دانشگاه صنعتی شاهرود

پایان‌نامه کارشناسی ارشد

محاسبه‌ی کوانتومی تحمل خطا

استاد راهنما:

دکتر حسین موحدیان

ارائه دهنده:

شهلا نیکبخت

تابستان ۱۳۸۶


بسم الله الرحمن الرحيم

تقدیم به

کلمه

که خدا بود

و با عشق در من دمید

و هستی‌ام بخشید

و تقدیم به

اندیشه

که احساسم، روحم و هستی‌ام را اعتلاء بخشید

و به خدا

پیوندم زد

تقدیم به مادرم

به پاس تمام مهربانی‌هایش

نگرانی‌ها و دلواپسی‌هایش

و تقدیم به پدرم

به پاس رنجها و فداکاریهای بی‌پایانش

و خستگی همیشگی دستهایش

که از آغاز وجودم تا به امروز بزرگترین پشتوانه‌ی زندگیم بوده‌اند

با سپاس و تشکر

از استاد عزیزم جناب آقای دکتر موحدیان، که مرا در انجام این پروژه یاری نموده‌اند.

چکیده

چشم‌انداز آینده برای محاسبه‌ی کوانتومی، پیشرفت عظیمی از این دستآورد که تصحیح خطای کوانتومی واقعا امکان پذیر است، را دریافت کرده است. اما این دستآورد به تنهایی برای اطمینان از این مسئله که یک کامپیوتر کوانتومیِ نویزدار می‌تواند به طور قابل اطمینانی عمل کند، کافی نمی‌باشد. برای اجرای پروتکل تصحیح خطای کوانتومی، در ابتدا باید اطلاعات کوانتومی را که می‌خواهیم محافظت کنیم، کدگذاری کنیم و سپس عملیات بازیابی را مکررا اعمال کنیم تا خطاهایی که انباشته می‌شوند، بازگردانده شوند. اما کدگذاری و بازیابی، محاسبات کوانتومیِ پیچیده‌ای هستند و خطاها به طور اجتناب ناپذیری در زمان اعمال این عملها اتفاق می‌افتند. بدین ترتیب لازم است روشی برای بازیابی از خطاها بیابیم که به اندازه کافی مقتدر باشد تا با قابلیت اطمینان بالایی موفق عمل کند، حتی زمانیکه ما خطاهایی را در طول مرحله بازیابی موجب می‌شویم.

به علاوه برای راه اندازی یک کامپیوتر کوانتومی، تنها ذخیره اطلاعات کافی نیست، ما باید اطلاعات را پردازش کنیم و قادرباشیم که گیتهای کوانتومی را اعمال کنیم. وقتی دو یا بیش از دو کیوبیت کدگذاری شده به سمت هم می‌آیند و با یکدیگر برهمکنش می‌کنند، اگر یک خطا در یکی از این کیوبیتها رخ دهد و سپس آن کیوبیت با دیگری از طریق عمل یک گیت کوانتومی برهمکنش کند، خطا احتمالا به کیوبیت دوم انتشار می‌یابد. لذا ما باید گیت‌هایمان را طوری طراحی کنیم که انتشار خطا را به مینیمم مقدار ممکن برسانند. دستگاهی که با وجود اجزای بنیادی معیوب و ناقصش، به طور موثری عمل کند،FT (Fault Tolerant) می‌باشد. این پایان‌نامه به نظریه محاسبه کوانتومی FT اختصاص دارد.

فهرست مطالب

عنوان | صفحه

پیشگفتار ۱

فصل اول: مبانی مکانیک کوانتومی

مقدمه ۳
۱-۱- فرضیات مکانیک کوانتومی ۳
۱-۱-۱- عملگر چگالی ۵
۱-۱-۲- تجزیه اشمیت ۹
۱-۱-۳- خالص سازی ۱۰
۱-۱-۴- کره بلاخ ۱۱
۱-۲- اندازه‌گیری ۱۵
۱-۲-۱- اندازه‌گیری عام ۱۶
۱-۲-۲- اندازه‌گیری‌های غیر متعامد ۱۸
۱-۲-۳- اندازه‌گیری‌های عام *POVM* ۲۰
۱-۲-۴- اندازه‌گیری روی سیستم‌های مرکب ۲۴

فصل دوم: مدارهای کوانتومی

مقدمه ۲۹
۲-۱- مدل مداری برای محاسبات کلاسیک ۲۹
۲-۱-۱- مدارهای کلاسیک برگشت پذیر ۳۱
۲-۲- مدارهای کوانتومی ۳۳
۲-۲-۱- مفهوم دقت در گیت‌های کوانتومی ۳۵
۲-۲-۲- یک مجموعه‌ی عملگرهای جهانی ۳۷
۲-۲-۳- عملهای تک کیوبیتی ۴۰
۲-۲-۴- عملیات *Controlled* ۴۴

فصل سوم: تصحیح خطای کوانتومی

مقدمه ۵۵
۳-۱- عملهای کوانتومی و نویز کوانتومی ۵۵
۳-۱-۱- کد بیت برگردان سه کیوبیتی ۵۹
۳-۱-۲- اصلاح تحلیل خطا ۶۲
۳-۱-۳- کد فاز برگردان سه کیوبیتی ۶۵
۳-۱-۴- کد شُور ۶۷
۳-۲- نظریه تصحیح خطای کوانتومی ۷۰
۳-۲-۱- گسستگی خطاها ۷۳
۳-۲-۲- نمونه‌های خطای مستقل ۷۴
۳-۲-۳- کدهای تبهگن ۷۹
۳-۲-۴- کران کوانتومی همینگ ۸۰
۳-۳- ایجاد کدهای کوانتومی ۸۲
۳-۳-۱- تصحیح خطای کلاسیک ۸۲
۳-۳-۲- کدهای خطی ۸۹
۳-۳-۳- ساختار کدهای خطی ۹۱
۳-۳-۴- یک رابطه تعامد مهم بین یک کد و کد عمود بر آن ۹۹
۳-۴- کدهای CSS ۱۰۰
۳-۴-۱- کد استین ۱۰۱
۳-۵- کدهای تثبیت کننده ۱۰۲
۳-۵-۱- فرمالیزم تثبیت کننده ۱۰۳
۳-۵-۲- گیتهای یکانی و فرمالیزم تثبیت کننده ۱۱۲
۳-۵-۳- اندازه‌گیری در فرمالیزم تثبیت کننده ۱۱۷

فصل چهارم: تحمل خطای کوانتومی (FT)

مقدمه ۱۲۲
۴-۱- چگونگی تصحیح خطای کوانتومی (کد هفت کیوبیتی استین) ۱۲۳
۴-۲- بازیابی FT ۱۳۱

۴-۲-۱- آماده‌سازی حالت کمکی ۱۳۴
۴-۲-۲- بازبینی کمکی ۱۳۷
۴-۲-۳- بازبینی نشانه ۱۳۹
۴-۲-۴- اندازه‌گیری و کدگذاری ۱۴۱
۴-۳- گیتهای FT ۱۴۲
۴-۳-۱- موضوعات بنیادی ۱۴۲
۴-۳-۲- عملهای FT: تعاریف ۱۴۵
۴-۳-۳- مثال: گیت FTی controlled-Not ۱۴۷
۴-۳-۴- کدهای اتصال و قضیه آستانه ۱۵۰
۴-۴- استدلال کوانتومی FT ۱۵۳
۴-۴-۱- عملهای نرمالیزکننده ۱۵۴
۴-۴-۲- گیت FTی $\pi/8$ ۱۵۸
۴-۴-۳- اندازه گیری FT ۱۶۲
۴-۴-۵- اندازه‌گیری مولدهای تثبیت کننده ۱۶۷

فصل پنجم: نتیجه‌گیری و پیشنهادات

نتیجه‌گیری و پیشنهادات ۱۷۰
فهرست مراجع ۱۷۳

فهرست اشکال

عنوان | صفحه

فصل اول: مبانی مکانیک کوانتومی

شکل (۱-۱): در یک آزمایش اشترن گرلاخ غیر ایده‌آل، ذراتی که از دستگاه آزمایش بیرون می-آیند لزوما حالت‌های متعامد بر هم ندارند. ۱۹
شکل(۱-۲): اندازه‌گیری تصویری در امتداد بردارهای فضای بزرگ از دید ناظری که در یک زیرفضا قرار دارد یک اندازه‌گیری تعمیم یافته است. ۲۳

فصل دوم: مدارهای کوانتومی

شکل (۲-۱): نام، نمایش و ماتریسهای یکانی برای گیتهای تک کیوبیتی معمول ۴۴
شکل (۲-۲): نمایش مداری برای گیت $CNOT$، خط بالا نمایش دهنده کیوبیت کنترل و خط پایین نمایش دهنده کیوبیت هدف است. ۴۴
شکل (۲-۳): نمایش مداری برای عمل $Controlled-U$، خط بالا نمایش دهنده کیوبیت کنترل و خط پایین نمایش دهنده کیوبیت هدف است. ۴۵
شکل (۲-۴): گیت تغییر فاز $Controlled$ و یک مدار معادل برای ۲ کیوبیت. ۴۷
شکل (۲-۵): نمایش مداری عمل $Controlled-U$ برای تک کیوبیت U، به طوریکه α، A، B و C در شرط $ABC=I$ و $U=e^{i\alpha}AXBXC$ صدق می‌کند. ۴۷
شکل (۲-۶): نمونه نمایش مداری برای عمل $C^n(U)$ در حالیکه U یک عملگر یکانی روی k کیوبیت باشد، برای $n=4$ و $k=3$. ۴۸
شکل (۲-۷): نمایش مداری برای گیت $C^n(U)$. V هر عملگر یکانی که در $V^2=U$ صدق کند. حالت خاص $V\equiv(1-i)(I+iX)/2$ متناظر با گیت تافولی می‌باشد. ۴۹
شکل (۲-۸): نمایش گیت تافولی با استفاده از گیتهای هادامارد، فاز، $CNOT$ و $\pi/8$. ۴۹
شکل (۲-۹): نمایش شبکه‌ای عمل $C^n(U)$ برای حالت $n=5$. ۵۰

شکل (۲-۱۰): عمل *Controlled* با یک گیت *NOT* که روی کیوبیت دوم اعمال شده است مشروط بر اینکه کیوبیت اول روی $|0\rangle$ تنظیم شده باشد..... ۵۱
شکل (۲-۱۱): عمل $Controlled-U$ و معادل آن بر حسب اجزاء مداری که از قبل چگونگی عمل آنها را می‌دانیم. U روی چهارمین کیوبیت اعمال می‌شود اگر اولین و سومین کیوبیت روی صفر و کیوبیت دوم روی یک تنظیم شده باشد..... ۵۲
شکل (۲-۱۲): گیت $Controlled-Not$ با چندین کیوبیت هدف ۵۲

فصل سوم: تصحیح خطای کوانتومی

شکل(۳-۱): مدار کدگذاری برای کد بیت برگردان سه کیوبیتی..... ۶۰
شکل (۳-۲): مدارهای کدگذاری برای کد وارون فازی ۶۶
شکل (۳-۳): مدار کدگذاری برای کد ۹ کیوبیتی شُور..... ۶۸
شکل (۳-۴): بسته فضای هیلبرت در کدگذاری کوانتومی. الف) کد نامناسب با فضاهای تغییر شکل یافته و نامتعامد. ب) کد مناسب با فضاهای متعامد (قابل تمایز) و تغییر شکل نایافته..... ۷۲
شکل (۳-۵): مراحل مختلف کد کردن و گشودن یک پیام..... ۸۳
شکل(۳-۶): نحوه تشخیص و خنثی کردن خطا..... ۸۷
شکل (۳-۷)یک خطا باعث می‌شود که بردار یک کلمه از زیرفضای کد خارج شود..... ۹۲
شکل (۳-۸): مولدهای تثبیت کننده برای کد ۷ کیوبیتی اِستین. ضرب تانسوری روی کیوبیتها را به ترتیب نشان می‌دهد، به عنوان مثال $ZIZIZI = Z\otimes I\otimes Z\otimes I\otimes Z\otimes I = Z_1Z_3Z_5Z_7$ ۱۰۷
شکل (۳-۹): ویژگیهای تبدیل عناصر گروه پائولی تحت کانجوگیشن با عملهای مختلف. $Controlled-Not$ کیوبیت ۱ را به عنوان کیوبیت کنترل و کیوبیت ۲ را به عنوان کیوبیت هدف داراست..... ۱۱۴
شکل (۳-۱۰): مدار معاوضه‌ای دو کیوبیتی و یک طرح کلی معادل برای آن..... ۱۱۵

فصل چهارم: تحمل خطای کوانتومی (FT)

شکل (۴-۱): محاسبه‌ی نشانه‌ی وارون بیتی برای کد ۷ کیوبیتی استین. با تکرار محاسبات در پایه‌ی چرخیده شده، خطاهای وارون فازی تشخیص داده می‌شود. برای اینکه روند را FT بسازیم، هر کیوبیت کمکی باید توسط ۴ کیوبیت در یک حالت مناسب جایگزین شوند..... ۱۲۷

شکل (۴-۲): یک تساوی مفید. کنترل و هدف یک گیت $CNot$ قابل تعویض هستند اگر ما یک تغییر در پایه با چرخشهای هادامارد انجام دهیم ۱۳۲
شکل (۴-۳): مدلهای خوب و بد اندازه‌گیری نشانه. مدار بد بیت کمکی مشابه را چندین بار به کار می‌برد، مدار خوب هر بیت کمکی را تنها یک بار به کار می‌برد ۱۳۲
شکل (۴-۴): (a) روندی برای محاسبه یک بیت از نشانه خطای وارون بیتی به صورت شماتیکی نمایش داده شده است. گیت هادامارد که روی *حالت گربه* اعمال شده است، آماده سازی حالت شُور را تکمیل می‌کند. گیتهای $CNot$ و هادامارد در دیاگرام در حقیقت چهار گیت را که به صورت یکسان و همزمان اعمال شده است را نمایش می‌دهد. (b) روندی برای محاسبه یک بیت از نشانه‌ی خطای وارون فازی که به طور شماتیکی نشان داده شده است و مشابه (a) می‌باشد، اما روی داده‌ها در پایه چرخیده شده، اعمال شده‌است. (c) یک مدار معادل با (b)، که با استفاده از تساوی شکل (۴-۲)، ساده سازی شده است. ۱۳۵
شکل (۴-۵): نمونه‌ای از $CNot$ کردن کیوبیتهای دسته با کیوبیتهای کمکی ۱۳۶
شکل (۴-۶): ساخت و بازبینی حالت شُور. اگر نتیجه‌ی اندازه‌گیری ۱ باشد، در این صورت این حالت رد شده و یک حالت جدید شور آماده می‌شود ۱۳۷
شکل (۴-۷): مدار کاملی برای بازیابی خطای استین. $|0\rangle$ های کدگذاری شده آماده می‌شوند، سپس بازبینی می‌شوند. $|0\rangle$های بازبینی شده به عنوان آنسیلاها برای محاسبه‌ی نشانه‌های وارون‌بیتی و وارون فازی به کار برده می‌شوند که هر دو، دو بار اندازه‌گیری می‌شوند. دایره‌های بزرگ به عملهایی که بسته به نتیجه‌ی اندازه‌گیری برای اصلاح حالتهای کمکی به کار برده می‌شوند و یا در حالت نهایی، برای اصلاح دسته‌ی داده‌ها، به کار برده می‌شود، اشاره دارد ۱۴۰
شکل (۴-۸): یک مدار ساده کوانتومی. اگر هر یک از اجزاء در مدار با احتمال p، موفق عمل نکنند، در این صورت احتمال یک خطا در خروجی $O(p)$ می‌باشد. ۱۴۲
شکل (۴-۹): یک شبیه سازی از مدار شکل (۴-۸) با استفاده از کیوبیتهای کدگذاری شده و عملهای منطقیِ کدگذاری شده ۱۴۳
شکل (۴-۱۰): یک گیت $CNot$ می‌تواند سبب انتشار یک خطا شود، بنابراین بجای یک کیوبیت، روی دو کیوبیت اثر می‌کند. این مسئله در مورد کیوبیتهای کدگذاری شده نیز صادق می‌باشد ۱۴۴
شکل (۴-۱۱): دیاگرام ساختار روند FT، شامل تصحیح خطا ۱۴۷
شکل (۴-۱۲): یک کد با دو بار تسلسل که یک تک کیوبیت را در ۹ کیوبیت کدگذاری می‌کند. در اینجا یک کد سه کیوبیتی صرفا به خاطر ساده سازی شکل آورده شده است. اما در عمل

کدهایی مانند کد استین به کار برده می‌شوند که می‌توانند خطاهایی را روی یک یا بیش از یک کیوبیت تصحیح کنند..... ۱۵۱
شکل (۴-۱۳): گیت هادامارد عرضی روی یک کیوبیت کدگذاری شده در کد استین..... ۱۵۴
شکل (۴-۱۴): $CNot$ عرضی بین دو کیوبیت که در دسته‌های جدا توسط کد استین کدگذاری شده‌اند..... ۱۵۷
شکل (۴-۱۵): مدار کوانتومی که به صورت FT یک گیت $\pi/8$ را اجرا می‌کند. مستطیل نقطه چین شده روند آماده سازی (FT نیست) برای حالت کمکی $\left(|0\rangle+\exp(i\pi/4)|1\rangle\right)/\sqrt{2}$ را نشان می‌دهد. علامت اِسلش روی سیم، معرف یک دسته هفت کیوبیتی می‌باشد و سیم دو خطی بیت کلاسیکی که از اندازه‌گیری ناشی می‌شود را نشان می‌دهد. توجه کنید که عمل نهایی SX توسط نتیجه‌ی اندازه‌گیری کنترل می‌شود..... ۱۶۰
شکل (۴-۱۶): مدار کوانتومی برای اندازه‌گیری یک عملگر تک کیوبیتی M با مقادیر ویژه‌ی ±1. کیوبیت بالایی حالتی کمکی است که برای اندازه‌گیری استفاده می‌شود و کیوبیت پایینی در حال اندازه‌گیری شدن است..... ۱۶۳
شکل (۴-۱۷): روند شماتیک برای اجرای یک اندازه‌گیری از مشاهده‌پذیر کدگذاری شده‌ی M با یک اجرای عرضی با اعمال بیت به بیت M'. مدار FT نیست. توجه کنید که یک کد واقعی بیش از سه کیبویت نیاز دارد..... ۱۶۴
شکل (۴-۱۸): روند شماتیک برای اندازه‌گیری FT یک مشاهده‌پذیر M، که که روی داده‌ی کدگذاری شده اجرا می‌شود. این روند سه بار تکرار می‌شود و یک رای اکثریت از نتایج اندازه-گیری گرفته می‌شود..... ۱۶۵
شکل (۴-۱۹): روند شماتیک برای اجرای یک اندازه‌گیری FT از عملگر XZX روی سه کیوبیت.. ۱۶۸

پیشگفتار

به طور کلی کامپیوترهای کوانتومی با سرعت بسیار بیشتری نسبت به هر کامپیوتر کلاسیکی ممکن، قادر به حل مسائل می‌باشند. با این وجود، عملا تکنولوژی محاسبه کوانتومی هنوز در ابتدای راه خود می‌باشد. با وجود اینکه یک کامپیوتر کوانتومی عملی و مناسب سرانجام ساخته خواهد شد، اما در حال حاضر ما نمی‌توانیم در مورد سخت افزار دقیق آن نظری بدهیم. اما با این وجود می‌دانیم که هر کامپیوتر کوانتومی، چندین نوع تصحیح خطا را در عملیاتش وارد می‌کند.

کامپیوترهای کوانتومی در مقایسه با کامپیوترهای دیجیتالی امروزی، بیشتر مستعد ایجاد خطا هستند و لذا روشهایی برای کنترل و تصحیح این گونه خطاها جهت جلوگیری از تخریب یک کامپیوتر کوانتومی لازم می‌باشد. می‌دانیم که چگونه یک حالت کوانتومی از یک گربه، که برهم نهی‌ای از یک گربه‌ی مرده و یک گربه‌ی زنده می‌باشد را آماده کنیم، اما هرگز نمی‌توانیم برهمنهی ماکروسکوپیکِ آن را ببینیم زیرا آنها بسیار ناپایدار هستند. یک گربه واقعی نمی‌تواند کاملا نسبت به محیط خود منزوی باشد. محیط، گربه را اندازه‌گیری می‌کند و فورا آن را به یک حالت کاملا مرده و یا کاملا زنده تصویر می‌کند (می‌برد). یک کامپیوتر کوانتومی ممکن است که به اندازه یک گربه پیچیده نباشد اما یک سیستم کوانتومیِ پیچیده است و مانند یک گربه به طور اجتناب ناپذیری با محیط برهم‌کنش می‌کند.

فصل اول:
مبانی مکانیک کوانتومی

مقدمه

مکانیک کوانتومی یک چارچوب ریاضی برای توسعه نظریات فیزیکی می‌باشد و در واقع در مورد این مسئله که یک سیستم کوانتومی از چه قوانینی باید تبعیت کند سخن نمی‌گوید بلکه یک چارچوب ریاضی برای بسط و توسعه این قوانین ایجاد می‌کند. در این فصل، در ابتدا فرضیات اساسی مکانیک کوانتومی را ارائه داده و سپس با توضیحاتی در مورد عملگر چگالی، این فرضیات را بازنویسی می‌کنیم. سپس چند نمونه از اندازه‌گیری‌ها را معرفی کرده و توضیحاتی در مورد آنها ارائه می‌دهیم

۱-۱- فرضیات مکانیک کوانتومی

در اینجا یک شرح کلی در مورد فرضیات اساسی مکانیک کوانتومی آورده شده است. این فرضیات ارتباطی بین جهان فیزیکی و فرمالیزم ریاضی مکانیک کوانتومی برقرار می‌کند.

فرضیه۱) به هر سیستم فیزیکی منزوی، یک فضای برداری مختلط (یعنی یک فضای هیلبرت) نسبت داده می‌شود، که فضای حالت[۱] سیستم نامیده می‌شود. سیستم به طور کامل توسط بردار حالت[۲] سیستم که یک بردار واحد در فضای حالت سیستم می‌باشد، توصیف می‌شود. ساده‌ترین سیستم مکانیک کوانتومی، کیوبیت می‌باشد. یک کیوبیت، یک فضای حالت دو بعدی دارد. با فرض

---

۱ state space
۲ state vector

اینکه $|0\rangle$ و $|1\rangle$، یک پایه متعامد برای فضای حالت تشکیل دهند، یک بردار حالت اختیاری فضای حالت، را می‌توان به صورت زیر نوشت:

$$|\psi\rangle = a|0\rangle + b|1\rangle \qquad (۱-۱)$$

که a و b اعداد مختلط هستند. شرط اینکه $|\psi\rangle$ یک بردار واحد باشد، $\langle\psi|\psi\rangle = 1$، این است که: $|a|^2 + |b|^2 = 1$، که این شرط، شرط نرمالیزاسیون نامیده می‌شود.

فرضیه ۲) تحول یک سیستم کوانتومی منزوی، با یک تبدیل یکانی توصیف می‌شود. یعنی حالت $|\psi\rangle$ یک سیستم در زمان t به حالت $|\psi'\rangle$ در زمان t'، با یک عملگر یکانی، U، مربوط می‌شود که تنها بستگی به زمان t و t' دارد:

$$|\psi'\rangle = U|\psi\rangle \qquad (۲-۱)$$

فرضیه ۳) اندازه‌گیری‌های کوانتومی با یک مجموعه $\{M_m\}$ از عملگرهای اندازه‌گیری[۱] توصیف می‌شوند. اینها عملگرهایی هستند که روی فضای حالت سیستمی که اندازه‌گیری می‌شود، اعمال می‌شوند. شاخص m مربوط به نتایج اندازه‌گیری که ممکن است در آزمایش اتفاق بیفتد، می‌باشد. اگر حالت سیستم کوانتومی درست قبل از اندازه‌گیری $|\psi\rangle$ باشد، احتمال اینکه نتیجه m اتفاق بیفتد، خواهد شد:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \qquad (۳-۱)$$

و حالت سیستم بعد از اندازه‌گیری خواهد بود:

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \qquad (۴-۱)$$

لازم به ذکر است که عملگرهای اندازه‌گیری رابطه مکملیت را ارضاء می‌کنند.

---

[۱] measurement operator

روی حالات مختلف کاملا یکنواخت است مثل وقتی که با قطبش یک باریکه از فوتون‌ها سر و کار داریم و می‌گوییم که ۵۰ درصد از آنها جهت قطبش x و ۵۰ درصد آنها جهت قطبش y دارند. می‌خواهیم ببینیم که در چنین حالت‌هایی دستگاه کوانتومی را چگونه می‌بایست توصیف کنیم. فرض کنید که خاصیتی مثل خاصیت M را می‌خواهیم اندازه گیری کنیم. برای یک دستگاه مخلوط مطابق فوق متوسط خاصیت M به شکل زیر محاسبه خواهد شد:

$$\langle M\rangle = \sum_i p_i \langle \psi_i | M | \psi_i \rangle = tr(\rho M) \qquad (۶-۱)$$

که در آن ρ عبارت است از:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \qquad (۷-۱)$$

و ماتریس چگالی دستگاه کوانتومی خوانده می‌شود. بنابراین حالت چنین دستگاهی به جای آنکه با یک بردار حالت مشخص شود با یک ماتریس چگالی مشخص می‌شود. این ماتریش چگالی در بردارنده تمام اطلاعاتی است که ما می‌توانیم از دستگاه کوانتومی کسب کنیم. نخست بهتر است که خواص ماتریس چگالی را بررسی کنیم. ماتریس چگالی خاصیت‌های زیر را دارد:

$$\begin{aligned} &tr(\rho) = 1 \\ &\rho^\dagger = \rho \\ &\rho \geq 0 \end{aligned} \qquad (۸-۱)$$

می‌توان ماتریس چگالی ρ را در پایه ویژه بردارهای خودش نوشت. در این صورت خواهیم داشت:

$$\rho = \sum_{i=1}^{N} \lambda_i |\alpha_i\rangle\langle\alpha_i| \qquad (۹-۱)$$

که در آن N بعد فضای هیلبرت است. دقت کنید که رابطه (۱-۷) یک تجزیه طیفی نیست و به همین دلیل بردارهای $|\psi_i\rangle$ یک مجموعه متعامد تشکیل نمی‌دهند و تعداد آنها نیز هیچ ربطی به بعد ماتریس ρ ندارند، اما رابطه (۱-۹) تجزیه طیفی ماتریس چگالی را بیان می‌کند و بردارهای $|\alpha_i\rangle$

ویژه بردارهای ماتریس چگالی هستند و تعداد آنها نیز برابر با بعد ماتریس چگالی یا بعد فضای هیلبرت است.

از تجزیه طیفی یک خاصیت دیگر را نیز می‌توان به دست آورد و آن اینکه:

$$tr(\rho^2) \equiv \sum_i \lambda_i^2 \leq 1 \qquad (۱۰-۱)$$

که در آن از مثبت بودن λ_i ها و اینکه مجموع همه آنها برابر با یک است استفاده کرده‌ایم. همچنین از تجزیه طیفی قضیه زیر را بدست می‌آوریم که اثبات آن ساده است:

قضیه: حالت ρ یک حالت خالص است اگر و فقط اگر $tr(\rho)^2 = 1$.

تاکنون می‌توانستیم متوسط خاصیت M را وقتی که دستگاه در حالت ρ قرار دارد به دست آوریم. حال می‌پرسیم در اندازه‌گیری خاصیت M احتمال اینکه مقدار m به دست بیاید چقدر است و بعد از اندازه‌گیری دستگاه در چه حالتی است. برای آنکه احتمال اندازه‌گیری m را به دست آوریم به ترتیب زیر عمل می‌کنیم:

$$P(m) = \sum_i p_i \langle \psi_i | P_m | \psi_i \rangle = tr(P_m \rho) \qquad (۱۱-۱)$$

که در آن از این موضوع استفاده کرده‌ایم که احتمال به دست آوردن مقدار m برای وقتی که دستگاه کوانتومی در حالت خالص $|\psi\rangle$ است برابر است با $\langle \psi | P_m | \psi \rangle$. بالاخره می‌خواهیم بفهمیم که بعد از اندازه‌گیری خاصیت M و یافتن مقدار m دستگاه کوانتومی در چه حالتی است. پاسخ این امر ساده است. دستگاه کوانتومی با ماتریس چگالی P_m توصیف می‌شود. البته این در حالتی است که مقدار m را به دست آورده باشیم و با اندازه‌گیری خود این دسته از ذرات را (به عنوان دستگاه‌های کوانتومی) از دیگر ذرات جدا کرده باشیم. هرگاه چنین جداسازی‌ای انجام نداده باشیم حالت دستگاه بعد از اندازه-گیری به صورت زیر خواهد بود:

$$\rho_1 = \sum_m q_m P_m \qquad (۱۲-۱)$$

که در آن q_m احتمال این است که مقدار m به دست آمده باشد. با توجه به رابطه (۱-۱۱) که این احتمال را تعیین می‌کند، می‌توان این رابطه را به شکل زیر بازنویسی کرد:

$$\rho_1 = \sum_m tr(P_m \rho) P_m \qquad (۱۳-۱)$$

از یک زاویه دیگر نیز می‌توان به ماتریس چگالی نگاه کرد. فرض کنید که دو ذره اسپین $\frac{1}{2}$ داریم و این دو ذره در حالتی مثل حالت زیر قرار دارند:

$$|\psi\rangle_{AB} = a|+,+\rangle + b|+,-\rangle + c|-,+\rangle + d|-,-\rangle \qquad (۱۴-۱)$$

می‌پرسیم که حالت ذره A چیست. در اینجا درست است که هر دو ذره در یک حالت مشخص قرار دارند ولی نمی‌توان به ذره A بردار حالت مشخصی نسبت داد. در این مورد تمامی موارد مشابه که دستگاه کوانتومی مورد نظر ما جزئی از یک دستگاه بزرگتر است حالت آن با یک ماتریس چگالی مشخص می‌شود. برای اینکه این موضوع را به طور کلی مورد بحث قرار دهیم فرض کنید که دو دستگاه A و B در یک حالت کوانتومی قرار دارند که بر حسب بردارهای پایه فضای هیلبرت سیستم A و سیستم B بسط آن به شکل زیر است:

$$|\psi\rangle_{AB} = \sum_{i,\mu} \psi_{i\mu} |i,\mu\rangle \qquad (۱۵-۱)$$

حال هر عملگر M_A روی دستگاه A چیزی نیست جز عملگری به شکل $M \otimes I$. در نتیجه خواهیم داشت:

$$\langle M\rangle_A = \langle\psi|M\otimes I|\psi\rangle = tr_{AB}\left((M\otimes I)|\psi\rangle\langle\psi|\right) = tr_A\left(tr_B\left(M\otimes I\right)|\psi\rangle\langle\psi|\right)\right) = tr_A\left(M\rho_A\right) \qquad (۱۶-۱)$$

که در آن

$$\rho_A = tr_B\left(|\psi\rangle\langle\psi|\right) \qquad (۱۷-۱)$$

ماتریس چگالی دستگاه A نامیده می‌شود. به این ترتیب هر عنصر ماتریسی روی دستگاه را می‌توان به صورت $tr(M\rho)$ نوشت که در آن ρ از رابطه بالا تعیین می‌شود و جانشین حالت کوانتومی دستگاه A است. به طریق مشابه ماتریس چگالی دستگاه B با رابطه $\rho_B = tr_A\left(|\psi\rangle\langle\psi|\right)$ داده می‌شود. می‌توان فرم صحیح‌تر ماتریس چگالی را نیز به دست آورد. با توجه به رابطه (۱-۱۵) خواهیم داشت:

$$\rho_A = \sum_{i,j} \rho_{ij} |i\rangle\langle j| \qquad (۱-۱۸)$$

که در آن

$$(\rho_A)_{ij} = \sum_{\mu} \psi_{i\mu}\psi^*_{j\mu} \qquad (۱-۱۹)$$

$$\rho_B = \sum_{i} \rho_{\mu\nu} |\mu\rangle\langle n| \qquad (۱-۲۰)$$

که در آن

$$(\rho_B)_{\mu\nu} = \sum_{i} \psi_{i\mu}\psi^*_{i\nu} \qquad (۱-۲۱)$$

با توجه به این عبارت‌ها به راحتی می‌توان خواص سه گانه ماتریس چگالی را تحقیق کرد یعنی این که ρ یک ماتریس هرمیتی مثبت با رد برابر با واحد است.

۱-۱-۲- تجزیه اشمیت[۱]

فرض کنید که دستگاه مرکب $A+B$ در یک حالت خالص $|\psi\rangle_{AB}$ قرار دارد. در این صورت همواره می‌توان این حالت را به شکل زیر باز نویسی کرد:

$$|\psi\rangle_{AB} = \sum_i \lambda_i |i,\hat{i}\rangle \qquad (۱-۲۲)$$

[۱] schmidt decomposition

که در آن λ_i ها اعداد مثبت و $\{|i\rangle\}$و $\{|\hat{i}\rangle\}$ به ترتیب مجموعه بردارهای متعامد یکه در فضای هیلبرت دستگاه‌های A و B هستند. این تجزیه را تجزیه اشمیت می‌خوانند. برای پیدا کردن این تجزیه به ترتیب زیر عمل می‌کنیم. برای فضای هیلبرت H_A پایه‌ای انتخاب می‌کنیم که در آن ماتریس ρ_A قطری باشد. این پایه را با $\{|i\rangle\}$ نشان می‌دهیم. در نتیجه بردار حالت به شکل زیر نوشته می‌شود:

$$|\psi\rangle_{AB}=\sum_i |i\rangle|\phi_i\rangle \qquad (۲۳-۱)$$

که در آن بردارهای $\{\varphi_i\}$ بردارهایی نه الزاما متعامد و یا یکه در فضای هیلبرت H_B هستند. حال دقت می‌کنیم که بنابر تعریف:

$$\rho_A=tr_B\left(|\psi\rangle_{AB\ AB}\langle\psi|\right)=\sum_i |i\rangle\langle j|\langle\varphi_i|\varphi_j\rangle \qquad (۲۴-۱)$$

اما چون ماتریس چگالی ρ_A در پایه انتخاب شده قطری است پس به دست می‌آوریم که:

$$\langle\phi_i|\phi_j\rangle=\lambda_i^2\delta_{ij} \qquad (۲۵-۱)$$

با تعریف $|\phi_i\rangle=\lambda_i|\hat{i}\rangle$ به تجزیه اشمیت یعنی رابطه (۱-۲۲) می‌رسیم.

۱-۱-۳- خالص سازی[۱]

فرض کنید که دستگاه A توسط یک ماتریس چگالی ρ توصیف می‌شود. آیا می‌توان دستگاهی مثل B و حالتی از دستگاه مرکب $A+B$ مثل $|\psi\rangle_{AB}$ چنان یافت که:

$$\rho=tr_B\left(|\psi\rangle_{AB\ AB}\langle\psi|\right) \qquad (۲۶-۱)$$

[۱] purification

باشد. اگر چنین حالتی پیدا کنیم حالت $|\psi\rangle_{AB}$ را حالت خالص شده ماتریس چگالی ρ می‌خوانیم. برای اینکه حالت خالص شده یک ماتریس چگالی ρ_A با ویژه مقدارهای p_i را پیدا کنیم به ترتیب زیر عمل می‌کنیم. دستگاه B را دستگاهی می‌گیریم که بعد فضای هیلبرت آن یعنی H_B حداقل با بعد H_A یکی باشد. هرگاه بردارهای $\{|i\rangle\}$ یک پایه متعامد برای دستگاه A باشند قرار می‌دهیم:

$$|\psi\rangle_{AB}=\sum_i \sqrt{p_i}\,|i,\hat{i}\rangle \qquad (۲۷-۱)$$

که در آن $\{|\hat{i}\rangle\}$ یک مجموعه بردار متعامد یکه برای فضای H_B هستند. در این صورت $|\psi\rangle_{AB}$ یک خالص سازی ρ_A است.

۱-۱-۴- کره بلاخ[۱]

کلی ترین حالت یک ذره اسپین $\frac{1}{2}$ و یا هر ذره دیگری که فضای هیلبرت آن دو بعدی است با یک ماتریس چگالی 2×2 داده می‌شود. این ماتریس را با ρ نشان می‌دهیم. از آنجا که ماتریس I و ماتریس‌های پائولی یک پایه برای فضای ماتریس‌های 2×2 تشکیل می‌دهند. می‌توان این ماتریس را به شکل زیر نوشت:

$$\rho=\frac{1}{2}\left(r_0 I+\boldsymbol{r}.\boldsymbol{\sigma}\right)=\frac{1}{2}\begin{pmatrix} r_0+z & x-iy \\ x+iy & r_0-z \end{pmatrix} \qquad (۲۸-۱)$$

حال دقت می‌کنیم که:

الف: ρ هرمیتی است. بنابراین ضرائب $\boldsymbol{r}$ و r_0 حقیقی هستند.

ب: $tr(\rho)=1$. بنابراین $r_0=1$.

---

[۱] bloch sphere

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:

$$\lambda_{1,2} = \frac{1}{2}(1 \pm r) \qquad (۲۹-۱)$$

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

بنابراین برای مثبت بودن کافی است که طول بردار $\boldsymbol{r}$ از یک کمتر باشد: یعنی $r \leq 1$. به این ترتیب بین هر ماتریس چگالی و یک نقطه از یک کره به شعاع واحد یک تناظر یک به یک برقرار می‌شود. این کره، کره بلاخ نام دارد. 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 $\boldsymbol{r}$ برابر با یک بردار یکه $\boldsymbol{n}$ باشد آنگاه

$$\rho \equiv \frac{1}{2}(I + \boldsymbol{n}.\boldsymbol{\sigma}) = |n\rangle\langle n| \qquad (۳۰-۱)$$

که در آن $|n\rangle$ حالت ذره با اسپین در جهت بردار یکه n است. از طرف دیگر مرکز کره یعنی $r = 0$ متناظر با حالت کاملا مخلوط $\rho = \frac{1}{2}I$ است. هر چه از مرکز کره به طرف مرز پیش برویم به درجه خلوص حالت‌ها اضافه می‌شود. می‌دانیم که یک حالت مخلوط را می‌توان به صورت مخلوطی از حالتهای خالص در نظر گرفت. چگونه می‌توان یک حالت مخلوط برای یک ذره اسپین $\frac{1}{2}$ را تجزیه کرد؟ این تجزیه چگونه روی کره بلاخ نشان داده می‌شود؟ پاسخ این سوال ساده است. فرض کنید که یک حالت مخلوط متناظر با بردار $\boldsymbol{r}$ روی کره داده شده است. می‌خواهیم این حالت را به صورت مجموع دو حالت خالص تجزیه کنیم. برای این کار از نوک بردار $\boldsymbol{r}$ وتری از کره رسم می‌کنیم که سطح کره را در دو نقطه n_1 و n_2 قطع کند. هرگاه طول دو پاره خط ایجاد شده را با l_1 و l_2 نشان

دهیم آنگاه یک محاسبه ساده نشان می‌دهد که می‌توان حالت مخلوط $\rho=\frac{1}{2}(I+\boldsymbol{r}.\boldsymbol{\sigma})$ را به شکل زیر تجزیه کرد:

$$\rho = p_1|n_1\rangle\langle n_1| + p_2|n_2\rangle\langle n_2| \qquad (۳۱-۱)$$

که در آن $p_1=\frac{l_1}{l_1+l_2}$ و $p_2=\frac{l_2}{l_1+l_2}$. از آنجا که وتر مربوطه را به بی‌نهایت طریق می‌توان رسم کرد، پس بی‌نهایت تجزیه دوتایی برای حالت مخلوط وجود دارد. آیا تجزیه‌های بیش از دو تایی هم وجود دارد؟ پاسخ این سوال هم مثبت است. فرض کنید که نقاط $n_1,n_2,...n_N$ روی سطح کره داده شده‌اند. حال ضرایب $\sum_{i=1}^{N}p_i=1$ ، $p_1,p_2,...p_N$ را چنان تعیین می‌کنیم که شرط زیر تحقق یابد:

$$\sum_{i=1}^{N}p_i n_i = r \qquad (۳۲-۱)$$

در این صورت می‌توان نوشت:

$$\rho=\frac{1}{2}(I+\boldsymbol{r}.\boldsymbol{\sigma})=\sum_{i=1}^{N}p_i\frac{1}{2}(I+\boldsymbol{n}_i.\boldsymbol{\sigma})=\sum_{i=1}^{N}p_i|n_i\rangle\langle n_i| \qquad (۳۳-۱)$$

به این ترتیب حالت مخلوط ρ را می‌توان به بی‌نهایت طریق به صورت مجموعی از حالت‌های خالص و یا حتی به صورت انتگرالی از حالت‌های خالص تجزیه کرد که در حالت اخیر خواهیم نوشت:

$$\rho=\int d\varphi\, d\cos\theta\; p(\theta,\varphi)\left|n(\theta,\varphi)\right\rangle\left\langle n(\theta,\varphi)\right| \qquad (۳۴-۱)$$

با این شرط که $\int d\phi d\cos\theta p(\theta,\phi)=1$.

تعاریف و توضیحاتی که در مورد عملگر چگالی داده شد، این اجازه را به ما می‌دهد که فرضیات مکانیک کوانتومی (که در ابتدای فصل ذکر شد) را در سایه عمگر چگالی بازنویسی کنیم.

۱- به هر سیستم فیزیکی منزوی، یک فضای برداری مختلط (یعنی یک فضای هیلبرت) نسبت داده می‌شود، که فضای حالت[۱] سیستم نامیده می‌شود. سیستم به طور کامل توسط عملگر چگالی[۲] توصیف می‌شود. این عملگر که روی فضای حالت سیستم عمل می‌کند، مثبت و با رد یک ($tr(\rho)=1$)، می‌باشد. اگر یک سیستم کوانتومی با احتمال p_i در حالت ρ_i باشد، در این صورت عملگر چگالی برای این سیستم $\sum_i p_i\rho_i$ می‌باشد.

۲- تحول یک سیستم کوانتومی منزوی، با یک تبدیل یکانی توصیف می‌شود. یعنی حالت ρ یک سیستم در زمان t به حالت ρ' در زمان t'، با یک عملگر یکانی، U، مربوط می‌شود که تنها بستگی به زمان t و t' دارد:

$$\rho' = U\rho U^{\dagger} \qquad (۳۵-۱)$$

۳- اندازه‌گیریهای کوانتومی با یک مجموعه $\{M_m\}$ از عملگرهای اندازه‌گیری[۳] توصیف می‌شوند. اینها عملگرهایی هستند که روی فضای حالت سیستمی که اندازه‌گیری می‌شود، اعمال می‌شوند. شاخص m مربوط به نتایج اندازه‌گیری که ممکن است در آزمایش اتفاق بیفتد، می‌باشد. اگر حالت سیستم کوانتومی قبل از اندازه‌گیری ρ باشد، احتمال اینکه نتیجه m اتفاق بیفتد، خواهد شد:

$$p(m) = tr\left(M_m^{\dagger} M_m \rho\right) \qquad (۳۶-۱)$$

و حالت سیستم بعد از اندازه‌گیری خواهد بود:

$$\frac{M_m \rho M_m^{\dagger}}{tr\left(M_m^{\dagger} M_m \rho\right)} \qquad (۳۷-۱)$$

---

[۱] state space
[۲] density operator
[۳] measurement operator

لازم به ذکر است که عملگرهای اندازه‌گیری رابطه مکملیت را ارضاء می‌کنند.

$$\sum_m M_m^\dagger M_m = I \qquad (۳۸-۱)$$

۴- فضای حالت یک سیستم فیزیکی مرکب، حاصلضرب تانسوری فضاهای حالت سیستم‌های فیزیکی تشکیل دهنده آن می‌باشد. بعلاوه اگر n سیستم داشته باشیم و سیستم iام با حالت ρ_i مشخص شود، در این صورت حالت کل سیستم برابر با $\rho_1 \otimes \rho_2 ... \rho_n$ خواهد بود.

۱-۲- اندازه گیری

یک دستگاه اشترن گرلاخ کارش این است که ذرات را به طور تصادفی و با احتمالی که قابل محاسبه و آزمون است به دو حالت متمایز از هم جدا می‌کند.

یک پولاروید که جلوی باریکه نور قرار می‌گیرد نیز همین کار را انجام می‌دهد و بعضی از فوتون‌ها را جذب و بعضی دیگر را از خود عبور می‌دهد. همچنین است یک آینه نیم شفاف که بعضی از فوتون‌ها را از خود عبور می‌دهد و بعضی دیگر را منعکس می‌کند. یک بلور کالسیت نیز که ضریب شکست آن بستگی به قطبش نور تابیده دارد، فوتون‌های تابیده شده به آن را از هم جدا می‌کند. تمام این آزمایش‌ها خصلت‌های زیر را به طور مشترک دارا هستند که همگی محصول مستقیم تجربه هستند.

۱- نتیجه این آزمایشها همواره به طور تصادفی است و هرگز نمی‌توان رفتار دو ذره کاملا یکسان را در این آزمایش‌ها و یا اندازه‌گیری‌ها پیش‌بینی کرد. اما احتمالات، تابع قوانین دقیق هستند.

۲- نمی‌توان گفت که این آزمایش‌ها یک خاصیت از قبل موجود ذره را «مشاهده» می‌کنند و می‌سنجند. تنها می‌توان گفت که این آزمایش‌ها یا اندازه‌گیری‌ها ذرات را به نحوی از هم جدا می‌کنند. ذراتی که بعد از آزمایش جدا می‌شوند دارای خصلت‌هایی هستند که ما یک مدل

نظری به آنها نسبت می‌دهیم. به عنوان مثال ذراتی که از خروجی بالای یک آزمایش اشترن گرلاخ بیرون می‌آیند در حالت $|z_+\rangle$ هستند و ذراتی که از شکاف پایینی بیرون می‌آیند در حالت $|z_-\rangle$ هستند. به هیچ وجه نمی‌توان گفت که مولفه اسپین این ذرات از قبل دارای این مقادیر بوده است. .

