\cos[(2R+1)\frac{\theta}{4}] \neq 0$ باشد آنگاه :

$$\chi(|\psi_R^G\rangle) \in \{2, 3, \dots, \min(|f^{-1}(1)| + 1, 2^{\lfloor \frac{n}{4} \rfloor})\}$$

است در غیر این صورت

$$\chi(|\psi_R^G\rangle) \in \{2, 3, \dots, \min(|f^{-1}(1)|, 2^{\lfloor \frac{n}{r} \rfloor})\}$$

می‌شود.

ب. فرض می‌کنیم که $\sqrt{2^{k-1}}(\sum_{x \in S} |x\rangle - \sum_{x \in T} |x\rangle)$ در آن $k \in \{2, \dots, q+1\}$ و $S \cap T = \emptyset$ و $S \cup T = \{0, 1\}^{n-k+1}$ و $|T| = 2^{q-k+1}(2p+1)$ است و $\sqrt{2^{k-1}}(\sum_{x \in S} |x\rangle - \sum_{x \in T} |x\rangle)$ کاملاً در هم‌تنیده باشد آنگاه:

اگر $\cos[(2R+1)\frac{\theta}{r}] = 0$ و $P = 0$ و $|\psi_1^O\rangle$ جدایی‌پذیر مرتبه $q+1$ باشد آنگاه داریم:

$$\chi(|\psi_1^O\rangle), \chi(|\psi_1^G\rangle), \dots, \chi(|\psi_{R-1}^O\rangle), \chi(|\psi_{R-1}^G\rangle), \chi(|\psi_R^O\rangle)$$

$$\in \{2, 3, \dots, \min(|T|+1, 2^{\lfloor \frac{n-1+k}{r} \rfloor})\}$$

و

$$\chi(|\psi_1^O\rangle) = \chi(|\psi_1^G\rangle) = \dots = \chi(|\psi_{R-1}^O\rangle) = \chi(|\psi_{R-1}^G\rangle) = \chi(|\psi_R^O\rangle) = 2$$

علاوه بر این اگر $\cos[(2R+1)\frac{\theta}{r}] \neq 0$ باشد آنگاه

$$\chi(|\psi_R^G\rangle) \in \{2, 3, \dots, \min(|T|+1, 2^{\lfloor \frac{n-1+k}{r} \rfloor})\}$$

در غیر این صورت

$$\chi(|\psi_R^G\rangle) \in \{1, 2, 3, \dots, \min(|T|, 2^{\lfloor \frac{n-1+k}{r} \rfloor})\}$$

می‌شود. ج. اگر $\cos[(2R+1)\frac{\theta}{r}] = 0$ و $P = 0$ باشد و $|\psi_1^O\rangle$ جدایی‌پذیر مرتبه

$q+1$ باشد آنگاه $\chi(|\psi_R^G\rangle) = 1$ است.

۲.۴ نتایج

با توجه به رابطه

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

اگر $f^{-1}(1) \notin \{0, 2^n\}$ آنگاه اگر تعداد جواب‌های مسئله فرد باشند در نتیجه یک حالت کاملاً درهم‌تنیده داریم و اگر تعداد جواب‌های مسئله زوج باشند یک حالت کاملاً جدایی‌پذیر داریم. که با توجه به بیشترین عدد اشمیت در صورتی یک حالت جدایی‌پذیر

داریم که $\chi(|\psi\rangle)$ یعنی بیشترین عدد اشمیت یک شود. ما توصیفات کمی و کیفی از درهم‌تنیدگی دینامیک الگوریتم جستجوی گراور را بیان کردیم.

فرض می‌کنیم $|f^{-1}(1)| \in (0, 2^n)$ می‌باشد. در بیشتر موارد $\cos[(2R+1)\frac{\theta}{4}] \neq 0$ است بنابراین درجات جدپذیری عبارت‌های $|\psi_1^O\rangle, |\psi_1^G\rangle, \dots, |\psi_R^O\rangle, |\psi_R^G\rangle$ تقریباً یکنواخت و ثابتند.

بنابراین در بیشتر موارد عبارت $|\psi_1^O\rangle$ کاملاً در هم‌تنیده می‌باشد و از آنجا عبارات $|\psi_1^G\rangle, \dots, |\psi_R^O\rangle, |\psi_R^G\rangle$ نیز کاملاً در هم‌تنیده می‌باشد.

بنابراین دینامیک الگوریتم جستجوی گراور تقریباً با حالت‌های کاملاً در هم‌تنیده پر شده است و بیشترین اعداد اشمیت عبارات $|\psi_1^G\rangle, |\psi_1^O\rangle, |\psi_1^G\rangle, \dots, |\psi_R^O\rangle$ ، در یک مرتبه یکسانی هستند.