۳- ذرات خارج شده از این دستگاه حالتهای کاملا متمایز دارند به این معنا که می‌توان به راحتی تک تک آنها را با انجام آزمایشی از همان نوع از یکدیگر و به طور قطع تمیز داد.

توجه به این موضوع بسیار مهم است که در موارد سه گانه بالا هیچ اثری از عملگری که به یک مشاهده پذیرنسبت داده شود، وجود ندارد. در واقع این عملگر در اندازه‌گیری نقش کاملا فرعی و ثانوی ایفا می‌کند و برای تعریف اندازه‌گیری توجه به آن ضرورت ندارد. درباره این موضوع و چگونگی وارد شدن عملگر مربوط به یک مشاهده‌پذیر در ادامه بحث خواهیم کرد.

۱-۲-۱- اندازه‌گیری عام

یک دستگاه اندازه‌گیری با مجموعه‌ای از عملگرهای تصویرگر مثل $\{P_m, m = 1,...K\}$ مشخص می‌شود. این عملگرهای مصور خاصیت‌های زیر را دارند:

$$P_m P_n = \delta_{mn} P_m \qquad \sum_m P_m = I \tag{۳۹-۱}$$

هر عملگر P_m به یک نتیجه از آزمایش اندازه‌گیری مثل نتیجه m وابسته است. اندازه‌گیری روی حالت ρ با احتمال $P(m) = tr(P_m \rho P_m)$ نتیجه m را به دست می‌دهد. حالت‌های نهایی که نتیجه m را دارند عبارتند از

$$\rho_m = \frac{P_m \rho P_m}{tr(P_m \rho P_m)} \tag{۴۰-۱}$$

هرگاه نتیجه m را آنچنان تعبیر کنیم که خاصیتی مثل A مقدار a_m را داشته باشد می‌توانیم مقدار متوسط این خاصیت را به طریق زیر حساب کنیم:

$$\langle A\rangle_\rho = \sum_m a_m P(m) = \sum_m a_m tr(P_m \rho P_m) = \sum_m a_m tr(P_m \rho) = tr(\hat{A}\rho) \qquad (۴۱-۱)$$

که در آن

$$\hat{A} = \sum_m a_m P_m \qquad (۴۲-۱)$$

عملگری هرمیتی است که به خاصیت A نسبت داده‌ایم. هرگاه تصویرگرهای P_m یک بعدی باشند، احتمالات $P(m)$ به شکل زیر در می‌آیند:

$$P(m) = tr(|m\rangle\langle m|\rho) = \langle m|\rho|m\rangle \qquad (۴۳-۱)$$

و حالت بعد از به دست آوردن نتیجه‌ی m برابر خواهد شد با

$$\rho_m = \frac{P_m \rho P_m}{tr(P_m \rho P_m)} = \frac{|m\rangle\langle m|\rho|m\rangle}{\langle m|\rho|m\rangle} = |m\rangle\langle m| \qquad (۴۴-۱)$$

ضمنا اگر حالت اولیه خالص باشد، یعنی $\rho = |\psi\rangle\langle\psi|$، این احتمالات به

$$P(m) = \langle m|\psi\rangle\langle\psi|m\rangle = |\langle m|\psi\rangle|^2 \qquad (۴۵-۱)$$

تبدیل خواهند شد. عبارات اخیر بیان می‌کنند که اندازه‌گیری مشاهده پذیر A، حالت $|\psi\rangle$ را به یکی از ویژه حالت‌های عملگر $\hat{A}$ با احتمال $|\langle m|\psi\rangle|^2$ می‌برد.

هر گاه بعد از عبور از دستگاه اندازه‌گیری این حالت‌ها را از هم جدا نکنیم، حالت خروجی با یک آنسامبل مخلوط از حالت‌ها یعنی آنسامبل زیر داده می‌شود:

$$\rho' = \sum_m P(m)\rho_m = \sum_m P_m \rho P_m \qquad (۴۶-۱)$$

آنچه که در بالا گفتیم مربوط به اندازه‌گیری‌های متعامد یا تصویری است. ولی این نوع اندازه‌گیری قابل انجام در آزمایشگاه نیست. ممکن است که در یک اندازه‌گیری ذرات را از هم جدا کنیم ولی ذرات جدا شده کاملا از هم قابل تمیز نباشند. در واقع اندازه‌گیری تصویری یک ایده‌آل است که در آن فرض می-کنیم ذراتی که در اثر آزمایش جدا شده‌اند. (مثلا ذرات اسپین $\frac{1}{2}$ در آزمایش اشترن گرلاخ) تحت شیب میدان مغناطیسی در دو جهت مختلف نیرو احساس می‌کنند و جدا می‌شوند ولی تحت تاثیر خود میدان مغناطیسی نیز قرار گرفته و اسپین آنها حول میدان متوسط می‌چرخد. بنابراین در یک آزمایش واقعی اشترن گرلاخ که نتوان از اثرات حرکت وضعی اسپین‌ها صرفنظر کرد، حالتهای خروجی $|z,+\rangle$ و $|z,-\rangle$ نیستند، بلکه این حالتها $U|z,+\rangle$ و $U|z,-\rangle$ هستند که U نشان دهنده اثر میدان مغناطیسی بر حرکت وضعی اسپین‌هاست. این امر به این معناست که این اندازه‌گیری با عملگرهای تصویری $P_+ = |z,+\rangle\langle z,+|$ و $P_- = |z,-\rangle\langle z,-|$ مشخص نمی‌شود بلکه با عملگرهای $M_+ = UP_+$ و $M_- = UP_-$ مشخص می‌شود. واضح است که این عملگرها دیگر تصویری نیستند و حالت‌های جدا شده از هم کاملا متمایز نیستند.

۱-۲-۲- اندازه‌گیری‌های غیر متعامد

یک اندازه‌گیری غیر متعامد یا تعمیم یافته با مجموعه‌ای از عملگرهای $\{M_m, m = 1...K\}$ مشخص می‌شود که در شرط

$$M_m^\dagger M_m = I \qquad (۴۷-۱)$$

صدق می‌کنند. اندازه‌گیری روی حالت ρ با احتمال $P(m) = tr(M_m \rho M_m^\dagger)$ نتیجه m را به دست می‌دهد. حالتهایی که نتیجه m را دارند، عبارتند از:

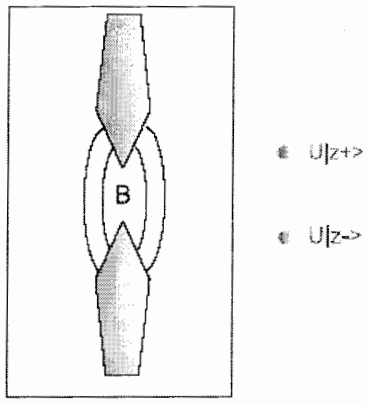
$$\rho_m = \frac{M_m \rho M_m^\dagger}{tr\left(M_m \rho M_m^\dagger\right)} \qquad (۴۸-۱)$$

هر گاه بعد از عبور از دستگاه اندازه‌گیری این حالت‌ها را از هم جدا نکنیم، حالت خروجی با یک آنسامبل مخلوط از حالت‌ها یعنی با آنسامبل زیر داده می‌شود:

$$\rho' = \sum_m P(m)\rho_m = \sum_m M_m \rho M_m^\dagger \qquad (۴۹-۱)$$

همانطور که گفتیم یک راه برای عملی شدن اندازه‌گیری غیر متعامد (شکل (۱-۱) را ملاحظه کنید) آن است که یک اندازه‌گیری تصویری و ایده‌آل را با یک تحول زمانی دنبال کنیم. در این صورت خواهیم داشت

$$M_m = UP_m \qquad (۵۰-۱)$$



شکل (۱-۱): در یک آزمایش اشترن گرلاخ غیر ایده‌آل، ذراتی که از دستگاه آزمایش بیرون می‌آیند لزوما حالت‌های متعامد بر هم ندارند.

که در آن U عملگر یکانی تحول است. در این شرایط با توجه به تعریف اندازه‌گیری متعامد خواهیم داشت:

$$\sum_m M_m^\dagger M_m = \sum_m P_m U^\dagger U P_m = \sum P_m = I \qquad (۵۱-۱)$$

و

$$P(m) = U \frac{P_m \rho P_m}{tr(P_m \rho P_m)} U^\dagger = \frac{M_m \rho M^\dagger{}_m}{tr(M_m \rho M_m)} \qquad (۵۲-۱)$$

۱-۲-۳- اندازه‌گیری‌های عام *POVM*

در بسیاری از اوقات ما تنها به آمار اندازه‌گیری و نه به حالتهای پس از اندازه‌گیری علاقه‌مند هستیم. در واقع بیشتر اندازه‌گیری‌های ما از این نوع هستند. در چنین مواردی که تنها به احتمال رویداد علاقه‌مند هستیم می‌توانیم بنویسیم

$$P(m) = tr(M_m \rho M_m^\dagger) = tr(M_m^\dagger M_m \rho) = tr(E_m \rho) \qquad (۵۳-۱)$$

که در آن E_m ها عملگرهای مثبت هستند و در شرط

$$\sum_m E_m = I \qquad (۵۴-۱)$$

صدق می‌کنند. به این ترتیب به نوعی از اندازه‌گیری می‌رسیم که با مجموعه‌ای از عملگرهای مثبت که $\{E_m, m = 1...K\}$ که در شرط (۱-۵۴) صدق می‌کنند تعریف می‌شود. این نوع اندازه‌گیری را اصطلاحا اندازه‌گیری $POVM$ می‌گویند که از حروف اول کلمات Positive Operator Valued Measure ساخته شده است. اندازه‌گیری $POVM$ می‌تواند قدرتمندتر از یک اندازه‌گیری تصویری باشد به این معنا که این نوع اندازه‌گیری می‌تواند قدرت تمیز بیشتری داشته باشد. برای درک این نکته به یک مثال توجه می‌کنیم.

فرض کنید که آلیس تعداد زیادی از حالتهای $|\psi_1\rangle$ و $|\psi_2\rangle$ در اختیار دارد و این حالت‌ها را به طور تصادفی برای باب می‌فرستد. باب می‌بایست با انجام بهترین اندازه‌گیری‌ها بتواند تا حد ممکن تشخیص دهد که آیا آلیس حالت $|\psi_1\rangle$ را برای وی فرستاده است یا حالت $|\psi_2\rangle$ را.

$$|\psi_1\rangle = |0\rangle \qquad |\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \tag{۵۵-۱}$$

واضح است که اندازه‌گیری تصویری در پایه $|0\rangle$ و $|1\rangle$ نمی‌تواند به باب کمک کند، زیرا هر وقت که وی نتیجه 0 را به دست می‌آورد (یعنی در ۷۵ درصد موارد) نمی‌داند که کدام یک از حالت‌های دوگانه فوق برای وی ارسال شده است. وی تنها در ۲۵ درصد موارد که نتیجه 1 را به دست می‌آورد مطمئن است که حالت $|\psi_2\rangle$ برای وی ارسال شده است. به جای این نوع اندازه‌گیری وی یک اندازه-گیری $POVM$ با عملگرهای زیر انجام می‌دهد:

$$E_1 = \alpha|1\rangle\langle 1|, \qquad E_2\beta\left(|0\rangle - |1\rangle\right)\left(\langle 0| - \langle 1|\right) \tag{۵۶-۱}$$

و

$$E_3 = I - E_1 - E_2 = (1-\beta)|0\rangle\langle 0| + (1-\alpha-\beta)|1\rangle\langle 1| + \beta\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right)$$
$$= \begin{pmatrix} 1-\beta & \beta \\ \beta & 1-\alpha-\beta \end{pmatrix} \tag{۵۷-۱}$$

که درآن‌ها α و β اعداد مثبتی هستند که می‌بایست چنان انتخاب شوند که عملگر E_3 نیز مثبت باشد. می‌خواهیم ببینیم که باب در چند درصد موارد می‌تواند با قطعیت نوع حالت ارسال شده را تشخیص دهد. برای این کار دقت می‌کنیم که آنسامبل حالتهای ارسال شده به صورت زیر است:

$$\rho = \frac{1}{2}\left(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|\right) \tag{۵۸-۱}$$

همچنین می‌دانیم که وقتی نتیجه ۱ به دست آید وی با اطمینان می‌گوید که حالت $|\psi_1\rangle$ برای وی ارسال شده است. تنها در حالت بدست آوردن نتیجه ۳ است که وی همچنان مردد باقی خواهد ماند. بنابراین احتمال موفقیت با $P(1)+P(2)$ که در آن

$$P(1) = tr(\rho E_1) = \frac{1}{2}\langle\psi_2|E_1|\psi_2\rangle = \frac{1}{4}\alpha \tag{۵۹-۱}$$

$$P(2)=tr(\rho E_2)=\frac{1}{2}\langle\psi_1|E_2|\psi_1\rangle=\frac{1}{2}\beta \qquad (۶۰-۱)$$

با بیشینه کردن این مقدار احتمالات ضمن رعایت قید مثبت بودن E_3 می‌بینیم که بهترین انتخاب برای پارامترهای α و β برابر است با:

$$\alpha=\frac{\sqrt{2}}{1+\sqrt{2}} \qquad \beta=\frac{1}{2}\frac{\sqrt{2}}{1+\sqrt{2}} \qquad (۶۱-۱)$$

در نتیجه خواهیم داشت:

$$P_{correct}=\frac{1}{4}\alpha+\frac{1}{2}\beta=\frac{1}{2}\frac{\sqrt{2}}{1+\sqrt{2}}=0.29 \qquad (۶۲-۱)$$

یعنی این بار بر خلاف قبل باب می‌تواند در ۲۹ درصد از موارد، حالت‌ها را به دقت تشخیص دهد.

$$|1\rangle=\frac{1}{2}|e_1\rangle+\frac{1}{2}|e_2\rangle+\frac{1}{\sqrt{2}}|e_3\rangle$$

$$|2\rangle=\frac{1}{\sqrt{2}}|e_1\rangle-\frac{1}{\sqrt{2}}|e_2\rangle \qquad (۶۳-۱)$$

$$|3\rangle=\frac{1}{2}|e_1\rangle+\frac{1}{2}|e_2\rangle-\frac{1}{\sqrt{2}}|e_3\rangle$$

آیا اندازه‌گیری‌های $POVM$ تنها یک امکان خیالی و نظری است یا اینکه واقعا می‌توان چنین اندازه-گیری‌هایی را انجام داد. برای فهم اندازه‌گیری $POVM$ به شکل(۱-۲) مراجعه می‌کنیم. در این شکل حالت اولیه در زیرفضایی که توسط بردارهای $|1\rangle$ و $|2\rangle$جاروب می‌شود قرار گرفته است. ممکن است که به دلایل تجربی، اندازه‌گیری را در فضای بزرگتری که با بردارهای $|e_1\rangle$، $|e_2\rangle$ و $|e_3\rangle$ جاروب می-شود، انجام دهیم. این اندازه‌گیری از دید ناظری که در همان زیرفضای کوچک زندگی می‌کند یک اندازه‌گیری تصویری نیست. در واقع می‌توان نشان داد که هر اندازه‌گیری $POVM$ را می‌توان به این

شکل بازسازی کرد. نخست به یک مثال توجه می‌کنیم. فرض کنید که بردارهای نشان داده شده در شکل به صورت زیر باشند:

$$|e_1\rangle = \frac{1}{2}|1\rangle + \frac{1}{\sqrt{2}}|2\rangle + \frac{1}{2}|3\rangle$$

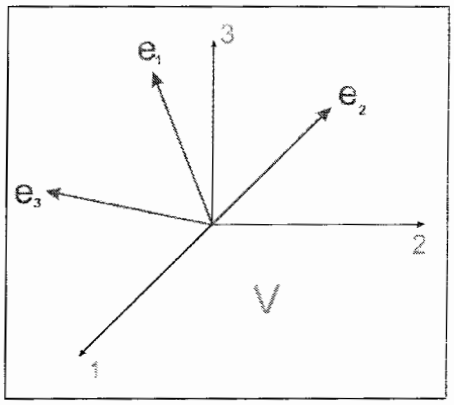
$$|e_2\rangle = \frac{1}{2}|1\rangle - \frac{1}{\sqrt{2}}|2\rangle + \frac{1}{2}|3\rangle \qquad (۶۴-۱)$$

$$|e_3\rangle = \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|3\rangle$$

حال یک اندازه‌گیری تصویری در امتداد بردارهای فوق روی حالت زیر انجام می‌دهیم. این بردار در زیرفضای V قرار گرفته است ولی اندازه‌گیری ما در فضای بزرگ W انجام می‌شود.

فرض کنید که برداری که روی آن اندازه‌گیری می‌کنیم به صورت زیر باشد:

$$|\psi\rangle = a|1\rangle + b|2\rangle = \left(\frac{a}{2} + \frac{b}{\sqrt{2}}\right)|e_1\rangle + \left(\frac{a}{2} - \frac{b}{\sqrt{2}}\right)|e_2\rangle + \frac{a}{\sqrt{2}}|e_3\rangle \qquad (۶۵-۱)$$



شکل(۱-۲): اندازه‌گیری تصویری در امتداد بردارهای فضای بزرگ از دید ناظری که در یک زیرفضا قرار دارد یک اندازه-گیری تعمیم یافته است.

در این صورت اندازه‌گیری تصویری روی این بردار حالت در امتداد $|e_1\rangle$، $|e_2\rangle$ و $|e_3\rangle$ با احتمالات زیر مرتبط است:

$$P(e_1)=\left(\frac{a}{2}+\frac{b}{\sqrt{2}}\right)^2$$
$$P(e_2)=\left(\frac{a}{2}-\frac{b}{\sqrt{2}}\right)^2 \qquad (۶۶-۱)$$
$$P(e_3)=\frac{a^2}{2}$$

به این معنا که با احتمالات فوق حالت ذره به یکی از حالت‌های $|e_1\rangle$، $|e_2\rangle$ یا $|e_3\rangle$تصویر خواهد شد. اما نتیجه اندازه‌گیری را می‌بایست از دید ناظر درون زیرفضای V نگاه کنیم. در نتیجه می‌بایست بردارهای فوق را به زیرفضای V تصویر کنیم. بنابراین نتیجه آن خواهد شد که اندازه‌گیری انجام شده از دید این ناظر، بردار حالت را با احتمالات بالا به یکی از حالتهای غیر متعامد زیر تصویر می‌کند.

$$|\nu_1\rangle=\sqrt{\frac{1}{3}}|1\rangle+\sqrt{\frac{2}{3}}|2\rangle$$
$$|\nu_2\rangle=\sqrt{\frac{1}{3}}|1\rangle-\sqrt{\frac{2}{3}}|2\rangle \qquad (۶۷-۱)$$
$$|\nu_3\rangle=|1\rangle$$

این مثال نشان می‌دهد که چگونه یک اندازه گیری غیر متعامد از یک اندازه‌گیری تصویری یا متعامد در یک فضای بزرگ‌تر به وجود می‌آید. این مثال نمونه‌ای از یک قضیه کلی است که نشان می‌دهد هر نوع اندازه‌گیری $POVM$ به این طریق قابل بازسازی است.

۱-۲-۴- اندازه‌گیری روی سیستم‌های مرکب

نخست یک مثال ساده را بررسی می‌کنیم. فرض کنید که یک ذره اسپین $\frac{1}{2}$ در حالت $|\psi\rangle=a|+\rangle+b|-\rangle$ است که در آن $|+\rangle$ و $|-\rangle$ ویژه حالت‌های عملگر S_z هستند. ممکن است

به دلایلی اندازه‌گیری اسپین این ذره در راستای z برای ما امکان پذیر نباشد ولی بتوانیم اسپین کل یک سیستم دو ذره‌ای را مشخص کنیم. برای سادگی فرض می‌کنیم که ذره دوم در حالت $|+\rangle$ قرار داشته باشد. در این صورت سیستم مرکب در حالت

$$|\Psi\rangle = a|+,+\rangle + b|-,+\rangle \qquad (۶۸-۱)$$

قرار دارد. برای اندازه‌گیری اسپین کل یعنی S^2 این دو ذره، حالت فوق را به صورت زیر بسط می‌دهیم:

$$|\Psi\rangle = a|1,1\rangle + b\frac{1}{\sqrt{2}}\left(|1,0\rangle - |0,0\rangle\right) \qquad (۶۹-۱)$$

در اینجا از نمادهای $|l,m\rangle$ مربوط به تکانه زاویه‌ای استفاده کرده‌ایم. از آنجا که اندازه‌گیری اسپین کل انجام می‌شود، این سیستم دو ذره‌ای با احتمالات زیر به حالت‌های نوشته شده تصویر می‌شود:

$$\begin{aligned} P(1) &= a^2 + \frac{b^2}{2} & & \frac{1}{\sqrt{a^2+\frac{b^2}{2}}}\left(|1,1\rangle + |1,0\rangle\right) \\ P(0) &= \frac{b^2}{2} & & |0,0\rangle \end{aligned} \qquad (۷۰-۱)$$

یا با بازنویسی حالت‌ها

$$\begin{aligned} P(1) &= a^2 + \frac{b^2}{2} & & \frac{1}{\sqrt{a^2+\frac{b^2}{2}}}\left(a|+,+\rangle + \frac{b}{\sqrt{2}}\left(|+,-\rangle + |-,+\rangle\right)\right) \\ P(0) &= \frac{b^2}{2} & & \frac{1}{\sqrt{2}}\left(|+,-\rangle - |-,+\rangle\right) \end{aligned} \qquad (۷۱-۱)$$

برای آنکه حالتهای بعد از اندازه‌گیری را برای ذره اول تشخیص دهیم، می‌بایست ماتریس چگالی آن را محاسبه کنیم. به دست می‌آوریم:

$$P(1)=a^2+\frac{b^2}{2} \qquad \rho_1=\left(a^2+\frac{b^2}{2}\right)|+\rangle\langle+|+\frac{b^2}{2}|-\rangle\langle-|+\frac{ab}{\sqrt{2}}\left(|+\rangle\langle-|+|-\rangle\langle+|\right)$$
$$P(0)=\frac{b^2}{2} \qquad \rho_0=\frac{1}{2}I \tag{۷۲-۱}$$

و حالتهای ρ_0 و ρ_1 بر هم عمود نیستند و حال آنکه اندازه‌گیری اسپین کل، یک اندازه‌گیری تصویری و متعامد است. در ادامه به صورت کلی این نوع اندازه‌گیری را مطالعه می‌کنیم.

فرض کنید که روی سیستم AB یک اندازه‌گیری تصویری با عملگرهای $\{P_m, m=1...K\}$ انجام دهیم. در این صورت احتمال به دست آوردن نتیجه m برابر است با

$$P_m(m)=tr\left(P_m\left(\rho_A\otimes\rho_B\right)\right) \tag{۷۳-۱}$$

حال احتمال $P_A(m)$ را می‌بایست چنان بازنویسی کنیم که مستقیما به چگالی ρ_A مرتبط شود. می‌نویسیم:

$$\begin{aligned}P_m(m)&=tr\left(P_m\left(\rho_A\otimes\rho_B\right)\right)=\langle i,\mu|P_m|j,\nu\rangle\langle j,\nu|\rho_A\otimes\rho_B|i,\mu\rangle\\&=\langle i,\mu|P_m|j,\nu\rangle\left(\rho_A\right)_{ji}\langle\nu|\rho_B|\mu\rangle=\left(E_m\right)_{ij}=tr_A\left(E_m\rho_A\right)\end{aligned} \tag{۷۴-۱}$$

که در آن E_m ماتریسی است با درایه‌های زیر:

$$\left(E_m\right)_{ij}=\langle i,\mu|P_m|j,\nu\rangle\langle\nu|\rho_B|\mu\rangle=\left(P_m\right)_{i\mu,j\nu}\left(\rho_B\right)_{\nu\mu} \tag{۷۵-۱}$$

به راحتی معلوم می‌شود که

$$\begin{aligned}\sum_m\left(E_m\right)_{ij}&=\langle i,\mu|\sum_m P_m|j,\nu\rangle\langle\nu|\rho_B|\mu\rangle+\langle i,\mu|I|j,\nu\rangle\langle\nu|\rho_B|\mu\rangle\\&=\delta_{ij}\delta_{\mu,\nu}\langle\nu|\rho_B|\mu\rangle=\delta_{ij}tr\left(\rho_B\right)=\delta_{ij}\end{aligned} \tag{۷۶-۱}$$

و در نتیجه شرط $\sum_m E_m=I_A$ برقرار می‌شود. همچنین می‌توانیم ثابت کنیم که عملگرهای E_m همگی نامنفی هستند. برای این کار عنصر ماتریسی E_m روی یک بردار دلخواهی $|\nu\rangle\in V_A$ حساب می‌کنیم.

حال $|\omega\rangle$ را با درایه‌های زیر تعریف می‌کنیم

$$\omega_\mu = (e_m)_{i\mu}\, v_i^* \qquad (۷۷-۱)$$

که با توجه به آن می‌توان نوشت

$$\langle \nu|E_m|\nu\rangle = \omega_\nu^*(\rho_B)_{\nu\mu}\omega_\mu = \langle\omega|\rho_B|\omega\rangle \geq 0 \qquad (۷۸-۱)$$

بنابراین عملگرهای E_m مثبت هستند. به این ترتیب ثابت کرده‌ایم که یک اندازه‌گیری تصویری روی فضای $V_A \otimes V_B$ یک اندازه‌گیری $POVM$ روی فضای V_A است. [۱۳,۵,۳]

فصل دوم:
مدارهای کوانتومی

مقدمه

در این فصل در ابتدا با مدل مداری برای محاسبات کلاسیک آشنا می‌شویم و در ادامه به بحث در مورد مدارهای کوانتومی و گیتهای کوانتومی می‌پردازیم و یک مجموعه عملگر جهانی را ارائه می-دهیم.

۲-۱- مدل مداری برای محاسبات کلاسیک

می‌دانیم که در کامپیوترهای کلاسیک تمام اطلاعات به شکل رشته‌ای از متغیرهای 1 و 0 ذخیره می‌شوند. پردازش داده‌ها از هر نوع که باشد، چیزی نیست جز انجام اعمال منطقی روی این رشته-ها. هر متغیر دو حالته که می‌تواند دو مقدار 0 یا 1 را اختیار کند یک بیت نامیده می‌شود. یک بیت را با متغیر x نشان می‌دهیم. یک رشته دو بیتی با نماد x_1x_0 و یک رشته‌ی n بیتی با نماد $x_{n-1}x_{n-2}...x_1x_0$ نشان می‌دهیم که در این صورت مقدار عددی آن عبارت خواهد بود از

$$x = x_{n-1} \times 2^{n-1} \times x_{n-2} \times 2^{n-2} + ...x_1 \times 2^1 + x_0 \times 2^0 \qquad (۱-۲)$$

مجموعه تمام متغیرهای n بیتی را با B_n نمایش می‌دهیم. چنین مجموعه‌ای 2^n عضو دارد که ارزش عددی آنها بین مقدار 0 تا 2^2-1 تغییر می‌کند. هر نوع پردازش اطلاعات چیزی نیست جز یکی سلسله توابع پی در پی که روی یک رشته‌ی ورودی با طول معین انجام می‌شود. تمام این توابع را می‌توان با ترکیب توابعی مقدماتی که تنها روی یک بیت و یا دو بیت اثر می‌کنند، ساخت.

ساده‌ترین توابع مقدماتی عبارتند از توابع NOT، OR، AND و XOR که به صورت زیر تعریف می‌شوند:

$$NOT : x \to \bar{x} = x + 1 \bmod 2 \qquad (۲-۲)$$

$$OR : (x, y) \to x \vee y = x + y - xy \bmod 2 \qquad (۳-۲)$$

$$AND : (x, y) \to x \wedge y = xy \qquad (۴-۲)$$

$$XOR : (x, y) \to x \oplus y = x + y - 2xy \qquad (۵-۲)$$

هر کدام از این توابع مقدماتی را اصطلاحا یک گیت می‌نامند. همچنین از این خاصیت مهم نیز استفاده می‌شود که از یک بیت کلاسیک مثل x همواره می‌توان نسخه‌های متعدد به دست آورد. توابع مقدماتی فوق خواص ساده و در عین حال مهمی دارند. مهمترین این خواص را در زیر می‌نویسیم.

الف) تمام توابع دوتایی جابجایی و شرکت پذیر هستند یعنی

$$x \bigcirc y = y \bigcirc x \qquad (۶-۲)$$

$$(x \bigcirc y) \bigcirc z = x \bigcirc (y \bigcirc z) \qquad \bigcirc \in \{\wedge, \vee, \oplus\} \qquad (۷-۲)$$

ب: اثر این توابع روی مقادیر خاص به صورت زیر است:

$$x \vee 0 = x, \qquad x \vee 1 = 1, \qquad x \vee x = x \qquad x \vee \bar{x} = 1 \qquad (۸-۲)$$

$$x \wedge 0 = 0, \qquad x \wedge 1 = 1, \qquad x \wedge x = x, \qquad x \wedge \bar{x} = 0 \qquad (۹-۲)$$

$$x \oplus 0 = x, \qquad x \oplus 1 = \bar{x}, \qquad x \oplus x = 0, \qquad x \oplus \bar{x} = 1 \qquad (۱۰-۲)$$

ج: ترکیب NOT و توابع AND و NOT، روابط زیر اصطلاحا به قوانین دمورگان مشهور هستند:

$$\overline{x \vee y} = \bar{x} \wedge y \qquad \overline{x \wedge y} = \bar{x} \vee \bar{y} \qquad (۱۱-۲)$$

د: ترکیب NOT و تابع XOR که کاربردهای زیادی در اثبات قضایا و خواص دیگر آن دارد.

$$\overline{x \oplus y} = \bar{x} \oplus y = x \oplus \bar{y}$$
$$\bar{x} \oplus \bar{y} = x \oplus y \qquad (۱۲-۲)$$

سوالی که اینجا مطرح می‌شود این است که آیا گیتهای مقدماتی فوق برای ساختن هر تابع دلخواه کافی هستند یا خیر. قضیه زیر در واقع پاسخ مثبتی به این سوال است.

قضیه: هر تابع دلخواه $f : B_m \to B_n$ را می‌توان با ترکیب تعدادی متناهی تابع NOT، AND و OR ساخت. به عبارت دیگر این گیتهای مقدماتی یک مجموعه گیتهای جهانی[1] هستند.

اثبات: می‌دانیم که هر تابع $f : B_m \to B_n$ چیزی نیست جز n تابع متفاوت از B_m به B_1. بنابراین قضیه را برای این توابع ثابت می‌کنیم. برای اثبات از استقراء استفاده می‌کنیم. می‌دانیم که برای $n=1$ قضیه برقرار است زیرا تنها توابع ممکن عبارتند از تابع همانی و تابع NOT. حال فرض کنید که قضیه برای n برقرار است. عبارت $f(x_1, x_2, ..., x_{n+1})$ را در نظر بگیرید.

می‌دانیم که

$$f(x_1, x_2, ...x_n, x_{n+1}) = \begin{cases} f(x_1, x_2, ...x_n, 0) & if \quad x_{n+1} = 0 \\ f(x_1, x_2, ...x_n, 1) & if \quad x_{n+1} = 1 \end{cases} \qquad (۱۳-۲)$$

رابطه فوق را می‌توان به صورت زیر نوشت:

$$f(x_1, x_2, ...x_n, x_{n+1}) = \left[\overline{x_{n+1}} \wedge f(x_1, x_2, ...x_n, 0)\right] \vee \left[f(x_1, x_2, ...x_n, 1)\right] \qquad (۱۴-۲)$$

اما توابع درون کروشه توابع n متغیره هستند که فرض استقراء می‌گوید می‌توان آنها را بر حسب گیت‌های مقدماتی نوشت.

۲-۱-۱- مدارهای کلاسیک برگشت پذیر

توابع مقدماتی‌ای که به آنها اشاره کردیم وارون پذیر نیستند. یک تابع وارون‌پذیر به لحاظ نظری حتما توانی مصرفی می‌کند که نمی‌توان با هیچ پیشرفتی در فناوری از آن جلوگیری کرد. یعنی هر چقدر هم که بکوشیم از هدر رفتن انرژی در مدارها و قطعات جلوگیری کنیم، یک حد تئوریک از

[1] universal set of gates

اتلاف انرژی وجود دارد که از آن نمی‌توانیم حذر کنیم. این حد را نخستین بار رالف لاندائر[1] در ۱۹۶۹ نشان داده است. مبنای استدلال او این است که در تابع وارون ناپذیر مقداری، اطلاعات گم می‌شود (زیرا نمی‌توان از خروجی تابع به ورودی آن پی برد) و هر نوع پاک کردن اطلاعات نیز با کاهش آنتروپی سیستم و افزایش آنتروپی محیط همراه است. کافی است برای درک این نکته به ساده ترین تعبیه یک بیت نگاه کنیم. فرض کنید که یک اتاقک میکروسکوپی ساخته‌ایم که در درون آن یک مولکول وجود دارد، وقتی که مولکول در سمت راست اتاقک است مقدار بیت برابر 1 و وقتی که در سمت چپ اتاقک است مقدار بیت برابر صفر است. تعداد N تا این بیتها را در نظر بگیرید که مجموعا یک عدد را نشان می‌دهند.

پاک کردن اطلاعات به معنای آن است که این عدد را صرف نظر از مقداری که دارد به یک عدد مرجع مثل 000...0 برگردانیم. این کار را می‌توانیم به کمک یک پیستون و دیواره‌ی بدون اصطکاک که در وسط اتاقک تعبیه کرده‌ایم انجام دهیم. اما این کار نهایتا باعث کاهش آنتروپی سیستم به اندازه $kN\ln 2$ و افزایش آنتروپی محیط به همین مقدار خواهد شد. بنابراین به ازای پاک کردن هر بیت اطلاعات می‌بایست کاری معادل $KT\ln 2$ ژول انجام دهیم که در آن T دمای محیط است.

بنابراین اگر با تابع وارون ناپذیر کار کنیم با این حد نظری از مصرف انرژی روبرو هستیم. کار مهم چارلز بنت[2] آن بوده که نشان داده است می‌توان با انجام محاسبات به صورت وارون‌پذیر مصرف انرژی را در کامپیوترها لااقل به لحاظ نظری به صفر رساند.

چگونه می‌توان محاسبات را به صورت برگشت پذیر انجام داد و حال آنکه اغلب توابع وارون پذیر نیستند به خصوص می‌دانیم گیتهای جهان شمولی که تمام مدارهای منطقی از آنها ساخته می‌شوند، مثل گیت‌های AND و OR وارون‌پذیر نیستند.

---

[1] Ralph Landauer
[2] Charles Bennett

برای این کار نخست نشان می‌دهیم که با اضافه کردن مجموعه‌ای ازبیت‌ها به اسم بیت کمکی[۱]، می‌توان هر تابع دلخواه را به صورت برگشت پذیر نیز تعبیه کرد. فرض کنید که $f : B_m \to B_n$ یک تابع دلخواه است. تابع $f_r : B_{m+n} \to B_{+mn}$ را به شکل زیر تعریف می‌کنیم:

$$f_r(x,y) := (x, f(x) \oplus y) \qquad (۱۵-۲)$$

در این رابطه $x \in B_m, f(x), y \in B_n$ و تابع $f(x) \oplus y$ به صورت بیت به بیت تعریف شده است. به عبارت دیگر:

$$f_r(x_1, x_2, ...x_m, y_1, y_2, ...y_n) := (x_1, x_2, ...x_m, f_1(x_1...x_m) \oplus y_1 ... f_n(x_1...x_m) \oplus y_n) \qquad (۱۶-۲)$$

حال دقت می‌کنیم که

$$f_r(x,0) = (x, f(x) \oplus 0) = (x, f(x)) \qquad (۱۷-۲)$$

بنابراین تابع اولیه f به ازای مقدار 0 روی بیت‌های کمکی در خروجی ظاهر می‌شود. هم چنین تابع f_r وارون‌پذیر است زیرا

$$\begin{aligned} & f_r(x,y) = f_r(x',y') \to (x, f(x) \oplus y) = (x', f(x') \oplus y) \\ & \to x = x' \ , \ f(x) \oplus y = f(x) \oplus y' \end{aligned} \qquad (۱۸-۲)$$

اما از تساوی $f(x) \oplus y = f(x) \oplus y'$ به راحتی و با استفاده از خواص تابع XOR ثابت می‌شود که $y = y'$. بنابراین تابع f_r یک تابع برگشت پذیر است که تابع f را به ازای مقادیر معینی از بیت‌های کمکی در خود نهفته دارد.

۲-۲- مدارهای کوانتومی[۲]

گیت کوانتومی یک عملگر یکانی است که روی یک بردار دلخواه عمل می‌کند. اگر یک حافظه‌ی n کیوبیتی داشته باشیم فضای هیلبرت حالتهای آن عبارت است از $H = C^{2 \otimes n}$ که در آن C^2 یک فضای دو بعدی مختلط است. بعد این فضا برابر است با 2^n و یک گیت دلخواه یعنی یک عملگر

[۱] ancilla bit
[۲] quantum circuits

یکانی که روی این فضای هیلبرت عمل می‌کند. چنین عملگری با یک ماتریس مربعی $2^n \times 2^n$ نشان داده می‌شود که دارای تعداد 2^{2n} پارامتر است، به عنوان مثال فضای گیتهای دو کیوبیتی یک فضای ۱۶ پارامتری است. دقت کنید که این فضاها همه پیوسته هستند و بینهایت نقطه دارند که هر نقطه آنها نشان دهنده یک عملگر یکانی است و تعداد پارامترهایی که بر شمردیم تنها تعداد پارامترهای لازم برای برچسب زدن روی نقاط این فضاها را مشخص می‌کند. به این ترتیب فضای سه بعدی متعارف دکارتی در مقابل همه این فضاها کوچک است زیرا هر نقطه‌اش تنها با سه پارامتر مشخص می‌شود. به این ترتیب با اولین دشواری خود در نظریه و همچنین ساخت کامپیوترهای کوانتومی مواجه می‌شویم. آیا می‌توان با یک مجموعه متناهی از گیتها آنچنان که در کامپیوترهای کلاسیک انجام می‌شود، تمام گیتهای ممکن را پیاده‌سازی کرد؟ اگر بتوان یک مجموعه متناهی مثل $G := \{G_1, G_2, ...G_K\}$ پیدا کرد که به کمک آنها بتوان تمام گیتهای یکانی را پیاده سازی کرد، می‌گوییم مجموعه‌ی G یک مجموعه‌ی گیتهای جهانی را تشکیل می‌دهد. در همین ابتدا باید دو نکته مهم را توضیح دهیم.

نکته اول: مسلم است با یک مجموعه متناهی هرگز نمی‌توان یک مجموعه پیوسته از گیتها را پیاده سازی کرد مگر اینکه خود را قانع به پیاده سازی تقریبی از گیتها کنیم. بنابراین فرض کنید که حد دقتی که در نظر داریم برابر با εباشد. در این صورت هر گاه به جای عملگر U، با استفاده از گیتهای عام خود، عملگر $\tilde{U}$ را چنان بسازیم که شرط

$$E(U,\tilde{U}) := Max_{|\psi\rangle} \left\| (U - \tilde{U})|\psi\rangle \right\| < \varepsilon \qquad (۱۹-۲)$$

برقرار شود، می‌گوییم که گیت U را با دقت خوبی (یعنی با دقت قابل قبول ε) پیاده سازی کرده‌ایم.

نکته دوم: در پیاده سازی گیتها مهم است که از چه تعداد گیت جهانی برای ساختن یک گیت دلخواه استفاده می‌کنیم و این تعداد چه نسبتی با n، یعنی تعداد کیوبیتها و همچنین دقتی که

می‌خواهیم به کار ببریم یعنی ε دارد. اگر مجبور شویم برای بالا بردن دقت خود و یا تعداد کیوبیتها تعداد گیتهای یونیورسالی را که به کار می‌بریم به طور نمایی افزایش دهیم، باز هم پروژه ساخت کامپیوترهای کوانتومی با شکست مواجه خواهد شد. خوشبختانه چنین نیست و این موضوع نیز از دلایلی است که ما را به ساختن کامپیوترهای کوانتومی امیدوار می‌کند.

۲-۲-۱- مفهوم دقت در گیت‌های کوانتومی

در این بخش می‌خواهیم مفهوم عملی رابطه (۲-۱۹) را بفهمیم. فرض کنید که قرار است روی حالت اولیه $|\psi\rangle$، گیت U اثر کند و حالت $|\phi\rangle$ تولید شود ولی اشتباها یا به خاطر عدم دقتی که ما در ساخت گیت‌های کوانتومی داریم گیت $\tilde{U}$ روی این حالت اثر می‌کند و حالت $|\tilde{\varphi}\rangle$ تولید می‌شود. در این صورت می‌خواهیم ببینیم که نتایج اندازه‌گیری روی حالتهای $|\phi\rangle$ و $|\tilde{\phi}\rangle$ چقدر با هم تفاوت دارند. فرض کنید که E یک عملگر $POVM$ باشد که مربوط به یک نتیجه (یا خروجی) خاص باشد. در این صورت احتمال مشاهده این نتیجه خاص را برای دو حالت با هم مقایسه می‌کنیم، داریم:

$$P = \langle\phi|E|\phi\rangle = \langle\psi|U^{\dagger}EU|\psi\rangle \qquad \tilde{P} = \langle\tilde{\varphi}|E|\tilde{\varphi}\rangle = \langle\psi|\tilde{U}^{\dagger}E\tilde{U}|\psi\rangle \tag{۲-۲۰}$$

بنابراین

$$\left|\tilde{P} - P\right| = \left|\langle\tilde{\phi}|E|\tilde{\phi}\rangle - \langle\phi|E|\phi\rangle\right| \tag{۲-۲۱}$$

حالت $|\Delta\rangle$ را به شکل زیر تعریف می‌کنیم:

$$|\Delta\rangle := |\tilde{\phi}\rangle - |\phi\rangle = |(\tilde{U} - U)|\psi\rangle| \tag{۲-۲۲}$$

در نتیجه می‌توانیم رابطه (۲-۲۱) را به شکل زیر بنویسیم:

$$\left|\tilde{P} - P\right| = \left|\langle\tilde{\phi}|E|\Delta\rangle + \langle\Delta|E|\phi\rangle\right| \tag{۲-۲۳}$$

حال نخست از نامساوی مثلث $|a+b|\le|a|+|b|$ و سپس از نامساوی کوشی- شوارتز استفاده می-کنیم و نتیجه می‌گیریم

$$\left|\widetilde{P}-P\right|\le\left|\left\langle\widetilde{\phi}\left|E\right|\Delta\right\rangle\right|+\left|\left\langle\Delta\left|E\right|\phi\right\rangle\right|\le\left\|\Delta\right\|+\left\|\Delta\right\|=2\left\|(\widetilde{U}-U)|\psi\rangle\right\|\le 2\varepsilon. \qquad (۲۴-۲)$$

بنابراین اگر فاصله $E(\widetilde{U},U)$ از ε کمتر باشد، این امر به این معناست که نتایج همه اندازه‌گیری-های ممکنی که روی یک حالت دلخواه $|\psi\rangle$ انجام می‌دهیم حداکثر به اندازه 2ε دچار خطا می-شود.

حال فرض کنید که قرار است رشته‌ای از گیتهای $U_1,U_2,...,U_N$ را روی یک حالت اعمال کنیم و به خاطر عدم دقتی که داریم رشته‌ی $\widetilde{U}_1\widetilde{U}_2...\widetilde{U}_N$ را روی آن حالت اعمال می‌کنیم که هر کدام از این گیت‌ها به معنایی که در بالا توضیح دادیم خطای ε دارند. می‌خواهیم ببینیم که خطای این رشته از گیت‌ها چه ربطی به N دارد. اگر این خطا رابطه‌ای نمایی با N داشته باشد، خبر بدی است. ولی نشان می‌دهیم که

$$E(\widetilde{U}_1\widetilde{U}_2...\widetilde{U}_N,U_1U_2...U_N)\le N\varepsilon \qquad (۲۵-۲)$$

که به معنای آن است که خطا به صورت خطی با تعداد گیتها زیاد می‌شود. بنابراین کافی است که دقت اولیه گیت‌ها را به اندازه $\frac{\varepsilon}{N}$ بالا ببریم تا خطای کل کمتر از ε باشد. برای اثبات رابطه (۲-۲۵) حالت $N=2$ را در نظر می‌گیریم که ایده کلی اثبات را در بر دارد. می‌دانیم که به ازای هر حالت $|\psi\rangle$

$$\begin{aligned}\left\|(\widetilde{U}_1\widetilde{U}_2-U_1U_2)|\psi\rangle\right\|&=\left\|(\widetilde{U}_1\widetilde{U}_2-U_1\widetilde{U}_2)|\psi\rangle+(U_1\widetilde{U}_2-U_1U_2)|\psi\rangle\right\|\\&\le\left\|(\widetilde{U}_1\widetilde{U}_2+U_1\widetilde{U}_2)|\psi\rangle\right\|+\left\|U_1\widetilde{U}_2-U_1U_2)|\psi\rangle\right\| \qquad (۲۶-۲)\\&\le\left\|(\widetilde{U}_1-U_1)\widetilde{U}_2|\psi\rangle\right\|+\left\|U_1(\widetilde{U}_2-U_2)|\psi\rangle\right\|\end{aligned}$$

حال برای جمله اول در سمت راست از تعریف $E(\tilde{U}_1,U_1)$و برای جمله دوم نیز، بعد از اینکه U_1 بدلیل اینکه نرم بردار را عوض نمی‌کند برداشتیم، از تعریف $E(\tilde{U}_2,U_2)$ استفاده می‌کنیم و بدست می‌آوریم:

$$\left\|\tilde{U}_1\tilde{U}_2-U_1U_2\right\|\le E(\tilde{U}_1,U_1)+E(\tilde{U}_2,U_2) \qquad (۲۷-۲)$$

این اثبات به همین شکل برای N دلخواه تعمیم پیدا می‌کند.

۲-۲-۲- یک مجموعه‌ی عملگرهای جهانی

در اینجا نشان می‌دهیم که اگر بتوانیم عملگرهای دلخواه تک کیوبیتی و $CNOT$را بسازیم آنگاه می‌توانیم هر عملگر چند کیوبیتی متعلق به $U(N)$ را بسازیم. دقت کنیدکه برای n کیوبیت بعد فضای هیلبرت برابر با $N=2^n$ است در نتیجه عملگرهای n بیتی متعلق به $U(N)=U(2^n)$ هستند. در این نحوه ساخت فرض کرده‌ایم که هر عملگر تک کیوبیتی را می‌توانیم بسازیم. این البته فرض دور از ذهنی نیست، زیرا مثلا اگر کیوبیت را اسپین یک هسته در نظر بگیریم، می-توانیم با تاباندن امواج با فرکانس رادیویی به طرز مناسب و عمل میدان مغناطیسی آنها روی اسپین هر نوع دورانی را روی اسپین انجام دهیم. اگر تنها یک مجموعه گسسته از عملگرهای یک کیوبیتی در اختیار داشته باشیم، آنگاه می‌توانیم با هر دقت دلخواهی عملگرهای تک کیوبیتی را بسازیم. استدلال ما از اینجا شروع می‌شود که نشان می‌دهیم هر عملگر یکانی n بیتی را می‌توانیم به حاصلضربی از عملگرهای ساده‌تر تجزیه کنیم. نخست احتیاج به یک تعریف داریم.

تعریف: فرض کنید که $\tilde{U}$ یک عمگر یکانی متعلق به $U(n)$ باشد که فقط یک زیر ماتریس 2×2 آن غیر بدیهی باشد، به این معنا که این عملگر فقط روی یک زیرفضای دوبعدی به صورت

عملگر U عمل می‌کند و روی هر بردار دیگری خارج از این زیر فضا مثل عملگر واحد عمل می‌کند. در این صورت این عملگر دوترازی[1] خوانده می‌شود.

به عنوان مثال فرض کنید که $U=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. در این صورت ماتریسهای زیر همگی عملگرهای دو ترازی متعلق به $U(4)$ هستند:

$$\widetilde{U}_1=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix} \qquad (۲۸-۲)$$

$$\widetilde{U}_2=\begin{pmatrix} a & 0 & 0 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ c & 0 & 0 & d \end{pmatrix} \qquad (۲۹-۲)$$

$$\widetilde{U}_3=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & c & 0 & d \end{pmatrix} \qquad (۳۰-۲)$$

قضیه: هر عملگر یکانی $U\in U(n)$ را می‌توان به صورت حاصلضرب عملگرهای یکانی دو ترازی نوشت.

اثبات:

ایده کلی این اثبات این است که یک ماتریس یکانی دلخواه را همواره می‌توان با ضرب کردن ماتریس‌های یکانی و دو ترازی مناسب از سمت چپ به شکل ماتریس واحد در آورد. این کار درواقع چیزی نیست جز فرایند تقلیل گاوس - جردن، با این تفاوت که این بار با ضرب ماتریس‌های یکانی انجام می‌شود. اگر این ماتریس‌ها را U_1,U_2,U_3 و ... بنامیم آنگاه معنای سخن بالا آن است که

[1] two level unitary operator

$$U_K U_{K-1} ... U_2 U_1 = I \qquad (۳۱-۲)$$

که نتیجه‌اش این است که

$$U = U_1^{-1} U_2^{-1} ... U_K^{-1} \qquad (۳۲-۲)$$

این ایده را با یک مثال ساده توضیح می‌دهیم. ماتریس یکانی U را به شکل زیر در نظر می‌گیریم:

$$U \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix} \qquad (۳۳-۲)$$

ماتریس U_1 می‌بایست طوری انتخاب شود که عنصر b را در این ماتریس صفر کند. بنابراین قرار می‌دهیم:

$$U_1 = \begin{pmatrix} x & y & 0 \\ z & w & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (۳۴-۲)$$

که در آن $za + dw = 0$ و یا $z = -kd$ و $w = ka$. برای آنکه U_1 یکانی شود، x و y را به نحو مناسب انتخاب می‌کنیم و قرار می‌دهیم:

$$U_1 = \begin{pmatrix} ka^* & kd^* & 0 \\ -kd & ka & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (۳۵-۲)$$

که در آن $k := \frac{1}{\sqrt{|a|^2 + |d|^2}}$، حال مطمئن هستیم که $U_1 U$ شکل زیر را دارد:

$$U_1 U = \begin{pmatrix} a' & b' & c' \\ 0 & e' & f' \\ g' & h' & k' \end{pmatrix} \qquad (۳۶-۲)$$

به همین نحو می‌توان ماتریسی مثل U_2 یافت که شرط زیر حاصل می‌شود. (به طور نمادین همه داریه‌های جدید را با علامت ´ نشان می‌دهیم.)

$$U_2U_1U=\begin{pmatrix} a' & b' & c' \\ 0 & e' & f' \\ 0 & h' & k' \end{pmatrix} \qquad (۳۷-۲)$$

یکانی بودن U ایجاب می‌کند که a' یک فاز خالص باشد و در نتیجه $b'=c'=0$. این فاز خالص را می‌توان با ضرب یک ماتریس که تنها درایه ۱۱ آن غیر صفر است از بین برد. بنابراین

$$U_3U_2U_1U=\begin{pmatrix} 1 & 0 & 0 \\ 0 & e' & f' \\ 0 & h' & k' \end{pmatrix} \qquad (۳۸-۲)$$

اما ماتریس طرف راست چیزی نیست جز یک ماتریس یکانی دو ترازی و در نتیجه با ضرب طرفین این رابطه در $U_1^{-1}U_2^{-1}U_3^{-1}$، U به صورت حاصلضربی از ماتریس‌های یکانی دو ترازی در می‌آید. برای ماتریس‌های بزرگ‌تر این کار را می‌توان در صورت لزوم ارائه داد.

۲-۲-۳- عملهای تک کیوبیتی

در ابتدا به طور خلاصه مطالبی را در مورد گیتهای تک کیوبیتی عنوان می‌کنیم:

یک تک کیوبیت، یک بردار $|\psi\rangle=a|0\rangle+b|1\rangle$ است که توسط دو عدد مختلط a و b که در شرط $|a|^2+|b|^2=1$ صدق می‌کنند، مشخص می‌شود. عملیات روی یک تک کیوبیت باید این نرم را حفظ کند، لذا توسط ماتریسهای یونیتاری 2×2 توصیف می‌شوند. ماتریسهای پائولی بعضی از مهمترین این ماتریسها هستند که عبارتند از:

$$X=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y=\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} Z=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad (۳۹-۲)$$

سه گیت کوانتومی دیگر که کاربرد فراوانی دارند عبارتند از : گیت هادامارد که با H نمایش داده می‌شود، گیت فاز که با S نمایش داده می‌شود و گیت $\pi/8$ که با T نمایش داده می‌شود.

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad S=\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T=\begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix} \qquad (۴۰-۲)$$

دو صورت جبری برای به خاطر سپردن آنها این است که :

۱) $H=(X-Z)/\sqrt{2}$ ۲) $S=T^2$

ممکن است تعجب کنید که چرا گیت T، گیت $\pi/8$ نامیده شده است، در حالیکه در ظاهر آن $\pi/4$ وجود دارد، دلیل آن این است که به لحاظ تاریخی به آن گیت $\pi/8$ نسبت داده می‌شده است چرا که :

$$T=\exp(i\frac{\pi}{8})\begin{bmatrix}\exp(-i\pi/8) & 0\\ 0 & \exp(-i\pi/8)\end{bmatrix} \quad (۴۱-۲)$$

و در عناصر روی قطرش $\pm i\pi/8$ مشاهده می‌کنیم.

یاآوری می‌کنیم که یک تک کیوبیت در حالت $a|0\rangle+b|1\rangle$ می‌تواند به عنوان یک نقطه با مختصات (θ,ϕ)روی یک کره واحد تعبیر شود به طوریکه $a=\cos\frac{\theta}{2}, b=e^{i\phi}\sin\frac{\theta}{2}$ و a می تواند یک عدد حقیقی منظور شود، زیرا فاز کل حالت غیر قابل مشاهده است. به این نوع نمایش، نمایش کره بلاخ گفته می‌شود و بردار $(\cos\phi\sin\theta,\sin\phi\sin\theta,\cos\theta)$ بردار بلاخ نامیده می‌شود. ماتریسهای پائولی سه دسته مفید از ماتریسهای یکانی را به وجود می‌آورند، زمانی که زمانی که نمایی می‌شوند، عملگرهای چرخشی حول X، Y و Z با معادلات زیر نمایش داده می‌شوند.

$$R_x(\theta)\equiv e^{-i\theta X/2}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}X=\begin{bmatrix}\cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix} \quad (۴۲-۲)$$

$$R_Y(\theta)\equiv e^{-i\theta Y/2}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Y=\begin{bmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix} \quad (۴۳-۲)$$

$$R_Z(\theta)\equiv e^{-i\theta Z/2}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Z=\begin{bmatrix}e^{-i\frac{\theta}{2}} & 0\\ 0 & e^{i\frac{\theta}{2}}\end{bmatrix} \quad (۴۴-۲)$$

با استفاده از این مسئله که اگر a یک عدد حقیقی باشد و A یک ماتریس بـه طوریکـه $A^2 = I$، در نتیجه:

$$\exp(iAx) = \cos I + i \sin|x|A \qquad (۴۵-۲)$$

یک اپراتور یکانی اختیاری روی یک تـک کیوبیـت بـه صـورت ترکیبهـای مختلفـی از اپراتورهـای چرخشی روی کیوبیت، می‌تواند نوشته شود. نظریه زیر مفهوم چرخش یک تک کیوبیت اختیـاری، که به ویژه در کاربردهای بعدی عملیات *Controlled* مفید خواهد بود، را بیان می‌کند.

قضیه (۲-۱): ترکیب $Y-Z$ برای یک تک کیوبیت:

فرض کنید U یک عمـل یکـانی روی یـک تـک کیوبیـت اسـت، در ایـن صـورت اعـداد حقیقـی $\delta,\gamma,\beta,\alpha$ وجود دارند به طوریکه:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) \qquad (۴۶-۲)$$

اثبات: از آنجائیکه U یکانی است، سـطرها و سـتونهای آن متعامـد هـستند، لـذا اعـداد حقیقـی γ,β,α و δ وجود دارد به طوریکه:

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & e^{-i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix} \qquad (۴۷-۲)$$

اکنون معادله (۲-۴۶) از تعریف ماتریسهای چرخش و ضرب ماتریس تبعیت می کند.

اگر فرض کنیم که m و n بردارهای واحد حقیقی غیر موازی در سـه بعـد باشـند، بـا اسـتفاده از قضیه (۲-۱) می‌توان نشان داد که یک عملگر یکانی تک کیوبیتی اختیاری می‌تواند به صورت زیـر نوشته شود:

$$U = e^{i\alpha} R_n(\beta) R_m(\gamma) R_n(\delta) \qquad (۴۸-۲)$$

کارآیی قضیه (۲-۱) در نتیجه‌ی زیر آمده است که کلیدی برای ساختار عملگرهای یکانی چند کیوبیتی *Controlled* می‌باشد.

نتیجه (۲-۱): فرض کنید که U یک گیت یکانی روی یک تک کیوبیت باشد، در این صورت عملگرهای A، B و C روی یک تک کیوبیت وجود دارند به طوریکه $ABC = I$ و $U = e^{i\alpha} AXBXC$ به طوریکه α، ضریب فاز کل می‌باشد.

اثبات:

با توجه به قضیه (۲-۱) اگر قرار دهیم:

$$A \equiv R_z(\beta)R_y(\gamma/2) \quad \text{و} \quad A \equiv R_y(-\gamma/2)R_z(-(\delta+\beta)/2) \quad \text{و} \quad C \equiv R_z((\delta-\beta)/2)$$

می‌بینیم که

$$ABC = I \tag{۴۹-۲}$$

چون $X^2 = I$ و با استفاده این مسئله که $XYX = -Y$ و در پی آن $XR_y(\theta)X = R_y(-\theta)$ خواهیم داشت:

$$XBX = XR_y(-\frac{\gamma}{2})XXR_z..... \tag{۵۰-۲}$$

بدین ترتیب

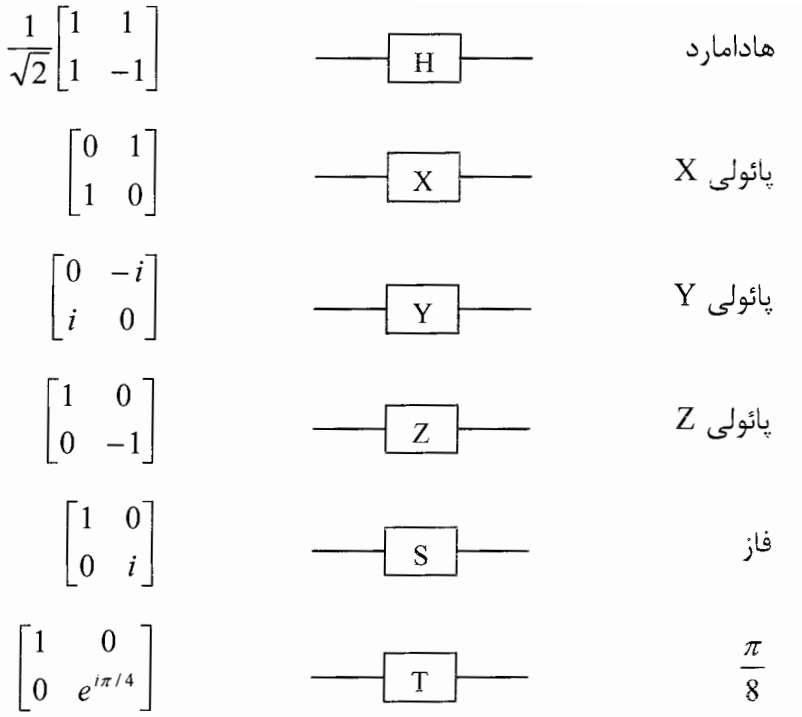
$$AXBXC = ... = R_z(\beta)R_y(\gamma)R_z(\delta) \tag{۵۱-۲}$$

و لذا همانطور که می خواستیم: $U = e^{i\alpha} AXBXC$ و $ABC = I$.

ساده سازی مدار با توسط اتحادهای شناخته شده‌ی زیر سودمند می باشد:

$$HXH = Z \qquad HYH = -Y \qquad HZH = X$$

نمایشهای معمول برای گیتهای تک کیوبیتی در شکل (۲-۱) آورده شده است. ویژگیهای اساسی مدارهای کوانتومی را یادآوری می‌کنیم که اولا مدارها از چپ به راست بررسی می‌شوند و ثانیا سیمها نمایش دهنده کیوبیتها می‌باشند.

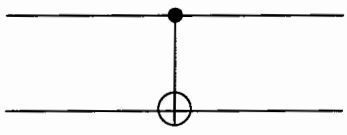


شکل (۲-۱): نام، نمایش و ماتریسهای یکانی برای گیتهای تک کیوبیتی معمول

۲-۲-۴- عملیات *Controlled*

"اگر A صحیح است، B را انجام بده". این نوع عمل (*Controlled*) یکی از مهمترین موارد در محاسبات کوانتومی و کلاسیکی می‌باشد. در این بخش ما توضیح می‌دهیم که چگونه عملیات *Controlled* پیچیده با استفاده از مدارهای ساخته شده از عملیات ابتدایی، انجام می‌شود.

نمونه اولیه عملیات *Controlled*، $Controlled - Not$ می‌باشد. یادآوری می‌کنیم که این گیت که از آن با نام *CNot* عنوان می‌کنیم، یک گیت کوانتومی با دو کیوبیت ورودی با نامهای کیوبیت کنترل و کیوبیت هدف می‌باشد که در شکل (۲-۲) نمایش داده شده است.



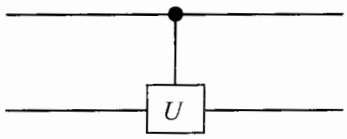
شکل (۲-۲): نمایش مداری برای گیت *CNOT*، خط بالا نمایش دهنده کیوبیت کنترل و خط پایین نمایش دهنده کیوبیت هدف است.

بر حسب پایه محاسباتی عمل $CNOT$ توسط $|c\rangle|+\rangle \to |c\rangle|t \oplus c\rangle$ داده می‌شود یعنی اگر کیوبیت کنترل روی $|1\rangle$ تنظیم شده باشد، در این صورت کیوبیت هدف وارون می‌شود در غیر این صورت کیوبیت هدف بدون تغییر باقی می‌ماند. بدین ترتیب در پایه‌های محاسباتی $|control, target\rangle$ نمایش ماتریسی $CNOT$ به شکل زیر است:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad (۵۲-۲)$$

به طور کلی‌تر فرض کنید که U یک عمل یونیتاری تک کیوبیتی اختیاری باشد. عمل $Controlled-U$ یک عمل دو کیوبیتی، مجددا با یک کیوبیت کنترل و یک کیوبیت هدف می‌باشد. اگر کیوبیت کنترل روی یک تنظیم شده باشد، در این صورت U روی کیوبیت هدف به کار برده می‌شود و در غیر این صورت کیوبیت هدف بدون تغییر باقی می‌ماند.

یعنی $|c\rangle|t\rangle \to |c\rangle U^c|t\rangle$. عملیات $Controlled-U$ توسط مدار در شکل (۲-۳) نمایش داده شده است.



شکل (۲-۳): نمایش مداری برای عمل $Controlled-U$، خط بالا نمایش دهنده کیوبیت کنترل و خط پایین نمایش دهنده کیوبیت هدف است.

یک گیت $CNOT$ را می‌توان از یک گیت $Controlled-Z$ یعنی گیتی که به صورت زیر نمایش داده می‌شود و دو گیت هادامارد نیز ساخت.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \equiv Controlled-Z \qquad (۵۳-۲)$$

نقش کنترل و هدف در گیتهای کوانتومی ایده‌آل اختیاری است و بستگی دارد که شما چه پایه‌هایی در نظر بگیرید. قبلا توضیح دادیم که چگونه $CNOT$ با توجه به پایه‌های محاسباتی عمل می‌کند و با این توصیف حالت کیوبیت اول تغییر نمی‌کند در صورتیکه اگر در یک پایه متفاوت کار کنیم، کیوبیت کنترل تغییر خواهد کرد. ما نشان خواهیم داد که بسته به حالت کیوبیت هدف، فازش تغییر خواهد کرد. می‌توان نشان داد که:

با معرفی حالتهای پایه $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$ و به کار بردن تساوی بالا اثر یک $CNOT$ با کیوبیت اول به عنوان کیوبیت کنترل و کیوبیت دوم به عنوان کیوبیت هدف به صورت زیر است:

$$|+\rangle|+\rangle \rightarrow |+\rangle|+\rangle \qquad (۵۴-۲)$$

$$|-\rangle|+\rangle \rightarrow |-\rangle|+\rangle \qquad (۵۵-۲)$$

$$|+\rangle|-\rangle \rightarrow |-\rangle|-\rangle \qquad (۵۶-۲)$$

$$|-\rangle|-\rangle \rightarrow |+\rangle|-\rangle \qquad (۵۷-۲)$$

بدین ترتیب با توجه به پایه جدید، اگر هدف به صورت $|-\rangle$ در ابتدا ظاهر شود حالت کیوبیت هدف تغییر نمی‌کند، در حالیکه حالت کیوبیت کنترل وارون می‌شود یعنی در این پایه کنترل و هدف نقشها را مبادله کرده‌اند.

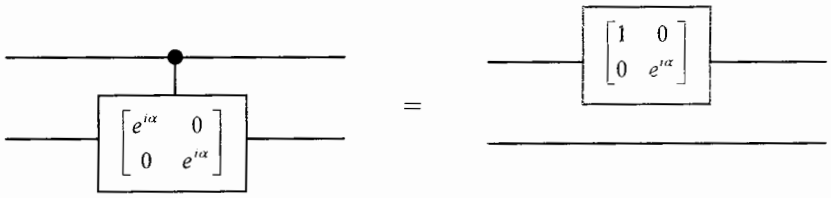
هدف ما فهمیدن این مسئله است که چگونه عمل $Controlled-U$ را برای تک کیوبیت اختیاری، با به کار بردن تنها عملهای تک کیوبیتی و گیت $CNOT$ اعمال کنیم. روشی که در پیش می‌گیریم شامل دو بخش است که بر اساس ترکیب $U = e^{i\alpha} AXBXC$ داده شده در نتیجه‌ی (۲-۱) پایه ریزی شده‌است. گام اول ما این خواهد بود که جابجایی فاز $e^{i\alpha}$ را روی کیوبیت هدف اعمال کنیم، که با کیوبیت کنترل، کنترل می‌شود. یعنی اگر کیوبیت کنترل $|0\rangle$است در این

صورت کیوبیت هدف بدون تغییر باقی می‌ماند، در حالیکه اگر کیوبیت کنترل $|1\rangle$ است جابجایی فاز $e^{i\alpha}$ روی هدف اعمال می‌شود. یک مداری که این عمل را تنها با استفاده از یک گیت یکانی تک کیوبیتی نمایش می‌دهد در سمت راست شکل (۲-۴) آورده شده است.

برای اینکه بررسی کنیم که آیا این مدار به طور صحیح کار می‌کند، توجه کنید که اثر مدار در طرف راست:

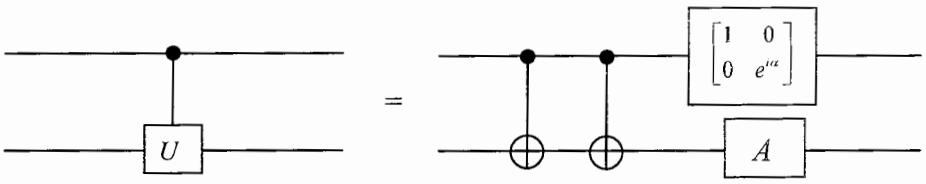
$$|00\rangle \to |00\rangle \ , \ |01\rangle \to |01\rangle \ , \ |10\rangle \to e^{i\alpha}|10\rangle \ , \ |11\rangle \to e^{i\alpha}|11\rangle \qquad (۵۸-۲)$$

می‌باشد که دقیقا همان چیزی است که برای عمل *Controlled* در سمت چپ لازم می‌باشد.



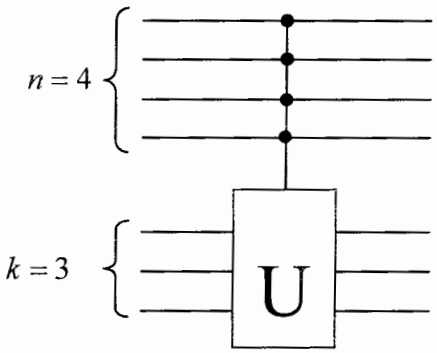
شکل (۲-۴): گیت تغییر فاز *Controlled* و یک مدار معادل برای ۲ کیوبیت

اکنون ما می‌توانیم ساختار عمل $Controlled-U$ را همانطور که در شکل (۲-۴) نشان داده شده است، کامل کنیم. برای اینکه بفهمیم چرا این مدار کار می‌کند، از نتیجه‌ی (۲-۱) یادآوری می‌کنیم که U می‌تواند به شکل $U = e^{i\alpha} AXBXC$ نوشته شود به طوریکه A، B و C عملهای تک کیوبیتی هستند و $ABC = I$. فرض کنید که کیوبیت کنترل روی $|1\rangle$تنظیم شده باشد. در این صورت عمل $U = e^{i\alpha} AXBXC$ بر روی کیوبیت دوم اعمال می‌شود. اگر از طرف دیگر، کیوبیت کنترل روی $|1\rangle$ تنظیم نشده باشد، در این صورت عمل $ABC = I$ به کیوبیت دوم اعمال می‌شود، یعنی هیچ تغییری ایجاد نمی‌شود. به عبارتی این مدار عمل $Controlled-U$ را انجام می‌دهد.



شکل (۲-۵): نمایش مداری عمل $Controlled-U$ برای تک کیوبیت U، به طوریکه α، A، B و Cدر شرط $ABC = I$ و $U = e^{i\alpha} AXBXC$ صدق می‌کند.

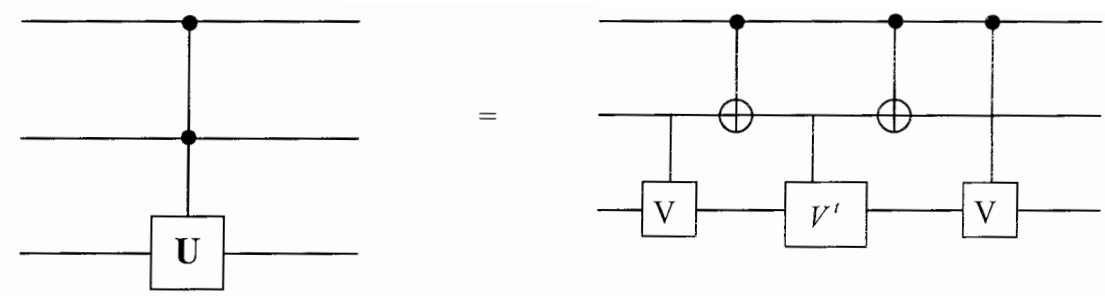
اما شرط گذاری روی کیوبیتهای چند تایی چگونه است؟ یک مثال از شرایط چند کیوبیتی‌ها، گیت تافولی[1] می‌باشد که سومین کیوبیت که کیوبیت هدف است، را وارون می‌کند. با این شرط که دو کیوبیت اول (کیوبیتهای کنترل) روی $|1\rangle$ تنظیم شده باشند. به طور کلی‌تر فرض کنید که $n+k$ کیوبیت داریم و U یک عملگر یکانی k کیوبیتی است. در این صورت عمل *Controlled* $(C^n(U))$ را با معادله $C^n(U)|x_1x_2...x_n\rangle|\psi\rangle = |x_1x_2...x_n\rangle U^{x_1x_2...x_n}|\psi\rangle$ مشخص می‌شود به طوریکه $x_1x_2...x_n$ در توان U حاصلضرب بیتهای $x_n,...,x_2,x_1$ می‌باشند. یعنی عملگر U روی k کیوبیت آخر اعمال می‌شود اگر n کیوبیت اول همگی $|1\rangle$باشند، در غیر این صورت هیچ عملی صورت نمی‌گیرد. یک نمایش مداری ویژه را برای این عملیات در شکل (۲-۶) آمده است. برای آنچه بعد از این آورده شده است (برای ساده سازی) ما فرض کرده‌ایم که $k=1$ باشد. برای k های بزرگتر پیچیدگی بیشتری وجود دارد که در مورد چگونگی عملیات اختیاری روی k کیوبیت، اطلاعات چندانی در دست نیست.



شکل (۲-۶): نمونه نمایش مداری برای عمل $C^n(U)$در حالیکه U یک عملگر یکانی روی kکیوبیت باشد، برای $n=4$ و $k=3$.

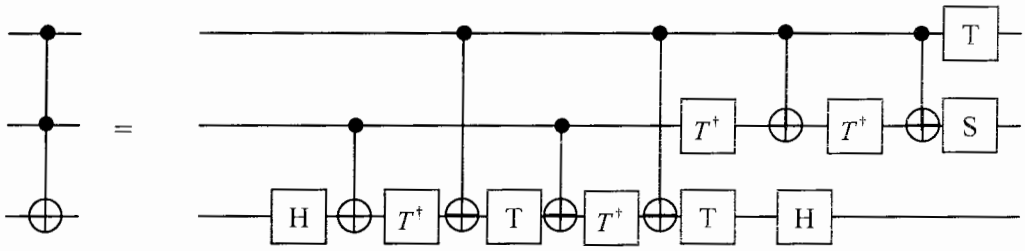
فرض کنید U یک اپراتور یکانی تک کیوبیتی و V یک عملگر یکانی اختیاری باشد و لذا $V^2=U$. در این صورت عمل $C^n(U)$ با استفاده از مدار در شکل ۲-۷ نشان داده شده است.

[1] toffoli



شکل (۲-۷): نمایش مداری برای گیت $C^n(U)$. V هر عملگر یکانی که در $V^2 = U$ صدق کند. حالت خاص $V \equiv (1-i)(I+iX)/2$ متناظر با گیت تافولی می‌باشد.

گیت تافولی یک حالت ویژه از عمل $C^2(U)$ است، در حالتی که داشته باشیم $C^2(X)$. با تعریف $V \equiv (1-i)(I+ix)/2$ و با توجه به اینکه $V^2 = X$ ما می‌بینیم که شکل (۲-۷) یک نمایش از گیت تافولی را بر حسب عملهای یک یا دو کیوبیتی می‌دهد. از نقطه نظر کلاسیکی این یک نتیجه فوق‌العاده است. یادآوری می‌کنیم که گیتهای یک یا دو کیوبیتی کلاسیکی برگشت پذیر برای انجام یک گیت تافولی کافی نیستند. در نهایت ما نشان خواهیم داد که هر عمل یکانی می‌تواند به گیتهای هادامارد، فاز، $CNOT$، و $\pi/8$ تجزیه می‌شود. به خاطر مفید بودن بسیار زیاد گیت تافولی، این مسئله جالب خواهد بود که بدانیم چگونه این گیت فقط از گیتهای هادامارد، فاز، $CNOT$ و $\pi/8$ تشکیل شده است، شکل (۲-۸).

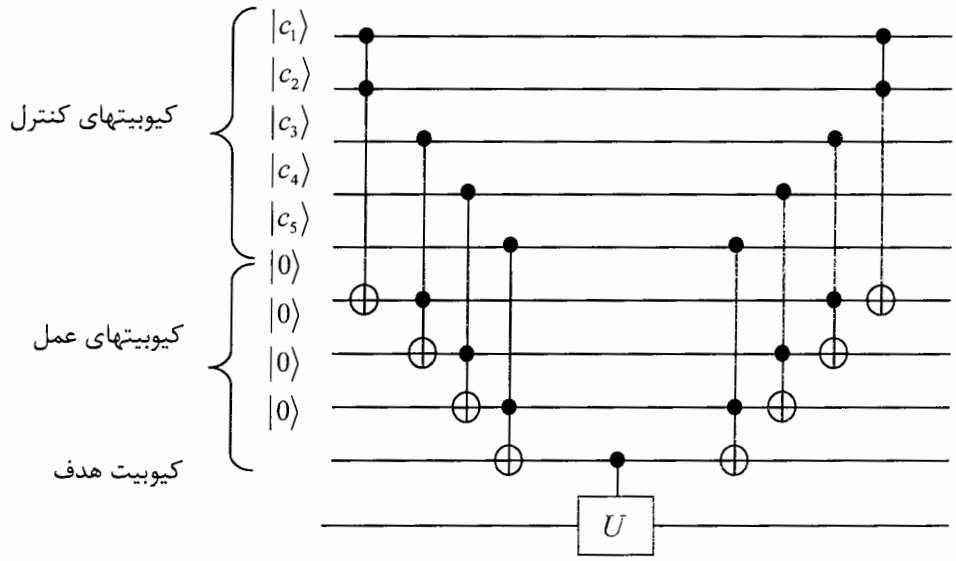


شکل (۲-۸): نمایش گیت تافولی با استفاده از گیتهای هادامارد، فاز، $CNOT$ و $\pi/8$.

چگونه ما می‌توانیم گیتهای $C^n(U)$را با استفاده از مجموعه گیتهای موجود، نمایش دهیم به طوریکه U یک عمل یکانی تک کیوبیتی اختیاری است. یک مدار ساده مخصوص، برای دستیابی به این عمل در شکل (۲-۹) نشان داده شده است. مدار به سه قسمت تقسیم شده است و تعداد

$n-1$ تا از کیوبیتهای عمل را مورد استفاده قرار می‌دهیم به طوریکه همه آنها با حالت $|0\rangle$ شروع و خاتمه می‌یابند.

فرض کنید که کیوبیتهای کنترل در حالت پایه محاسباتی، $|c_1,c_2,...,c_n\rangle$باشند. قسمت اول مدار برای این است که همه بیتهای کنترل $c_1,c_2,...,c_n$ را با یکدیگر AND می‌کنیم تا حاصلضرب $c_1.c_2...c_n$را ایجاد کنیم. برای انجام این کار، گیت اول در مدار c_1 و c_2 را با یکدیگر AND می‌کند، با استفاده از گیت تافولی، حالت کیوبیت عمل اول را به $|c_1.c_2\rangle$تغییر می‌دهد. گیت تافولی بعدی c_3 را با حاصلضرب $c_1.c_2$، AND می‌کند و کیوبیت عمل دوم به $|c_1.c_2.c_3\rangle$تغییر می‌یابد.



شکل (۲-۹): نمایش شبکه‌ای عمل $C^n(U)$برای حالت $n=5$.

ما اعمال گیتهای تافولی را ادامه می‌دهیم تا زمانی که آخرین کیوبیت عمل در حالت $|c_1.c_2....c_n\rangle$ قرار گیرد. سپس یک عمل U روی کیوبیت هدف اعمال می‌شود، با این شرط که آخرین کیوبیت عمل روی $|1\rangle$ تنظیم شده باشد. یعنی U تنها در صورتی اعمال می‌شود (اگر و تنها اگر) که همه c_1 تا c_nها روی $|1\rangle$تنظیم شده باشند. آخرین بخش مدار، تنها گامهای مرحله اول را معکوس می‌کند. یعنی همه کیوبیتهای عمل را به حالت اولیه‌شان $|0\rangle$، برمی‌گرداند.

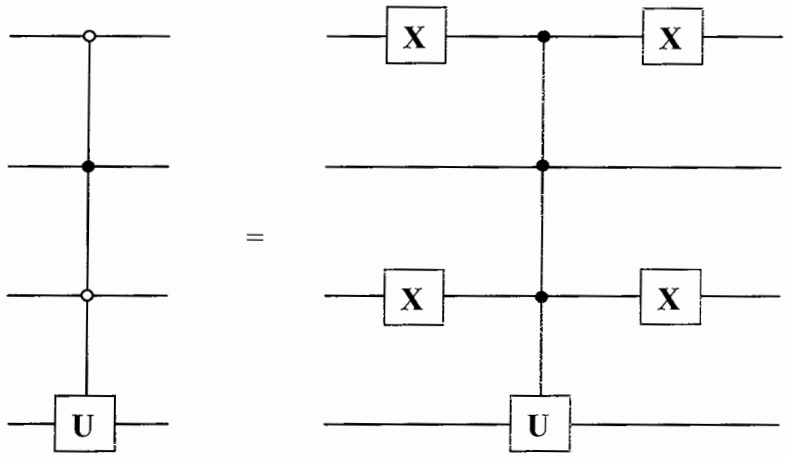
نتیجه حاصله اینکه، عملگر یکانی U به کیوبیت هدف اعمال می‌شود اگر و تنها اگر همه بیتهای کنترل c_1 تا c_n، روی 1 تنظیم شده باشند.

در گیتهای $Controlled$ ملاحظه کردیم که شرایط دینامیکی روی کیوبیت هدف در صورتی اتفاق می‌افتاد که بیتهای کنترل روی $|1\rangle$تنظیم شده باشند. البته اغلب این مسئله مفید خواهد بود که دینامیک را زمانی که بیت کنترل روی صفر تنظیم شده باشد، نیز در نظر بگیریم. به عنوان مثال، در شکل (۲-۱۰) نمایش مداری برای یک گیت دو کیوبیتی را به همراه یک مدار معادل (با این شرط که کیوبیت اول روی صفر تنظیم شده باشد)، بر حسب گیتهایی که ما قبلا آنها را معرفی کرده‌ایم، ارائه می‌دهیم.

شکل (۲-۱۰): عمل $Controlled$ با یک گیت NOT که روی کیوبیت دوم اعمال شده است مشروط بر اینکه کیوبیت اول روی $|0\rangle$ تنظیم شده باشد.

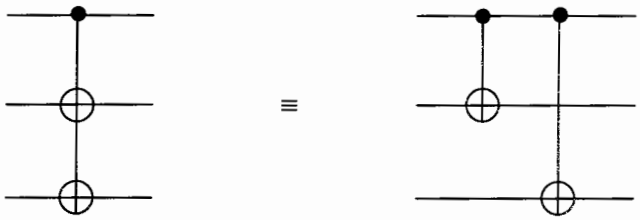
به طور کلی، دایره تو خالی شرایط را در مورد کیوبیتی که روی صفر تنظیم شده باشد و دایره توپر شرایط را در مورد کیوبیتی که روی یک تنظیم شده باشد، مشخص می‌کند.

یک مثال پیچیده‌تر این قرارداد، شامل ۳ کیوبیت کنترل، در شکل (۲-۱۱) نمایش داده شده است. عمل U در صورتی روی هدف اعمال می‌شود که کیوبیتهای اول و سوم روی صفر و کیوبیت دوم روی یک تنظیم شده باشد. بررسی این مسئله بسیار ساده است که مدار سمت راست عمل مورد نظر را انجام می‌دهد. به طور کلی‌تر تبدیل یک مدار که کیوبیتهایش روی یک تنظیم شده به مداری که کیوبیتهایش روی صفر تنظیم شده است، با جایگذاری گیتهای X در مکانهای مناسب، امکان‌پذیر می‌باشد که این عمل در شکل(۲-۱۱) نمایش داده شده است.



شکل (۲-۱۱): عمل $Controlled-U$ و معادل آن بر حسب اجزاء مداری که از قبل چگونگی عمل آنها را می‌دانیم. U روی چهارمین کیوبیت اعمال می‌شود اگر اولین و سومین کیوبیت روی صفر و کیوبیت دوم روی یک تنظیم شده باشد.

یک قرارداد دیگر که اغلب اوقات مفید است، این است که به گیتهای $Controlled-U$ این اجازه را بدهیم که چندین هدف داشته باشند، همانطور که در شکل (۲-۱۲) نشان داده شده است.



شکل (۲-۱۲): گیت $Controlled-Not$ با چندین کیوبیت هدف

این نمایش بدان معنی است که وقتی کیوبیت کنترل $|1\rangle$است، همه کیوبیتهای مشخص شده با یک $\oplus$ وارون می‌شوند و در غیر این صورت هیچ اتفاقی صورت نمی‌گیرد. این مسئله برای به عنوان مثال ساختن توابع کلاسیکی مانند جایگشتها و یا در کدگذاری و کدگشایی کردن مدارهای تصحیح غلطهای کوانتومی، همانطور که خواهیم دید، مناسب است.

در ادامه، با داشتن C به عنوان گیت $CNOT$ و کیوبیت ۱ به عنوان کیوبیت کنترل و کیوبیت ۲ بعنوان مثال کیوبیت هدف، تساوی هایی که برای ادامه کار مفید و البته قابل اثبات می‌باشند آورده شده است.[۱۳,۵,۳]

$$CX_1C = X_1X_2 \quad (۵۹-۲)$$

$$CY_1C = Y_1X_2 \quad (۶۰-۲)$$

$$CZ_1C = Z_1 \quad (۶۱-۲)$$

$$CX_2C = X_2 \quad (۶۲-۲)$$

$$CY_2C = Z_1Y_2 \quad (۶۳-۲)$$

$$CZ_2C = Z_1Z_2 \quad (۶۴-۲)$$

$$R_{z,1}(\theta)C = CR_{z,1}(\theta) \quad (۶۵-۲)$$

$$R_{x,2}(\theta)C = CR_{x,2}(\theta) \quad (۶۶-۲)$$

فصل سوم:
تصحیح خطای کوانتومی

مقدمه

سیستم‌های کوانتومی بسته، سیستم‌هایی هستند که هیچ برهمکنشی با جهان اطراف ندارد. اگر چه نتایج جالبی از پردازش اطلاعات در این سیستمهای ایده‌آل گرفته می‌شود، اما حقیقت امر این است که در جهان واقعی، هیچ سیستم کاملا بسته‌ای وجود ندارد، به جز خود جهان! سیستم‌های واقعی تحت برهمکنشهای ناخواسته با محیط بیرون قرار می‌گیرند. این برهمکنش‌های ناخواسته، به عنوان نویز در سیستمهای پردازش اطلاعات کوانتومی ظاهر می‌شوند. نیاز است که طرز عمل اینگونه نویزها و روش کنترل آنها را برای ساخت سیستم‌های پردازش اطلاعات کوانتومی مناسب، بدانیم.

۳-۱- عملهای کوانتومی[۱] و نویز کوانتومی

فرمالیزم عملهای کوانتومی، یک ابزار عمومی برای توصیف تبدیل سیستم‌های کوانتومی می‌باشد. حالتهای کوانتومی به صورت زیر تغییر می‌یابند.

$$\rho' = \varepsilon(\rho) \qquad (۱-۳)$$

نگاشت ε در رابطه بالا، یک عمل کوانتومی می‌باشد. دو مثال ساده از عملهای کوانتومی، تبدیلها و اندازه‌گیری‌های یونیتاری $\varepsilon(\rho) = U\rho U'$ و $\varepsilon_m(\rho) = M_m \rho M_m^\dagger$ می‌باشند. ρ حالت اولیه سیستم

[۱] quantum operation

قبل از فرآیند و $\varepsilon(\rho)$ حالت نهایی بعد از رخ دادن فرآیند می‌باشد. چنین نگاشتی چهار خاصیت عمده زیر را دارد:

الف) خطی است

ب) ماتریس هرمیتی را به ماتریس هرمیتی می‌نگارد.

ج) ماتریس مثبت را به ماتریس مثبت می‌نگارد.

د) رد ماتریس را حفظ می‌کند.

به چنین نگاشتی، یک نگاشت مثبت و رد نگه دار[۱] گفته می‌شود. معمولا نام کانال[۲] برای این نگاشت‌ها به کار برده می‌شود که یادآور تاثیر محیط بر یک حالت کوانتومی است که از جایی به جای دیگر ارسال شده است. در ادامه چند کانال معمول را معرفی می‌کنیم:

کانال بیت برگردان[۳]: این کانال حالت یک کیوبیت را از $|0\rangle$ به $|1\rangle$ و بالعکس با احتمال p برمی‌گرداند و با احتمال $1-p$ بدون تغییر آن را باقی می‌گذارد.

$$X: \quad |0\rangle \to |1\rangle \qquad X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad (۲-۳)$$
$$\quad |1\rangle \to |0\rangle$$

کانال فاز برگردان[۴]: این کانال به صورت زیر عمل می‌کند:

$$Z: \quad |0\rangle \to |0\rangle \qquad Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \qquad (۳-۳)$$
$$\quad |1\rangle \to -|1\rangle$$

---

[۱] trace preserving positive map
[۲] channel
[۳] bit flip channel
[۴] phase flip channel

کانال واقطبش[1]: کانال واقطبش یک نوع مهم از نویز کوانتومی است. فرض کنید که یک تک کیوبیت در اختیار داریم و با احتمال p آن کیوبیت واقطبیده می‌شود، یعنی توسط یک حالت کاملا آمیخته جایگزین می‌شود ($\frac{I}{2}$) و با احتمال $1-p$، کیوبیت بدون تغییر باقی می‌ماند. حالت این سیستم کوانتومی بعد از نویز به صورت زیر است:

$$\varepsilon(\rho)=\frac{pI}{2}+(1-p)\rho \qquad (۴-۳)$$

به طوریکه $\frac{I}{2}=\frac{\rho+X\rho X+Y\rho Y+Z\rho Z}{4}$.

کانال میرایی دامنه: فرض کنید که بخواهیم فوتونهای تک رنگ را از یک نقطه به یک نقطه دیگر از طریق یک فیبر نوری یا هوا بفرستیم. در بین راه ممکن است فوتونها جذب محیط شده و از سیستم خارج شوند. کانال میراکننده دامنه، کانالی است که چنین تحولی را نشان می‌دهد و عمل کوانتومی متناظر با آن $\varepsilon(\rho)=E_0\rho E_0^\dagger+E_1\rho E_1^\dagger$ می‌باشد.

کانال میرایی فاز: یک ترکیب خطی از دو حالت پایه $|0\rangle$ و $|1\rangle$ را با یک فاز نسبی در نظر بگیرید ($|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$). عمل این کانال با اعمال عملگری مانند $R_z(\theta)$ به صورت نامنظم و با یک تابع گوسی که روی حالتهای $|0\rangle$ و $|1\rangle$ اختلاف فاز θ ایجاد می‌کند، مشخص می‌شود.

در ادامه، به چگونگی پردازش اطلاعات کوانتومی در حضور نویز می‌پردازیم.

نویزها یک عامل مخرب عمده درسیستمهای پردازش اطلاعات هستند. تا جایی که امکان دارد ما سیستمهایی می‌سازیم که به طور کامل در برابر نویز ایمن باشند، اما زمانی که دیگر این امکان وجود نداشته باشد، تلاش می‌کنیم که سیستم در برابر اثرات این نویزها محافظت شود. جزئیات تکنیکهای

[1] depolarizing channel

بکار برده شده برای حفظ اطلاعات، نسبتا پیچیده است، اما اصول اولیه آن قابل بررسی می‌باشند. ایده اصلی این است که برای محافظت از یک پیغام در برابر اثرات نویز، ما باید با اضافه کردن اطلاعات اضافی به پیغام، آن را کدگذاری کنیم. در این صورت حتی اگر به واسطه اثرات نویز در پیغام تغییری صورت گرفت، به دلیل وجود کدهای اضافی در پیغام کدگذاری شده، امکان بازیابی پیغام پس از کدگشایی، وجود دارد.