(پیوست) اثبات روابط موجود در

فصل آخر

۱.۲.۴ اثبات فرمول ۱ فصل ۴

جمع روی i هایی که جواب نیستند

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum'' |i\rangle$$

جمع روی i هایی که جواب هستند

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum' |i\rangle \quad ,$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle = \frac{1}{\sqrt{N}} (\sum'' |i\rangle + \sum' |i\rangle)$$

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$$

$$|\psi_1^G\rangle = \cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle$$

$$\Rightarrow |\psi_1^G\rangle \xrightarrow{I_2} \cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle = \psi_2$$

$$\Rightarrow |\psi_2^G\rangle \xrightarrow{I_3} (\psi_1 |\psi_1\rangle \langle\psi_1| - I) |\psi_2\rangle = \psi_2^G$$

$$\Rightarrow \psi_2^G = \psi_1 [(\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle)(\cos \frac{\theta}{2} \langle\alpha| + \sin \frac{\theta}{2} \langle\beta|)$$

$$(\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle) - (\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle)]$$

$$= (\psi_1 \cos \frac{\theta}{2} |\alpha\rangle \langle\alpha| + \psi_1 \cos \frac{\theta}{2} \sin \frac{\theta}{2} |\alpha\rangle \langle\beta|$$

$$+ \psi_1 \cos \frac{\theta}{2} \sin \frac{\theta}{2} |\beta\rangle \langle\alpha| + \psi_1 \sin \frac{\theta}{2} |\beta\rangle \langle\beta|)$$

$$(\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle) - (\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle)$$

$$= (\psi_1 \cos \frac{\theta}{2} |\alpha\rangle - \psi_1 \cos \frac{\theta}{2} \sin \frac{\theta}{2} |\alpha\rangle + \psi_1 \sin \frac{\theta}{2} \cos \frac{\theta}{2} |\beta\rangle$$

$$- \psi_1 \sin \frac{\theta}{2} |\beta\rangle) - (\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle) = \psi_1 \cos \frac{\theta}{2} |\alpha\rangle [\cos \frac{\theta}{2} - \sin \frac{\theta}{2}]$$

$$+ \psi_1 \sin \frac{\theta}{2} |\beta\rangle [\cos \frac{\theta}{2} - \sin \frac{\theta}{2}] - [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle]$$

$$= \psi_1 [\cos \frac{\theta}{2} - \sin \frac{\theta}{2}] [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle] - [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle]$$

$$= \psi_1 \cos \theta [\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle] - [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle]$$

$$= [\psi_1 \cos \theta \cos \frac{\theta}{2} |\alpha\rangle + \psi_1 \cos \theta \sin \frac{\theta}{2} |\beta\rangle] - [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle]$$

(۲۶.۴)

از روابط مثلثاتی زیر استفاده می‌کنیم و در رابطه بالا جایگذاری می‌کنیم

$$\cos \theta \cos \beta = \frac{1}{2} [\cos(\theta - \beta) + \cos(\theta + \beta)] \quad (27.4)$$

$$\sin \beta \cos \alpha = \frac{1}{2} [\sin(\beta + \alpha) + \sin(\alpha - \beta)]$$

$$\cos \theta \cos \frac{\theta}{2} = \frac{1}{2} [\cos(\theta - \frac{\theta}{2}) + \cos(\theta + \frac{\theta}{2})] = \frac{1}{2} [\cos \frac{\theta}{2} + \cos \frac{3\theta}{2}]$$

$$\cos \theta \sin \frac{\theta}{2} = \frac{1}{2} [\sin(\theta + \frac{\theta}{2}) + \sin(\frac{\theta}{2} - \theta)] = \frac{1}{2} [\sin \frac{3\theta}{2} - \sin \frac{\theta}{2}] \quad (28.4)$$

و بعد از جایگذاری به صورت زیر در می‌آید:

$$\begin{aligned} &\Rightarrow 2 \cdot \frac{1}{2} [\cos \frac{\theta}{2} + \cos \frac{3\theta}{2}] |\alpha\rangle + 2 \cdot \frac{1}{2} [\sin \frac{3\theta}{2} - \sin \frac{\theta}{2}] |\beta\rangle - [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle] \\ &= \cos \frac{3\theta}{2} |\alpha\rangle + \sin \frac{3\theta}{2} |\beta\rangle \end{aligned} \quad (29.4)$$

از $|\alpha\rangle$ و $|\beta\rangle$ که در ابتدا توضیح داده شد داریم:

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum'' |i\rangle \Rightarrow \sqrt{\frac{N-M}{N}} = \cos \frac{\theta}{2} \Rightarrow \sqrt{N-M} = \cos \frac{\theta}{2} \sqrt{N}$$

$$\sqrt{N} = \sqrt{2^n} \Rightarrow |\alpha\rangle = \frac{1}{\sqrt{2^n} \cos \frac{\theta}{2}} \sum'' |i\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum' |i\rangle \Rightarrow \sqrt{\frac{M}{N}} = \sin \frac{\theta}{2} \Rightarrow \sqrt{M} = \sin \frac{\theta}{2} \sqrt{N}$$

$$\sqrt{N} = \sqrt{2^n} \Rightarrow |\beta\rangle = \frac{1}{\sqrt{2^n} \sin \frac{\theta}{2}} \sum' |i\rangle \quad (30.4)$$

و برای یک حالت، با یک مرحله تکرار گراور داریم:

$$\psi_{\frac{3}{2}}^G = \frac{\cos \frac{3\theta}{2}}{\sqrt{2^n} \cos \frac{\theta}{2}} \sum'' |i\rangle + \frac{\sin \frac{3\theta}{2}}{\sqrt{2^n} \sin \frac{\theta}{2}} \sum' |i\rangle \quad (31.4)$$

۲.۲.۴ اثبات فرمول ۲ فصل ۴

$$f(x) = \begin{cases} 1 & x \\ 0 & x \end{cases} \quad (32.4)$$

$$|x\rangle \xrightarrow{Oracle} (-1)^{f(x)} |x\rangle \quad (33.4)$$

اگر x جواب باشد حالت زیر را داریم:

$$|x\rangle \xrightarrow{Oracle} -|x\rangle \quad (34.4)$$

اگر x جواب نباشد حالت زیر را داریم:

$$|x\rangle \xrightarrow{Oracle} |x\rangle \quad (۳۵.۴)$$

$$\begin{aligned}
|\psi_1^O\rangle &= \cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle \\
\Rightarrow |\psi_1^O\rangle &\xrightarrow{I_2} \cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle = \psi_2 \\
\Rightarrow |\psi_2^O\rangle &\xrightarrow{I_3} (\mathbb{I} |\psi_1\rangle \langle \psi_1| - I) |\psi_2\rangle = \psi_3 \\
\Rightarrow \psi_3^O &= \mathbb{I}[(\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle)(\cos \frac{\theta}{2} \langle \alpha| - \sin \frac{\theta}{2} \langle \beta|) \\
&\quad (\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle) - (\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle)] \\
&= (\mathbb{I} \cos^2 \frac{\theta}{2} |\alpha\rangle \langle \alpha| - \mathbb{I} \cos \frac{\theta}{2} \sin \frac{\theta}{2} |\alpha\rangle \langle \beta| \\
&\quad - \mathbb{I} \cos \frac{\theta}{2} \sin \frac{\theta}{2} |\beta\rangle \langle \alpha| + \mathbb{I} \sin^2 \frac{\theta}{2} |\beta\rangle \langle \beta|) \\
&\quad (\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle) - (\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle) \\
&= (\mathbb{I} \cos^2 \frac{\theta}{2} |\alpha\rangle - \mathbb{I} \cos \frac{\theta}{2} \sin \frac{\theta}{2} |\alpha\rangle - \mathbb{I} \sin \frac{\theta}{2} \cos \frac{\theta}{2} |\beta\rangle \\
&\quad + \sin^2 \frac{\theta}{2} |\beta\rangle) - (\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle) = \mathbb{I} \cos \frac{\theta}{2} |\alpha\rangle [\cos^2 \frac{\theta}{2} - \sin^2 \frac{\theta}{2}] \\
&\quad - \mathbb{I} \sin \frac{\theta}{2} |\beta\rangle [\cos^2 \frac{\theta}{2} - \sin^2 \frac{\theta}{2}] - [\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle] \\
&= \mathbb{I} [\cos^2 \frac{\theta}{2} - \sin^2 \frac{\theta}{2}] [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle] - [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle] \\
&= \mathbb{I} \cos \theta [\cos \frac{\theta}{2} |\alpha\rangle - \sin \frac{\theta}{2} |\beta\rangle] - [\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle] \\
&= [\mathbb{I} \cos \theta \cos \frac{\theta}{2} |\alpha\rangle - \mathbb{I} \cos \theta \sin \frac{\theta}{2} |\beta\rangle] - [\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle] \\
&= \mathbb{I} \cdot \frac{1}{2} [\cos \frac{\theta}{2} + \cos \frac{3\theta}{2}] |\alpha\rangle - \mathbb{I} \cdot \frac{1}{2} [\sin \frac{3\theta}{2} - \sin \frac{\theta}{2}] |\beta\rangle - [\cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle] \\
&= \mathbb{I} \cos \frac{3\theta}{2} |\alpha\rangle - \mathbb{I} \sin \frac{3\theta}{2} |\beta\rangle
\end{aligned} \quad (۳۶.۴)$$