به عنوان مثال فرض کنید که می‌خواهید یک بیت را از یک مکان به مکان دیگر از طریق یک کانال ارتباطی کلاسیکی حاوی نویز، بفرستید. اثر نویز در کانال به این ترتیب است که با احتمال $P>0$ بیت را وارون می‌کند (یعنی $|0\rangle$ را به $|1\rangle$ و $|1\rangle$ را به $|0\rangle$ تبدیل می‌کند) و با احتمال $1-P$ هیچ تغییری در آن صورت نمی‌گیرد. این کانال یک کانال متقارن باینری[۱] نامیده می‌شود. یک روش ساده برای حفظ بیت در برابر اثرات نویز در این کانال متقارن باینری به این ترتیب است که بیت مورد نظر را با سه کپی از خودش جایگزین کنیم:

$$\begin{aligned} 0 &\rightarrow 000 \\ 1 &\rightarrow 111 \end{aligned} \qquad (۵-۳)$$

عناوین 0 منطقی[۲] و 1 منطقی[۳] به رشته‌های 000 و 111 نسبت داده می‌شوند. اکنون هر سه بیت را از داخل کانال عبور می‌دهیم. دریافت کننده در انتهای کانال بیتها را دریافت کرده و باید حدس بزند که بیت اصلی فرستاده شده چه بوده است. فرض کنید که خروجی کانال 001 باشد. مشروط بر اینکه احتمال تغییر بیت (p) در کانال خیلی زیاد نیست، این امر بسیار محتمل است که بیت سوم وارون شده است و بیت اصلی فرستاده شده، بیت 0 می‌باشد.

---

[۱] binary symmetric channel
[۲] logical 0
[۳] logical 1

این روش کدگشایی، رای‌گیری اکثریت[1] نامیده می‌شود. در صورتیکه دو یا بیش از دو بیت در این کانال وارون شود این روش کدگشایی موثر نخواهد بود. کدی که در این روش توصیف شد، کد تکرار[2] نامیده می‌شود.

۳-۱-۱- کد بیت برگردان سه کیوبیتی

برای حفظ حالات کوانتومی در برابر اثرات نویز، ما باید کدهای تصحیح خطای کوانتومی را گسترش دهیم. تفاوتهایی بین اطلاعات کلاسیکی و اطلاعات کوانتومی می‌باشد که لازم می‌دارد ایده‌های جدیدی برای ساخت یک چنین کدهای تصحیح خطای کوانتومی، معرفی کنیم. سه مورد عمده در زیر آورده شده است:

۱- No cloning: این قضیه می‌گوید که حالات کوانتومی نمی‌توانند کپی برداری شوند. در صورتیکه به عنوان مثال در کد کوانتومی تکرار ما باید از یک حالت، سه بار یا بیشتر کپی برداری کنیم.

۲- خطاها پیوسته هستند. یک رشته پیوسته از خطاهای مختلف ممکن است روی یک تک کیوبیت اتفاق بیفتد. تعیین این که کدام خطا صورت گرفته است تا تصحیح شود نیازمند یک دقت نامحدود و بنابراین منابع نامحدود می‌باشد.

۳- اندازه‌گیری باعث تغییر اطلاعات کوانتومی می‌شود. در تصحیح خطای کلاسیکی، ما خروجی را از کانال مشاهده می‌کردیم و سپس تعیین می‌کردیم که کدام روش کدگشایی

---

[1] majority voting
[2] repetition code

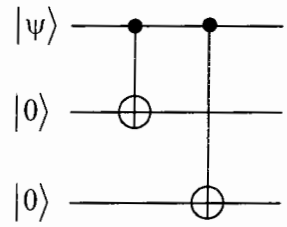
باید اتخاذ گردد. مشاهده در مکانیک کوانتومی به طور کلی باعث تخریب حالت کوانتومی می‌شود و بازیابی آن را غیر ممکن می‌سازد.

خوشبختانه همانطور که در ادامه شرح خواهیم داد، هیچکدام از این موارد، مشکل ساز نخواهند بود. فرض کنید که کیوبیتهایی را از طریق یک کانال که با احتمال $1-P$ بدون تغییر و با احتمال P آنها را وارون می‌کند، بفرستیم، یعنی با احتمال P، حالت $|\psi\rangle$ به حالت $X|\psi\rangle$ تغییر می‌یابد، به طوریکه X عملگر سیگمای x پائولی یا به عبارتی عملگر بیت برگردان می‌باشد. این کانال، کانال بیت برگردان نامیده می‌شود. در اینجا کد بیت برگردان، که برای محافظت کیوبیتها در برابر اثرات نویز این کانال استفاده می‌شود، را توضیح می‌دهیم.

فرض کنید که حالت تک کیوبیتی $a|0\rangle+b|1\rangle$ را، در سه کیوبیت به صورت $a|000\rangle+b|111\rangle$ کدگذاری کنیم. یک قرارداد برای نوشتن این روش کدگذاری به صورت زیر اتخاذ می‌کنیم:

$$|0\rangle \rightarrow |0_L\rangle \equiv |000\rangle$$
$$|1\rangle \rightarrow |1_L\rangle \equiv |111\rangle \qquad (۶-۳)$$

به طوریکه برهم نهی حالتهای پایه، متناظر با برهم نهی حالتهای کدگذاری شده می‌باشد. نمادهای $|0_L\rangle$ و $|1_L\rangle$ نشان می‌دهد که اینها حالتهای $|0\rangle$ منطقی و $|1\rangle$ منطقی می‌باشند و نه حالتهای صفر و یک فیزیکی. اعمال این روش کدگذاری در شکل (۳-۱) نمایش داده شده است.



شکل(۳-۱): مدار کدگذاری برای کد بیت برگردان سه کیوبیتی.

پس از کدگذاری، هر کدام از سه کیوبیت از از داخل کانال بیت برگردان عبور داده می‌شوند. فرض کنید عمل وارون بیتی روی یک کیوبیت صورت گرفته باشد و یا هیچ وارون بیتی رخ نداده باشد. دو مرحله ساده برای بازیابی حالت کوانتومی صحیح به ترتیب زیر می‌باشد:

۱- آشکارسازی خطا[۱] یا تشخیص نشانه[۲]: ما یک اندازه گیری اعمال می‌کنیم که به ما می‌گوید که چه خطایی روی حالت کوانتومی رخ داده است. نتیجه اندازه‌گیری، نشانه خطا[۳] نامیده می‌شود. برای کانال بیت برگردان، چهار نشانه خطا، متناظر با چهار عملگر تصویری زیر می‌باشند.

$$P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111| \qquad (۳-۷)$$

$$P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011| \qquad (۳-۸)$$

$$P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101| \qquad (۳-۹)$$

$$P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110| \qquad (۳-۱۰)$$

فرض کنید به عنوان مثال یک وارون بیتی روی کیوبیت اول صورت گیرد، لذا حالت تغییر یافته، $a|100\rangle + b|011\rangle$ خواهد بود. توجه کنید که $\langle\psi|P_1|\psi\rangle$، در این حالت برابر یک می‌باشد، بنابراین نتیجه اندازه گیری و یا به عبارتی دیگر، نشانه خطا مطمئنا 1 می‌باشد، به علاوه اندازه-گیری نشانه هیچ تغییری در حالت ایجاد نمی‌کند، یعنی قبل و بعد از اندازه‌گیری نشانه، داریم: $a|100\rangle + b|011\rangle$. توجه کنیدکه نشانه، تنها شامل اطلاعاتی درمورد این که چه خطاهایی صورت گرفته است، می‌باشد و به ما اجازه هیچ گونه استنباطی در مورد مقادیر a و b را نمی‌دهد، یعنی هیچ اطلاعاتی در مورد حالتهایی که محافظت می‌شوند، را ارائه نمی‌دهد. این یک ویژگی عمومی از

---

[۱] error detection
[۲] syndrome diagnosis
[۳] error syndrome

اندازه‌گیریهای نشانه می‌باشد در صورتیکه که برای کسب اطلاعات در مورد هویت و خصوصیات یک حالت کوانتومی، نیاز به برهم زدن حالت می‌باشد.

۲- بازیابی[۱]: مقدار نشانه‌ی خطا را برای بازیابی حالت اولیه به کار می‌بریم. به عنوان مثال، اگر نشانه خطا، $\hat{1}$ باشد که نشان‌دهنده‌ی وارون بیتی در بیت اول است، در این صورت ما این بیت را دوباره وارون می‌کنیم که حالت اصلی $a|000\rangle+b|111\rangle$ را با دقت تمام به ما می‌دهد. چهار نشانه‌ی خطای ممکن و روشهای بازیابی در هر حالت به صورت زیر می‌باشند:

الف) 0(هیچ خطایی صورت نگرفته است): عملی برای بازیابی انجام نمی‌شود.

ب) 1 (وارون بیتی روی کیوبیت اول): کیوبیت اول را دوباره وارون می‌کنیم.

ج) 2 (وارون بیتی روی کیوبیت دوم): کیوبیت دوم را دوباره وارون می‌کنیم.

د) 3 (وارون بیتی روی کیوبیت سوم): کیوبیت سوم را دوباره وارون می‌کنیم.

این روند تصحیح خطا به طور کامل و بدون عیب عمل می‌کند، به شرط آنکه وارون بیتی روی یک کیوبیت اتفاق بیفتد. این امر با احتمال $(1-p)^3+3p(1-p)^2=1-3p^2+2p^3$ اتفاق می‌افتد. احتمال اینکه یک خطا بدون تصحیح باقی بماند $3p^2-2p^3$ می‌باشد که در مواردی صورت می‌گیرد که در بیش از یک کیوبیت وارون بیتی رخ داده باشد.

۳-۱-۲- اصلاح تحلیل خطا

تحلیل خطا روش کامل و کافی برای تصحیح خطا نمی‌باشد. مشکل اساسی این است که همه خطاها و حالتها در مکانیک کوانتومی به طور معادل ایجاد نشده‌اند و فضایی هم که حالتهای کوانتومی در آن قرار دارند، فضایی پیوسته است. بنابراین این احتمال وجود دارد که بعضی از خطاها تنها تغییر کوچکی

[۱] recovery

در یک حالت بدهند در حالیکه بعضی دیگر آن حالت را کاملا عوض کنند. یک مثال واضح، خطای وارون بیتی می‌باشد که توسط X صورت می‌گیرد. این خطا هیچ اثری روی حالت $\left(|0\rangle+|1\rangle\right)/\sqrt{2}$ ندارد، در صورتیکه حالت $|0\rangle$ را کاملا تغییر داده و وارون کرده و به $|1\rangle$ تبدیل می‌کند. برای بررسی این مشکل، از کمیت ضریب اطمینان[1] استفاده می‌کنیم.

یادآوری می‌کنیم که ضریب اطمینان یک حالت خالص و یک حالت مرکب توسط رابطه زیر داده می‌شود:

$$F\left(|\psi\rangle,\rho\right)=\sqrt{\left(\langle\psi|\rho|\psi\rangle\right)} \qquad (۱۱-۳)$$

نقش تصحیح خطای کوانتومی، افزایش ضریب اطمینان تا بیشترین حد ممکن (نزدیک به یک) می‌باشد. در اینجا مینیمم مقدار ضریب اطمینان که از کد وارون بیتی سه کیوبیتی به دست آمده است را با ضریب اطمینان حالتی که تصحیح خطا روی آن صورت نگرفته است، مقایسه می‌کنیم.

فرض کنید که حالت کوانتومی مورد نظر $|\psi\rangle$ باشد. بدون به کار بردن کد تصحیح خطا، حالت کیوبیت بعد از عبور از کانال به شکل زیر خواهد بود:

$$\rho=(1-P)|\psi\rangle\langle\psi|+PX|\psi\rangle\langle\psi|X \qquad (۱۲-۳)$$

لذا ضریب اطمینان به صورت زیر داده می‌شود:

$$F=\sqrt{\langle\psi|\rho|\psi\rangle}=\sqrt{(1-P)+P\langle\psi|X|\psi\rangle\langle\psi|X|\psi\rangle} \qquad (۱۳-۳)$$

جمله دوم زیر رادیکال غیر منفی است و اگر $|\psi\rangle=0$ باشد، این جمله صفر خواهد شد. لذا می‌بینیم که مینیمم مقدار ضریب اطمینان $F=\sqrt{1-p}$ می‌باشد. حال فرض می‌کنیم که کد تصحیح خطا برای محافظت از حالت $|\psi\rangle=a|0_L\rangle+b|1_L\rangle$ به کار برده شود، حالت کوانتومی پس از اثر نویز و سپس تصحیح خطا به شکل زیر خواهد بود:

---

[1] fidelity

$$\rho = \left[(1-p)^3 + 3p(1-p)^2 \right] |\psi\rangle\langle\psi| + \ldots \qquad (۱۴-۳)$$

جملات حذف شده مربوط به وارون بیتی روی دو یا هر سه کیوبیت است. همه جملات حذف شده مثبت هستند، لذا ضریب اطمینانی را که ما محاسبه می‌کنیم، کران پایینی از ضریب اطمینان صحیح (یعنی بدون حذف جملات) می‌باشد. مشاهده می‌کنیم که

$$F = \sqrt{\langle\psi|\rho|\psi\rangle} \geq \sqrt{(1-p)^3 + 3p(1-p)^2} \qquad (۱۵-۳)$$

یعنی حداقل ضریب اطمینان $\sqrt{1-3p^2+2p^3}$ می‌باشد، لذا میزان ضریب اطمینان برای حالت کوانتومی مورد نظر (با داشتن $p<\frac{1}{2}$) افزایش پیدا کرده است. یک روش متفاوت برای فهم نشانه خطا که در تعمیم کد سه کیوبیتی مفید است، وجود دارد. فرض کنید که به جای اندازه‌گیری چهار تصویرگر P_0، P_1، P_2 و P_3 ما دو اندازه‌گیری انجام دهیم. اولی، اندازه‌گیری مشاهده‌پذیر Z_1Z_2 (که $Z\otimes Z\otimes I$ می‌باشد) و دوم، اندازه‌گیری مشاهده‌پذیر Z_2Z_3. هر کدام از این مشاهده‌پذیرها، مقادیر ویژه ± 1 را دارند. اندازه‌گیری اولیه از Z_1Z_2 می‌تواند به عنوان مقایسه‌کننده‌ی کیوبیتهای اول و دوم محسوب شود تا مشخص شود که آیا مشابه هستند یا خیر. توجه کنید که Z_1Z_2 تجزیه طیفیِ

$$Z_1Z_2 = \left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)\otimes I - \left(|01\rangle\langle 01| + |10\rangle\langle 10|\right)\otimes I \qquad (۱۶-۳)$$

را دارد که متناظر با عملگرهای تصویری $\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)\otimes I$ و $\left(|01\rangle\langle 01| + |10\rangle\langle 10|\right)\otimes I$ می‌باشد. لذا اندازه‌گیری Z_1Z_2 به عنوان مقایسه کننده‌ی مقادیر کیوبیتهای اول و دوم محسوب می‌شود و جواب $+1$ را در صورتیکه کیوبیتها مشابه باشند و -1 را در صورتیکه متفاوت باشند، به ما می‌دهد. به طور مشابه، اندازه‌گیری Z_2Z_3 مقادیر کیوبیتهای دوم و سوم را مقایسه می‌کند. با بررسی این دو اندازه‌گیری، می‌توانیم مشخص کنیم که آیا خطای وارون بیتی صورت گرفته است یا خیر و اگر صورت گرفته، روی کدام کیوبیت؟ اگر هر دو اندازه‌گیری نتیجه $+1$ را به ما بدهد، در این صورت هیچ-

گونه خطایی صورت نگرفته است. اگر نتیجه اندازه‌گیری Z_1Z_2 برابر $+1$ و نتیجه اندازه‌گیری Z_2Z_3 برابر -1 باشد، در این صورت با احتمال بسیار بالایی کیوبیت سوم وارون شده است. اگر نتیجه اندازه-گیری Z_1Z_2 برابر -1 باشد و نتیجه اندازه‌گیری Z_2Z_3 برابر $+1$ باشد، در این صورت با احتمال بسیار بالایی کیوبیت دوم وارون شده است. آنچه در مورد موفقیت این نوع اندازه‌گیری قطعی است، این است که اندازه‌گیری، هیچ اطلاعاتی درباره دامنه‌های a و bی حالتهای کوانتومی کدگذاری شده به ما نمی‌دهد و بدین ترتیب اندازه‌گیری باعث برهم زدن حالتها نمی‌شود.

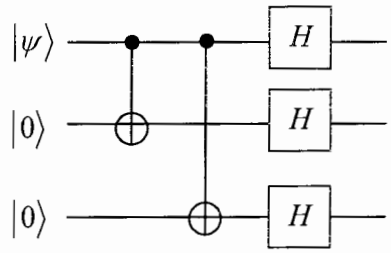
۳-۱-۳- کد فاز برگردان سه کیوبیتی

علاوه بر وارونی بیت، خطاهای دیگری نیز ممکن است بر روی کیوبیت اتفاق بیفتد. یکی از این خطاها، وارونی فاز[۱] روی یک تک کیوبیت می‌باشد. در این مدل خطا، کیوبیت با احتمال $1-p$ بدون تغییر باقی می‌ماند و با احتمال p، فاز مربوط به حالتهای $|0\rangle$ و $|1\rangle$ وارون می‌شود. به طور دقیق‌تر، عملگر فاز برگردان Z، با احتمال $p>0$، روی کیوبیت اعمال می‌شود. بنابراین حالت $a|0\rangle+b|1\rangle$ تحت عمل وارون فازی، به حالت $a|0\rangle-b|1\rangle$ تبدیل می‌شود. یک روش ساده برای تبدیل کانال وارون فازی به کانال وارون بیتی وجود دارد. فرض کنید که ما در پایه $|+\rangle\equiv(|0\rangle+|1\rangle)/\sqrt{2}$ و $|-\rangle\equiv(|0\rangle-|1\rangle)$ کار می‌کنیم. نسبت به این پایه‌ها، عملگر Z، $|+\rangle$ را به $|-\rangle$ و $|-\rangle$ را به $|+\rangle$ تبدیل می‌کند، یعنی دقیقا مانند عمل وارون بیتی و البته با برچسب‌های $+$ و $-$. بدین ترتیب حالتهای $|0_L\rangle\equiv|+++\rangle$ و $|1_L\rangle\equiv|---\rangle$ به عنوان حالتهای منطقی صفر و یک، برای محافظت در برابر خطاهای وارون فازی به کار برده می‌شوند.

---

[۱] phase flip

همه عملهای مورد نیاز برای تصحیح خطا (کدگذاری، آشکارسازی خطا و بازیابی) دقیقا مانند کانال بیت برگردان اعمال می‌شوند، اما با پایه‌های $|+\rangle$ و $|-\rangle$ به جای پایه‌های $|0\rangle$ و $|1\rangle$. برای اینکه عمل تغییر پایه را انجام دهیم، به سادگی گیت هادامارد را در نقاط مناسب اعمال می‌کنیم.



شکل (۳-۲): مدارهای کدگذاری برای کد وارون فازی

به طور واضح‌تر، کدگذاری برای کانال فاز برگردان، در دو مرحله صورت می‌گیرد:

۱- دقیقا مانند کانال بیت برگردان، در سه کیوبیت کدگذاری صورت می‌گیرد.

۲- یک گیت هادامارد به هر کیوبیت اعمال می‌شود، همانطور که در شکل (۳-۲) نمایش داده شده است. آشکارسازی خطا با اعمال اندازه‌گیری‌های تصویری، مشابه قبل صورت می‌گیرد، اما توسط گیت هادامارد، همیوغ شده‌اند:

$$P_j \to P_j' \equiv H^{\otimes 3} P_j H^{\otimes 3} \qquad (۱۷-۳)$$

به طور مشابه، اندازه‌گیری نشانه، با اندازه‌گیری مشاهده‌پذیرهای $H^{\otimes 3} Z_1 Z_2 H^{\otimes 3} = X_1 X_2$ و $H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3$ صورت می‌گیرد. اندازه‌گیری مشاهده‌پذیرهای $X_1 X_2$ و $X_2 X_3$ متناظر با مقایسه علامت کیوبیتهای اول و دوم و نیز کیوبیتهای دوم و سوم، به ترتیب می‌باشند، به طوریکه به در اندازه‌گیری $X_1 X_2$، به عنوان مثال، $+1$ را برای حالتهای مانند $(...)\otimes|+\rangle|+\rangle$ یا $(...)\otimes|-\rangle|-\rangle$ و -1 را برای حالتهایی مانند $(...)\otimes|-\rangle|+\rangle$ یا $(...)\otimes|+\rangle|-\rangle$ نتیجه می‌دهد. سرانجام، تصحیح خطا با اعمال عمل بازیابی کد وارون بیتی که البته توسط هادامارد همیوغ شده باشد، به پایان می‌رسد. به

عنوان مثال فرض کنید که یک وارونی در علامت کیوبیت اول از $|+\rangle$ به $|-\rangle$، آشکارسازی شده است. در این صورت ما با اعمال $HX_1H = Z_1$ بر روی اولین کیوبیت عمل بازیابی را انجام می‌دهیم. روندهای مشابه برای نشانه‌های خطای دیگر به کار برده می‌شوند.

واضح است که این کد برای کانال وارون فازی، ویژگیهای مشابه با کد کانال وارون بیتی را داراست، بویژه مینیمم ضریب اطمینان برای هر دو مشابه می‌باشد. گفته می‌شود که این دو کانال به طور منحصر به فردی متعادل هستند، زیرا یک عملگر یکانی U (که در اینجا گیت هادامارد است) وجود دارد بطوریکه عمل یک کانال مشابه کانال دیگری است مشروط بر اینکه کانال اول با عملگرهای U و U^+ همراه شود.

۳-۱-۴- کد شُور[۱]

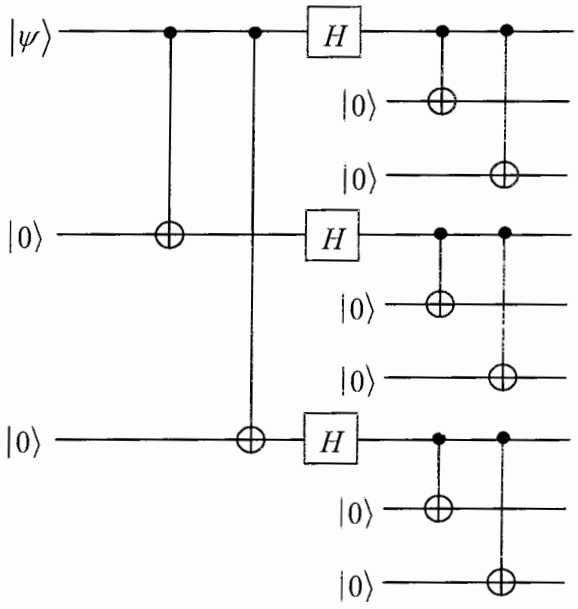
یک کد کوانتومی ساده وجود دارد که می‌تواند از اثرات یک خطای اختیاری روی یک تک کیوبیت محافظت کند. این کد، کد شُور نام دارد. این کد یک ترکیب از سه کد وارون بیتی و وارون فازی می‌باشد. در ابتدا ما کیوبیت را با استفاده از کد وارون فازی کدگذاری می‌کنیم: $|0\rangle \to |+++\rangle$ و $|1\rangle \to |---\rangle$. سپس هر یک از این کیوبیتها را با استفاده از کد وارون بیتی سه کیوبیتی کدگذاری می‌کنیم: $|+\rangle$ به صورت $(|000\rangle + |111\rangle)/\sqrt{2}$ و $|-\rangle$ به صورت $(|000\rangle - |111\rangle)/\sqrt{2}$ کدگذاری می‌شوند. نتیجه، یک کد ۹ کیوبیتی می‌باشد که کد-کلمه‌های[۲] آن به صورت زیر داده می‌شود:

$$|0\rangle \to |0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \qquad (۱۸-۳)$$

---

[۱] Shor code
[۲] code words

$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} \qquad (۱۹-۳)$$



شکل (۳-۳): مدار کدگذاری برای کد ۹ کیوبیتی شُور.

مدار کوانتومی که کد شُور را کد گذاری می‌کند در شکل (۳-۳) نشان داده شده است. هما نطور که در بالا توصیف شد، بخش اول مدار کیوبیت را با استفاده از کد وارون فازی سه کیوبیتی کدگذاری می‌کند. مقایسه آن با شکل (۳-۲) نشان می‌دهد که مدارها مشابه می‌باشند. بخش دوم مدار هر یک از این سه کیوبیت را با استفاده از کد وارون بیتی کدگذاری می‌کند.

کد شُور قادر به محافظت در برابر خطاهای وارون فازی و وارون بیتی روی هر کیوبیت می‌باشد. برای مشاهده این مطلب، فرض کنید که یک خطای وارون بیتی روی کیوبیت اول اتفاق بیفتد. برای کد وارون بیتی یک اندازه‌گیری از Z_1Z_2 که کیوبیتهای اول و دوم را مقایسه می‌کند، اعمال می‌کنیم و می‌بینیم که آنها متفاوت هستند. لذا نتیجه می‌گیریم که یک خطای وارون بیتی روی کیوبیت اول یا

دوم رخ داده است. سپس کیوبیت دوم و سوم را با اعمال یک اندازه‌گیری از Z_2Z_3، مقایسه می‌کنیم و می‌بینیم که آنها مشابه هم هستند، نتیجه می‌گیریم که کیوبیت اول وارون شده است و با وارونی مجدد آن، عمل بازیابی انجام می‌گیرد و به حالت اولیه تبدیل می‌شود. به طریق مشابه می‌توان اثرات خطاهای وارون بیتی را روی هر یک از ۹ کیوبیت در این کد، آشکارسازی و بازیابی کرد.

با یک روش مشابه، خطای وارون فازی را نیز روی این کیوبیتها می‌توان آشکارسازی و بازیابی کرد. فرض کنید که یک وارون فازی روی کیوبیت اول رخ دهد. این وارون فازی، علامت بلوک اول از کیوبیتها را با تغییر $|000\rangle+|111\rangle$ به $|000\rangle-|111\rangle$ و بالعکس، وارون می‌کند. در حقیقت یک وارونی فاز روی هر یک از سه کیوبیت اول این اثر را دارد و روند تصحیح خطا برای هر یک از این سه خطاهای ممکن موثر می‌باشد. اندازه‌گیری نشانه با مقایسه علامت بلولکهای اول و دوم از سه کیوبیت آغاز می‌شود، دقیقا مانند اندازه‌گیری نشانه برای کد وارون فازی که با مقایسه علامت کیوبیتهای اول و دوم شروع شد. به عنوان مثال $(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)$ علامت مشابه $(-)$ را در هر دو بلوک از کیوبیتها دارا می‌باشد در حالیکه $(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)$ علامتهای متفاوتی را داراست. وقتی که یک وارونی فاز روی یکی از سه کیوبیت اول اتفاق می‌افتد، می‌بینیم که علامتهای بلوکهای اول و دوم متفاوت هستند. مرحله دوم و آخر اندازه‌گیری نشانه، مقایسه علامت بلوکهای دوم و سوم از کیوبیتها می‌باشد. می‌بینیم که آنها مشابه هستند و نتیجه می‌گیریم که فاز باید در بلوک اول از سه کیوبیت وارون شده باشد. با وارونی علامت بلوک اول از سه کیوبیتها عمل بازیابی صورت می‌گیرد و به حالت اولیه باز می‌گردیم.

فرض کنید که هر دو خطای وارون فازی و وارون بیتی روی کیوبیت اول اتفاق بیفتد، یعنی عملگر Z_1X_1 روی آن کیوبیت اعمال می‌شود. در این صورت واضح است که روند آشکارسازی یک خطای وارون بیتی یک بیت وارون شده را روی کیوبیت اول، آشکارسازی و آن را تصحیح می‌کند و روند

آشکارسازی یک خطای وارون فازی یک وارونی فاز را روی بلوک اول از سه کیوبیت آشکارسازی و آن را تصحیح می‌کند. بدین ترتیب ، کد شُور قادر به تصحیح خطاهای مرکب از وارون فازی و وارون بیتی روی یک تک کیوبیت می‌باشد. در حقیقت کد شُور از هر خطای اختیاری، مشروط بر اینکه تنها روی یک تک کیوبیت اثر کند، به طور کامل محافظت می‌کند.

۳-۲- نظریه تصحیح خطای کوانتومی

آیا می‌توانیم یک نظریه عمومی از کدهای تصحیح خطای کوانتومی ایجاد کنیم؟ دراین بخش یک چارچوب عمومی برای مطالعه تصحیح خطای کوانتومی ایجاد می‌کنیم که شامل شرایط تصحیح خطای کوانتومی می‌باشد، یعنی مجموعه معادلاتی که باید برقرار باشند تا تصحیح خطای کوانتومی ممکن باشد. البته داشتن چنین چارچوبی، وجود کدهای مناسب برای تصحیح خطا را تضمین نمی-کند، اما زمینه‌ای را ایجاد می‌کند که ما را قادر به یافتن چنین کدهایی می‌کند.

طرحهای ساده‌ای که توسط شُور معرفی شد، تعمیم می‌یابد. حالتهای کوانتومی توسط یک عمل یکانی به یک کد تصحیح خطای کوانتومی کدگذاری می‌شوند و رسما به عنوان یک زیر مجموعه C از فضای هیلبرت معرفی می‌شوند. داشتن یک نمایش برای عملگر تصویر روی فضای کد C مفید می‌باشد، بنابراین ما شکل P را برای آن به کار می‌بریم. مثلا برای کد وارون بیتی ۳ کیوبیتی، P به شکل زیر خواهد بود:

$$P = |000\rangle\langle 000| + |111\rangle\langle 111| \qquad (۲۰-۳)$$

بعد کدگذاری، کد در معرض نویز قرار می‌گیرد و در ادامه یک اندازه‌گیری اعمال می‌شود تا مشخص کند که چه نوع خطایی اتفاق افتاده است که به آن نشانه خطا گفته می‌شود. پس از مشخص شدن خطا، عمل بازیابی اعمال می‌شود تا سیستم کوانتومی را به حالت اولیه کد برگرداند. نمایش ساده‌ای که

در شکل (۳-۴) آورده شده است این توضیح را می‌دهد که: نشانه‌های مختلف خطا متناظر با زیرفضاهای متعامد و تغییر شکل نیافته فضای کل هیلبرت می‌باشد. زیرفضاها باید متعامد باشند در غیر این صورت به طور مطمئنی نمی‌توانند توسط اندازه‌گیری نشانه متمایز شوند. به علاوه زیرفضاهای مختلف باید ورژنهای تغییر نایافته‌ای از فضای اصلی باشند تا اندازه‌ای که انعکاس خطا روی زیرفضاهای مختلف، کد-کلمه‌ها را به حالتهای متعامد ببرد تا قادر به برطرف کردن خطا باشد.

برای توسعه نظریه عمومی تصحیح خطای کوانتومی، ما مجبور به طرح فرضیاتی درباره طبیعت خطا و روشی که برای تصحیح خطا به کاربرده می‌شود، می‌باشیم. یعنی لزوما ما فرض نمی‌کنیم که تصحیح خطا از طریق دو مرحله صورت می‌گیرد و هیچ فرضیه‌ای در مورد خطای اتفاق افتاده بر روی سیستم کیوبیتی و یا ضعیف بودن آن نمی‌سازیم، بلکه فقط دو فرض کلی می‌کنیم: خطا توسط یک عمل کوانتومی ε توصیف می‌شود و روند تصحیح خطای کامل توسط یک عمل کوانتومی R، با حفظ رد، که عمل تصحیح خطا نامیده می‌شود، اعمال می‌شود. عمل تصحیح خطا ۲ مرحله آشکارسازی و بازیابی خطا را یک جا در خود دارد.

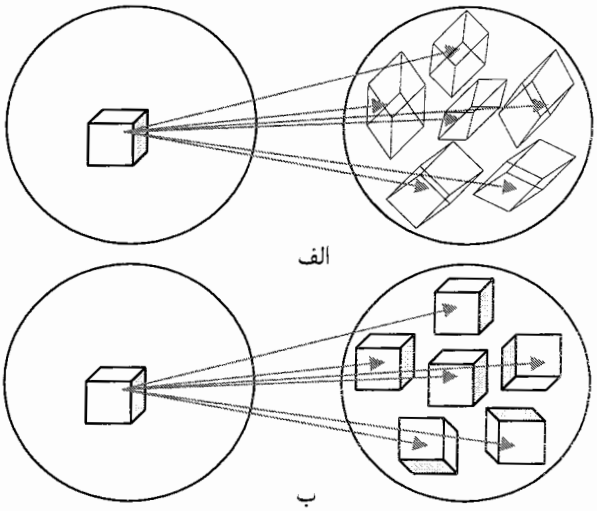
برای اینکه تصحیح خطا موفقیت‌آمیز شمرده شود باید به ازای هر حالت ρ، داشته باشیم:

$$(R\circ\varepsilon)(\rho)\propto\rho \qquad (۲۱-۳)$$

ممکن است تعجب کنید که چرا در رابطه بالا به جای تساوی، $\propto$ را به کار برده‌ایم. در صورتیکه ε یک عمل کوانتومی رد نگهدار باشد، در این صورت با گرفتن رد از دو طرف معادله مشاهده می‌کنیم که $\propto$ به $=$ تبدیل می‌شود.

به هر حال گاهی اوقات ممکن است عملهای کوانتومی ε رد نگهدار نباشند که در این صورت علامت $\propto$، مناسب خواهد بود. البته مرحله تصحیح خطا، R، باید با احتمال یک، با موفقیت عمل کند و دلیل آنکه گفتیم که R باید رد نگهدار باشد، همین است.

شرایط تصحیح خطای کوانتومی یک مجموعه ساده از معادلاتی هستند که باید بررسی شوند تا مشخص شود که آیا کد تصحیح خطا در برابر یک نوع خطای خاص ε، محافظت می‌شود یا خیر. این شرایط را برای کشف ویژگی‌های عمومی کدهای تصحیح خطا به کار می‌بریم.



شکل (۳-۴): بسته فضای هیلبرت در کدگذاری کوانتومی. الف) کد نامناسب با فضاهای تغییر شکل یافته و نامتعامد. ب) کد مناسب با فضاهای متعامد (قابل تمایز) و تغییر شکل نایافته.

قضیه ۳-۱) شرایط تصحیح خطای کوانتومی: فرض کنید که C یک کد کوانتومی می‌باشد و P عملگر تصویر کننده روی C باشد. همچنین فرض می‌کنیم که ε یک عمل کوانتومی با عناصر عمل $\{\mathrm{E_i}\}$ می‌باشد. شرط لازم و کافی برای وجود یک عمل تصحیح خطا (R)، که ε را روی C تصحیح کند، این است که

$$PE_i^{\dagger}E_jP=\alpha_{ij}P \qquad (۲۲-۳)$$

به ازای ماتریس هرمیتی α با اعداد مختلط. ما عناصر عمل $\{E_i\}$ را برای نویز ε، خطا می‌نامیم و اگر R وجود داشته باشد، می‌گوییم که $\{E_i\}$، یک مجموعه تصحیح پذیر از خطاها را تشکیل می‌دهد.

۳-۲-۱- گسستگی خطاها

در مورد حفظ اطلاعات کوانتومی در برابر یک نویز مشخص ε صحبت کردیم اما به طور کلی دقیقا در مورد خطای وارد بر یک سیستم کوانتومی چیزی نمی‌دانیم.

اگر یک کد C و عمل تصحیح کوانتومی R بتواند برای حفظ در برابر یک بخش کامل از فرآیندهای خطا به کار برده شود، کار مفیدی صورت گرفته است.

قضیه ۳-۲) فرض کنید که C یک کد کوانتومی و R عمل تصحیح خطای کوانتومی برای بازیابی از یک فرآیند خطا (ε) با عناصر عمل $\{E_i\}$ است، همچنین فرض کنید که F یک عمل کوانتومی با عناصر عمل $\{F_i\}$ که ترکیبات خطی از E_i هستند، باشد یعنی $F_j = \sum_i m_{ji} E_i$، به طوریکه m_{ji} یک ماتریس با اعداد مختلط باشد. در این صورت عمل تصحیح خطای R، اثرات فرآیند نویزی F روی کد C را نیز تصحیح می‌کند.

این قضیه ما را قادر به معرفی یک زبان قوی برای توصیف کدهای تصحیح خطا می‌سازد. به جای صحبت در مورد دسته بندی فرآیندهای خطای تصحیح پذیر توسط یک کد C و عمل تصحیح خطای R، ما می‌توانیم در مورد یک مجموعه از عملگرهای خطا ($\{E_i\}$) که تصحیح پذیر هستند، صحبت کنیم. منظور این است که شرایط تصحیح خطای کوانتومی برای این عملگرها برقرار است.

$$PE_i E_j^{\dagger} P = \alpha_{ij} P \qquad (۲۳-۳)$$

قضیه‌های (۳-۱) و (۳-۲)، با یکدیگر بیان می‌کنند که هر فرآیند خطای ε که عناصر عمل آن از ترکیب خطی عملگرهای $\{E_i\}$ ساخته شده‌اند، توسط عمل بازیابی R، تصحیح پذیر می‌باشند. در اینجا یک مثال عملی از این دیدگاه جدید را بررسی می‌کنیم.

فرض کنید که ε یک عمل کوانتومی روی یک تک کیوبیت باشد. در این صورت عناصر عمل آن ($\{E_i\}$)، هر کدام می‌توانند به عنوان ترکیب خطی از ماتریسهای پائولی σ_0، σ_1، σ_2 و σ_3 نوشته شوند. بنابراین برای اینکه بررسی کنیم که به عنوان مثال کد شُور، خطای تک کیوبیتی اختیاری را روی کیوبیت اول تصحیح می‌کند، کافیست بررسی کنیم که عبارت $P\sigma_i^1\sigma_j^1P=\alpha_{ij}P$ برقرار است به طوریکه σ_i^1ها ماتریسهای پائولی (I,X,Y,Z) هستند که روی کیوبیت اول اثر می‌کنند. اگر این برقرارشود، این اطمینان حاصل می‌شود که هر فرآیند خطا هر چند بار که روی کیوبیت اول اثر کند، تصحیح می‌شود.

به طور خلاصه ما آموختیم که این امکان وجود دارد که خطاهای کوانتومی را گسسته کنیم تا با خطاهای پیوسته ممکن روی یک تک کیوبیت مقابله کنیم، کافیست در برابر یک مجموعه محدود از خطاها پیروز شویم (ماتریس پائولی). نتایج مشابه برای سیستم‌های کوانتومی با ابعاد بالاتر نیز صادق است.

۳-۲-۲- نمونه‌های خطای مستقل

چگونه می‌توانیم ارتباط بین تصحیح خطای کوانتومی و آستانه‌ای برای انجام پردازش اطلاعات کوانتومی معتبر که در قسمتهای قبل معرفی شد، برقرار کنیم؟ در این بخش ما ایده اساسی چگونگی امکان این مسئله را با به کار بردن فرضیه خطاهای مستقل روی کیوبیت‌های مختلف توضیح می‌دهیم. به طور شهودی، اگر یک فرآیند خطا به طور مستقل روی کیوبیتهای مختلف در کد عمل کند، در این صورت مشروط بر اینکه نویز به اندازه کافی ضعیف باشد، تصحیح خطا باید ضریب اطمینان حالت کدگذاری شده را روی حالت کدگذاری نشده افزایش دهد.

برای شرح این مسئله با مثال کانال واقطبش آغاز می‌کنیم که یک توصیف ساده‌ی ویژه از ایده‌های اساسی ایجاد می‌کند و سپس این ایده را به کانال‌های مهم دیگر تعمیم می‌دهیم. یادآوری می‌کنیم که کانال واقطبش توسط یک تک پارامتر، (احتمال p) توصیف می‌شود. عمل کانال واقطبش روی یک تک کیوبیت توسط عبارت:

$$\varepsilon(\rho)=(1-p)\rho+\frac{p}{3}[X\rho X+Y\rho Y+Z\rho Z] \qquad (۲۴-۳)$$

مشخص می‌شود و می‌توان گفت که با احتمال $1-p$ هیچ اتفاقی صورت نمی‌گیرد و هر سه پارامتر X، Y و Z با احتمال $p/3$ بر کیوبیت اثر می‌کنند. کانال واقطبش به ویژه برای آنالیز بافت تصحیح خطای کوانتومی مناسب است زیرا شکل مناسب و خوبی بر حسب ۴ خطای ساده‌ی I، X، Y و Z که معمولترین کاربرد را در آنالیز کدهای کوانتومی دارند، دارا می‌باشد. ما چگونگی انجام این آنالیز را توضیح خواهیم داد و سپس به این سوال برمی‌گردیم که برای فرآیندی که شکل ساده‌ای برحسب I، X، Y و Z ندارد، چه باید بکنیم. یک محاسبه ساده نشان می‌دهد که مینیمم ضریب اطمینان برای حالتهای فرستاده شده به داخل یک کانال واقطبش $F=\sqrt{1-2\frac{p}{3}}=1-\frac{p}{3}+o\left(p^2\right)$ می‌باشد.

فرض کنید که یک تک کیوبیت از اطلاعات را در یک کد کوانتومی nکیوبیتی کدگذاری کنیم که خطاها را روی هر تک کیوبیت تصحیح می‌کند و همچنین فرض کنید که کانال واقطبش با پارامتر p، روی هر کیوبیت به طور مستقل عمل کند:

$$\varepsilon^{\otimes n}(\rho)=(1-p)^n\rho+\sum_{j=1}^{n}\sum_{k=1}^{3}(1-p)^{n-1}\frac{p}{3}\sigma_k^j\rho\sigma_k^j+... \qquad (۲۵-۳)$$

به طوریکه "..." به جملات با مراتب بالاتر اشاره دارد که آنالیز نمی‌شوند، بعد از اینکه تصحیح خطا اعمال شد، همه جملات ظاهرشده در این مجموع به حالت ρ برگشت داده می‌شود.

$$\left(R\otimes\varepsilon^{\otimes n}\right)(\rho)=\left[(1-p)^n+n(1-p)^{n-1}p\right]\rho+\ldots \qquad (۲۶-۳)$$

بنابراین خواهیم داشت:

$$F\geq\sqrt{(1-p)^{n-1}(1-p+np)}=1-\frac{\binom{n}{2}}{2}p^2+O\left(p^3\right) \qquad (۲۷-۳)$$

بدین ترتیب مشروط بر اینکه احتمال خطا p به اندازه کافی کم باشد، کد تحصیح خطا منتهی به یک افزایش در ضریب اطمینان حالتهای کوانتومی می‌شود که با کدها محافظت می‌شوند. همه‌ی کانالهای ایجاد خطا به عنوان یک ترکیب تصادفی از عدم خطا، وارونی بیت، وارونی فاز یا ترکیبی از این دو، عمل نمی‌کنند. بسیاری از کانالهای کوانتومی به صورت طبیعی اینگونه نیستند. یک مثال از میرایی دامنه را در نظر بگیرید که عناصر عمل E_0 و E_1 را داراست:

$$E_0=\begin{bmatrix}1 & 0\\ 0 & \sqrt{1-\gamma}\end{bmatrix}\qquad E_1=\begin{bmatrix}0 & \sqrt{\gamma}\\ 0 & 0\end{bmatrix} \qquad (۲۸-۳)$$

پارامتر γ یک پارامتر کوچک مثبت می‌باشد که نشان دهنده قدرت فرآیند میرایی دامنه می‌باشد. هر چه γ به صفر نزدیکتر شود، قدرت کاهش پیدا می‌کند.

ما به طور معقول تقریبا می‌توانیم حدس بزنیم که کانال میرایی دامنه، یک توصیف معادل بر حسب یک مجموعه از عناصر عمل که شامل یک جمله متناسب با I ($\{f(\gamma)I,E_1',E_2',\ldots\}$) به طوریکه زمانی که $\gamma\to 0$ داریم: $f(\gamma)\to 1$. در این صورت یک آنالیز از تصحیح خطا برای کانال میرایی دامنه که به طور مستقل روی چندین کیوبیت عمل می‌کند، می‌تواند صورت گیرد که مشابه با آنالیز تصحیح خطای انجام شده برای کانال واقطبش بود. اما ثابت می‌شود که یک چنین توصیفی امکان ندارد. این به راحتی نتیجه‌گیری می‌شود زیرا برای $\gamma>0$، هیچ ترکیب خطی از E_0 و E_1 نمی‌تواند

متناسب با I باشد و بدین ترتیب هیچ مجموعه‌ای از عناصر عمل برای کانال میرایی دامنه نمی‌تواند شامل یک جمله متناسب با I باشد.

یک محاسبه ساده نشان می‌دهد که مینیمم ضریب اطمینان برای کانال میرایی دامنه که بر یک تک کیوبیت اعمال شده، $\sqrt{1-\gamma}$ می‌باشد. فرض کنید که کیوبیت در یک کد کوانتومی nکیوبیتی، کدگذاری می‌شود که قادر به تصحیح خطاهای اختیاری روی یک تک کیوبیت باشد و کانال میرایی دامنه با پارامتر γ، به طور مستقل روی هر کیوبیت عمل کند.

ما ایده اساسی را طوری طراحی می‌کنیم که نشان می‌دهد اثر تصحیح خطای کوانتومی، تغییر ضریب اطمینان به $1-I\left(\gamma^2\right)$ می‌باشد، بنابراین برای γ کوچک، کدگذاری کیوبیت در یک کد کوانتومی منجر به حذف خطا می‌شود.

با به کار بردن $E_{j,k}$، برای مشخص کردن عمل E_j روی kامین کیوبیت، اثر نویز روی کیوبیت‌های کدگذاری شده خواهد شد:

$$\varepsilon^{\otimes n}(\rho)=\left(E_{0,1}\otimes E_{0,2}\otimes\ldots\otimes E_{0,m}\right)\rho\left({E_{0,1}}^{\dagger}\otimes {E_{0,2}}^{\dagger}\otimes\ldots\otimes {E_{0,n}}^{\dagger}\right)$$
$$+\sum_{j=1}^{n}\left[E_{1,j}\otimes\left(\bigotimes_{k\neq j}E_{0,k}\right)\right]\rho\left[{E_{1,j}}^{\dagger}\otimes\left(\bigotimes_{k\neq j}E_{0,k}^{\dagger}\right)\right]+O\left(\gamma^2\right) \qquad (۲۹-۳)$$

فرض کنید که بنویسیم

$$E_0=\left(1-\frac{\gamma}{2}\right)I+\gamma\frac{Z}{4}+O\left(\gamma^2\right) \qquad (۳۰-۳)$$

و

$$E_1=\sqrt{\gamma}\left(X+iY\right)/2 \qquad (۳۱-۳)$$

با جانشینی اینها در عبارت (۳-۲۹) خواهیم داشت:

(۳۲-۳)

$$\varepsilon^{\otimes n} =$$
$$\left(1-\frac{\gamma}{4}\right)^{2n}\rho+\frac{\gamma}{4}\left(1-\frac{\gamma}{4}\right)^{2n-1}\sum_{j=1}^{n}\left(Z_j\rho+\rho Z_j\right)+\frac{\gamma}{4}\left(1-\frac{\gamma}{4}\right)^{2n-2}\sum_{j=1}^{n}\left(X_j+iY_j\right)\rho\left(X_j-iY_j\right)+O\left(\gamma^2\right)$$

فرض کنید که ρ یک حالت از کد باشد، واضح است که اثر تصحیح خطا روی ρ این است که آن را ناوردا باقی بگذارد. اثر تصحیح خطا روی جمله‌هایی مثل $Z_j\rho$ و ρZ_j اغلب به آسانی با ملاحظه اثر آن روی $Z_j|\psi\rangle\langle\psi|$ ناپدید می‌شوند.

بدین ترتیب جملاتی شبیه $Z_j\rho$ بعد از تصحیح خطا حذف می‌شوند به علاوه تصحیح خطا $X_j\rho X_j$ و $Y_j\rho Y_j$ را به حالت ρ بر می‌گردانند زیرا کد می‌تواند خطاها را روی یک کیوبیت تصحیح کند. بنابراین بعد از تصحیح خطا حالت سیستم خواهد شد:

$$\left(1-\frac{\gamma}{4}\right)^{2n}\rho+2n\frac{\gamma}{4}\left(1-\frac{\gamma}{4}\right)^{2n-2}\rho+O\left(\gamma^2\right)=\rho+O\left(\gamma^2\right) \qquad (۳۳-۳)$$

بدین ترتیب، تصحیح خطا تا مرتبه γ^2، حالت را به حالت اصلی ρ برمی‌گرداند و برای نویزهای ضعیف (γهای کوچک)، تصحیح خطا حذف خطاها را منجر می‌شود، درست مثل کانال واقطبش.

تحلیلهای ما در اینجا برای مدل نویز میرایی دامنه بود. اما تعمیم این بحث مشکل نیست. لذا نتیجه-گیری‌های مشابهی برای مدلهای دیگر نویز، به دست می‌آوریم. به طور کلی در ادامه ما عمدتا با مدلهای نویزی که به عنوان کاربرد تصادفی خطاهای متناظر با ماتریس‌های پائولی، تعبیر می‌شوند، کار می‌کنیم، مانند کانال واقطبش، که به ما اجازه می‌دهد که آنالیزها را با به کاربردن مفاهیم مشابه از نظریه احتمالی کلاسیکی[۱] انجام دهیم. به خاطر داشته باشید که ایده‌هایی که ما گفتیم می‌توانند به

[۱] classical probability theory

فراتر از مدل خطای ساده تعمیم داده شوند تا برای یک محدوده بیشتری از مدلهای خطا با استفاده از اصول مشابه با آنچه ما فقط بیان کردیم، به کاربرده شوند.

۳-۲-۳- کدهای تبهگن[۱]

از بسیاری از جهات کدهای تصحیح کننده خطا مشابه با کدهای کلاسیکی هستند. یک خطا با اندازه-گیری نشانه خطا مشخص می‌شود و سپس همانطور که مناسب است، مثل حالت کلاسیکی تصحیح می‌شود. در هر صورت یک دسته‌ی جالب از کدهای کوانتومی وجود دارند که کدهای تبهگن نامیده می‌شوند و دارای یک ویژگی جالب هستند که کدهای کلاسیکی آن را دارا نمی‌باشند. این ایده به شکل بسیار راحتی برای کد شُور توضیح داده می‌شود. اثر خطاهای Z_1 و Z_2 را روی کد–کلمه‌های کد شُور در نظر بگیرید. همانطور که قبلا ملاحظه کردید، اثر این خطاها روی هر دو کد–کلمه مشابه می-باشد. برای کدهای تصحیح خطای کلاسیکی اثر خطاها روی بیتهای مختلف، لزوما منتهی به کد – کلمه‌های معیوب می‌شود. پدیده کدهای کوانتومی تبهگن، یک نوع از وضعیت good news-bad news برای کدهای کوانتومی می‌باشد.

Bad news بعضی از تکنیک‌های اثباتی هستند که به طور کلاسیکی به کار برده می‌شوند تا ثابت کنند که کرانها در تصحیح خطا ناموفق هستند، زیرا نمی‌توانند برای کدهای تبهگن به کار برده شوند.

Good news، کدهای کوانتومی تبهگن هستند که به نظر می‌آید جالبترین کدها در میان کدهای کوانتومی می‌باشند. از بعضی لحاظ آنها نسبت به کدهای کلاسیکی، بیشتر قادر به بسته بندی اطلاعات هستند، زیرا خطاهای ناهمسان، لزوما مجبور نیستند که فضای کد را به فضاهای متعامد ببرند و این

---

[۱] degenerate codes

امکان وجود دارد (هرچند که تا الان نشان داده نشده است) که این توانایی فوق‌العاده، منجر شود که کدهای تبهگن اطلاعات کوانتومی را به طور موثرتری نسبت به کدهای غیر تبهگن ذخیره کنند.

۳-۲-۴- کران کوانتومی همینگ [۱]

ما معمولا مایل به استفاده از بهترین کدهای کوانتومی ممکن هستیم. این که "بهترین" در هر شرایطی به چه معناست به کاربرد آن بستگی دارد. به همین دلیل ما مایل به داشتن آستانه‌ای هستیم تا تعیین کند که آیا یک کد با ویژگی‌های مخصوص وجود دارد یا خیر؟ در این بخش ما کران کوانتومی همینگ را که یک کران ساده می‌باشد و مقداری اطلاعات به صورت ویژگیهای عمومی کدهای تبهگن به ما می‌دهد، را ارائه می‌دهیم.

فرض کنید که یک کد غیر تبهگن برای کد گذاری k کیوبیت در n کیوبیت به کار برده شود به طوریکه قادر به تصحیح خطاها در هر زیر مجموعه‌ای از t کیوبیت یا کمتر از آن باشد. فرض کنید که j خطا روی دهد به طوریکه $j \le t$، در این صورت، $\binom{n}{j}$ مجموعه از موقعیتها وجود دارد که خطاها ممکن است در آنجا اتفاق بیفتند. برای هر مجموعه از موقعیتها، ۳ خطای ممکن وجود دارد (ماتریسهای پائولی X، Y و Z که ممکن است در هر کیوبیت اتفاق بیفتند) لذا مجموعا برای هر مجموعه از موقعیتها 3^j خطای ممکن وجود دارد.

بنابراین مجموع تعداد خطاهایی که ممکن است روی t کیوبیت یا کمتر اتفاق بیفتد، خواهد بود:

$$\sum_{j=0}^{t}\binom{n}{j}3^j \qquad (۳۴-۳)$$

[۱] quantum hamming bound

(توجه کنید که $j=0$ متناظر با حالتی است که خطایی روی کیوبیت صورت نگرفته است، یعنی خطای I.) برای کدگذاری k کیوبیت دریک روش غیر تبهگن، هر کدام از این خطاها باید متناظر با یک زیرفضای 2^k بعدی باشد. همه این زیرفضاها باید با فضای کل 2^n بعدی قابل استفاده برای n کیوبیت متناسب شوند (هم اندازه شوند)، که منتهی می‌شود به نامساوی زیر:

$$\sum_{j=0}^{t}\binom{n}{j}3^j 2^k \le 2^n \qquad (۳۵-۳)$$

که کران کوانتومی همینگ می‌باشد. به عنوان مثال حالتی را در نظر بگیرید که می‌خواهیم یک کیوبیت را در n کیوبیت به طوری کدگذاری کنیم که خطاها روی یک کیوبیت مجاز باشند. در این حالت کران کوانتومی همینگ خواهد شد:

$$2\left(1+3n\right) \le 2^n \qquad (۳۶-۳)$$

جایگذاری نشان می‌دهد که این نامساوی برای $n \le 4$ برقرار نیست در حالیکه برای $n \ge 5$، صادق می‌باشد. بنابراین هیچ کد غیر تبهگن برای کدگذاری کردن یک کد در کمتر از ۵ کیوبیت به طوریکه از همه خطاهای ممکن روی کیوبیت محافظت کند، وجود ندارد.

البته همه کدهای کوانتومی، غیرتبهگن نیستند و همچنین کرانهایی وجود دارند که بر روی همه کدهای کوانتومی (و نه فقط کدهای غیر تبهگن) اعمال می‌شوند، مانند کران Singleton کوانتومی که بیان می‌کند هر کد کوانتومی که k کیوبیت را در n کیوبیت کد گذاری می‌کند و قادر به تصحیح خطا روی هر t کیوبیتی می‌باشد، باید در این رابطه صدق کند: $n \ge 4+k$ صدق کند. لذا کوچکترین کدی که یک تک کیوبیت را کدگذاری می‌کند و قادر به تصحیح یک خطای اختیاری روی یک تک کیوبیت می‌باشد، باید رابطه $n \ge 4+k=5$ را ارضا کند که در قسمتهای آینده این کد ۵ کیوبیتی را معرفی خواهیم کرد.

۳-۳- ایجاد کدهای کوانتومی

تا اینجا یک چارچوب تئوریکی برای مطالعه کدهای تصحیح خطای کوانتومی ارائه دادیم. در ادامه نمونه‌هایی از این کدها را معرفی می‌کنیم. قبل از معرفی این کدها، خلاصه‌ای از اصول کدهای خطی کلاسیکی را ارائه می‌دهیم و سپس توضیح خواهیم داد که چگونه ایده‌هایی از کدهای خطی کلاسیکی می‌توانند برای ایجاد دسته بزرگی از کدهای کوانتومی که کدهای CSS [۱] نامیده می‌شوند، به کار برده شوند. در ادامه کدهای تثبیت کننده که یک دسته بزرگتر و کلی‌تر از کدهای CSS می‌باشند، را معرفی خواهیم کرد.

۳-۳-۱- تصحیح خطای کلاسیک

می‌دانیم که هر نوع اطلاعات کلاسیک به صورت رشته‌ای از علائم 0 و 1 کد می‌شوند. این نوع کد کردن، اصطلاحا کد گذاری منبع[۲] نامیده می‌شود و قبل از ارسال اطلاعات به درون کانال صورت می‌گیرد و هدف آن تنها این است که اطلاعاتی که به صورت متن، صدا یا تصویر است به صورت رشته‌ای از علائم ساده و قابل حمل در بیت‌های کلاسیک درآید. در کد گذاری منبع، مسئله‌ای به نام تصحیح خطا وجود ندارد، زیرا هنوز اطلاعات به درون کانال (جایی است که خطاها در آن صورت می‌گیرد) ارسال نشده است. به عنوان مثال فرض کنید که منبع ما تنها از چهار حرف A، B، C و D تشکیل شده است. یک راه برای کد کردن منبع آن است که حروف را به رشته‌های زیر کد کنیم:

---

[۱] Calderbank-Shor-Stean codes
[۲] source coding

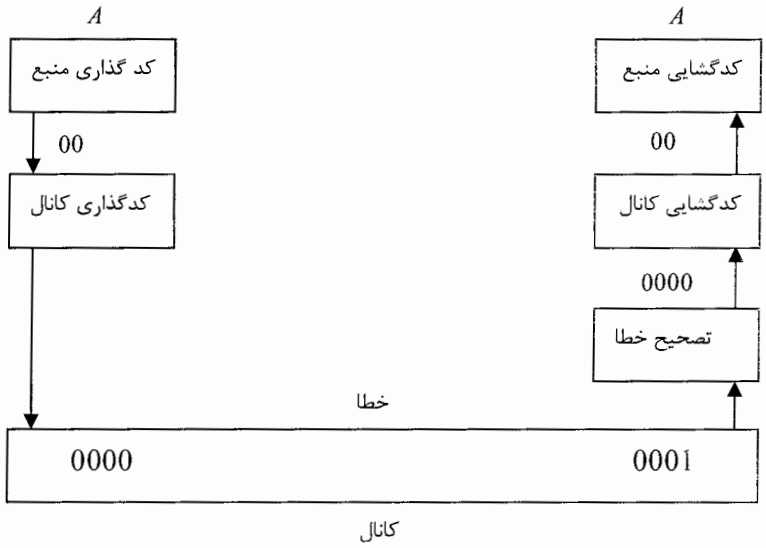
$$A \to 00$$
$$B \to 01$$
$$C \to 10$$
$$C \to 11$$

(۳۷-۳)

در مقصد نیز وقتی که این رشته‌ها به دست گیرنده می‌رسد او نیز همین روش را برای گشودن کد به کار می‌برد که به آن کدگشایی منبع[۱] می‌گوییم. در حالت ساده بالا این عمل به صورت زیر انجام می‌شود:

$$00 \to A$$
$$01 \to B$$
$$10 \to C$$
$$11 \to D$$

(۳۸-۳)



شکل (۳-۵): مراحل مختلف کد کردن و گشودن یک پیام

اما وقتی که همین رشته‌ها را به درون کانال می‌فرستیم، می‌توانند دچار خطا شوند. به عنوان مثال رشته 01 می‌تواند در اثر بروز یک خطا در بیت اول تبدیل به 11 شود که در مقصد به صورت حرف

[۱] source decoding

D تعبیر خواهد شد. بنابراین برای تصحیح این گونه خطاها که در کانال اتفاق می‌افتد می‌بایست در ابتدای کانال یک نوع کدگذاری به کار برد که به آن کد گذاری کانال[۱]، می‌گوییم. به عنوان مثال یک نوع ساده از کدگذاری کانال آن است که رشته‌های چهارگانه فوق را به صورت زیر کد کنیم:

$$\begin{aligned} &00 \to 0000 \\ &01 \to 0101 \\ &10 \to 1010 \\ &11 \to 1111 \end{aligned} \qquad (۳۹-۳)$$

در گیرنده نیز می‌بایست این رشته‌ها را به صورت زیر بگشاییم که به آن کدگشایی کانال[۲] می‌گوییم:

$$\begin{aligned} &0000 \to 00 \\ &0101 \to 01 \\ &1010 \to 10 \\ &1111 \to 11 \end{aligned} \qquad (۴۰-۳)$$

مراحل چهارگانه فوق در شکل (۳-۵) نشان داده شده است.

با این مقدمه می‌توانیم تعریف کلی از کدهای کلاسیک را ارائه دهیم. قبل از آن می‌بایست نمادگذاری خود را روشن کنیم.

تعریف: مجموعه $Z_2^n := Z_2 \times Z_2 \times ... \times Z_2$ عبارت است از مجموعه تمام n تایی‌های مرتب که عناصر آن از 0 و 1 تشکیل شده‌اند.

$$Z_2^n := \{x = x_1 x_2 x_3 ... x_n \mid x_{i=} 0,1\} \qquad (۴۱-۳)$$

دقت کنید که در نوشتن عناصر Z_2^n، نماد $x_1 x_2 x_3 ... x_n$ را به جای نماد $(x_1, x_2, x_3, ..., x_n)$ به کار برده‌ایم. به هر عضو از Z_2^n یک کلمه می‌گوییم. تعداد کلمه‌های Z_2^n برابر است با 2^n.

---

[۱] channel encoding
[۲] channel decoding

تعریف: هرگاه $e \in Z_2^n$ یک کلمه n بیتی باشد، وزن همینگ[1] آن برابر است با تعداد 1 های آن. این وزن را با $w(e)$ نشان می‌دهیم. بنابراین کلمه $e = 001110$ دارای وزن 3 است، یا $w(e) = 3$.

تعریف: هرگاه $x, y \in Z_2^n$ دو کلمه n بیتی باشند، فاصله همینگ[2] آنها برابر است با تعداد بیت‌هایی که با یکدیگر تفاوت دارند. به عبارت دیگر $d(x,y) := w(x-y)$. این فاصله با $d(x,y)$ نشان داده می‌شود و می‌توان نوشت:

$$d(x,y) = \sum_{i=1}^{n} |x_i - y_i| = \sum_{i=1}^{n} (x_i - y_i)^2 \qquad (۴۲-۳)$$

به راحتی می‌توان نشان داد که فاصله همینگ تمام خصوصیات فاصله را دارد، یعنی:

$$\begin{aligned} &d(x,y) \geq 0 \quad , \quad x = y \rightarrow d(x,y) = 0, d(x,y) = 0 \rightarrow x = y \\ &d(x,y) = d(y,x) \\ &d(x,y) \leq d(x,z) + d(z,y) \end{aligned} \qquad (۴۳-۳)$$

فرض کنید که کلمه‌ای مثل v دچار خطای e شود و تبدیل به کلمه $v' = v + e$ شود. در این صورت تعداد خطاهای صورت گرفته در این کلمه برابر است با تعداد ۱ های درون e که برابر است با $w(e)$. دقت کنید که به ازای هر i در e، یک خطا روی v ایجاد می‌شود. به عنوان مثال هر گاه $e = 00110101$ باشد به این معناست که در مکان‌های ۳، ۴، ۶ و ۸ کلمه v دچار خطا شده است.

هر گاه احتمال وقوع یک خطا در یک بیت برابر با p باشد و فرض کنیم که خطاهای بیت‌های مختلف از هم مستقل هستند آنگاه می‌توان احتمال وقوع یک خطای e را حساب کرد. این خطا برابر است با:

$$P(e) = p^{\omega(e)} (1-p)^{n-\omega(e)} \approx p^{\omega(e)} \qquad (۴۴-۳)$$

---

[1] hamming weight
[2] hamming distance

که در تساوی تقریبی آخر از این استفاده کرده‌ایم که p معمولا عدد بسیار کوچکی است. هر گاه $x \in Z_2^n$ یک کلمه‌ی n بیتی باشد، کره همینگ به شعاع d به مرکز x شامل تمام نقاطی است که فاصله آنها از x مساوی یا کمتر از d است. این کره را با $B_d(x)$ نشان می‌دهیم:

$$B_d(x) := \{y \in Z_2^n \mid d(x,y) \le d\} \qquad (۴۵-۳)$$

ایده اصلی کد گذاری کانال آن است که از 2^n نقطه در فضای Z_2^n تعداد کمتری نقطه انتخاب کنیم و آنها را برای کدکردن $(k<n)2^k$ کلمه به کار ببریم و این کار را به نحوی انجام دهیم که فاصله این کلمه‌ها با یکدیگر زیاد باشد به نحوی که اشتباهاتی که در طول کانال رخ می‌دهد آنها را تبدیل به یکدیگر نکند. بنابراین تعریف رسمی یک کد به صورت زیر است:

تعریف: یک کد عبارت است از یک زیرمجموعه از Z_2^n. این زیرمجموعه را با C نشان می‌دهیم و تعداد اعضای آن را برابر 2^k می‌گیریم. به هر عضو یک کد– کلمه می‌گوییم. بنابراین می‌گوییم که کد-کلمه‌های C، k بیت حرف را کدگذاری می‌کنند، چون تعدادشان برابر با 2^k است.

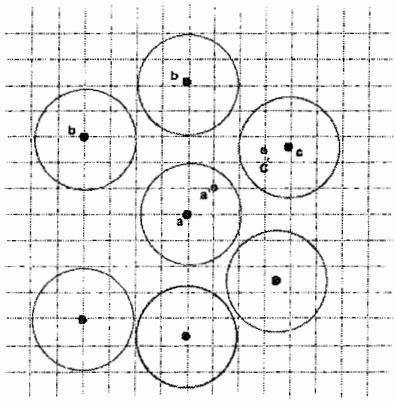
تعریف: فاصله یک کد C که آن را با $d(C)$ یا d نشان می‌دهیم برابر است با کمترین فاصله‌ای که بین کلمات آن وجود دارد. به عبارت دیگر

$$d(C) := \min_{x,y \in C} d(x,y) \qquad (۴۶-۳)$$

نمادگذاری: کدی را که در فضای Z_2^n نوشته می‌شود و برای کدگذاری k بیت به کار برده می‌شود، و فاصله آن برابر با d است را با نماد $[n,k,d]$ نشان داده می‌شود.

یک نحوه تصحیح خطاها در یک کد کلاسیک در شکل (۳-۶) نشان داده شده است. هر گاه فاصله کد برابر با $d = 2t+1$ باشد، حول هر کد-کلمه یک کره همینگ به شعاع t رسم می‌کنیم. در این صورت هر گاه نقطه‌ای دریافت کنیم که متعلق به C نباشد، به این معناست که خطایی صورت گرفته است و آن را به صورت کلمه‌ای که نزدیک‌ترین فاصله را با آن دارد تصحیح می‌کنیم. به عنوان مثال در شکل

(۳-۶) کلمه‌های دریافتی a' و c' متعلق به C نیستند و به کلمه‌های a و c تصحیح می‌شوند. به این ترتیب می‌گوییم که کدی که فاصله آن برابر با $d=2t+1$ است قادر است که خطاهای با وزن t یا اصطلاحا t خطا را تصحیح کند.



شکل(۳-۶): نحوه تشخیص و خنثی کردن خطا

به عنوان مثال کد $C=\{000,111\}$ را در نظر بگیرید. این کد که اصطلاحا کد تکرار سه‌تایی نامیده می‌شود، کدی است از نوع $[3,1,3]$ و می‌تواند یک خطا را تشخیص دهد و تصحیح کند. همچنین کد $C=\{000000,101010,010101,111111\}$ از نوع $[6,2,3]$ است و می‌تواند یک خطا را تشخیص دهد و تصحیح کند. می‌توان این کد را برای کد کردن دو بیت به صورت زیر به کار برد:

$$\begin{aligned} &00\rightarrow 00000\\ &01\rightarrow 010101\\ &10\rightarrow 101010\\ &11\rightarrow 111111 \end{aligned} \qquad (۴۷-۳)$$

کد زیر را نیز در نظر بگیرید:

$$C=\{000,011,101,110\} \qquad (۴۸-۳)$$

در این کد، بیت سوم که به بیت پاریته موسوم است، پاریته دو بیت اول را تعیین می‌کند. به این معنا که اگر مجموع این دو بیت برابر با صفر باشد مقدار این بیت برابر صفر و در غیر این صورت مقدار آن برابر با یک است. به عبارت دیگر در هر کلمه‌ی این کد داریم $x_3 = x_1 + x_2$. با این حساب خواهیم داشت $x_1 + x_2 + x_3 = 0$، یعنی پاریته مجموع سه عدد برابر با صفر خواهد بود. به این ترتیب این کد می‌تواند یک خطا را آشکار کند، زیرا وقوع یک خطا پاریته کلمه را تغییر خواهد داد. اما این کد تنها می‌تواند این خطا را آشکار کند و قادر به تصحیح آن نیست. مثلا معلوم نیست که کلمه دریافتی 111 کدام یک از سه کلمه ارسالی 011، 101 و 110 بوده است که دچار خطا شده است. کمی دقت نشان می‌دهد که فاصله این کد برابر با دو است و به همین دلیل است که نمی‌تواند تشخیص دهد که یک کلمه معیوب ناشی از ایجاد خطا بر روی کدام کد کلمه بوده است زیرا کره‌های همینگ به شعاع یک برای سه کلمه فوق همگی نقطه‌ی 111 را در بر دارند.

به عنوان مثال دیگر کد زیر را در نظر بگیرید:

$$C = \{00000, 01011, 01011, 01110, 10011, 10110, 110000, 11101\} \qquad (۴۹-۳)$$

این کد از نوع $[5,3,2]$ می‌باشد و می‌تواند یک خطا را تشخیص دهد ولی نمی‌تواند آن را تصحیح کند. در این کد رابطه زیر برقرار است:

$$Z_4 = x_1 + x_2 \qquad x_5 = x_1 + x_2 + x_3 \qquad (۵۰-۳)$$

بنابراین بیت چهارم پاریته دو بیت اول و بیت پنجم پاریته سه بیت اول را در خود نگاه می‌دارد. سه بیت اول معمولا بیت‌های پیام[۱] و دو بیت آخر، بیتهای پاریته[۲] نامیده می‌شوند.

[۱] message bits
[۲] parity bits

۳-۳-۲- کدهای خطی

می‌دانیم که مجموعه Z_2^n یک ساختار خطی دارد و می‌توان آن را به عنوان یک فضای برداری روی میدان Z_2 در نظر گرفت. هرگاه $x = x_1x_2...x_n \in Z_2^n$ و $y = y_1y_2...y_n \in Z_2^n$، آنگاه جمع این دو بردار به شکل زیر تعریف می‌شود:

$$x + y = z_1z_2...z_n \qquad (۵۱-۳)$$

که در آن

$$z_i = x_i + y_i \mod 2 \qquad (۵۲-۳)$$

همچنین به صورت بدیهی می‌توان هر برداری مثل x را در عددی مثل $\alpha \in Z_2$ ضرب کرد. همه مفاهیمی که برای فضاهای برداری می‌شناسیم مثل استقلال خطی بردارها، پایه، بعد و نظایر آن برای این فضا نیز تعریف می‌شوند، با این تفاوت که بایستی همواره در نظر داشته باشیم که میدان اعداد در اینجا میدان اعداد $Z_2 = \{0,1\}$ است. در این فضا می‌توان یک ضرب داخلی نیز به شکل زیر تعریف کرد:

$$x.y = \sum_{i=1}^{n} x_i y_i \qquad (۵۳-۳)$$

تعداد عناصر این فضای خطی محدود و برابر با 2^n است.

در قسمتهای قبلی کد را به صورت زیر مجموعه‌ای از Z_2^n تعریف کردیم. برای کدهای خطی، طبیعی است که از خاصیت خطی بودن فضای Z_2^n استفاده کنیم. به همین دلیل کد خطی را به شکل زیر تعریف می‌کنیم.

تعریف: در فضای خطی Z_2^n، یک کد خطی چیزی نیست جز یک زیرفضای C از Z_2^n. هرگاه این زیر فضا k بعدی باشد آن را به شکل زیر برای کد کردن k بیت به کار می‌بریم. فرض کنید که

$B=\{\nu_1,\nu_2,...,\nu_k\}$ یک پایه برای C و $\alpha=\alpha_1\alpha_2...\alpha_k\in Z_2^k$ یک کلمه k بیتی باشد. در این صورت این کلمه را به صورت زیر در n بیت کدگذاری می‌کنیم:

$$\alpha\to\nu(\alpha)=\alpha_1\nu_1+\alpha_2\nu_2+...\alpha_k\nu_k \qquad (۵۴-۳)$$

در چنین مواردی می‌نویسیم

$$C=\langle\nu_1,\nu_2,...,\nu_k\rangle \qquad (۵۵-۳)$$

مثلا در فضای Z_2^5 یک کد سه بعدی در نظر بگیرید که با بردارهای پایه $B=\{00111,11000,10001\}$ جاروب می‌شود. در این صورت کلمه‌ی سه بیتی $\alpha=\alpha_1\alpha_2\alpha_3$ به صورت زیر کد می‌شود:

$$\alpha\to\nu(\alpha)=\alpha_1(00111)+\alpha_2(11000)+\alpha_3(10001)=(\alpha_2+\alpha_3,\alpha_2,\alpha_1,\alpha_1,\alpha_1+\alpha_3) \qquad (۵۶-۳)$$

بنابراین در این کد خطی کلمات سه بیتی به صورت زیر کد می‌شوند:

$$\begin{aligned}
&000\to00000\\
&001\to10001\\
&010\to11000\\
&011\to01001\\
&100\to00111\\
&101\to10110\\
&110\to11111\\
&111\to01110
\end{aligned} \qquad (۵۷-۳)$$

نوشتن کدهای خطی بسیار آسان است، کافی است که مجموعه‌ای از بردارهای مستقل از فضای Z_2^n در نظر گرفت و کلمات را به صوت ترکیب‌های خطی آنها کد کرد. اما معلوم نیست که انتخاب ما انتخاب خوبی باشد یعنی این کد بتواند خطاها را تصحیح کند. بنابراین سوالی که با آن مواجه هستیم آن است که چگونه می‌توان خواص کدهای خطی نظیر فاصله را تعیین کرد و این که آیا راه ساده‌ای برای تشخیص و تصحیح خطاها توسط این کدها وجود دارد یا نه؟ در واقع با استفاده از ساختار خطی

کد می‌بایست بتوانیم برای این سوالها پاسخ‌های روشنی بیابیم. برای پاسخ به این سوال‌ها می‌بایست ساختار کدهای خطی را بهتر بشناسیم.

۳-۳-۳- ساختار کدهای خطی

فرض کنید که یک کد خطی با پایه $B_C = \{v_1, v_2, ..., v_k\}$ تعریف شده باشد. در این صورت هر کلمه‌ی α به صورت کد-کلمه‌ی $v(\alpha)$ کد می‌شود که در آن

$$v(\alpha) = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_k \alpha_k = (\alpha_1, \alpha_2, ..., \alpha_k) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} \quad (۵۸-۳)$$

با تعریف ماتریس $G = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix}$ که بعد $k \times n$ را دارد، می‌توانیم رابطه بالا را به شکل فشرده زیر بنویسیم:

$$v(\alpha) = \alpha G \quad (۵۹-۳)$$

دقت کنید که ماتریس G یک ماتریس با رتبه‌ی k است زیرا همه سطرهای آن مستقل خطی‌اند. ماتریس G ماتریس مولد[۱] نام دارد.

به عنوان مثال کد خطی C با پایه $B_C = \{1000, 1010, 0101\}$ دارای عناصر زیراست:

$$\{0000, 1000, 1010, 0101, 0010, 1101, 1111, 0111\} \quad (۶۰-۳)$$

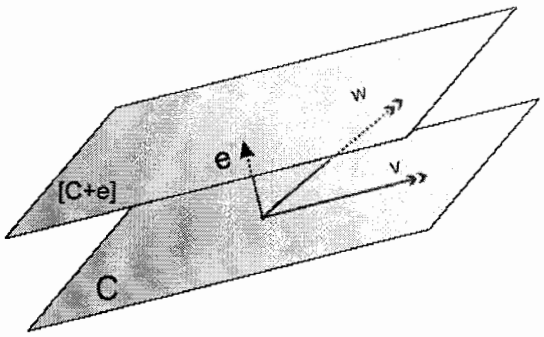
ماتریس مولد این کد عبارت است از:

[۱] generator matrix

$$G=\begin{pmatrix}1000\\1010\\0101\end{pmatrix} \qquad (۶۱-۳)$$

می‌دانیم که یک کد خطی C با یک زیرفضا در فضای برداری Z_2^n مشخص می‌شود (شکل (۳-۷)) این کد برای نوشتن سه بیت در ۴ بیت به کار می‌رود. هر کلمه سه بیتی مثل $\alpha=\alpha_1\alpha_2\alpha_3$ به صورت زیر به یک کلمه چهار بیتی کد می‌شود:

$$\alpha\to v(\alpha)=(\alpha_1,\alpha_2,\alpha_3)\begin{pmatrix}1&0&0&0\\1&0&1&0\\0&1&0&1\end{pmatrix}=(\alpha_1+\alpha_2\quad\alpha_3\quad\alpha_2\quad\alpha_3) \qquad (۶۲-۳)$$



شکل (۳-۷): یک خطا باعث می‌شود که بردار یک کلمه از زیرفضای کد خارج شود.

برای تشخیص خطا باید دقت کنیم که هر خطایی باعث می‌شود که بردار مربوط به یک کد-کلمه از زیرفضای C خارج شود (شکل (۳-۷)). (در اینجا توجه به یک نکته اهمیت دارد و آن این است که در یک کد ممکن است یک کلمه در اثر خطا تبدیل به یک کلمه دیگر واقع در درون کد شود. هیچ کدی نمی‌تواند این نوع خطا را آشکار کرده و تصحیح کند. البته احتمال وقوع چنین خطاهایی بسیار کم است.)

چگونه می‌توان تشخیص داد که برداری دچار خطا شده است؟ چگونه می‌توان فهمید که برداری از زیرفضای C خارج شده است؟ اگر به شکل (۳-۷) نگاه کنیم یک راه ساده می‌توانیم برای آن پیدا کنیم. می‌توان از یک نشانه خیلی ساده برای این کار استفاده کرد. برای درک این نشانه احتیاج به مقدمات ساده‌ای داریم.

قضیه ۳-۳) هرگاه V یک فضای برداری و C یک زیر فضای آن باشد، مجموعه بردارهایی که بر C عمود هستند تشکیل یک زیرفضا می‌دهند.

تعریف: اگر C یک زیرفضا باشد، فضای برداری تشکیل شده از بردارهای عمود بر C را با $C^{\perp}$ نشان می‌دهیم.

قضیه ۳-۴) اگر $C \subset V$ باشد، رابطه زیر بین ابعاد C و $C^{\perp}$برقرار است:

$$\dim(C)+\dim(C^{\perp})=n \qquad (۶۳-۳)$$

اثبات: فرض کنید که $\dim(V)=n$ و $B_C=\{v_1,v_2,...v_k\}$ یک پایه برای فضای C باشد. در این صورت اگر $\omega \in C^{\perp}$، آنگاه:

$$\begin{aligned}&\omega.v_1=0\\&\omega.v_2=0\\&\vdots\\&\omega.v_k=0\end{aligned} \qquad (۶۴-۳)$$

این معادلات یک دستگاه از k معادله و n مجهول را تشکیل می‌دهند که با توجه به مستقل بودن v_iها، جواب کلی آن دارای $n-k$ پارامتر آزاد خواهد بود که به این معناست که فضای جواب‌های این معادلات یک فضای $n-k$ بعدی است.

برای فضای $C^{\perp}$ می‌توان $n-k$ بردار پایه انتخاب کرد که آنها را با $\omega_1,\omega_2,...,\omega_{n-k}$ نشان می‌دهیم. بنابراین خواهیم داشت:

$$\omega_i.\nu_j = 0 \qquad \forall i,j \tag{۶۵-۳}$$

می‌توان بردارهای $\omega_1,\omega_2,...,\omega_{n-k}$ را در یک ماتریس H به صورت زیر جای داد:

$$H = \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_{n-k} \end{pmatrix} \tag{۶۶-۳}$$

ماتریس H یک ماتریس $(n-k)\times n$ بعدی خواهد بود و ماتریس کنترلی پاریته[1] نامیده می‌شود. با توجه به رابطه (۳-۶۵)، رابطه زیر برقرار خواهد بود:

$$GH^T = 0 \tag{۶۷-۳}$$

با توجه به این رابطه هر بردار ν متعلق به کد C در خاصیت زیر صدق می‌کند:

$$\nu H \equiv \nu(\alpha) H^T = \alpha G H^T = 0 \tag{۶۸-۳}$$

حال اگر بردار ν دچار خطا شود و تبدیل به برداری مثل $\omega = \nu + e$ شود (شکل (۳-۷))، در این صورت خواهیم داشت:

$$\omega H^T = (\nu + e) H^T = e H^T \neq 0 \tag{۶۹-۳}$$

بنابراین صفر نشدن ωH^T به معنای آن است که بردار ω یک بردار متعلق به کد نیست و حتما خطایی اتفاق افتاده است. ولی چگونه می‌توانیم نوع خطا را بفهمیم و در جهت تصحیح آن اقدام کنیم. نکته‌ای که وجود دارد آن است که یک بردار معیوب مثل ω ممکن است به طرق مختلفی تولید شده باشد. به عنوان مثال این بردار می‌تواند حاصل خطای e_1 بر بردار ν_1، یا خطای e_2 بر بردار ν_2 باشد به نحوی که

[1] parity check matrix

$$v_1 + e_1 = v_2 + e_2 = \omega \qquad (۷۰-۳)$$

از میان خطاهای ممکن می‌بایست محتمل‌ترین خطا، یعنی خطایی با کمترین وزن همینگ را درنظر گرفت و فرض کرد که $\omega = v + e_0$ که در آن e_0 کمترین وزن ممکن را دارد و در نتیجه می‌بایست ω را به شکل زیر تصحیح کرد:

$$\omega \to \omega + e_0 \qquad (۷۱-۳)$$

می‌توان مطالب بالا را به زبان دقیق و ریاضی نیز بیان کرد. اگر به شکل (۳-۷) نگاه کنیم متوجه می‌شویم که C یعنی خود کد، یک زیرفضاست و بقیه صفحات در واقع یکسان با C هستند ولی زیرفضا نیستند زیرا شامل بردار 0 نیستند. برای پیشتر رفتن به تعاریف زیر احتیاج داریم.

تعریف: فرض کنید که V یک فضای برداری و C یک زیر فضای آن باشد. در این صورت هر دو بردار $\omega_1, \omega_2 \in V$ را هم ارز می‌گوییم هرگاه رابطه زیر برقرار باشد:

$$\omega_1 - \omega_2 \in C \qquad (۷۲-۳)$$

به راحتی می‌توان ثابت کرد که این رابطه یک رابطه هم ارزی است و بنابراین فضای V (در اینجا Z_2^n) توسط زیرفضای C (که در اینجا هما فضای کد-کلمه هاست) به زیر مجموعه‌هایی که عناصر آنها با یکدیگر هم ارز هستند افراز می‌شود. هر کلاس هم ارز یک هم‌مجموعه[۱] نامیده می‌شود. اگر به شکل (۳-۷) نگاه کنیم متوجه می‌شویم که از نظر هندسی هر مجموعه، یک صفحه موازی با صفحه C است. باید دقت کنیم که شکل (۳-۷) تا حدودی به درک شهودی ما کمک می‌کند و از بعضی جهات می‌تواند گمراه کننده باشد، زیرا ما در اینجا با یک فضای برداری روی میدان $Z_2 = \{0,1\}$ سر و کار داریم نه یک فضای برداری حقیقی. به همین دلیل تعداد بردارهای کل فضا و همچنین زیرفضای C و تمام کلاس‌های هم ارز محدود است.

---

[۱] coset

فرض کنید که بردارهای فضای کد، یعنی C را به صورت زیر نمایش می‌دهیم:

$$C := \{\nu_1, \nu_2, \nu_3, ..., \nu_K\} \qquad (۷۳-۳)$$

که در آن $K = 2^k$ (زیرا فرض کرده‌ایم که C یک فضای k بعدی است)، دراین صورت به ازای هر برداری مثل e_i که متعلق به C نباشد یک کلاس هم ارزی داریم که برابر است با:

$$[e_i] \equiv e_i + C = \{\nu_1 + e_i, \nu_2 + e_i, ..., \nu_K + e_i\} \qquad (۷۴-۳)$$

به دو نکته باید دقت کرد:

نکته اول: برای تمام عناصر یک کلاس، اثر H یکسان و برابر است با e_iH. هم چنین اثر H روی هیچ دو کلاس متفاوتی، یکسان نیست، زیرا

$$\omega_1 H^T = 0, \qquad \omega_2 H^T = 0 \to (\omega_1 - \omega_2) H^T = 0 \to \omega_1 - \omega_2 \in C \to [\omega_1] = [\omega_2] \qquad (۷۵-۳)$$

بنابراین اثر H روی یک کد دریافتی تنها به کلاس هم ارزی بستگی دارد و می‌توان آن را به عنوان شناسنده کلاس هم ارزی یا نشانه خطا به کار برد.

نکته دوم: یک کلاس هم ارزی مثل کلاس (۳-۴۱) را می‌توان به صورت کلاس $[e_i + \nu_1]$ یا کلاس $[e_i + \nu_2]$ یا کلاس $[e_i + \nu_k]$ نیز نامید و در وهله اول هیچ ترجیحی در نامگذاری یک کلاس به یکی از این صورت‌ها نیست. از این به بعد نماینده کلاس را برداری می‌گیریم که کمترین وزن همینگ را دارد. بنابراین وقتی می‌گوییم کلاس $[e_i]$، یعنی بردار e_i در این کلاس کمترین وزن همینگ را دارد.

دو نکته فوق به ما می‌آموزند که چگونه باید خطاها را آشکار کرده و تصحیح کنیم.

نحوه تصحیح خطا: هر بردار ω که دریافت می‌شود، ωH^T برای آن محاسبه می‌شود. اگر $\omega H^T = 0$ باشد به این معناست که خطایی صورت نگرفته است. اگر $\omega H^T \neq 0$، می‌فهمیم که خطایی صورت گرفته است. مقدار ωH در واقع نشانه خطاست و برای ما کلاس هم ارزی $[e_i]$ را تعیین می‌کند. در

این کلاس، e_i کمترین وزن همینگ را دارد و بنابراین محتمل ترین خطا همان e_i است. بنابراین کلمه دریافتی ω را به صورت $\nu = \omega + e_i$ تصحیح می‌کنیم.

دیدیم که در یک کد خطی C ماتریس مولد از بردارهای پایه ساخته می‌شود. هرگاه $B_C = \{\nu_1, \nu_2, ..., \nu_k\}$ یک پایه برای C باشد، ماتریس مولد این کد که آن را با G نمایش می‌دهیم به صورت زیر نوشته می‌شود:

$$G = \begin{pmatrix} \nu_1 \\ \nu_2 \\ \vdots \\ \nu_k \end{pmatrix} \qquad (۷۶-۳)$$

از آنجا که بردارهای پایه از هم مستقل هستند نتیجه می‌گیریم که رتبه ماتریس G برابر با k است . همچنین می‌توانیم به جای پایه فوق پایه دیگری مثل $\{u_1, u_2, ..., u_k\}$ به کار ببریم که بردارهای آن با عوض کردن ترتیب بردارهای پایه اولیه و یا ترکیبی خطی از آنها به دست آمده است. این امر به این معناست که می‌توان با انتخاب پایه مناسب ماتریس G را به شکل استاندارد زیر در آورد:

$$G\left(I_k \mid X_{k,n-k}\right) \qquad (۷۷-۳)$$

که در آن I_k ماتریس یکه با بعد k است و $X_{k,n-k}$ یک ماتریس با بعد $k \times n-k$ است. تحت این شرایط معلوم می‌شود که ماتریس H به شکل زیر در می‌آید زیرا می‌بایست در شرط $GH^T = 0$ صدق کند:

$$H^T = \left(\frac{X_{k,n-k}}{I_{n-k}}\right) \rightarrow H = \left(X^T_{n-k,k} \mid I_{n-k}\right) \qquad (۷۸-۳)$$

از رابطه $GH^T = 0$ نتیجه می‌گیریم که $HG^T = 0$. این رابطه بیان می‌کند که یک کد دیگر وجود دارد که ماتریس مولد آن H و ماتریس پاریته آن G است. اما این کد چیزی نیست جز $C^{\perp}$.

یک دسته مهم از کدهای تصحیح خطای کوانتومی، کدهای همینگ[1] می‌باشند. فرض کنید که $r \geq 2$ یک عدد صحیح و H ماتریسی باشد که ستونهایش همه رشته‌های $2^r - 1$ بیتی با طول r باشد که به طور یکسان 0 نیستند. این ماتریس کنترلی پاریته، یک کد خطی $\left[2^r - 1, 2^r - r - 1\right]$ را تعریف می‌کند که کد همینگ نام دارد. یک مثال مهم از تصحیح خطاهای کوانتومی، حالت $r = 3$ است که کد $[7,4]$ با ماتریس کنترلی پاریته زیر می‌باشد:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \qquad (۷۹-۳)$$

از طرفی اگر در یک ماتریس کنترلی پاریته، هر $d-1$ ستون مستقل خطی باشند، اما یک مجموعه از d ستون که وابسته خطی هستند، وجود داشته باشد، ثابت می‌شود که فاصله این ماتریس d باشد. در اینجا نیز مشاهده می‌کنیم که هر دو ستون از H متفاوت و بنابراین مستقل خطی‌اند و 3 ستون اول وابسته خطی هستند، لذا فاصله این کد 3 می‌باشد که نشان می‌دهد این کد قادر به تصحیح یک خطا روی هر کیوبیت می‌باشد.

در حقیقت این روش تصحیح خطا بسیار آسان است. فرض کنید که یک خطا روی j امین بیت اتفاق بیفتد. رابطه (۳-۷۹) نشان می‌دهد که نشانه He_j، یک نمایش باینری برای j می‌باشد که بیانگر این است که کدام بیت باید وارون شود تا خطا تصحیح شود.

[1] Hamming codes

۳-۳-۴- یک رابطه تعامد مهم بین یک کد و کد عمود بر آن

در اینجا یک رابطه مهم بین دو کد C و $C^{\perp}$ را ثابت می‌کنیم که در ساختن کدهای کوانتومی نقش مهمی ایفا می‌کند. نخست به اتحاد زیر توجه می‌کنیم:

$$\sum_{x\in\{0,1\}} (-1)^{xy} = 2\delta_{y,0} \qquad (۸۰-۳)$$

و یا تعمیم آن به n بیت که به صورت زیر بیان می‌شود:

$$\sum_{x\in\{0,1\}^n} (-1)^{x.y} = 2^n \delta_{y,0} \qquad (۸۱-۳)$$

دقت کنید که هر گاه x و y را به صورت بردارهای سطری در نظر بگیریم، آنگاه می‌توانیم بنویسیم $x.y = xy^T$. این نکته در درک رابطه بعدی اهمیت دارد.