و مجدداً از $|\alpha\rangle$ و $|\beta\rangle$ که در ابتدا توضیح داده شد داریم :

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum'' |i\rangle \Rightarrow \sqrt{\frac{N-M}{N}} = \cos \frac{\theta}{\sqrt{r}} \Rightarrow \sqrt{N-M} = \cos \frac{\theta}{\sqrt{r}} \sqrt{N}$$

$$\sqrt{N} = \sqrt{r^n} \Rightarrow |\alpha\rangle = \frac{1}{\sqrt{r^n} \cos \frac{\theta}{\sqrt{r}}} \sum'' |i\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum' |i\rangle \Rightarrow \sqrt{\frac{M}{N}} = \sin \frac{\theta}{\sqrt{r}} \Rightarrow \sqrt{M} = \sin \frac{\theta}{\sqrt{r}} \sqrt{N}$$

$$\sqrt{N} = \sqrt{r^n} \Rightarrow |\beta\rangle = \frac{1}{\sqrt{r^n} \sin \frac{\theta}{\sqrt{r}}} \sum' |i\rangle$$

$$\psi_r^O = \frac{\cos \frac{r\theta}{\sqrt{r}}}{\sqrt{r^n} \cos \frac{\theta}{\sqrt{r}}} \sum'' |i\rangle - \frac{\sin \frac{r\theta}{\sqrt{r}}}{\sqrt{r^n} \sin \frac{\theta}{\sqrt{r}}} \sum' |i\rangle$$

(۳۷.۴)

مراجع

- [1] J.J.Sakurai,(revised edition 1999), "Modern Quantum Mechanics" , Addison-Wesly,USA.
- [2] Preskill,J.Quantum Information and Quantum Computation ,(2009).
- [3] D.McMahon ,D.Quantum Computing Explained.John Wiley Sons,(2007).
- [4] M. Nielsen, I.Chuang,(2000), "Quantum Computation and Quantum Information" , Cambridge, United Kingdom.
- [5] L.Grover,(1996), "A fast Quantum mechanical algorithm for database search" , In Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, PP 212-219.
- [6] D. Deutsch and R. Jozsa, Proc. R. Soc. London A 439, 553 (1992).
- [7] Ri Qu and Yan-ru Bao, e-print arXiv:quant-ph/1207.2518.
- [8] G. Vidal, J. Mod. Opt. 47, 355 (2000).
- [9] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935).
- [10] E. Schrödinger, Naturwissenschaften 23, 807 (1935).
- [11] D. Bruß and C. Macchiavello, Phys. Rev. A 83, 052313 (2011).

-
- [12] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. 81, 865 (2009).
- [13] L. Grover, Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (ACM Press, New York, 1996), p. 212.
- [14] Grover, L. K. Quantum Mechanics Helps in Searching for a Needle in a Haystack. Physical Review Letters. 79,325, (1997).
- [15] Ri Qu, Juan Wang, Zong-shang Li, Su-li Zhao, Yan-ru Bao, Xiaochun Cao School of Computer Science Technology, Tianjin University, Tianjin 300072, China.

Aabstract

A celebrated result in quantum computation is the discovery of some quantum algorithms able to solve problems faster than any known classical algorithm. One of such algorithms is Grover's search algorithm where a quadratic speedup over the best classical one is shown. In Grover's algorithm, we start with an initial n bit input state $|0\rangle^{\otimes n}$ and apply $H^{\otimes n}$ to this state to generate superposition state.

In this thesis We firstly investigate the multipartite entanglement features of the quantum states, including the iteration states achieved by repeated application of Grover iteration and the Oracle ones into which the above iteration states evolve by applying single Oracle operation, employed in Grover's search algorithm by means of the separable degree and the entanglement measure. Then we give the quantitative and qualitative descriptions of the entanglement dynamics in Grover's search algorithm.



Shahrood University of technology
Faculty Of Mathematical Sciences

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

Grovers search algorithm using multipartite entanglement

Supervisor

Dr.Hossein Movahhedian

Advisor

by

safoora mahmoodi koreh kabijari

2016