می‌خواهیم ببینیم که اگر در رابطه بالا به جای همه $x\in Z_2^n$ تنها روی کدکلمه‌های درون C که زیرفضایی از Z_2^n است، جمع بزنیم چه چیزی به دست می‌آوریم.

دقت می‌کنیم که به ازای هر $y\in Z_2^n$

$$\begin{aligned}\sum_{v(\alpha)\in C} (-1)^{v(\alpha).y} &= \sum_{\alpha\in\{0,1\}^k} (-1)^{\alpha G.y} \\ &= \sum_{\alpha\in\{0,1\}^k} (-1)^{\alpha G y^T} = 2^k \delta_{Gy^T,0}\end{aligned} \qquad (۸۲-۳)$$

اما می‌دانیم که G ماتریس پاریته کد $C^{\perp}$ است و در نتیجه هر گاه yG^T برابر صفر باشد به این معناست که $y\in C^{\perp}$. بنابراین رابطه بالا را می‌توان به صورت زیر نوشت:

$$\sum_{v(\alpha)\in C} (-1)^{v(\alpha).y} = \begin{cases} 2^k & if \quad y\in C^{\perp} \\ 0 & if \quad y\notin C^{\perp} \end{cases} \qquad (۸۳-۳)$$

۳-۴- کدهای CSS

یکی از مثالهای کدهای تصحیح خطای کوانتومی، کدهای CSS می‌باشند. این کدها یک زیرگروه از مجموعه کلی‌تر کدهای تثبیت کننده[۱] هستند.

فرض کنید که C_1 و C_2 کدهای خطی کلاسیکی $[n,k_1]$ و $[n,k_2]$ باشند به طوریکه $C_2 \subset C_1$ باشد و C_1 و $C_2^{\perp}$ هر دو t خطا را تصحیح کنند. کد کوانتومی $[n,k_1-k_2]$ را معرفی می‌کنیم (CSS)، که قادر به تصحیح خطا روی t کیوبیت می‌باشد. فرض کنید که $x \in C_1$ یک کد-کلمه در کد C_1 باشد. حالت کوانتومی $|x \oplus C_2\rangle$، توسط رابطه زیر تعریف می‌شود:

$$|x \oplus C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x \oplus y\rangle \qquad (۸۴-۳)$$

فرض کنید که x' یک عنصر از C_1 باشد به طوریکه $x - x' \in C_2$ باشد. در این صورت واضح است که $|x \oplus C_2\rangle = |x' \oplus C_2\rangle$ و بدین ترتیب حالت $|x \oplus C_2\rangle$ تنها به هم‌مجموعه C_1/C_2، که x در آن می‌باشد بستگی دارد. به علاوه اگر x و x' متعلق به هم‌مجموعه‌های متفاوت از C_2 باشند در این صورت برای هیچکدام از $y, y' \in C_2$، این رابطه برقرار نیست $x \oplus y = x' \oplus y'$ و بنابراین $|x + C_2\rangle$ و $|x' + C_2\rangle$ حالتهای متعامد می‌باشند. کد کوانتومی $CSS(C_1, C_2)$ فضای برداری تعریف می‌شود که توسط حالت $|x + C_2\rangle$ برای همه $x \in C_1$ تعیین می‌شود. تعداد هم‌مجموعه‌های C_2 در C_1، $|C_1|/|C_2|$ می‌باشد، بنابراین بُعد $CSS(C_1, C_2)$، $|C_1|/|C_2| = 2^{k_1 - k_2}$ است، پس $CSS(C_1, C_2)$ یک کد کوانتومی $[n, k_1 - k_2]$ می‌باشد. می‌توان از ویژگی‌های C_1 و $C_2^{\perp}$ برای آشکارسازی و تصحیح خطای کوانتومی استفاده کرد.

---

[۱] stabilizer code

۳-۴-۱- کد استین [1]

یک مثال مهم از کد CSS با استفاده از کد همینگ $[7,4,3]$، که ماتریس کنترلی پاریته آن به شکل زیر است، را در زیر آورده‌ایم:

$$H=\begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix} \qquad (۸۵-۳)$$

فرض کنید که ما این کد را C بنامیم و تعاریف زیر را نیز داشته باشیم: $C_2\equiv C^{\perp}$ و $C_1\equiv C$. برای استفاده از این کدها برای تعریف کد CSS، در ابتدا لازم است که بررسی کنیم که آیا $C_2\subset C_1$ هست یا خیر. با مشخص کردن ماتریس کنترلی پاریته $C_2=C^{\perp}$ که ترانهاده ماتریس مولد $C_1=C$ است:

$$H[C_2]=G[C_1]^T=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix} \qquad (۸۶-۳)$$

با مقایسه (۳-۸۵) می‌خواهیم ببینیم که محدوده سطرهای $H[C_2]$ دقیقا شامل محدوده سطرهای $H[C_1]$ است و از آنجائیکه کدهای متناظر، کرنل‌های $H[C_2]$ و $H[C_1]$ هستند، لذا ما نتیجه می‌گیریم که $C_2\subset C_1$ است. بعلاوه $C_2^{\perp}=\left(C^{\perp}\right)^{\perp}=C$، بنابراین هر دو کد C_1و $C_2^{\perp}$، کدهایی با فاصله ۳ هستند که می‌توانند خطاها را روی یک بیت تصحیح کنند.

چون کد C_1 برابر $[7,4]$ و کد C_2، $[7,3]$ می‌باشند، لذا $CSS(C_1,C_2)$، کد کوانتومی $[7,1]$خواهد بود که خطاها را روی یک تک کیوبیت تصحیح می‌کند.

این کد کوانتومی $[7,1]$ ویژگی‌های جالبی دارد که کار کردن با آن را آسان می‌کند. این کد به نام کد استین شناخته می‌شود.

---

[1] Stean code

کد- کلمه‌های C_2 به آسانی از (۳-۸۶) به دست می‌آیند. به جای اینکه صراحتا آنها را بنویسیم، آنها را به صورت منطقی $|0_L\rangle$ می‌نویسیم. برای کد استین

$|0+C_2\rangle$:

$$|0_L\rangle=\frac{1}{\sqrt{8}}\begin{bmatrix}|0000000\rangle+|1010101\rangle+|0110011\rangle\\+|1100110\rangle+|0001111\rangle+|1011010\rangle\\+|0111100\rangle+|1101001\rangle\end{bmatrix} \qquad (۸۷-۳)$$

برای اینکه کد-کلمه منطقی دیگر را تعیین کنیم، باید اعضای از C_1 را که در C_2 نیست پیدا کنیم. مثلا $|1111111\rangle$، لذا داریم:

$$|1_L\rangle=\frac{1}{\sqrt{8}}\begin{bmatrix}|1111111\rangle+|0101010\rangle+|1001100\rangle\\+|0011001\rangle+|1110000\rangle+|0100101\rangle\\+|1000011\rangle+|0010110\rangle\end{bmatrix} \qquad (۸۸-۳)$$

۳-۵- کدهای تثبیت کننده

کدهای تثبیت کننده که گاهی اوقات به عنوان کدهای کوانتومی افزاینده[۱] شناخته می‌شوند، یک دسته مهم از کدهای کوانتومی هستند که ساختارشان شبیه به کدهای خطی کلاسیکی است. برای فهم کدهای تثبیت کننده، بهتر است در ابتدا فرمالیزم تثبیت کننده که یک روش قدرتمند در فهم دسته-ی بزرگی از عملها در مکانیک کوانتومی می‌باشد، را توضیح دهیم. کاربرد فرمالیزم تثبیت کننده، فراتر از تصحیح خطای کوانتومی می‌باشد، در هر صورت در اینجا ما با این کاربرد ویژه سر و کار داریم. پس از مشخص کردن فرمالیزم تثبیت کننده، توضیح می‌دهیم که چگونه گیتهای یکانی و اندازه‌گیری‌ها با استفاده از آن توصیف می‌شوند و همچنین یک قضیه مهم را مطرح می‌کنیم که محدودیتهای عملهای

[۱] additive

تثبیت کننده را مشخص می‌کند. پس از آن ساختارهای تثبیت کننده را برای کدهای تثبیت کننده به همراه مثالهای روشن و واضح و یک شکل استاندارد برای یک کد تثبیت کننده ارائه می‌دهیم.

۳-۵-۱- فرمالیزم تثبیت کننده [۱]

برای فهم فرمالیزم تثبیت کننده، به مثال زیر توجه کنید. حالت EPR دو کیوبیت را در نظر بگیرید.

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad (۸۹-۳)$$

به آسانی مشخص می‌شود که این حالت در اتحادهای $X_1X_2|\psi\rangle = |\psi\rangle$ و $Z_1Z_2|\psi\rangle = |\psi\rangle$ صدق می‌کند، گوییم حالت $|\psi\rangle$ توسط عملگرهای X_1X_2 و Z_1Z_2، تثبیت شده‌اند. حالت $|\psi\rangle$ یک حالت کوانتومی یکتا (منحصر به فرد) می‌باشد که توسط عملگرهای X_1X_2 و Z_1Z_2، تثبیت شده است. یک ایده ساده از فرمالیزم تثبیت کننده این است که بیشتر حالات کوانتومی با کار کردن با عملگرهایی که آنها را تثبیت می‌کنند، راحت‌تر توصیف می‌شوند تا اینکه با خود حالتها مستقیما کار کنیم. این ادعا در وهله اول شاید تعجب آور به نظر برسد هر چند که حقیقت دارد. این نشان می‌دهد که بسیاری از کدهای کوانتومی (شامل کدهای CSS و کد شُور) با به کار بردن تثبیت کننده‌ها راحت‌تر توصیف می‌شوند تا با توصیف بردار حالت و حتی مهمتر اینکه خطاهای روی کیوبیتها و عملها مانند گیت هادامارد، گیت فاز و حتی $CNot$ و اندازه‌گیری‌ها در پایه محاسباتی با به کار بردن فرمالیزم تثبیت کننده، بسیار راحت‌تر توصیف می‌شوند.

کلید قدرتمند فرمالیزم تثبیت کننده، در کاربرد هوشمندانه نظریه گروه قرار دارد.

---

[۱] stabilizer formalism

گروه اصلی مورد نظر (گروه پائولی) G_n روی n کیوبیت می‌باشد. برای یک تک کیوبیت، گروه پائولی به صورت زیر تعریف می‌شود که شامل همه ماتریسهای پائولی به همراه ضرایب ضربی ± 1 و $\pm i$ می‌باشد:

$$G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \qquad (۹۰-۳)$$

این گروه از ماتریسها یک گروه تحت عمل ضرب ماتریسی تشکیل می‌دهند. ممکن است تعجب کنید که چرا، ضرایب ± 1 و $\pm i$ را حذف نمی‌کنیم. دلیل آوردن آنها این است که مطمئن شویم که G_1 نسبت به عمل ضرب بسته است و بدین ترتیب یک گروه درست تشکیل دهیم. گروه پائولی کلی روی n کیوبیت، شامل همه‌ی حاصلضربهای تانسوری ماتریسهای پائولی به همراه ضرایب ± 1 و $\pm i$ می‌باشد.

اکنون ما تثبیت کننده‌ها را یک مقدار دقیق‌تر می‌توانیم تعریف کنیم. فرض کنید که S یک زیرمجموعه از G_n باشد و V_s را به صورت یک مجموعه از حالتهای n کیوبیتی که با هر کدام از عناصر S، ثابت شده باشد، تعریف می‌کنیم. V_s تحت عمل عناصر S، ثابت می‌باشند. یک ترکیب خطی اختیاری از هر دو عنصر V_s، در V_s می‌باشد. بنابراین V_s یک زیر مجموعه از فضای حالت n کیوبیتی می‌باشد. ثابت می‌شود که V_s، بخش مشترک زیرفضاهایی می‌باشد که توسط هر یک از عملگرهای S ثابت شده‌اند.

مثال ساده‌ای از فرمالیزم تثبیت کننده را در عمل بررسی می‌کنیم. برای حالت $n=3$ کیوبیتی و $S \equiv \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$، زیرفضای ثابت شده توسط Z_1Z_2 با گستره $|000\rangle, |001\rangle, |110\rangle, |111\rangle$ و زیرفضای ثابت شده توسط Z_2Z_3 با گستره $|111\rangle, |011\rangle, |100\rangle, |000\rangle$ مشخص می‌شود.

توجه کنید که عناصر $|000\rangle$ و $|111\rangle$ در هر دو لیست وجود دارند. با این مشاهدات و اندکی فکر، در می‌یابیم که V_s باید زیرفضایی با حالتهای $|000\rangle$ و $|111\rangle$ باشد.

در این مثال ما به آسانی V_s را با توجه به زیرفضاهای تثبیت شده توسط دو عملگر در S، تعیین کردیم. این نمایانگر یک پدیده مهم کلی است (توصیف یک گروه توسط مولدهایش). می‌دانیم که یک مجموعه از عناصر $g_1, g_2, ..., g_l$ در یک گروه G، گروه G را تولید می‌کنند، و یا به عبارتی مولد گروه G هستند. اگر هر عنصر از G بتواند به صورت یک حاصلضرب عناصر موجود در لیست $g_1, g_2, ..., g_l$ نوشته شود و می‌نویسیم:

$$G = \langle g_1, g_2, ..., g_l \rangle . \qquad (۹۱-۳)$$

در مثال بالا $S = \langle Z_1Z_2, Z_2Z_3 \rangle$، زیرا $Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$ و $I = (Z_1Z_2)^2$. مزیت فوق‌العاده به کار بردن مولدها برای توصیف گروه‌ها این است که آنها یک شکل فشرده‌تر برای توصیف گروه‌ها ایجاد می‌کنند. در حقیقت یک گروه G با سایز $|G|$، حداکثر $\log(|G|)$، مولد دارد. بعلاوه برای اینکه ببینیم یک بردار (مشخص) توسط یک گروه S، تثبیت می‌شود، لازم است که فقط چک کنیم که بردار توسط مولدها، تثبیت شده باشد، زیرا در اینصورت به طور اتوماتیک توسط حاصلضرب مولدها نیز تثبیت می‌شود.

هر زیرگروهی از گروه پائولی نمی‌تواند به عنوان تثبیت کننده برای یک فضای برداری غیر بدیهی[۱] به کار برده شود. به عنوان مثال، زیرگروه G_1 که شامل $\{\pm I, \pm X\}$ می‌باشد، را در نظر بگیرید. واضح است که تنها جواب برای $-I|\psi\rangle = |\psi\rangle$ این است که $|\psi\rangle = 0$ باشد و بدین ترتیب $\{\pm I, \pm X\}$ تثبیت کننده برای فضای برداری بدیهی[۲] می‌باشد. چه شرایطی باید توسط S ارضاء شود تا آن که بتواند یک فضای برداری غیربدیهی (V_S)، را تثبیت کند. به راحتی به نظر می‌رسد که ۲ شرط لازم است:

۱- عناصر S باید جابجایی پذیر باشند.

---

[۱] nontrivial
[۲] trivial

۲- $-I$ عنصری از S نیست.

در اینجا ما ابزار کافی برای اثبات این مسئله نداریم ولی نشان خواهیم داد که این دو شرط برای اینکه V_s، غیربدیهی باشد، کافی هستند.

می‌توان ثابت کرد که $-I \notin S$ به منزله این است که $\pm iI \notin S$.

برای اینکه ببینیم که این دو شرط ضروری هستند، فرض کنید V_s، غیربدیهی (لذا شامل $|\psi\rangle = 0$ نمی‌باشد) باشد. بنابراین شامل بردار غیر صفر $|\psi\rangle$ می‌باشد. فرض کنید که M و N عناصر S باشند. در این صورت M و N حاصلضربهای تانسوری ماتریسهای پائولی و احتمالا با یک ضریب ضربی روی آنها می‌باشند. از آنجائیکه ماتریسهای پائولی همه با یکدیگر یا جابجایی‌پذیر و یا پاد جابجایی پذیر هستند، این ایجاب می‌کند که M و N نیز جابجایی‌پذیر یا پاد جابجایی‌پذیر باشند. برای اثبات شرط (1) که همه آنها جابجایی‌پذیر هستند ، فرض می‌کنیم که M و N پاد جابجایی شونده باشند و این فرض به یک تناقض منتهی می‌شود. با فرض اینکه $-NM = MN$ خواهیم داشت:

$$-|\psi\rangle = -NM|\psi\rangle = MN|\psi\rangle = |\psi\rangle \qquad (۹۲-۳)$$

تساوی‌های اول و آخر از این حقیقت ناشی شده است که M و N، $|\psi\rangle$ را تثبیت می‌کنند. لذا داریم: $|\psi\rangle = -|\psi\rangle$ که بیان می‌کند که $|\psi\rangle$ برابر صفر است که به تناقض مورد نظر رسیدیم. برای ثابت کردن شرط (2) که $-I \notin S$، فقط به این نکته توجه کنید که اگر $-I$ یکی از اعضای S باشد، در این صورت خواهیم داشت $|\psi\rangle = -I|\psi\rangle$، که دوباره به تناقض مورد نظر می‌رسیم.

در صورتی که S یک زیرگروه از G_n که با عناصر $g_1, g_2, ..., g_l$ تولید می‌شود، باشد همه عناصر S جابجایی‌پذیرند، اگر و تنها اگر g_i و g_j برای هر جفت i و j جابجایی‌پذیر باشند.

یک مثال جالب از فرمالیزم تثبیت کننده، کد اِستین هفت کیوبیتی می‌باشد. نشان داده می‌شود که ۶ مولد از g_1 تا g_6 که در شکل (۳-۸) آورده شده‌اند، یک تثبیت کننده برای فضای کدِ کد اِستین می-باشند.

نام	عملگر
g_1	$IIIXXXX$
g_2	$IXXIIXX$
g_3	$XIXIXIX$
g_4	$IIIZZZZ$
g_5	$IZZIIZZ$
g_6	$ZIZIZIZ$

شکل (۳-۸): مولدهای تثبیت کننده برای کد ۷ کیوبیتی اِستین. ضرب تانسوری روی کیوبیتها را به ترتیب نشان می-دهد، به عنوان مثال $ZIZIZI = Z \otimes I \otimes Z \otimes I \otimes Z \otimes I = Z_1 Z_3 Z_5 Z_7$.

مشاهده می‌کنیم که این توصیف چقدر مرتب‌تر و خلاصه‌تر از حالتی است که قبلا بر حسب بردارهای حالت در روابط (۳-۸۷) و (۳-۸۸) توصیف کردیم. به علاوه مزیتهای دیگر آن وقتی آشکار می‌شود که تصحیح خطا را از این طریق اعمال کنیم. همچنین به شباهت بین ساختار مولدها در شکل (۳-۸) و ماتریسهای کنترلی پاریته برای کدهای خطی کلاسیکی C_1 و $C_2^{\perp}$ که در ساختار کد اِستین به کار برده شده، توجه کنید. (یادآوری می‌کنیم که برای کد اِستین، $C_1 = C_2^{\perp}$، کد همینگ $[7,4,3]$ با ماتریس کنترلی پاریته که با (۳-۸۵) داده شده است، می‌باشد.) سه مولد اول، Xها را در موقعیتهای

متناظر با موقعیت ۱ در ماتریس کنترلی پاریته C_1 و سه مولد آخر (g_4 تا g_6) Z ها را در موقعیتهای متناظر با موقعیت ۱ در ماتریس کنترل پاریته $C_2^{\perp}$ دارند.

این کاربرد فرمالیزم تثبیت کننده برای توصیف یک کد کوانتومی حاکی از کاربرد بعدی تثبیت کننده برای توصیف یک دسته بزرگ از کدهای کوانتومی می‌باشد.

در عمل ما می‌خواهیم مولدهای $g_1, g_2, ..., g_l$، مستقل باشند به طوریکه با حذف هر یک از مولدها، گروه ایجاد شده کوچکتر شود:

$$\langle g_1, ..., g_{i-1}, g_{i+1}, ... g_l \rangle \neq \langle g_1, ..., g_l \rangle \qquad (۹۳-۳)$$

تعیین اینکه آیا یک مجموعه خاص از مولدها مستقل هستند یا خیر، با اطلاعات کنونی ما، وقت گیر است، خوشبختانه یک راه ساده وجود دارد که می‌تواند این عمل صورت گیرد که بر اساس طرحی که به عنوان ماتریس کنترلی[۱] شناخته می‌شود، پایه ریزی شده باشد. علت نامگذاریش این است که نقشی را که در نظریه کدهای تثبیت کننده بازی می‌کند مشابه نقشی است که ماتریس کنترلی پاریته در کدهای خطی کلاسیکی بازی می‌کرد.

فرض کنید که $S = \langle g_1, ..., g_l \rangle$. یک راه بسیار مناسب برای ارائه مولدهای $g_1, ..., g_l$ از S با به کار بردن ماتریس کنترلی وجود دارد. این ماتریس، یک ماتریس $l \times 2n$ است که سطرهای آن متناظر با مولدهای g_1 تا g_l هستند. سمت چپ ماتریس شامل 1 می‌باشد که نشان دهنده مولدهایی است که شامل X بوده‌اند و سمت راست شامل 1 برای مولدهایی که حاوی Z بوده‌اند و حضور 1 در دو طرف نشان می‌دهد که در مولدها، Y بوده‌است. به طور آشکارا، سطر iام به شکل زیر ساخته می‌شود: اگر g_i شامل یک I در روی jامین کیوبیت خود باشد، در این صورت عناصر jامین و $n+j$ امین ستون، صفر هستند. اگر jامین کیوبیت X باشد، در اینصورت عنصر ستون jام 1 و عنصر ستون

[۱] check matrix

$n+j$ام صفر می‌باشد. اگر jامین کیوبیت Z باشند، در این صورت عنصر ستون jام صفر و عنصر ستون $n+j$ ام ، 1 می باشد. اگر در j امین کیوبیت Y داشته باشد، در اینصورت عنصر j امین و $n+j$ امین ستون، هر دو 1 هستند.

در مورد کد ۷ کیوبیتی اِستین، ماتریس کنترلی آن خواهد شد:

$$\left[\begin{array}{ccccccc|ccccccc} 0&0&0&1&1&1&1&0&0&0&0&0&0&0\\ 0&1&1&0&0&1&1&0&0&0&0&0&0&0\\ 1&0&1&0&1&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1\\ 0&0&0&0&0&0&0&0&1&1&0&0&1&1\\ 0&0&0&0&0&0&0&1&0&1&0&1&0&1 \end{array}\right] \qquad (۹۴-۳)$$

ماتریس کنترلی هیچ اطلاعاتی در مورد ضرایب ضربی مولدها را شامل نمی‌شود، اما اطلاعات مفید دیگری دارد. ما $r(g)$ را برای نمایش بردار سطری $2n$ بعدی یک عضو g از گروه پائولی به کار می‌بریم.

فرض کنید که ماتریس $2n\times 2n$، Λ، را به صورت زیر تعریف کنیم:

$$\Lambda=\begin{bmatrix} 0 & I\\ I & 0 \end{bmatrix} \qquad (۹۵-۳)$$

به طوریکه ماتریس‌های I که روی غیر قطر اصلی می‌باشند، $n\times n$ هستند. عناصر g و g' گروه پائولی به آسانی ثابت می‌شود که جابجایی‌پذیر هستند، اگر و تنها اگر:

$$r(g)\Lambda r(g')^{T}=0 \qquad (۹۶-۳)$$

قضیه (۳-۵): فرض کنید که $s=\langle g_1,...,g_l\rangle$ باشد به طوریکه $-I$ عضو S نباشد، مولدهای g_1 تا g_l مستقل هستند اگر و تنها اگر ردیفهای متناظر با ماتریس کنترلی مستقل خطی باشند.

اثبات:

بر عکس آن را ثابت می‌کنیم. توجه کنید که به ازای همه iها، g_i^2 باید معادل I باشند. مشاهده می‌کنید که $r(g)+r(g')=r(gg')$. بنابراین جمع دو نمایش برداری سطرها متناظر با ضرب اجزای گروه می‌باشد. بدین ترتیب سطرهای ماتریس کنترل به طور خطی وابسته هستند، (بستگی خطی دارند) $\sum a_i r(g_i)=0$ و برای بعضی از jها $a_j \neq 0$ می‌باشد، اگر و تنها اگر $\prod_i g_i^{a_i}$ برابر با I باشد.

اما $-I \notin S$، لذا ضریب ضربی باید 1 باشد و شرط آخر متناظر با شرط

$$g_j = g_j^{-1} = \prod_{i \neq j} g_i^{a_i} \qquad (۹۷-۳)$$

است و بنابراین g_1 تا g_l، مولدهای مستقل نیستند.

قضیه (۳-۶): فرض کنید که $S=\langle g_1,...,g_l \rangle$ با l تا مولد مستقل، تولید شده باشد و داشته باشیم $-I \neq S$. در این صورت $g \in G_n$ وجود دارد به طوریکه $gg_i g^\dagger = -g_i$ و $gg_j g^\dagger = g_j$ برای همه $i \neq j$.

اثبات: فرض کنید که G ماتریس کنترلی مربوط به g_1 تا g_l باشد. سطرهای G با استفاده از قضیه (۳-۵)، مستقل خطی هستند. در این صورت یک بردار x، $2n$بعدی وجود دارد به طوریکه $G\Lambda x = e_i$، که e_i یک بردار l بعدی با یک 1 در iامین مکان و 0 در بقیه جاهایش می‌باشد.

فرض کنید که g طوری باشد که $r(g)=x^T$، در این صورت خواهیم داشت:

$$r(g_j)\Lambda r(g)^T = 0 \qquad for \qquad j \neq i \qquad (۹۸-۳)$$

و

$$r(g_i)\Lambda r(g)^T = 1 \qquad (۹۹-۳)$$

و بدین ترتیب داریم $gg_j g^\dagger = g_j$ و $gg_i g^\dagger = -g_i$ برای $j \neq i$.

اگر $l = n-k$، مولد وجود می‌داشت، در اینصورت معقول است که V_s، 2^k بعدی است و بر پایه این استدلال شهودی می‌باشد که هر مولد اضافی برای تثبیت کننده، دیمانسیون V_S را با ضریب $\frac{1}{2}$ کاهش می‌دهد، همانطور که از قبل قابل پیش‌بینی بود، زیرا ویژه فضاهای[۱] $+1$ و -1 برای یک ضرب تانسوری از ماتریسهای پائولی، کل فضای هیلبرت را به دو زیرفضا با دیمانسیون‌های برابر تقسیم می‌کند.

قضیه (۳-۷): فرض کنید که $S = \langle g_1,...,g_{n-k} \rangle$ توسط عناصر مستقل و جابجایی‌پذیر از G_n، تولید شده باشند به طوریکه $S \neq -I$، در این صورت V_S یک فضای برداری 2^k بعدی است.

در همه مباحث بعدی پیرامون فرمالیزم تثبیت کننده، ما این قرارداد را به کار می‌بریم که تثبیت کننده‌ها همیشه بر حسب مولدهای جابجایی‌پذیر مستقل توصیف می‌شوند به طوریکه $S \neq -I$.

اثبات: فرض کنید که $x = (x_1,...,x_{n-k})$ یک بردار $n-k$ بعدی عنصری از Z_2 باشد. P_S^x را به شکل زیر تعریف می‌کنیم:

$$P_S^x \equiv \frac{\prod_{j=1}^{n-k}\left(I+(-1)^{x_j} g_j\right)}{2^{n-k}} \qquad (۱۰۰-۳)$$

از آنجائیکه $(I+g_i)/2$ یک تصویرگر[۲] روی ویژه فضای 1 از g_j می‌باشد، لذا به راحتی مشخص می‌شود که $P_S^{(0...0)}$ باید یک تصویرگر روی V_S باشد. با استفاده از قضیه (۳-۶)، برای هر x، وجود دارد g_x ی در G_n به طوریکه $g_x P_S^{(0,...,0)} (g_x)^\dagger = P_S^x$ و بنابراین دیمانسیون P_S^x مشابه دیمانسیون V_S می‌باشد. به علاوه برای x های متمایز به آسانی دیده می‌شود که P_S^x ها متعامد هستند.

اثبات با اظهار عبارت زیر به پایان می‌رسد:

---

[۱] eigenspace
[۲] projector

$$I = \sum_{n} P_S^x \qquad (۱۰۱-۳)$$

سمت چپ یک تصویرگر روی یک فضای 2^nبعدی است در حالیکه سمت راست جمع 2^{n-k} تصویرگر متعامد با ابعادی برابر ابعاد V_S می‌باشد و لذا دیمانسیون V_S باید 2^k باشد.

۳-۵-۲- گیتهای یکانی و فرمالیزم تثبیت کننده

در مورد کاربرد فرمالیزم تثبیت کننده برای توصیف فضاهای برداری بحث کردیم. فرمالیزم همچنین می‌تواند برای توصیف دینامیک آن فضاهای برداری در فضای حالت بزرگتری به کار برده شود.

صرفنظر از تمایل ذاتی به فهم عملهای دینامیکی کوانتومی، این هدف به ویژه به این دلیل مطرح است که ما کدهای تصحیح خطای کوانتومی را با استفاده از فرمالیزم تثبیت کننده توضیح خواهیم داد.

فرض کنید که یک عمل یکانی U را روی فضای برداری V_S که توسط گروه S، تثبیت شده است، اعمال کنیم و فرض کنید که $|\psi\rangle$ یک عنصر از V_S باشد. لذا برای هر عنصر g از S

$$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger U|\psi\rangle \qquad (۱۰۲-۳)$$

و لذا حالت $U|\psi\rangle$ توسط $UgU^\dagger$، تثبیت شده است.

که از آن نتیجه می‌گیریم که فضای برداری UV_S تثبیت می‌شود توسط گروه

$$USU^\dagger \equiv \left\{UgU^\dagger \mid g \in S\right\} \qquad (۱۰۳-۳)$$

به علاوه اگر $g_1,...,g_l$ ، S را تولید کنند، در این صورت $Ug_1U,...,Ug_lU^\dagger$، $USU^\dagger$ را تولید می‌کند. لذا برای اینکه تغییر در تثبیت کننده را محاسبه کنیم، کافیست محاسبه کنیم که چگونه روی مولدهای تثبیت کننده اثر می‌گذارد.

مزیت فوق‌العاده دسترسی به دینامیک این است که برای عملهای یکانی خاص U، این تبدیل مولدها در یک شکل جالبی، صورت می‌پذیرد. فرض کنید، به عنوان مثال، ما یک گیت هادامارد را به روی یک تک کیوبیت اعمال کنیم، توجه کنید که

$$HXH^{\dagger} = Z \quad ; \quad HYH^{\dagger} = -Y \quad ; \quad HZH^{\dagger} = X \qquad (۱۰۴-۳)$$

به عنوان مثال به طور صحیح نتیجه می‌گیریم که بعد از اعمال یک گیت هادامارد بر روی حالت کوانتومی تثبیت شده توسط Z یعنی $\langle 0|)$، حالت نتیجه یعنی $\langle +|)$، توسط X، تثبیت خواهد شد. فرض کنید که n کیوبیت در یک حالت که تثبیت کننده آن $\langle Z_1, Z_2, ..., Z_n \rangle$ می‌باشد، قرار دارد. واضح است که این حالت $|0\rangle^{\otimes n}$ می‌باشد.

با اعمال گیت هادامارد روی هر n کیوبیت می‌بینیم که حالت مورد نظر، تثبیت کننده $\langle X_1, X_2, ..., X_n \rangle$ را داراست. ممکن است هنوز بگویید که بعد از اعمال گیت هادامارد به هر n کیوبیت، هیچ در هم‌تنیدگی در کامپیوتر کوانتومی وجود ندارد، اما یک توصیف موثر و کارآ از $CNot$ به همراه گیت هادامارد قادر به ایجاد درهم‌تنیدگی می‌باشد. برای اینکه بفهمیم که این امر چگونه صورت می‌پذیرد، در نظر بگیرید که چگونه عملگرهای X_1، X_2، Z_1 و Z_2 تحت کانجوگیشن[۱] توسط $CNot$، رفتار می‌کنند. U را گیت $CNot$ با کیوبیت ۱ به عنوان کیوبیت کنترل و کیوبیت ۲ به عنوان هدف در نظر می‌گیریم، لذا خواهیم داشت:

(۱۰۵-۳)

$$UX_1U^{\dagger} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = X_1X_2$$

[۱] conjugation

به طور مشابه محاسبات نشان می‌دهد که $UX_2U^\dagger = X_2$، $UZ_1U^\dagger = Z_1$ و $UZ_2U^\dagger = Z_1Z_2$، شکل (۳-۹) را ببینید). برای اینکه ببینیم U چگونه بقیه عملگرها را در گروه پائولی ۲ کیوبیتی همیوغ می‌کند، تنها باید مواردی را که از قبل می‌دانستیم در هم ضرب کنیم.

$$UX_1X_2U^\dagger = UX_1U^\dagger UX_2U^\dagger = (X_1X_2)X_2 = X_1 \qquad (۱۰۶-۳)$$

ماتریسهای پائولی Y به طور مشابه ممکن است در ارتباط باشد. به عنوان مثال

$$UY_2U^\dagger = iUX_2Z_2U^\dagger = iUX_2U^\dagger UZ_2U^\dagger = iX_2(Z_1Z_2) = Z_1Z_2 \qquad (۱۰۷-۳)$$

عملگر	ورودی	خروجی
Controlled – Not	X_1 X_2 Z_1 Z_2	X_1X_2 X_2 Z_1 Z_1Z_2
H	X Z	Z X
S	X Z	Y Z
X	X Z	X $-Z$
Y	X Z	$-X$ $-Z$
Z	X Z	$-X$ Z

شکل (۳-۹): ویژگیهای تبدیل عناصر گروه پائولی تحت کانجوگیشن با عملهای مختلف. *Controlled – Not* کیوبیت ۱ را به عنوان کیوبیت کنترل و کیوبیت ۲ را به عنوان کیوبیت هدف داراست.

به عنوان یک مثال از کاربرد فرمالیزم تثبیت کننده برای فهم دینامیک یکانی، مدار معاوضه‌ای[1] شکل (۳-۱۰) را در نظر بگیرید. روشی را که عملگرهای Z_1 و Z_2 با همیوغ شدن توسط گیتها در مدار تبدیل می‌شوند، را در نظر بگیرید. عملگر Z_1 به این ترتیب:

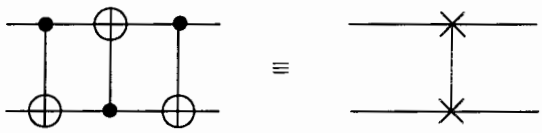
$$Z_1 \to Z_1 \to Z_1 Z_2 \to Z_2 \qquad (۱۰۸-۳)$$

و عملگر Z_2 به این ترتیب

$$Z_2 \to Z_1 Z_2 \to Z_1 \to Z_1 \qquad (۱۰۹-۳)$$

تبدیل می‌شوند.

به طور مشابه $X_1 \to X_2$ و $X_2 \to X_1$ تحت این مدار تبدیل می‌شوند. البته اگر ما U را به عنوان یک عملگر معاوضه‌ای در نظر بگیریم، در این صورت واضح است که $UZ_1U^\dagger = Z_2$ و $UZ_1U^\dagger = Z_2$ و به طور مشابه برای X_1 و X_2، $UX_1U^\dagger = X_2$ و $UX_2U^\dagger = X_1$ می‌باشد.



شکل (۳-۱۰): مدار معاوضه‌ای دو کیوبیتی و یک طرح کلی معادل برای آن.

مثال مدار معاوضه‌ای جالب هست اما در مورد ویژگی فرمالیزم تثبیت کننده که حقیقتا آن را مفید می‌سازد، (قادر بودن به توصیف نوع خاصی از درهم تنیدگی کوانتومی) چیزی نمی‌گوید. خواهیم دید که فرمالیزم تثبیت کننده در حقیقت می‌تواند برای توصیف یک دسته بزرگ از حالتهای در هم تنیده به کار برده شود که شامل تعداد زیادی از تصحیح خطای کوانتومی می‌باشد. چه گیتهایی علاوه بر

[1] swap circuit

هادامارد و $CNot$ می‌توانند توسط فرمالیزم تثبیت کننده توصیف شوند؟ مهمترین موردی که به این مجموعه اضافه می‌شود گیت فاز است، یک گیت تک کیوبیتی که تعریف آن را دوباره یادآوری می-کنیم:

$$S=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} \qquad (۱۱۰-۳)$$

عمل گیت فاز با کانجوگیشن روی ماتریسهای پائولی به آسانی محاسبه می‌شود:

$$SXS^{\dagger}=Y \qquad SZS^{\dagger}=Z \qquad (۱۱۱-۳)$$

در حقیقت این مسئله نشان می‌دهد که هر عمل یونیتاری که عناصر G_n را به عناصر G_n همیوغ شده می‌برد می‌تواند از گیتهای هادامارد، فاز و $CNot$ ایجاد شود. تعریف می‌کنیم که مجموعه U به طوریکه $UG_nU^{\dagger}=g_n$ برقرار باشد، نرمالیزکننده G_n می‌باشد و آن را با $N(G_n)$ نمایش می‌دهیم. لذا، ادعا می‌کنیم که نرمالیزکننده G_n توسط گیتهای هادامارد، فاز و $CNot$ ساخته می‌شوند.

قضیه (۳-۸): فرض کنید که U یک عملگر یکانی روی n کیوبیت باشد. با این ویژگی که اگر $g\in G_n$ باشد، داشته باشیم $UgU^{\dagger}\in G_n$ در این صورت U از $O(n^2)$ تا گیت هادامارد، فاز و $CNot$ ساخته شود.

دیدیم که بسیاری از گیتهای کوانتومی دلخواهمان در نرمالیزکننده $N(G_n)$، بودند. آیا گیتهایی هستند که در نرمالیزکننده نباشند؟ بیشتر گیتهای کوانتومی خارج از نرمالیزکننده هستند. ۲ گیت که در نرمالیزکننده نیستند، گیتهای $\pi/8$ و تافولی هستند. یادآوری می‌کنیم که T نمایش‌دهنده گیت $\pi/8$ بود. عمل کانجوگیشن توسط گیتهای $\pi/8$ و تافولی روی ماتریسهای پائولی به صورت زیر خواهد بود:

$$TZ_1T^{\dagger}=Z \qquad TXT^{\dagger}=\frac{X+Y}{\sqrt{2}}$$

$$
\begin{aligned}
UZ_1U^\dagger &= Z_1 \qquad & UX_1U^\dagger &= X_1 \otimes \frac{I + Z_2 + X_3 - Z_2Z_3}{2} \\
UZ_2U^\dagger &= Z_2 \qquad & UX_2U^\dagger &= X_2 \otimes \frac{I + Z_1 + X_3 - Z_2X_3}{2} \\
UX_3U^\dagger &= X_3 \qquad & UZ_3U^\dagger &= Z_3 \otimes \frac{I + Z_1 + Z_2 - Z_1Z_2}{2}
\end{aligned}
\qquad (۱۱۲-۳)
$$

متاسفانه این مسئله، آنالیز مدارهای کوانتومی شامل گیتهای $\pi/8$ و تافولی را از طریق نرمالیزکردن تثبیت‌کننده، نسبت به مدارهایی که تنها شامل گیتهای هادامارد، فاز و $CNot$ هستند، مشکل‌تر می‌کند.

خوشبختانه کدگذاری و کدگشایی، آشکارسازی خطا و بازیابی برای کدهای کوانتومی تثبیت کننده، می‌توانند با استفاده از گیتهای نرمالیزکننده انجام شوند، لذا فرمالیزم تثبیت کننده بسیار مناسب برای آنالیز کردن هر کدی می‌باشد.

۳-۵-۳- اندازه‌گیری در فرمالیزم تثبیت کننده

توضیح دادیم که چگونه یک دسته محدودی از گیتها به طور مناسبی توسط فرمالیزم تثبیت کننده توصیف شدند. اندازه‌گیری در پایه محاسباتی، همچنین می‌تواند توسط این فرمالیزم تثبیت کننده توصیف شود. برای فهم چگونگی این عمل، فرض کنید یک اندازه‌گیری از $g \in G_n$ انجام می‌دهیم (یادآوری می‌کنیم که g یک اپراتور هرمیتی است و لذا می‌تواند به عنوان یک مشاهده‌پذیر در نظر گرفته شود. به عنوان قرارداد، بدون از دست دادن کلیت، فرض می‌کنیم که g یک حاصلضرب از ماتریسهای پائولی بدون ضرایب ضربی -1 و $\pm i$ می‌باشد.

فرض می‌شود که سیستم در حالت $|\psi\rangle$ با تثبیت کننده $\langle g_1,...,g_n\rangle$ باشد. چگونه تثبیت کننده‌ی این حالت، تحت این اندازه‌گیری تبدیل می‌شود؟

دو احتمال وجود دارد؟

- g با همه مولدهای تثبیت کننده جابجایی کند.

- g با یکی یا بیش از یکی از مولدهای تثبیت کننده پادجابجایی کند.

فرض کنید که تثبیت کننده، مولدهای $g_1,...,g_n$ را دارد و g با g_1 پادجابجایی کند. بدون از دست دادن عمومیت، می‌توانیم فرض کنیم که g با g_2 تا g_n جابجایی کند، از آنجائیکه اگر با یکی از عناصر اینها (مثلا g_2) جابجایی نکند، در این صورت به آسانی مشخص می‌شود که g با g_1g_2 جابجایی می‌کند و به سادگی مولد g_2 را با g_1g_2 در لیست مولدهایمان برای تثبیت کننده، جایگزین می‌کنیم.

در اولین حالت چون برای هر مولد تثبیت کننده داریم: $g_ig|\psi\rangle = gg_i|\psi\rangle = g|\psi\rangle$، لذا $g|\psi\rangle$ در V_S است و بدین ترتیب یک مضرب از $|\psi\rangle$. از آنجائیکه $g^2 = I$ نتیجه می‌شود که $g|\psi\rangle = \pm|\psi\rangle$، لذا یا g و یا $-g$ باید در تثبیت کننده باشند. فرض می‌کنیم که g در تثبیت کننده باشد، بنابراین اندازه‌گیری g، $+1$ را با احتمال یک به ما می‌دهد و همچنین این اندازه‌گیری حالت سیستم را بر هم نمی‌زند و بدین ترتیب تثبیت کننده را ناوردا باقی می‌گذارد.

در مورد دومین حالت یعنی زمانی که g با g_1 پادجابجایی می‌کند و با همه مولدهای دیگر تثبیت-کننده جابجایی می‌کند: توجه کنید که g مقادیر ویژه ± 1 را داراست و بنابراین تصویرگرها برای نتایج اندازه‌گیری ± 1، توسط $(I \pm g)/2$، داده می‌شوند و بنابراین احتمالات اندازه‌گیری به صورت زیر خواهند بود:

$$P(+1) = tr\left(\frac{I+g}{2}|\psi\rangle\langle\psi|\right)$$
$$P(-1) = tr\left(\frac{I-g}{2}|\psi\rangle\langle\psi|\right) \qquad (۱۱۳-۳)$$

با استفاده از این حقیقت که $g|\psi\rangle=|\psi\rangle$ و $gg_1=-g_1g$ خواهیم داشت:

$$P(+1)=\left(tr\frac{(I+g)}{2}g_1|\psi\rangle\langle\psi|\right)=tr\left(g_1\frac{(I-g)}{2}|\psi\rangle\langle\psi|\right) \qquad (۱۱۴-۳)$$

با به کار بردن ویژگی چرخشی *trace*، g را به انتهای سمت راست *trace* می‌بریم و به $\langle\psi|$ اعمال می‌کنیم، با استفاده از $g_1=g^+$، خواهیم داشت:

$$P(+1)=tr\left(\frac{(I-g)}{2}|\psi\rangle\langle\psi|\right)=P(-1) \qquad (۱۱۵-۳)$$

از آنجائیکه $P(+1)+P(-1)=1$، نتیجه می‌گیریم که $P(+1)=P(-1)=\frac{1}{2}$. فرض کنید که نتیجه +1 اتفاق بیفتد. در این مورد حالت سیستم

$$|\psi^+\rangle\equiv(I+g)|\psi\rangle/\sqrt{2} \qquad (۱۱۶-۳)$$

است که تثبیت کننده‌های $\langle g,g_2,...,g_n\rangle$ را داراست. به طور مشابه اگر نتیجه -1 اتفاق بیفتد، حالت قبلی توسط $\langle -g,g_2,...,g_n\rangle$ تثبیت می‌شود.

قضیه (۳-۹) Gottesman – Knill : نتایج استفاده از تثبیت کننده‌ها برای توصیف دینامیک یکانی و اندازه‌گیری‌ها در قضیه‌ی برجسته Gottesman – Knill خلاصه شده است:

فرض کنید که یک محاسبه کوانتومی انجام شود که تنها شامل موارد زیر باشد: آماده‌سازی حالت آماده شده در پایه محاسباتی، گیتهای هادامارد، گیتهای فاز، گیتهای *CNot*، گیتهای پائولی و اندازه-گیریهای مشاهده پذیرها در گروه پائولی (که شامل اندازه‌گیری در پایه محاسباتی به عنوان یک حالت خاص می‌باشد) به همراه امکان کنترل کلاسیکی وضع شده بر روی نتیجه این اندازه‌گیرها. یک چنین محاسبه‌ای می‌تواند به طور موثر روی یک کامپیوتر کلاسیکی شبیه سازی شود.

ما قبلا به طور واضح این قضیه را ثابت کردیم. روشی که کامپیوتر کلاسیکی شبیه سازی را انجام می-دهد این است که اثری را که مولدهای تثبیت کننده که به عنوان عملهای متنوع که در محاسبه اعمال می‌شوند، را حفظ می‌کند. شبیه‌سازی آماده‌سازی حالت، گیت فاز، گیت $CNot$، گیتهای پائولی و اندازه‌گیری مشاهده‌پذیرها در گروه پائولی همه در $O(n^2)$ مرحله روی یک کامپیوتر کلاسیکی صورت می‌گیرد بنابراین یک محاسبه کوانتومی شامل m عمل از این مجموعه می‌توانند با استفاده از $O(n^n m)$ عمل روی یک کامپیوتر کلاسیکی شبیه سازی شوند.

قضیه Gottesman – Knill نشان می‌دهد که چقدر قدرت محاسبه کوانتومی ظریف است. این قضیه نشان می‌دهد که بعضی از محاسبه‌های کوانتومی شامل حالتهای شدیدا درهم‌تنیده به صورت بسیار موثر روی کامپیوترهای کلاسیکی شبیه‌سازی می‌شوند. البته همه محاسبات کوانتومی نمی‌توانند به طور موثری با فرمالیزم تثبیت کننده توصیف شوند (بنابراین همه حالتهای در هم تنیده نیز نمی-توانند)، اما انواع متعدد چشمگیری می‌توانند.[۲,۳,۵,۷,۸,۹,۱۱,۱۳]

فصل چهارم:
تحمل خطای کوانتومی (FT)

مقدمه

FT[1] ویژگی‌ای است که اگر تنها یک عضو در روند موفق عمل نکند، این شکست سبب نهایتا یک خطا در هر دسته از کیوبیتهای کدگذاری شده که از روند خارج می‌شوند، می‌باشد. این فصل را با یک مثال ساده و مهم از یک کد تصحیح خطای کوانتومی (کد ۷ کیوبیتی استین) آغاز می‌کنیم تا چگونگی تصحیح خطا را بررسی کنیم. سپس اجزای یک بازیابی FT را معرفی کرده و روشهایی برای کنترل انتشار خطا در طول بازیابی (که توسط شُور و استین پیشنهاد شده است) را ارائه می‌دهیم. در ادامه، با بحث کلی روی داده‌های کدگذاری شده، توضیح می‌دهیم که چگونه مسائل بنیادی انتشار خطا و تجمع خطا این نیاز را دارند که مدارهایمان برای محاسبه روی این داده‌ها، ضابطه FT را ارضاء کنند. سپس نمونه‌ی نویزی را برای مدارهای کوانتومی معرفی می‌کنیم که به ما اجازه می‌دهد تعاریف دقیقتری برای مفهوم یک عمل FT ارائه دهیم. از طریق یک مثال ویژه، یک عمل FT را به طور عملی بررسی می‌کنیم. با توضیح اینکه چگونه عملهای FT می‌توانند با یک روش که تسلسل[2] نامیده می‌شود، جمع آوری شوند تا نظریه آستانه برای محاسبه به دست آورده شود، کار را جمع بندی می‌کنیم و یک برآورد ساده برای آستانه ارائه می‌دهیم.

---

[1] fault tolerant (تحمل خطا)

[2] concatenation

۴-۱- چگونگی تصحیح خطای کوانتومی (کد هفت کیوبیتی استین)

یک کد تصحیح خطای کوانتومی تنها یک تعداد محدودی از خطاها در هر دسته را می‌تواند تصحیح کند. به عنوان مثال در مورد کد ۷ کیوبیتی استین، تنها یک خطا قابل تصحیح می‌باشد. این کد ما را قادر به ذخیره‌ی یک کیوبیت از اطلاعات کوانتومی (یک حالت اختیاری در یک فضای هیلبرت دو بعدی) با استفاده از مجموعا ۷ کیوبیت (با تعبیه‌ی فضای هیلبرت دو بعدی در یک فضای 2^7 بعدی) می‌سازد. کد استین به یک کد تصحیح خطای کلاسیکی آشنا، یعنی کد همینگ $[7,4,3]$ مربوط می‌باشد. برای پی بردن به عملکرد کد استین، در ابتدا باید کد همینگ کلاسیکی را بفهمیم.

کد همینگ یک دسته ۷ بیتی را برای کدگذاری ۴ بیت از اطلاعات کلاسیکی به کار می‌برد. یعنی $2^4=16$ رشته ۷ بیتی که کدکلمه‌های قابل قبولی می‌باشند، وجود دارد. کدکلمه‌ها توسط یک ماتریس کنترلی پاریته مشخص می‌شوند:

$$H=\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix} \qquad (۱-۴)$$

هر کدکلمه یک رشته ۷ بیتی (v_{code}) می‌باشد که در رابطه زیر صدق می‌کند:

$$\sum_k H_{jk}\left(v_{code}\right)_k = 0\left(\mathrm{mod}\ 2\right) \qquad (۲-۴)$$

یعنی ماتریس H هر کدکلمه را در مدِ ۲ از بین می‌برد (صفر می‌کند). از آنجائیکه $Z_2=\{0,1\}$ یک میدان محدود است، لذا نتایج مشابه جبر خطی در اینجا به دست می‌آید. H سه سطر مستقل خطی دارد و کرنل آن توسط ۴ بردار ستونی خطی مشخص می‌شود. ۱۶ کدکلمه با گرفتن همه‌ی ترکیبهای خطی ممکن از این ۴ رشته با ضرایبی از $\{0,1\}$ به دست می‌آید.

اکنون فرض کنید که v_{code} یک کدکلمه قابل قبول (ناشناخته) باشد و اینکه یک تک خطا (ناشناخته) رخ دهد: یکی از ۷ بیت وارون شود. ما باید تعیین کنیم که کدام یک از بیتها وارون شده است و بنابراین خطا می‌تواند تصحیح شود. این امر با اعمال ماتریس کنترلی پاریته به رشته انجام می‌شود. فرض کنید که e_i معرف رشته‌ای با یک 1 در i امین مکان و 0 در بقیه مکانها، باشد. در این صورت زمانی که i امین بیت وارون می‌شود، v_{code}، خواهد شد: $v_{code}+e_i$.

اگر ما H را به این رشته اعمال کنیم، خواهیم داشت:

$$H\left(v_{code}+e_i\right)=He_i \qquad (۳-۴)$$

که دقیقا iامین ستون از ماتریس H می‌باشد. از آنجائیکه همه ستونهای H متمایز هستند، ما می‌توانیم به i پی ببریم. پس توانستیم جایی که خطا رخ داده است را بیابیم و لذا می‌توانیم با وارون کردن دوباره‌ی iامین بیت، خطا را تصحیح کنیم. بدین ترتیب ما می‌توانیم داده‌های کدگذاری شده را به طور واضحی بازیابی کنیم اگر و تنها اگر فقط یک بیت وارون شده باشد. اما اگر دو بیت و یا بیش از دو بیت وارون شده باشد، داده‌های کدگذاری شده صدمه خواهند دید. این مسئله قابله ملاحظه می‌باشد که کمیت He_i موقعیت خطا را بدون گفتن هیچ مطلبی در مورد v_{code}، آشکار می‌کند.

کد استین این دسته از کدهای تصحیح خطای کلاسیکی را به کدهای تصحیح خطای کوانتومی تعمیم می‌دهد. این کد یک دسته ۷ کیوبیتی را برای کدگذاری یک کیوبیت از اطلاعات کوانتومی، به کار می‌برد، یعنی ما می‌توانیم یک حالت دلخواه را در یک فضای هیلبرت دو بعدی که با دو حالت، مشخص می‌شود، کدگذاری کنیم: صفر منطقی ($|0\rangle_{code}$) و یکِ منطقی ($|1\rangle_{code}$). کد طوری طراحی می‌شود که ما را به بازیابی از یک خطای اختیاری که ممکن است روی هر یک از ۷ کیوبیتِ این دسته رخ دهد، قادر می‌سازد.

و اما منظور ما از یک خطای اختیاری چیست؟ کیوبیت مورد نظر ما، ممکن است دستخوش یک تبدیل یکانی تصادفی شود و یا ممکن است با ایجاد درهم‌تنیدگی با حالتهای محیط انسجامش را از دست بدهد. فرض کنید که اگر هیچ خطایی اتفاق نیفتد، کیوبیت باید در حالت $a|0\rangle+b|1\rangle$ باشد. (البته این کیوبیت خاص ممکن است با بقیه در هم‌تنیده باشد و بنابراین ضرایب a و b لزومی ندارد که مختلط باشند و می‌توانند حالتهایی باشند که بر هر دو حالت $|0\rangle$و $|1\rangle$ عمود باشند، که ما فرض می‌کنیم که تحت تاثیر خطا قرار نمی‌گیرند.) اکنون اگر این کیوبیت تحت اثر یک خطای اختیاری قرار گیرد، حالت نتیجه شده، می‌تواند به شکل زیر توصیف شود:

$$\begin{aligned} a|0\rangle+b|1\rangle \rightarrow & \left(a|0\rangle+b|1\rangle\right)\otimes\left|A_{no\,error}\right\rangle_{env} \\ & +\left(a|1\rangle+b|0\rangle\right)\otimes\left|A_{bit\,flip}\right\rangle_{env} \\ & +\left(a|0\rangle-b|1\rangle\right)\otimes\left|A_{phase\,flip}\right\rangle_{env} \\ & +\left(a|1\rangle-b|0\rangle\right)\otimes\left|A_{both\,errors}\right\rangle_{env} \end{aligned} \qquad (۴-۴)$$

به طوریکه $|A_{env}\rangle$ معرف یک حالت از محیط می‌باشد. ما هیچ فرضی در مورد متعامد بودن و یا نرمالیزه بودن حالتهای $|A\rangle_{env}$ نمی‌کنیم، بنابراین رابطه (۴-۴) در اصل کلی نقصانی ایجاد نمی‌کند. نتیجه می‌گیریم که تبدیل این کیوبیت می‌تواند به عنوان یک ترکیب خطی از ۴ احتمال بیان شود:

۱- هیچ خطایی رخ ندهد.

۲- وارون بیتی $|1\rangle\leftrightarrow|0\rangle$ رخ دهد.

۳- فاز نسبی $|0\rangle$ و $|1\rangle$ وارون شود.

۴- هر دو خطای وارون فازی و وارون بیتی رخ دهد.

اکنون واضح است که یک کد تصحیح خطای کوانتومی باید عمل کند. با ایجاد یک اندازه‌گیری مناسب، ما در صدد تشخیص این مسئله هستیم که کدام یک از این چهار احتمال رخ داده است. البته به طور

کلی، حالت این کیوبیت، یک ترکیب خطی از این چهار حالت خواهد بود، اما اندازه‌گیری، باید حالت را به پایه‌ای که در رابطه (۴-۴) به کار برده شده‌است، تصویر کند. سپس ما می‌توانیم اقدام به تصحیح خطا با اعمال یکی از چهار تبدیل یونیتاری زیر کنیم:

$$(1)\ I \qquad (2)\ X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$(3)\ Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad (4)\ Y \equiv X.Z \tag{۵-۴}$$

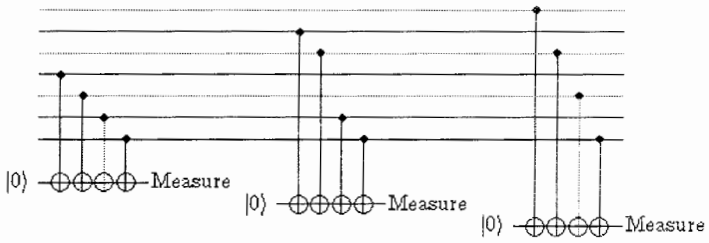
خروجی آزمایش به ما خواهد گفت که کدام یک را باید اعمال کنیم. با اعمال این تبدیل، ما کیوبیت را به مقدار اولیه‌اش بر می‌گردانیم و کاملا حالت کوانتومی کیوبیت را از حالت محیط جدا می‌کنیم. در هر صورت این مسئله مشهود است که در تشخیص خطا، ما در مورد اطلاعات کوانتومی کدگذاری شده هیچ آگاهیی نمی‌یابیم. برای یافتن اطلاعاتی در مورد ضرایب a و b در رابطه (۴-۴) ، لزوما انسجام کیوبیت از بین می‌رود.

اگر ما کد استین را به کار ببریم، یک اندازه‌گیری که موافق با این معیارها و ضوابط می‌باشد، امکان پذیر است. صفر منطقی برهمنهی موزون از همه‌ی هفت کدکلمه‌های کد همینگ با وزن زوج می‌باشد:

$$\begin{aligned} |0\rangle_{code} &= \frac{1}{\sqrt{8}}\left(\sum_{\substack{even\,\nu \\ \in Hamming}} |\nu\rangle \right) \\ &= \frac{1}{\sqrt{8}}(|0000000\rangle + |0001111\rangle + |0110011\rangle + |0111100\rangle \\ &+ |1010101\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle) \end{aligned} \tag{۶-۴}$$

و یکِ منطقی برهمنهی موزون از همه کدکلمه‌های کد همینگ با وزن فرد می‌باشد:

$$|1\rangle_{code} = \frac{1}{\sqrt{8}}\left(\sum_{\substack{odd\ \nu \\ \in Hamming}} |\nu\rangle\right)$$
$$= \frac{1}{\sqrt{8}}(|1111111\rangle + |1110000\rangle + |1001100\rangle + |1000011\rangle \qquad (۷-۴)$$
$$+ |0101010\rangle + |0100101\rangle + |0011001\rangle + |0010110\rangle)$$



شکل (۴-۱): محاسبه‌ی نشانه‌ی وارون بیتی برای کد ۷ کیوبیتی استین. با تکرار محاسبات در پایه‌ی چرخیده شده، خطاهای وارون فازی تشخیص داده می‌شود. برای اینکه روند را FT بسازیم، هر کیوبیت کمکی باید توسط ۴ کیوبیت در یک حالت مناسب جایگزین شوند.

از آنجائیکه همه حالتهای موجود در روابط (۴-۶) و (۴-۷) کدکلمه‌های همینگ هستند، تشخیص یک تک وارونی در دسته، توسط یک محاسبه کوانتومی ساده، همانطور که در شکل (۴-۱) نمایش داده شده است، آسان می‌باشد. دسته ۷ کیوبیتی را با سه بیت کمکی تکمیل می‌کنیم و عمل یکانی زیر را اعمال می‌کنیم:

$$|\nu\rangle \otimes |0\rangle_{anc} \rightarrow |\nu\rangle \otimes |H\nu\rangle_{anc} \qquad (۸-۴)$$

به طوری که H ماتریس کنترلی پاریته همینگ می‌باشد و $|0\rangle_{anc}$، معرف حالتِ سه بیت کمکی می‌باشد. اگر فرض کنیم که تنها یکی از ۷ کیوبیت در دسته، دچار خطا شود، اندازه‌گیری کمکی، آن کیوبیت را یا به یک حالت با یک بیت وارونی و یا یک حالت بدون وارون شدگی، تصویر می‌کند. اگر

بیت وارون شود، نتیجه اندازه‌گیری تشخیص می‌دهد که کدام بیت بوده است، البته بدون اینکه چیزی را در مورد اطلاعات کوانتومی که در دسته، کدگذاری شده است، آشکار کند.

اما برای انجام تصحیح خطا، لازم است که خطاهای فازی را نیز به خوبی خطاهای وارون بیتی تشخیص دهیم. برای انجام این امر، مشاهده می‌کنیم که می‌توانیم پایه را برای هر کیوبیت با اعمال چرخش هادامارد، عوض کنیم:

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad (۹-۴)$$

بنابراین خطاهای فازی در پایه $|0\rangle$ و $|1\rangle$ به خطاهای وارون بیتی در پایه‌ی چرخیده شده تبدیل می‌شوند:

$$|\tilde{0}\rangle\equiv\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \quad , \quad |\tilde{1}\rangle\equiv\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \qquad (۱۰-۴)$$

بنابراین اگر کدِ ما قادر به تشخیص خطاهای وارون بیتی در پایه چرخیده شده باشد، همین کافی خواهد بود. اما اگر ما چرخش هادامارد را به هر یک از ۷ کیوبیت اعمال کنیم، در این صورت صفر و یک‌های منطقیِ استین، در پایه‌ی چرخیده شده به صورت زیر خواهد بود:

$$\begin{aligned}|\tilde{0}\rangle_{code}&=\frac{1}{4}\left(\sum_{\nu\in Hamming}|\nu\rangle\right)=\frac{1}{\sqrt{2}}(|0\rangle_{code}+|1\rangle_{code})\\ |\tilde{1}\rangle_{code}&=\frac{1}{4}\left(\sum_{\nu\in Hamming}(-1)^{wt(\nu)}|\nu\rangle\right)=\frac{1}{\sqrt{2}}(|0\rangle_{code}-|1\rangle_{code})\end{aligned} \qquad (۱۱-۴)$$

به طوریکه $wt(\nu)$ معرف وزن ν می‌باشد. نکته کلیدی این است که $|\tilde{0}\rangle_{code}$ و $|\tilde{1}\rangle_{code}$، مانند $|0\rangle_{code}$ و $|1\rangle_{code}$، برهمنهی‌های کدکلمه‌های همینگ می‌باشند. از این رو در پایه چرخیده شده، همانند پایه اصلی، ما می‌توانیم ماتریس کنترل پاریته همینگ را برای تشخیص وارون بیتی‌ها که در پایه اصلی

وارونی فاز هستند، اعمال کنیم. با فرض اینکه تنها یک کیوبیت دچار خطا شده باشد، با اعمال ماتریس کنترل پاریته، در هر دو پایه، به طور کامل خطا را تشخیص داده و قادر به تصحیح آن خواهیم بود.

در توصیفات بالا از شکل تصحیح خطا، فرض کردیم که خطا تنها یکی از کیوبیتها در دسته را تحت تاثیر قرار دهد. واضح است که این فرض، واقع گرایانه نیست و همه‌ی کیوبیتها همانطور که انتظار می-رود تا اندازه‌ای با محیط برهم‌کنش دارند. به هر حال، همانطور که دیده‌ایم، این روند برای تعیین نشانه‌ی خطا، همانطور که مورد انتظار است، هر کیوبیت را به یک حالت که در آن هیچ خطایی رخ نداده است، تصویر می‌کند. برای هر کیوبیت، یک احتمال غیر صفر از یک خطا وجود دارد که فرض می‌شود کوچک باشد و آن خطا را ε می‌گوییم. حال یک فرض بسیار مهم را در اینجا مطرح می‌کنیم و آن این است که خطاهایی که روی کیوبیتهای مختلف در دسته مشابه عمل می‌کنند، کاملا با یکدیگر ناهمبسته هستند. تحت این فرض، احتمال دو خطا از مرتبه ε^2 می‌باشد و بنابراین کوچکتر از احتمال یک خطا می‌باشد، البته اگر ε به اندازه‌ی کافی کوچک باشد. بنابراین برای اینکه دقت ε را تنظیم کنیم، می‌توانیم توجهمان را به حالتی که نهایتا یک تک کیوبیت در هر دسته دچار خطا شود، محدود کنیم. (در حقیقت برای دستیابی به این نتیجه، واقعا نیازی نیست که خطاهایی که روی کیوبیتهای مختلف عمل می‌کنند، کاملا ناهمبسته باشند. اگر همه کیوبیتها در معرض میدان مغناطیسی ضعیف مشابهی قرار گیرند، هر کدام دارای یک احتمال وارونی (ε) می‌باشند که مجاز و صحیح می‌باشد، زیرا احتمال اینکه دو اسپین وارون شوند ε^2 می‌باشد. آنچه که سبب دردسر می‌شود، فرآیندی است که با احتمالی از مرتبه ε رخ می‌دهد و دو اسپین را در یک زمان وارون می‌کند.)

اما در رخداد غیر محتملی که دو خطا در یک دسته از کدها اتفاق می‌افتد، روند بازیابی‌مان همانطور که انتظار می‌رود، دچار شکست می‌شود. اگر دو بیت در یک دسته مشابه وارون شود، در این صورت

کنترل پاریته همینگ، خطا را تشخیص نخواهد داد. بازیابی، حالت کوانتومی را به زیرفضایی از کد باز می‌گرداند اما اطلاعات کوانتومی داخل دسته، دستخوش وارونی بیت می‌شود:

$$|0\rangle_{code} \to |1\rangle_{code} \quad , \quad |1\rangle_{code} \to |0\rangle_{code} \tag{۱۲-۴}$$

به طور مشابه، اگر دو خطای فاز در یک دسته مشابه وجود داشته باشد، دو خطای وارون بیتی در پایه چرخیده شده وجود دارد. بنابراین پس از بازیابی، دسته دستخوش یک وارون بیتی در پایه چرخیده شده و به عبارتی یک وارون فازی در پایه اصلی خواهد شد:

$$|0\rangle_{code} \to |0\rangle_{code} \quad , \quad |1\rangle_{code} \to -|1\rangle_{code} \tag{۱۳-۴}$$

اگر یک کیوبیت در دسته، یک خطای فاز و کیوبیت دیگر یک خطای وارون بیتی داشته باشد، در این صورت بازیابی موفقیت آمیز خواهد بود.

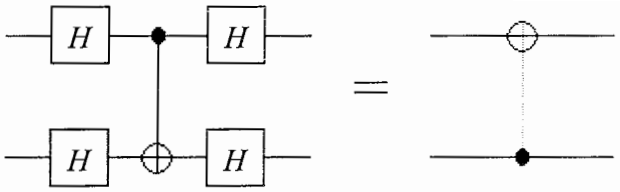
بدین ترتیب دیدیم که کد استین توانست قابلیت اطمینان اطلاعات کوانتومی ذخیره شده را افزایش دهد. فرض کنید که می‌خواهیم یک کیوبیت را در یک حالت خالص $|\psi\rangle$ ذخیره کنیم. به سبب نقص در ابزار ذخیره، حالت ρ_{out} پس از بازیابی افت ضریب اطمینان $F \equiv \langle\psi|\rho_{out}|\psi\rangle = 1-\varepsilon$ را خواهد داشت.

اما اگر ما کیوبیت را با استفاده از کد ۷ کیوبیتی استین ذخیره کنیم، در این صورت اگر هر ۷ کیوبیت با ضریب اطمینان $F = 1-\varepsilon$ حفظ شوند و اگر خطاهای روی کیوبیتها ناهمبسته باشند، و ما بتوانیم بازیابیِ خطا، کدگذاری و کدگشایی را بدون عیب انجام دهیم، در این صورت اطلاعات کدگذاری شده می‌توانند با یک ضریب اطمینان بهبود یافته‌ی $F = 1-O(\varepsilon^2)$ حفظ شوند.

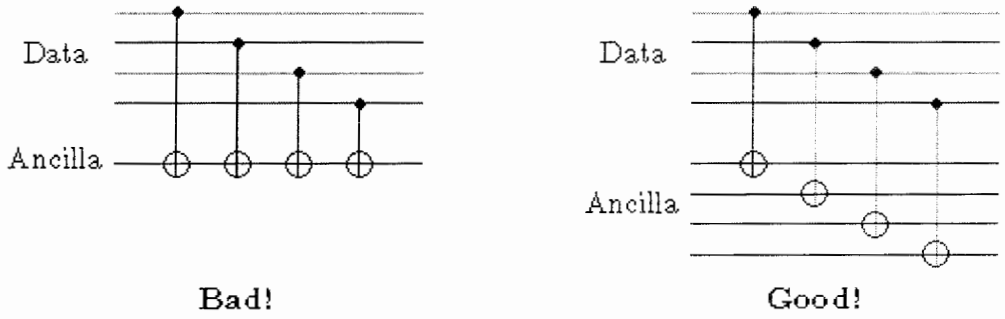
۴-۲- بازیابی FT

تا کنون ما فرض کرده‌ایم که می‌توانیم اطلاعات کوانتومی را کدگذاری کرده و بازیابی از خطا را بدون ایجاد هیچگونه اشتباهی انجام دهیم. اما بازیابی از خطا نمی‌تواند بدون نقص باشد. بازیابی، خود، یک محاسبه کوانتومی است که در معرض خطا می‌باشد. خطاهایی که در طول بازیابی رخ می‌دهند می‌توانند اطلاعات کوانتومی کدگذاری شده را تخریب کنند، از این رو بازیابی باید با دقت اجرا شود تا موثر واقع شود. اگر احتمال خطا برای هر بیت در دسته، ε باشد، در این صورت منطقی است که فرض کنیم که هر گیت کوانتومی که ما در روند بازیابی به خدمت می‌گیریم، احتمالی از مرتبه ε در وارد کردن یک خطا را دارا می‌باشد. اگر روند بازیابی‌مان با بی‌دقتی طراحی شده باشد، در این صورت احتمال آنکه این روند دچار شکست شود (به عنوان مثال، دو خطا در یک دسته مشابه رخ دهد) می‌تواند از مرتبه ε باشد. در این صورت ما هیچ سودی از به کار بردن کد تصحیح کوانتومی نبرده‌ایم. در حقیقت، احتمال خطا در هر کیوبیت حتی بیشتر از حالت بدون کدگذاری می‌باشد. بنابراین ما مجبور هستیم که به طور سیستماتیک، همه‌ی راههای ممکن که بازیابی ممکن است با احتمالی از مرتبه ε دچار شکست شود را در نظر بگیریم و مطمئن شویم که همه آنها رفع می‌شوند. تنها در این صورت روندمان FT می‌باشد و همچنین تنها در این صورت است که کدگذاری تضمین می‌کند که اگر ε به اندازه‌ی کافی کوچک باشد، می‌توان از خلاصی یافت.

یکی از نگرانی‌های جدی، انتشار خطا می‌باشد. اگر یک خطا در یک کیوبیت رخ دهد و سپس ما یک گیتی که آن کیوبیت را با کیوبیت دیگر برهمکنش می‌دهد، اعمال کنیم، خطا به طور محتملی به کیوبیت دوم وارد می‌شود. لازم است که مواظب باشیم تا محتوی خطا نباشیم و یا حداقل تلاش کنیم که از ظاهر شدن دو خطا در یک دسته مشابه جلوگیری کنیم.



شکل (۴-۲): یک تساوی مفید. کنترل و هدف یک گیت $CNot$ قابل تعویض هستند اگر ما یک تغییر در پایه با چرخشهای هادامارد انجام دهیم.



شکل (۴-۳): مدلهای خوب و بد اندازه‌گیری نشانه. مدار بد بیت کمکی مشابه را چندین بار به کار می‌برد، مدار خوب هر بیت کمکی را تنها یک بار به کار می‌برد.

در انجام بازیابی خطا، ما مکررا گیت $CNot$ دو کیوبیتی را به کار می‌بریم. این گیت می‌تواند خطاها را به دو روش مختلف منتشر کند. اول اینکه واضح است که اگر یک خطای وارون بیتی در کیوبیت اول رخ دهد و سپس آن کیوبیت به عنوان کیوبیت کنترل یک گیت $CNot$ به کار برده شود، در این صورت وارون بیتی به سمت جلو منتشر می‌شود و روی کیوبیت هدف اثر می‌گذارد. نوع دوم انتشار خطا با استفاده از تساوی نمایش داده شده در شکل (۴-۲)، قابل فهم است. اگر ما یک چرخش پایه با یک گیت هادامارد روی هر دو کیوبیت انجام دهیم، در این صورت کنترل و هدفِ گیت $CNot$ قابل تعویض هستند. یادآوری می‌کنیم که این تغییر پایه، همچنین یک خطای وارون بیتی را با یک خطای فاز عوض می‌کند و لذا استنباط می‌شود که اگر یک خطای فاز در کیوبیت اول رخ دهد و آن کیوبیت به عنوان کیوبیت هدف یک گیت $CNot$ به کار برده شود، در این صورت خطا به سمت عقب انتشار می‌یابد و روی کیوبیت کنترل اثر می‌گذارد. اکنون می‌توانیم ببینیم که مدار نشان داده شده در شکل

(۴-۱)، FT نمی‌باشد. مشکل این است که تک کیوبیت کمکی به عنوان یک هدف برای چهار گیت $CNot$ پی در پی به کار برده می‌شود. اگر تنها یک تک خطای فازی در کیوبیت کمکی در بعضی مراحل رخ دهد، آن یک خطا می‌تواند به دو یا بیش از دو کیوبیت در دسته برگشت داده شود. نتیجه این است که یک خطای فازیِ دسته با احتمالی از مرتبه‌ی ε رخ می‌دهد که قابل قبول نیست.

برای اینکه احتمال شکست را تا مرتبه‌ی ε^2 کاهش دهیم، باید مدار بازیابی را اصلاح کنیم و بنابراین هر کیوبیت کمکی تنها به یک کیوبیت در دسته‌ی کد، متصل می‌شود. یک روش برای انجام این کار این است که تعداد بیت کمکی را از یک بیت به ۴ بیت افزایش دهیم که هر بیت، هدفِ یک گیت $CNot$ باشد، همانطور که در شکل (۴-۳) آمده است. سپس می‌توانیم همه‌ی چهار بیت کمکی را اندازه‌گیری کنیم. بیت نشانه که ما در جستجوی آن هستیم، پاریته‌ی چهار بیت اندازه‌گیری شده می‌باشد. در واقع، ما مقداری اطلاعات در مورد خطایی که رخ داده است را از دسته‌ی داده‌ها به بیتهای کمکی کپی کردیم و زمانی که بیتهای کمکی را اندازه می‌گیریم، آن اطلاعات را می‌خوانیم.

اما این روند هنوز کافی نمی‌باشد، چرا که ما اطلاعات بیش از حدی را کپی کرده‌ایم. مدار، بیتهای کمکی را با خطایی که در داده رخ داده است گرفتار می‌کند، که البته این کار مفید می‌باشد، اما این مدار همچنین بیت‌های کمکی را با خودِ داده‌های کدگذاری شده نیز گرفتار می‌کند که نامفید می‌باشد. اندازه‌گیری بیتهای کمکی، برهمنهی حالتهای پایه که به صورت دقیق آماده شده بودند (روابط (۴-۶) و (۴-۷) برای $|0\rangle_{code}$ و $|1\rangle_{code}$) را خراب می‌کند. به عنوان مثال فرض کنید که در حال اندازه‌گیری اولین بیت نشانه، (همانطور که در شکل (۴-۱) نشان داده شده است) می‌باشیم، اما به جای یک بیت کمکی چهار بیت کمکی داشته باشیم. در این صورت ما در حال اندازه‌گیری چهار کیوبیت آخر دسته می‌باشیم. اگر نتیجه اندازه‌گیری مثلا $|0000\rangle_{anc}$ باشد، لذا ما $|0\rangle_{code}$ را به $|0000000\rangle$ و

$|1\rangle_{code}$ را به $|1110000\rangle$ تصویر کرده‌ایم، به عبارتی کدکلمه‌ها در برابر خطاهای فاز حفاظتشان را از دست داده‌اند.

۴-۲-۱- آماده‌سازی حالت کمکی

لازم است که روند بازیابی را بیشتر تصحیح کنیم که این عمل با حفظ ویژگیهای مفید آن، در حالیکه ویژگیهای بد آن را حذف می‌کنیم، صورت می‌پذیرد. می‌خواهیم که اطلاعات را در مورد خطاهای موجود در دسته‌ی داده‌ها در بیتهای کمکی کپی کنیم، البته بدون جلو بردن خطاهای فازی متعدد و همچنین بدون خراب شدن انسجام داده‌ها. برای رسیدن به این مقصود ما باید یک حالت کمکی مناسب قبل از اینکه محاسبه‌ی نشانه‌ی خطا آغاز شود، را آماده کنیم. این حالت طوری انتخاب می‌شود که نتیجه اندازه‌گیری کمکی، اطلاعات را در مورد خطاها، بدون فاش کردن چیزی در مورد حالت داده‌ها، آشکار می‌کند.

یک روش برای دستیابی به این ضابطه توسط پیتر شُور[۱] پیشنهاد شد. *حالت شُور* که پیشنهاد او بود حالتی از ۴ بیت کمکی می‌باشد که یک برهمنهی موزون از همه‌ی رشته‌های با وزن زوج می‌باشد:

$$|shor\rangle_{anc} = \frac{1}{\sqrt{8}} \sum_{even\ \nu} |\nu\rangle_{anc} \qquad (۱۴-۴)$$

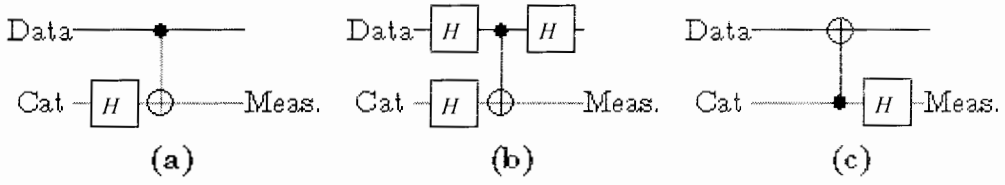
برای محاسبه کردن هر بیت نشانه، ما حالت کمکی را در یک حالت شُور آماده می‌کنیم، ۴ گیت $CNot$ را اعمال می‌کنیم (با کیوبیتهای مناسب در دسته‌ی داده‌ها به عنوان منابع و ۴ بیت از حالت شُور به عنوان هدفها)، و سپس حالت کمکی را اندازه می‌گیریم. اگر بیت نشانه که ما در حال اندازه‌گیری آن هستیم بدیهی باشد، در این صورت محاسبه، رشته‌ای با وزن زوج به حالت شُور اضافه می‌کند، که آن را بدون تغییر باقی می‌گذارد. اگر بیت نشانه غیر بدیهی باشد، حالت شُور به برهمنهی

---

[۱] Peter Shor

موزون از همه رشته‌های با وزن فرد تبدیل می‌شود. بدین ترتیب، پاریته‌ی نتیجه اندازه‌گیری مقدار بیت نشانه را آشکار می‌کند، اما هیچ اطلاعاتی در مورد حالت دسته نمی‌دهد. ما روشی را یافته‌ایم که نشانه را بدون از بین بردن کدکلمه‌ها بیرون می‌کشد. (رشته پاریته‌ی معین ویژه، که ما در اندازه‌گیری می‌یابیم، به طور تصادفی انتخاب می‌شود و هیچ کاری به حالت دسته‌ی داده‌ها ندارد. روی هم رفته، ۶ بیت نشانه وجود دارد (۳ بیت برای تشخیص خطاهای وارون بیتی و ۳ بیتی برای تشخیص خطاهای وارون فازی)، بنابراین اندازه‌گیری نشانه، ۲۴ بیت کمکی که در ۶ حالت شُور آماده شده است و نیز ۲۴ گیت $CNot$ را به کار می‌برد.

یک راه برای دستیابی به نشانه‌ی وارون فازی، این است که در ابتدا ۷ گیت مشابه Hرا به دسته‌ی داده‌ها اعمال کنیم تا پایه را بچرخاند، سپس اعمال $CNot$ همانطور که در شکل (۴-۱) نشان داده شده است (اما با حالت کمکی شُور و بالاخره اعمال ۷ گیت H برای چرخاندن داده‌ها به حالت اول. به هر حال ما می‌توانیم تساوی نشان داده شده در شکل (۴-۲) را برای بهبود این روند به کار ببریم. با معکوس کردن جهت گیتهای $CNot$ (یعنی با به کار بردن کمکی به عنوان کنترل و داده به عنوان هدف)، ما می‌توانیم از اعمال گیتهای H بر داده دوری کنیم و از این رو می‌توانیم احتمال خراب شدن داده با گیتهای معیوب و ناقص را کاهش دهیم، همانطور که در شکل (۴-۴) نشان داده شده است.

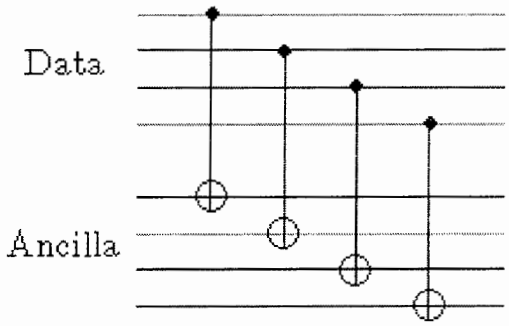


شکل (۴-۴): (a) روندی برای محاسبه یک بیت از نشانه خطای وارون بیتی به صورت شماتیکی نمایش داده شده است. گیت هادامارد که روی *حالت گربه* اعمال شده است، آماده سازی حالت شُور را تکمیل می‌کند. گیتهای $CNot$ و هادامارد در دیاگرام در حقیقت چهار گیت را که به صورت یکسان و همزمان اعمال شده است را نمایش می‌دهد. (b) روندی برای محاسبه یک بیت از نشانه‌ی خطای وارون فازی که به طور شماتیکی نشان داده شده است و مشابه (a) می‌باشد، اما روی داده‌ها در پایه چرخیده شده، اعمال شده‌است. (c) یک مدار معادل با (b)، که با استفاده از تساوی شکل (۴-۲)، ساده سازی شده است.

روش دیگر برای آماده سازی کمکی، توسط آندرو اِستین[1] پیشنهاد شد. حالت کمکی ۷ کیوبیتی او، برهم‌نهی موزون از همه کدکلمه‌های همینگ می‌باشد:

$$|stean\rangle_{anc} = \frac{1}{4}\sum_{v\in Hamming}|v\rangle \qquad (۱۵-۴)$$

(این حالت همچنین می‌تواند به صورت $\left(|0\rangle_{code}+|1\rangle_{code}\right)/\sqrt{2}$ بیان شود و می‌تواند با اعمال چرخش هادامارد به صورت بیت به بیت بر حالت $|0\rangle_{code}$، به دست بیاید.) برای محاسبه کردن نشانه وارون بیتی، هر کیوبیت از دسته را به کیوبیت کمکیِ متناظر $CNot$ کرده (شکل (۴-۵)) و کمکی را اندازه می‌گیریم. با اعمال ماتریس کنترلی پاریته همینگ H به نتیجه‌ی اندازه‌گیری کلاسیکی، نشانه وارون بیتی را بیرون می‌کشیم.

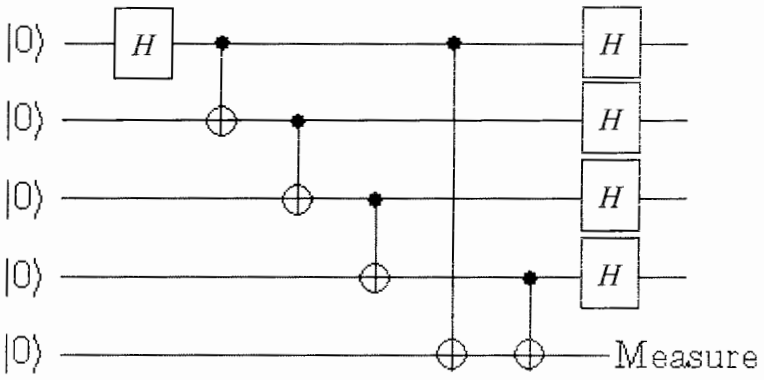


شکل (۴-۵): نمونه‌ای از $CNot$ کردن کیوبیتهای دسته با کیوبیتهای کمکی

همانند روند شُور، این روند، داده را در کمکی کپی می‌کند، در حالیکه حالت کمکی به دقت انتخاب شده است تا این اطمینان حاصل شود که تنها اطلاعاتی درباره‌ی خطا می‌تواند توسط اندازه‌گیری حالت کمکی خوانده شود. به عنوان مثال اگر هیچ خطایی وجود نداشته باشد، رشته‌ی ویژه‌ای که ما در

[1] Andrew Stean

اندازه‌گیری می‌یابیم یک کدکلمه‌ی همینگ انتخاب شده‌ی تصادفی می‌باشد و چیزی در مورد حالت داده به ما نمی‌گوید. روند مشابه در پایه‌ی چرخیده شده، برای یافتن نشانه وارون فازی انجام می‌شود. روش استین مزیتی را نسبت به روند شُور دارا می‌باشد و آن این است که تنها ۱۴ بیت کمکی و ۱۴ گیت *CNot* نیاز می‌باشد. اما این روش اشکالاتی نیز دارد و آن این است که آماده‌سازی کمکی پیچیده‌تر است، بنابراین، حالت کمکی، کمی بیشتر مستعد خطا می‌باشد.



شکل (۴-۶): ساخت و بازبینی حالت شُور. اگر نتیجه‌ی اندازه‌گیری ۱ باشد، در این صورت این حالت رد شده و یک حالت جدید شور آماده می‌شود.

۴-۲-۲- بازبینی کمکی

به سبب انتشار خطا، یک تک خطا که در طول آماده‌سازی حالت شُور و یا حالت استین رخ می‌دهد، می‌تواند سبب دو خطای فازی در این حالت شود و اگر کمکیی معیوب برای اندازه‌گیری نشانه به کار برده شده باشد، این دو می‌توانند به داده انتشار یابند. روند ما هنوز هم FT نیست.

بنابراین حالت کمکی باید برای چندین خطای فازی قبل از به کار برده شدن، تست شود. اگر این تست با شکست مواجه شد، رد می‌شود و یک حالت کمکی جدید باید ساخته شود. یک راه برای ساختن و بازبینی حالت شُور در شکل (۴-۶) نشان داده شده است. اولین گیت هادامارد و سه گیت اول *CNot*

در این مدار یک *حالت گربه* $\left(|0000\rangle+|1111\rangle\right)$ را آماده می‌کنند، (حالتی با بیشترین در هم تنیدگی برای ۴ بیت کمکی). ۴ گیت هادامارد آخر، حالت گربه را به حالت شُور می‌چرخاند. اما یک تک خطا که در طول دومین و یا سومین $CNot$ رخ می‌دهد، می‌تواند سبب دو خطا در حالت گربه شود (ممکن است به شکل $\left(|1100\rangle+|0011\rangle\right)$تبدیل شود). این دو خطای وارون بیتی در حالت گربه دو خطای وارون فازی در حالت شُور به همراه دارد که برگشت داده می‌شود و سبب یک خطای فاز دسته‌ای در طول اندازه‌گیری نشانه می‌شوند.

اما ملاحظه می‌کنیم که برای همه راههایی که یک گیت بدِ کوانتومی سبب بروز دو خطای وارون بیتی در حالت گربه می‌شود، اولین و چهارمین بیتِ حالت گربه، مقادیر متفاوتی خواهند داشت. بنابراین ما دو گیت آخریِ $CNot$ را به مدار اضافه می‌کنیم (به همراه یک اندازه‌گیری) تا بازبینی کند که آیا این دو بیتِ حالت گربه مشابه هستند یا خیر. اگر این بازبینی موفقیت آمیز بود، ما می‌توانیم اقدام به حفظ اندازه‌گیری نشانه کنیم با اطلاع از این مطلب که احتمال دو خطای فازی در حالت شُور از مرتبه ε^2 می‌باشد. اگر بازبینی موفقیت آمیز نبود (شکست خورد)، حالت گربه را کنار گذاشته و دوباره شروع می‌کنیم.

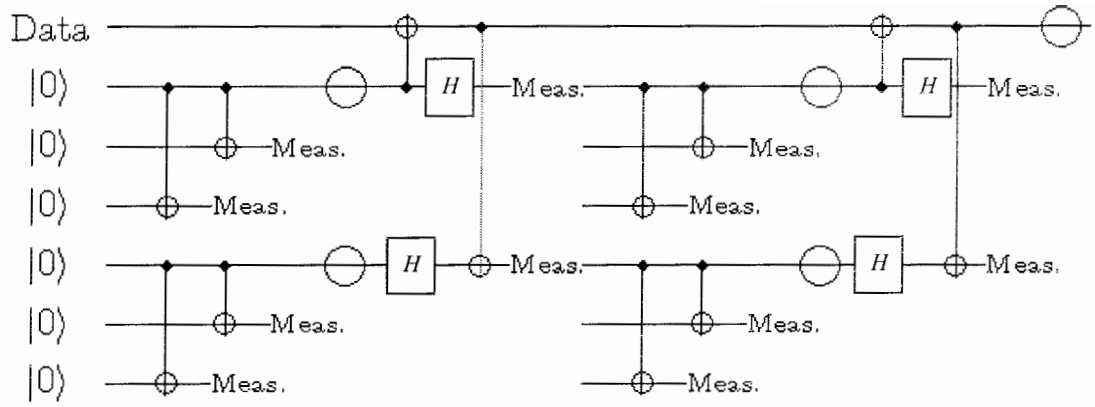
البته یک تک خطا در آماده‌سازی مدار می‌تواند همچنین سبب دو خطای فازی در حالت گربه شود و لذا دو خطای وارون بیتی در حالت شُور. ما هیچ گونه تلاشی برای بازبینی حالت شُور در مورد خطاهای وارون بیتی انجام نداده‌ایم. اما خطاهای وارون بیتی در حالت شُور نسبت به خطاهای فازی بسیار کم زحمت‌تر می‌باشند. خطاهای وارون بیتی باعث می‌شوند که اندازه‌گیری نشانه ناقص باشد، اما آنها به عقب برگشت داده نمی‌شوند و سبب تخریب داده نمی‌شوند.

۴-۲-۳- بازبینی نشانه

یک تک خطای وارون بیتی در کمکی یک نشانه‌ی معیوب را سبب می‌شود. این خطا ممکن است از اینجا ناشی شود که کمکی به طور ناصحیح آماده شده است یا به خاطر خطایی که در طول محاسبه‌ی نشانه رخ داده است. مخصوصا حالت دوم خطرناک است، زیرا یک تک خطا که با احتمالی از مرتبه‌ی ε رخ می‌دهد، می‌تواند نقصی هم در دسته‌ی داده‌ها و هم در کمکی ایجاد کند. این مسئله به این دلیل ممکن است اتفاق بیفتد که یک گیت $CNot$ معیوب، خطاهایی را در هر دو کیوبیت هدف و کنترل سبب می‌شود و یا به خاطر اینکه یک خطا در دسته‌ی داده‌ها که در طول اندازه‌گیری نشانه رخ می‌دهد، بعدا توسط $CNot$ به سمت جلو و به طرف کمکی منتشر می‌شود.

در چنین حالتهایی که ما نشانه خطای معیوب را می‌پذیریم و تلاش می‌کنیم تا آن را به حالت درست برگردانیم، در حقیقت یک خطای دوم به دسته وارد می‌کنیم. بنابراین روند ما هنوز کاملا FT نیست.

بنابراین ما باید راهی را پیدا کنیم که تضمین کند که نشانه قابل اطمینان‌تر باشد. راه واضح برای این امر این است که اندازه‌گیریِ نشانه را تکرار کنیم. در صورتی که اندازه‌گیری نشانه بدیهی باشد، نیازی به تکرار نمی‌باشد (نشان می‌دهد که هیچ خطایی رخ نداده است)، با این وجود، ممکن است خطایی در داده‌ها وجود داشته باشد که ما موفق به آشکارسازی آن نمی‌شویم. اگر از طرف دیگر، نشانه به یک خطا اشاره داشته باشد، در این صورت ما نشانه را برای دومین بار اندازه می‌گیریم. اگر نتیجه‌ای مشابه نتیجه‌ی قبلی به دست آوردیم، صحیح است که نشانه را بپذیریم و اقدام به بازیابی کنیم، چرا که هیچ راهی وجود ندارد که با احتمالی از مرتبه‌ی ε نشانه‌ی معیوب مشابهی دوبار پشت سر هم به دست آوریم.



شکل (۴-۷): مدار کاملی برای بازیابی خطای استین. $|0\rangle$ های کدگذاری شده آماده می‌شوند، سپس بازبینی می‌شوند. $|0\rangle$های بازبینی شده به عنوان کمکیها برای محاسبه‌ی نشانه‌های وارون‌بیتی و وارون فازی به کار برده می‌شوند که هر دو، دو بار اندازه‌گیری می‌شوند. دایره‌های بزرگ به عملهایی که بسته به نتیجه‌ی اندازه‌گیری برای اصلاح حالتهای کمکی به کار برده می‌شوند و یا در حالت نهایی، برای اصلاح دسته‌ی داده‌ها، به کار برده می‌شود، اشاره دارد.

اگر دو اندازه‌گیری اولِ نشانه، یکی نباشند، در این صورت ما اندازه‌گیری را ادامه می‌دهیم تا زمانی که نهایتا نتیجه‌ی مشابهی را دوبار پشت سر هم به دست آوریم، در واقع نتیجه‌ای که می‌توان به آن اعتماد کرد. ما می‌توانستیم این راه را انتخاب کنیم که کاری انجام ندهیم، تا زمانی که یک خطا به طور مطمئنی در دور بعدی از تصحیح خطا آشکار سازی شود. حداقل به این طریق با ترکیب خطا چیزی را بدتر از قبل نمی‌سازیم و اگر واقعا یک خطا در داده‌ها باشد، احتمالا آن را در دور بعدی آشکارسازی می‌کنیم.

سرانجام ما همه عناصر یک روند بازیابی FT را فرآهم کردیم. اگر ما همه احتیاطات و اقدامات لازم که در بالا ذکر شد را در نظر بگیریم، در این صورت بازیابی تنها در صورتی با شکست مواجه خواهد شد که دو خطای مستقل رخ دهد، بنابراین احتمال خطایی که به طور برگشت ناپذیری دسته‌ی کدگذاری شده را تخریب کند از مرتبه‌ی ε^2 خواهد بود.

یک مدار کوانتومی کامل برای تصحیح خطای استین در شکل (۴-۷) نمایش داده شده است. توجه کنید که هر دو تصحیح خطای وارون فازی و وارون بیتی، دو بار تکرار شده است. بازبینی حالتهای استین نیز نشان داده شده است.

۴-۲-۴- اندازه‌گیری و کدگذاری

ما مایل هستیم که کیوبیتهای کدگذاری شده را به طور قابل اطمینانی اندازه‌گیری کنیم. اما در قسمتهای قبل مشاهده کردیم که اندازه‌گیری مخرب دسته‌ی کد تنها در صورتی خوب کار می‌کند و موثر است که تنها یک کیوبیت در دسته، یک خطای وارون بیتی داشته باشد. اگر احتمال یک اندازه-گیری معیوب برای یک کیوبیت از مرتبه‌ی ε باشد، در این صورت اندازه‌گیری‌های معیوب دسته‌ی کد، با احتمالی از مرتبه‌ی ε^2 رخ می‌دهند. اندازه‌گیری غیرمخرب FT نیز می‌توانند صورت گیرند همانطور که قبلا در بحث بازبینی حالت استین ملاحظه کردیم. یک روند دیگر که اندازه‌گیری غیر مخرب را بدون هیچ‌گونه اصلاحی به کار می‌برد، در شکل ۴ به تصویر کشیده شده است. اگر چه کمکی، هدف گیتهای $CNot$ پی در پی هستند، خطاهای فازی که به دسته برگشت داده می‌شوند زیاد مضر نیستند چرا که آنها نمی‌توانند $|0\rangle_{code}$ را به $|1\rangle_{code}$ و یا بالعکس تبدیل کنند. به هر حال، چون یک تک خطای وارون بیتی (در دسته‌ی داده‌ها و یا در کیوبیت کمکی می‌تواند سبب یک اندازه-گیری پاریته‌ی معیوب شود، لذا اندازه‌گیری باید تکرار شود (بعد از تصحیح خطای وارون بیتی) تا دقتی از مرتبه‌ی ε^2 را به دست آورد (ما از این روند در توصیف بازبینی حالت استین اجتناب کردیم). اغلب می‌خواهیم که حالتهای کوانتومی کدگذاری شناخته شده را آماده کنیم، مانند $|0\rangle_{code}$. گفتیم که (در رابطه با آماده‌سازی حالت استین) چگونه این کدگذاری می‌تواند به طور قابل اطمینانی اجرا شود. در حقیقت مدار کدگذاری واقعا لازم نیست. حالت اولیه‌ی دسته هر چه باشد، تصحیح خطا (FT) آن

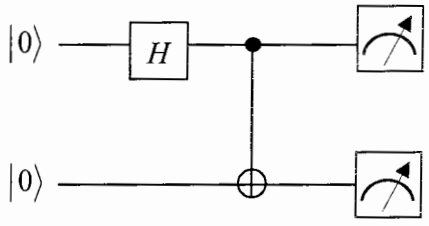
را به فضایی که توسط $\{|0\rangle_{code}, |1\rangle_{code}\}$ مشخص می‌شود، تصویر می‌کند و اندازه‌گیری (بازبینی شده)، $|0\rangle_{code}$ و یا $|1\rangle_{code}$ را ارائه می‌دهد. اگر نتیجه‌ی $|1\rangle_{code}$ به دست بیاید، در این صورت عملگر NOT به صورت بیت به بیت می‌تواند اعمال شود تا دسته را به حالت مورد نظر $|0\rangle_{code}$ برگرداند.

۴-۳- گیتهای FT

یکی از قدرتمندترین کاربردهای تصحیح خطای کوانتومی علاوه بر حفاظت از اطلاعات کوانتومیِ ذخیره شده یا فرستاده شده، حفاظت از اطلاعات کوانتومی، زمانی که به طور دینامیکی دستخوش محاسبه می‌شوند، می‌باشد. این مسئله نشان می‌دهد که به یک محاسبه کوانتومیِ خوب، حتی با گیتهای منطقی معیوب و ناقص نیز می‌توان دست یافت، مشروط بر اینکه احتمال خطا در هر گیت کمتر از یک آستانه‌ی[۱] ثابت مشخص باشد.

۴-۳-۱- موضوعات بنیادی

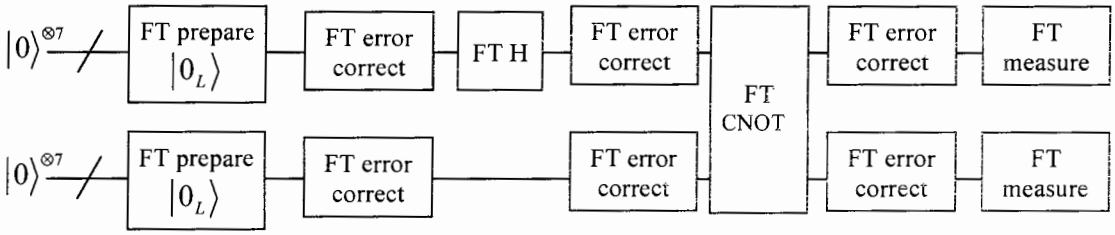
هدف اساسی از محاسبه کوانتومی FT، محاسبه مستقیم روی حالت‌های کوانتومی کدگذاری شده، به طوریکه نیازی به کدگشایی نباشد، می‌باشد. فرض کنید که یک مدار کوانتومی ساده به طوریکه در شکل (۴-۸) آمده است، داشته باشیم.



شکل (۴-۸): یک مدار ساده کوانتومی. اگر هر یک از اجزاء در مدار با احتمال p، موفق عمل نکنند، در این صورت احتمال یک خطا در خروجی $O(p)$ می‌باشد.

[۱] threshold

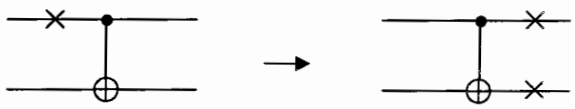
متاسفانه نویز، هر یک از اجزاء به کار برده شده (روندهای آماده‌سازی حالت، گیتهای منطقی کوانتومی، اندازه‌گیری خروجی و حتی انتقال اطلاعات کوانتومی در طول سیمهای کوانتومی) برای ساخت این مدار را دچار آسیب می‌کند. برای مقابله با این نویز، ما هر کیوبیت در مدار اصلی را با یک دسته‌ی کدگذاری شده (با استفاده از کد تصحیح خطا مانند کد هفت کیوبیتی اِستین) جایگزین می‌کنیم و هر گیت در مدار اصلی را با یک روند برای اعمال یک گیت کدگذاری شده که روی حالت کدگذاری شده عمل می‌کند، جایگزین می‌کنیم که در شکل(۴-۹) نمایش داده شده است.



شکل (۴-۹): یک شبیه سازی از مدار شکل (۴-۸) با استفاده از کیوبیتهای کدگذاری شده و عملهای منطقیِ کدگذاری شده.

با اعمال تصحیح خطا به طور متناوب روی حالت کدگذاری شده، از انباشته شدن خطاها در حالت، جلوگیری می‌کنیم. البته تنها اعمال متناوب تصحیح خطا برای جلوگیری از انتشار خطاها کافی نمی‌باشد حتی اگر بعد از هر گیت کدگذاری شده اعمال شود. دو دلیل برای این مسئله وجود دارد. اول و مهمترین این است که گیتهای کدگذاری شده سبب می‌شوند که خطا انتشار یابد: به عنوان مثال *CNot* کدگذاری شده که در شکل (۴-۱۰) آورده شده است، ممکن است سبب خطایی روی کیوبیت کنترل کدگذاری شده شود تا به سمت کیوبیت هدف کدگذاری شده انتشار بیابد. بدین ترتیب خطاها در کیوبیت‌هایی که کیوبیت کنترل کدگذاری شده را تشکیل می‌دهند، می‌توانند انتشار بیابند و خطاهایی در کیوبیت هدف کدگذاری شده را باعث شوند. بنابراین گیتهای کدگذاری شده باید بسیار با

دقت طراحی شوند تا یک شکست در طول روند که برای اعمال گیت کدگذاری شده صورت می‌گیرد تنها به تعداد کمی از کیوبیت‌ها



شکل (۴-۱۰): یک گیت $CNot$ می‌تواند سبب انتشار یک خطا شود، بنابراین بجای یک کیوبیت، روی دو کیوبیت اثر می‌کند. این مسئله در مورد کیوبیتهای کدگذاری شده نیز صادق می‌باشد.

در هر دسته از داده‌های کدگذاری شده انتشار می‌یابند، و لذا تصحیح خطا در رفع کردن خطاها موثر باشد. به این روشها برای اعمال گیتهای کدگذاری شده روشهای FT نسبت داده می‌شود و نشان خواهیم داد که این امکان وجود دارد که یک مجموعه جهانی از عملهای منطقی را با استفاده از روشهای FT اعمال کنیم (گیتهای هادامارد، فاز، $CNot$ و $\pi/8$). دلیل دوم که باید اشاره شود این است که خودِ تصحیح خطا یک سری خطاهایی را روی کیوبیت‌های کدگذاری شده وارد می‌کند، بنابراین ما باید تصحیح خطا را با دقت به شکلی طراحی کنیم که خطاهای زیادی را به داده‌های کدگذاری شده وارد نکند. این امر با استفاده از روشهای مشابه با آنچه برای جلوگیری از انتشار خطاها توسط گیتهای کدگذاری شده انجام گرفت (که اطمینان داد که خطاها در طول روند تصحیح خطا آنقدر انتشار نمی‌یابند تا تعداد زیادی خطا را روی داده‌های کدگذاری شده سبب شوند) صورت می‌پذیرد.

۴-۳-۲- عملهای FT: تعاریف

FT ویژگیی است که اگر تنها یک عضو در روند موفق عمل نکند این شکست سبب نهایتا یک خطا در هر دسته از کیوبیتهای کدگذاری شده که از روند خارج می‌شوند، می‌باشد. به عنوان مثال، شکست یک عضو در روند FT بازیابی، برای تصحیح خطای کوانتومی سبب می‌شود روند بازیابی تاحدود یک خطا روی یک تک کیوبیت خروجی به طور صحیح اعمال شود. منظور ما از «عضو» هرگونه عمل بنیادی در گیتهای کدگذاری شده می‌باشد که می‌تواند شامل گیتهای نویزدار، اندازه‌گیری‌های نویزدار، سیم‌های کوانتومی نویز دار و آماده سازی‌های نویزدار باشد. البته گیتهای کوانتومی کدگذاری شده، تمام آن چیزی که می‌خواهیم در طول محاسبات کوانتومی‌یمان اعمال کنیم، نمی‌باشد. همچنین در اینجا مفهوم یک روند FT اندازه‌گیری و آماده‌سازی FT حالت را بیان می‌کنیم. یک روند برای اندازه‌گیری یک مشاهده‌پذیر روی یک مجموعه از کیوبیتهای کدگذاری شده، FT می‌باشد، اگر شکست یک تک عضو در روند، یک خطا نهایتا در یک کیوبیت در هر دسته از کیوبیتهای کدگذاری شده در خروجی روند را سبب شود. به علاوه لازم است که اگر تنها یک عضو دچار شکست شود، نتیجه اندازه‌گیری گزارش شده باید دارای احتمال خطایی از مرتبه p^2 باشد، به طوریکه p ماکزیمم احتمال شکست در هر یک از اجزای به کاربرده شده برای اجرای روند اندازه‌گیری می‌باشد. روند آماده‌سازی یک حالت کدگذاری شده،ی ثابت، FT می‌باشد در صورتیکه اگر یک تک عضو در طول روند دچار شکست شود، نهایتا یک کیوبیت در هر دسته از کیوبیتهای کدگذاری شده که از روند خارج می‌شوند، دچار خطا شود. برای اینکه این مفاهیم را دقیق‌تر بیان کنیم، لازم است که روی نمونه خطایمان دقیق‌تر شویم. یکی از ساده‌سازی‌های عمده‌ای که ما در تحلیلمان انجام می‌دهیم توصیف خطاها روی کیوبیتها توسط یکی از ۴ مورد I، X، Y و Z می‌باشد که به طور تصادفی با احتمالهای مناسب اتفاق می‌افتند. خطا روی ۲ کیوبیت با اعمال گیتهایی مانند $CNot$ صورت می‌گیرد (که البته دوباره با یک احتمال اتفاق

می‌افتند. فرض می‌کنیم که این گیتها شکلی از حاصلضرب تانسوری ماتریس‌های پائولی می‌باشد) این تحلیل احتمالاتی، ما را قادر می‌کند تا از مفاهیم آشنایی از نظریه احتمال کلاسیکی برای تعیین احتمال کل (اینکه خروجی یک مدار صحیح است یا خیر) استفاده کنیم. در نمایش‌های پیچیده تری از FT، خطاهای مختلفی مورد ملاحظه قرار می‌گیرد. به عنوان مثال خطایی که به صورت تصادفی روی چندین کیوبیت صورت می‌گیرد. با این وجود تکنیک‌هایی که در این آنالیزهای پیچیده به کار برده می‌شود تعمیم مواردی است که ما توضیح دادیم.

با نمونه نویزی که در دست داریم، می‌توانیم مفهوم دقیق انتشار خطا در یک مدار را بفهمیم. به عنوان مثال یک گیت $CNot$ را در نظر بگیرید (شکل (۴-۱۰). فرض کنید که یک خطای X روی کیوبیت اول دقیقا قبل از اعمال گیت $CNot$ اتفاق بیفتد. اگر یک گیت یکانی $CNot$ را با U نمایش دهیم، در این صورت عمل موثر مدار به شکل زیر خواهد بود:

$$UX_1 = UX_1U^{\dagger}U = X_1X_2U \qquad (۱۶-۴)$$

یعنی مثل این است که گیت $CNot$به طور صحیح رخ داده است اما یک خطای X روی هر دو کیوبیت رخ داده است بعد از $CNot$ اتفاق می‌افتد. در ادامه این فصل ما مکررا از ترفند همیوغ کردن، برای بررسی اینکه چگونه یک خطا در طول مدارهایمان انتشار می‌یابند، استفاده می‌کنیم.

یک مثال چالش انگیز از انتشار خطا به این ترتیب است که فرض شود خودِ گیت $CNot$ موفق عمل نکند. در این صورت چه اتفاقی می‌افتد؟ فرض کنید که این گیت $CNot$ نویزدار، عمل کوانتومی εرا انجام دهد. در این صورت می‌توان نوشت:

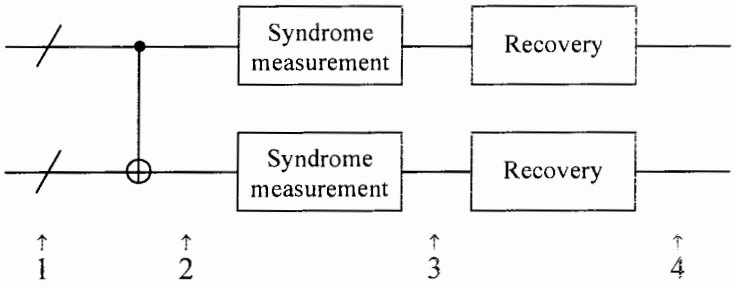
$$\varepsilon = \varepsilon \circ u^{-1} \circ u \qquad (۱۷-۴)$$

به طوریکه عمل کوانتومی u گیت صحیح $CNot$ را نشان می‌دهد. بدین ترتیب گیت نویزدار $CNot$ معادل با اعمال یک $CNot$ صحیح به همراه عمل $\varepsilon \circ u^{-1}$ می‌باشد که تقریبا همانی است. در صورتیکه

$CNot$ نویزدار بتواند به صورت خطایی از ضربهای تانسوری (مانند $X \otimes Z$ که با احتمال p روی ۲ کیوبیت رخ دهد) تعبیر شود. در ادامه این فصل، روندها را به طور جزئی‌تر توضیح خواهیم داد. ساختارهای حقیقی که توضیح می‌دهیم برای کد اِستین می‌باشد که البته به آسانی می‌توان به کدهای تثبیت کننده تعمیم داد. از اکنون فرض می‌کنیم که همه این روندها را در اختیار داریم. چگونه می‌توان آنها را در کنار هم قرار داد تا یک محاسبه کوانتومی انجام شود؟

۴-۳-۳- مثال: گیت FTای controlled-Not

در اینجا یک روند برای اجرای یک گیت FTای $CNot$ ، به همراه یک مرحله تصحیح خطای FT (همانطور که در شکل (۴-۱۱) مشاهده می‌کنید) را بررسی می‌کنیم.



شکل (۴-۱۱): دیاگرام ساختار روند FT، شامل تصحیح خطا.

مرحله یک، نقطه ورود به مدار می‌باشد، مرحله دوم بعد از اعمال گیت $CNot$ می‌باشد. مرحله سوم بعد از اندازه‌گیری نشانه و مرحله چهارم بعد از انجام عمل بازیابی می‌باشد. هدف ما نشان دادن این مطلب است که احتمال اینکه این مدار ۲ یا بیش از خطا را در دسته اول کدگذاری شده وارد کند از مرتبه p^2 می‌باشد ($O(p^2)$) به طوریکه p احتمال شکست فردی هر یک از اجزاء در مدار می‌باشد.

در واقع کدگشایی صحیح دسته اول از کیوبیتها تنها در صورتی دچار شکست می‌شود که ۲ یا بیش از ۲ خطا در دسته باشد.

برای نشان دادن این که این روند، ۲ خطا را به دسته کدگذاری شده‌ی اول، با احتمال $O(p^2)$ وارد می‌کند، همه راههای ممکن که این مدار می‌تواند ۲ یا بیش از دو خطا را به دسته کدگذاری شده اول کیوبیتها در خروجی وارد کند، مشخص می‌کنیم.

۱- یک تک خطای از پیش موجود، در هنگام ورود به مدار در مرحله اول در هر دسته از کیوبیتهای کدگذاری شده وجود دارد که می‌تواند ۲ خطا در خروجی از دسته اول را سبب شود، زیرا به عنوان مثال خطا روی دسته دوم در طول مدار $CNot$ کدگذاری شده منتشر می‌شود و سبب یک خطا روی دسته اول از کیوبیتها، می‌شود. به شرط آنکه عملها تا این مرحله به صورت FT انجام شده باشند، می‌توان گفت که احتمال آنکه یک چنین خطایی روی دسته اول وارد شود نهایتا $c_0 p$ برای مقدار ثابت c_0 باشد، زیرا یک چنین خطایی باید در طول اندازه‌گیری نشانه یا مراحل بازیابی در مرحله قبل از ورود به مدار کوانتومی رخ داده باشد. c_0 مجموع تعداد مکانهایی است که یک شکست در طول اندازه‌گیری نشانه یا بازیابی در مرحله قبل از ورود به مدار رخ می‌دهد. اگر برای ساده‌سازی فرض کنیم که احتمال یک تک خطای از پیش موجود که در مرحله‌ی یک، روی دسته دوم وارد می‌شود همان $c_0 p$ باشد و این دو خطا به طور مستقل رخ دهند، در این صورت احتمال این رخداد نهایتا $c_0^2 p^2$ می‌باشد. برای ساختار کد اِستین که در ادامه توضیح داده شده است، سهمهایی برای c_0 از ۶ اندازه‌گیری نشانه جداگانه وجود دارد (که هر کدام تقریبا 10^i موقعیت که یک شکست ممکن است در آنجا رخ دهد، دارا می‌باشند) به همراه یک عمل بازیابی شامل ۷ جزء. لذا مجموع تقریبی $c_0 \approx 70$ خواهد بود.

۲- ممکن است یک تک خطای از پیش موجود در مرحله ۱ روی دسته اول و یا دسته دوم از کیوبیتها وارد شود و یک تک شکست در طول $CNot$ (FT)، رخ دهد. احتمال این رخداد $c_1 p^2$ می‌باشد، به

طوریکه c_1 ثابتی است که تعداد جفت نقاطی که یک شکست در آن رخ می‌دهد را مشخص می‌کند. برای ساختار کد اِستین، گفتیم که به طور کلی ۷۰ موقعیت (ضرب) در ۲ دسته (که یک شکست در آن قسمتها رخ داده است) سبب می‌شود که یک خطا وارد مدار شود مجموعا ۱۴۰ موقعیت می‌شود. ۷ موقعیت دیگر که یک شکست در طول مدار ممکن است رخ دهد وجود دارد که برای مجموعا $c_1 \approx 7\times 140 \approx 10^3$ موقعیت که یک جفت خطا ممکن است رخ دهد.

۳- دو شکست در طول گیت FTی $CNot$ اتفاق می‌افتد. این اتفاق با احتمال نهایتا $c_2 p^2$ صورت می‌گیرد که c_2 تعداد جفت نقاطی است که یک شکست رخ می‌دهد. برای کد اِستین، $c_2 = 10^2$.

۴- ممکن است در طول $CNot$ و در طول اندازه‌گیری نشانه، شکستی رخ دهد. تنها راهی که ۲ یا بیش از ۲ خطا در خروجی می‌تواند اتفاق بیفتد، این است که اندازه‌گیری نشانه نتیجه ناصحیح دهد که با احتمال $c_3 p^2$ رخ می‌دهد (برای کد اِستین، $c_3 \approx 10^2$). در صورتیکه اندازه‌گیری نشانه نتیجه صحیح بدهد، خطایی که توسط $CNot$ وارد می‌شود به طور صحیح تشخیص و بازیابی می‌شود و تنها یک تک خطا روی خروجی باقی می‌گذارد که در طول اندازه‌گیری نشانه وارد شد.

۵- ۲ یا بیش از ۲ شکست در طول اندازه‌گیری نشانه رخ می‌دهد که احتمال آن نهایتا $c_4 p^2$ می‌باشد به طوریکه c_4 تعداد جفت نقاطی است که یک شکست ممکن است رخ دهد. برای کد اِستین، $c_4 \approx 70^2 \approx 5\times 10^3$.

۶- یک شکست ممکن است در طول اندازه‌گیری نشانه و یک شکست در طول بازیابی با احتمال نهایتا $c_5 p^2$ رخ می‌دهد به طوریکه c_5 تعداد جفت نقاطی است که یک شکست ممکن است رخ دهد، برای کد اِستین $c_5 \approx 70\times 7 \approx 50$.

۷- ۲ یا بیش از ۲ شکست در طول بازیابی ممکن است با احتمال $c_6 p^2$ رخ دهد به طوریکه c_6 تعداد جفت نقاطی است که یک شکست ممکن است در آن رخ دهد، برای کد اِستین، $c_6 \approx 7^2 \approx 50$.

بدین ترتیب احتمال اینکه این مدار ۲ یا بیش از ۲ خطا در دسته اول از کیوبیتهای کدگذاری شده وارد کند، cp^2 است به طوریکه ثابت c برابر است با

$$c = c_0^2 + c_1 + c_2 + c_3 + c_4 + c_5 + c_6 \qquad (۱۸-۴)$$

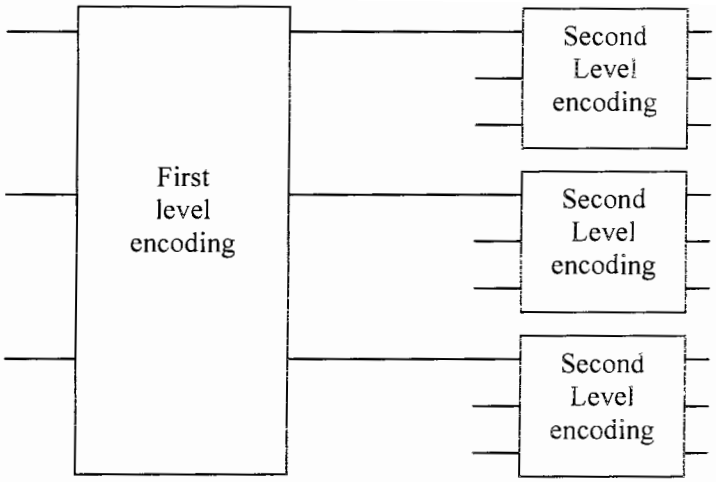
که تقریبا معادل با 10^4 برای کد استین می‌باشد. بنابراین اگر یک کدگشایی صحیح و کامل در انتهای مدار اعمال شود، احتمال یک خطا cp^2 خواهد بود.

این یک نتیجه قابل توجه است: ما موفق شدیم که یک اجرا پیاده‌سازی برای گیت *CNot* پیدا کنیم با این ویژگی که هر کدام از اجزاء ممکن است با احتمال p دچار شکست شوند اما روند کدگذاری شده، با احتمال $1-cp^2$ موفق می‌شود (مشروط بر اینکه p کوچک باشد (در این مثال $p<10^{-4}$)).

نتایج مشابه را برای همه عملهای دیگر که در طول یک محاسبه انجام می‌شوند، داریم. بنابراین با انجام هر یک از این عملها به صورت FT می‌توانیم احتمال یک شکست را از p به cp^2 کاهش دهیم. (برای ثابت c) ما c را برای *CNot* تخمین زدیم. در هر حال برآوردها برای بقیه عملهای FT تفاوت چندانی نمی‌کند و ما $c \approx 10^4$ را در برآوردهای عددی‌یمان استفاده می‌کنیم.

۴-۳-۴- کدهای اتصال و قضیه آستانه

یک ساختار زیبا بر پایه کدهای اتصال وجود دراد که می‌تواند برای کاهش میزان خطای موثر که با محاسبه کوانتومی به دست می‌آید، به کار برده شود. ایده به این شکل است که طرح توصیف شده در بالا را به صورت بازگشتی برای شبیه سازی یک مدار، با به کار بردن یک مدار کدگذاری شده (با ایجاد یک سلسله از مدارهای کوانتومی c_0 ، c_1، c_2 و . . .) به کار ببریم.



شکل (۴-۱۲): یک کد با دو بار تسلسل که یک تک کیوبیت را در ۹ کیوبیت کدگذاری می‌کند. در اینجا یک کد سه کیوبیتی صرفا به خاطر ساده سازی شکل آورده شده است. اما در عمل کدهایی مانند کد استین به کار برده می‌شوند که می‌توانند خطاهایی را روی یک یا بیش از یک کیوبیت تصحیح کنند.

در مرحله اول از این ساخت، هر کیوبیت در مدار اصلی در یک کد کوانتومی که کیوبیتهایش در یک کد کوانتومی کدگذاری شده‌اند، کدگذاری می‌شود که دوباره خود اینها کدگذاری شده‌اند و . . . (به طوریکه این عمل به طور نامحدود صورت گرفته است) همانطور که در شکل (۴-۱۲) آمده‌است. در مرحله دوم از این ساخت، هر گیت داده شده در مدار اصلی c_0 مانند یک گیت هادامارد، در مدار c_1 توسط یک روند FT که یک گیت هادامارد کدگذاری شده و تصحیح خطا را اجرا می‌کند، جایگزین می‌شود. هر کدام از اجزای به کار برده شده در مدار c_1 توسط یک روند FT که یک ورژن کدگذاری شده از آن جزء و تصحیح خطا را اجرا می‌کند، در مدار c_2 جایگزین می‌شود (به طوریکه این عمل به طور نامحدود ادامه می‌یابد)، فرض کنید که این دو مرحله تسلسل را انجام دهیم. اگر احتمال شکست در پایین‌ترین مرحله از تسلسل (کیوبیتهای فیزیکی واقعی) p باشد، در این صورت احتمال شکست در مرحله میانی (مرحله اول کدگذاری) نهایتا cp^2 و در بالاترین مرحله $c\left(cp^2\right)^2$ می‌باشد. بدین ترتیب اگر ما k بار تسلسل ایجاد کنیم، احتمال شکست برای یک روند در بالاترین مرحله

$\left((cp)^2\right)^k / c$ می‌باشد به طوریکه سایز مدار شبیه‌سازی، d^k برابر سایز مدار اصلی می‌شود که d یک ثابت است که نمایانگر تعداد ماکزیمم عملهای به کار برده شده در یک روند FT برای انجام یک گیت کدگذاری شده و تصحیح خطا می‌باشد. فرض کنید که می‌خواهیم یک مدار شامل $p(n)$ گیت را شبیه‌سازی کنیم، به طوریکه n بیانگر میزان اشکال و خرابی است و $p(n)$ یک تابع چند جمله‌ای در n می‌باشد. به عنوان مثال می‌توانیم الگوریتم عامل یابی کوانتومی را در نظر بگیریم. فرض کنید می‌خواهیم دقت نهایی ε در شبیه‌سازیمان از این الگوریتم را به دست بیاوریم. شبیه سازی هر گیت در این الگوریتم باید با دقت $\varepsilon / p(n)$ باشد. پس باید k بار تسلسل صورت گیرد به طوریکه

$$\frac{(cp)^{2^k}}{c} \le \frac{\varepsilon}{p(n)} \qquad (۱۹-۴)$$

مشروط بر اینکه $p < p_{th} \equiv 1/c$، این تعداد k، قابل دستیابی است. این شرط (که $p < p_{th}$) شرط آستانه برای محاسبه کوانتومی نامیده می‌شود. از این رو مشروط بر اینکه این شرط برقرار باشد، ما می‌توانیم محاسبات کوانتومی را با دقت دلخواه داشته باشیم.

سایز یک مدار کوانتومی چه قدر باید باشد تا به این میزان از دقت دست پیدا کنیم؟

توجه کنید که داریم:

$$d^k = \left(\frac{\log\left(p(n)/c\varepsilon\right)}{\log(1/pc)}\right)^{\log d} = O\left(poly\left(\log p(n)/\varepsilon\right)\right) \qquad (۲۰-۴)$$

به طوریکه $poly$ نمایانگر چند جمله درجه ثابت می‌باشد و بدین ترتیب مدار شبیه سازی شامل $O\left(poly\left(\log p(n)/\varepsilon\right) p(n)\right)$ گیت می‌باشد که فقط به صورت پلی لگاریتمی بزرگتر از سایز مدار اصلی می‌باشد. به طور خلاصه قضیه آستانه برای محاسبه کوانتومی را به صورت زیر داریم:

قضیه آستانه برای محاسبه کوانتومی: یک مدار کوانتومی شامل $p(n)$ گیت با احتمال نهایتا ε خطا، با استفاده از $O\left(poly\left(\log p(n)/\varepsilon\right)p(n)\right)$ گیت روی سخت افزاری که اجزاء آن با احتمال نهایتا p دچار شکست می‌شوند، می‌تواند شبیه سازی می‌شود، مشروط بر اینکه p کوچکتر از یک مقدار آستانه‌ی ثابت باشد ($p < p_{th}$).

مقدار p_{th} چه‌قدر است؟ برای کد اِستین، مطابق محاسباتمان می‌دانیم که $c \approx 10^4$، بنابراین یک تخمین تقریبی، مقدار $p_{th} \approx 10^{-4}$ را به ما می‌دهد. لازم است تاکید کنیم که تخمین‌هایمان خیلی با مقدار دقیق فاصله دارد. به طوریکه محاسبات پیچیده‌تر برای مقدار آستانه به عنوان نمونه، مقادیری در بازه‌ی $10^{-5} - 10^{-6}$ داده است. توجه کنید که مقدار دقیق آستانه به میزان زیادی به فرضیاتی که درباره‌ی امکانات محاسباتی صورت گرفت، بستگی دارد.

به عنوان مثال اگر عملیات موازی (همزمان و مشابه) امکان پذیر نباشد، در این صورت شرط آستانه قابل دستیابی نیست، زیرا خطاها در مدار به سرعت انباشته می‌شوند. محاسبه کوانتومی علاوه بر عملهای کوانتومی برای پردازش نشانه‌های اندازه‌گیری شده و تعیین اینکه کدام گیت کوانتومی برای تصحیح خطا باید اعمال شود، لازم می‌باشد.

۴-۴- استدلال کوانتومی FT

تکنیک اساسی در ساختار مدارهای کوانتومی FT، روش ایجاد عملهای FT برای لوجیک کردن حالتهای کدگذاری شده می‌باشد. می‌دانیم که که گیتهای هادامارد، فاز، $CNot$ و $\pi/8$ یک مجموعه جهانی را تشکیل می‌دهند. در اینجا توضیح می‌دهیم که چگونه هر یک از این گیتها می‌تواند به صورت FT اجرا شود.

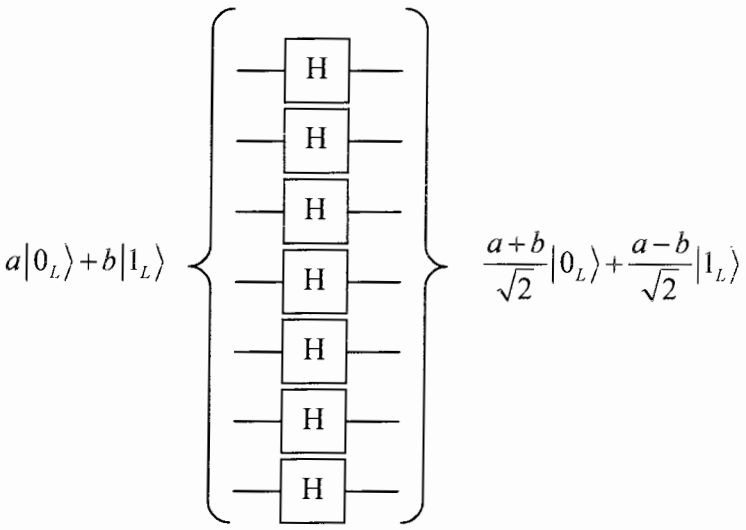
۴-۴-۱- عملهای نرمالیزکننده

با ساختارهای FT برای عملهای نرمالیزکننده (گیتهای هادامارد و فاز و $CNot$) برای حالت خاص کد استین شروع می‌کنیم. با داشتن اصول ساده‌ی این ساختارها برای این مثال عینی، به آسانی می‌توان آنها را به هر کد تشبیت کننده تعمیم داد.

یادآوری می‌کنیم که برای کد استین، عملگرهای $\bar{X}$ و $\bar{Z}$ پائولی روی حالتهای کدگذاری شده، می‌توانند بر حسب عملگرهایی روی کیوبیتهای کدگذاری نشده نوشته شوند:

$$\begin{aligned}\bar{Z} &= Z_1Z_2Z_3Z_4Z_5Z_6Z_7\\ \bar{X} &= X_1X_2X_3X_4X_5X_6X_7\end{aligned} \qquad (۲۱-۴)$$

یک گیت هادامارد کدگذاری شده $\bar{H}$ باید $\bar{Z}$ و $\bar{X}$ را تحت کانجوگیشن عوض کنند، دقیقا همانطور که گیت هادامارد Z و X را تحت کانجوگیشن عوض می‌کرد. $\bar{H} = H_1H_2H_3H_4H_5H_6H_7$ این کار را انجام می‌دهد، بنابراین یک هادامارد روی کیوبیت کدگذاری شده می‌تواند مانند آنچه در شکل (۴-۱۳) نمایش داده شده است، اجرا شود.



شکل (۴-۱۳): گیت هادامارد عرضی روی یک کیوبیت کدگذاری شده در کد استین

این گام اول خوبیست اما تنها لوجیک کردن حالتهای کدگذاری شده برای FT ساختن این عمل کافی نیست. همچنین لازم است بدانیم که خطا چگونه منتشر می‌شود. از آنجائیکه مداریکه $\bar{H} = H^{\otimes 7}$ را اجرا می‌کند بیش از یک کیوبیت در دسته کدگذاری شده در تحت تاثیر قرار نمی‌دهد، به لحاظ فیزیکی معقول است که فرض کنیم که شکست یک تک جزء در مدار سبب نهایتا یک خطا در دسته-ای از کیوبیتها می‌شود که از روند خارج می‌شوند. برای اثبات این مسئله، تصور کنید که یک خطا روی کیوبیت درست قبل از اعمال گیت H کدگذاری شده اتفاق بیفتد. به منظور تعریف، فرض کنیدکه خطا، خطای Z باشد، بنابراین عمل مرکب روی کیوبیت HZ می‌باشد. با توجه به تحلیل‌های اخیر از انتشار خطا برای گیت $CNot$، با قرار دادن عملگر یکانی $H^{\dagger}H = I$ داریم:

$$HZ = HZH^{\dagger}H = XH \qquad (۲۲-۴)$$

بنابراین یک چنین خطایی معادل با اعمال H و سپس رخ دادن خطای X می‌باشد. به طور مشابه یک شکست در طول خود عمل گیت، معادل با یک گیت بدون نقص به همراه یک مقدار کوچکی نویز که روی کیوبیت اثر می‌کند، می‌باشد که می‌تواند بر حسب نمونه‌های معمول X، Y و Z در نظر گرفت که با احتمال کمی اتفاق بیفتند. مدار شکل (۴-۱۳) بدین ترتیب واقعا یک عمل FT می‌باشد، زیرا یک تک شکست که در هر قسمت از روند رخ دهد انتشار نمی‌یابد تا روی بقیه کیوبیتها نیز اثر کند و بدین ترتیب نهایتا یک خطا در این دسته از کیوبیتها که از روند خارج می‌شوند را سبب می‌شود. آیا اصول کلی که بتوان از مدار شکل (۴-۱۳) دریافت کرد، وجود دارد؟

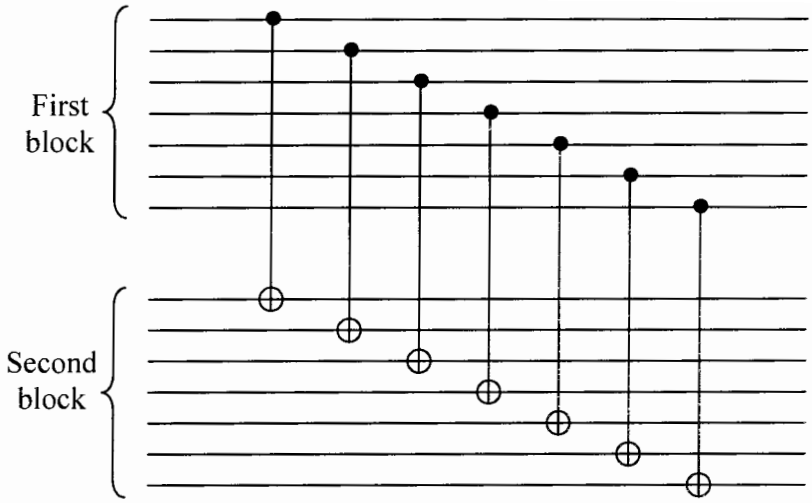
یکی از نظرات مفید این است که گیتهای کدگذاری شده به طور اتوماتیک FT هستند اگر به شکل بیت به بیت بتوانند اجرا شوند، زیرا این ویژگی این اطمینان را حاصل می‌کند که یک شکست در هر جایی از گیت کدگذاری شده، نهایتا یک خطا در هر دسته از کدها وارد می‌کند و بدین ترتیب احتمال

خطا تا حدی که خارج از کنترل و قابل تصحیح نباشد، افزایش نمی‌یابد. این ویژگی که یک گیت کدگذاری شده بتواند به صورت بیت به بیت اجرا شود ویژگیِ عرضیِ یک گیت کوانتومی کدگذاری شده نامیده می‌شود.

این ویژگی جالب است زیرا یک طرح کلی برای یافتن مدارهای کوانتومی FT را پیشنهاد می‌کند و در ادامه خواهیم دید که گیتهای زیادی علاوه بر گیتهای هادامارد می‌توانند عرضی باشند. توجه داشته باشید که این امکان وجود دارد که ساختارهایی از FT که عرضی نیستند را نیز بیابیم، همانطور که در ادامه مثالی از گیت FTی $\pi/8$ را توضیح خواهیم داد.

با استفاده از کد اِستین، گیتهای زیادی علاوه بر گیت هادامارد به آسانی اجراهای عرضی دارند. سه گیت جالب آن، علاوه بر گیت هادامارد، گیت فاز و گیتهای X و Z می‌باشند. فرض کنید که گیت Z را به صورت بیت به بیت به هر یک از ۷ کیوبیت کد اِستین اعمال کنیم. در این صورت هر عملگر Z، تحت کانجوگیشن به $-Z$ تبدیل می‌شود و لذا $\bar{Z} \to (-1)^7 \bar{Z} = -\bar{Z}$ و با اعمال بیت به بیت X، تحت کانجوگیشن $\bar{X}$ به $\bar{X}$ تبدیل می‌شود و بدین ترتیب این مدار عمل X کدگذاری شده را روی حالت‌های کد اِستین اثر می‌دهد. این مدار عرضی می‌باشد و بدین ترتیب به طور اتوماتیک FT است. به طور مشابه، با اعمال Z به صورت بیت به بیت به حالتهای کد اِستین یک اجرای FT از Z کدگذاری شده را خواهیم داشت.

اجرای عرضی گیت فاز کمی متفاوت است. تحت کانجوگیشن، $\bar{S}$ باید $\bar{Z}$ را به $\bar{Z}$ و $\bar{X}$ را به $\bar{Y} = i\bar{X}\bar{Z}$ ببرد. با استفاده از فرض مشهود $\bar{S} = S_1S_2S_3S_4S_5S_6S_7$، $\bar{Z}$ را تحت کانجوگیشن به $\bar{Z}$ و $\bar{X}$ را به $-\bar{Y}$ می‌برد. علامت منفی در مقابل $-\bar{Y}$ با اعمال $\bar{Z}$ درست می‌شود، به این ترتیب با اعمال عمل ZS به هر کیوبیت در کد، گیت فاز کدگذاری شده که عرضی می‌باشد، لذا FT اجرا می‌شود.



شکل (۴-۱۴): $CNot$ عرضی بین دو کیوبیت که در دسته‌های جدا توسط کد استین کدگذاری شده‌اند.

در مقایسه با گیت همانی هادامارد، پائولی و فاز، اجرای $CNot$ به صورت FT در ابتدا به نظر می‌رسد که متفاوت باشد، زیرا $CNot$ ۲ دسته کد جداگانه از ۷ کیوبیت را در بر می‌گیرد. چگونه می‌توان $CNot$ی را تحقق بخشید که بیش از یک خطا در هر دسته از کدها وارد نکند؟ خوشبختانه با استفاده از کد اِستین که در شکل (۴-۱۴) نمایش داده شده است، این امر ساده خواهد بود: به آسانی می‌بینیم که این امر توسط ۷ گیت $CNot$ که بین ۷ کیوبیت این دسته اعمال می‌شود صورت می‌گیرد. ممکن است نگران این مسئله باشید که این ساختارِ عرضی، قوانینمان را نقض کند. آیا گیت $CNot$ی که ما با آن کار می‌کنیم سبب نمی‌شود که خطاها روی بیش از یک کیوبیت منتشر شوند؟ این صحیح است اما مشکلی وجود ندارد زیرا انتشار خطا در هر صورت تنها نهایتا روی یک کیوبیت در دسته دیگر اثر می‌گذارد و روی کیوبیتهای دسته‌ی دیگر اثر نمی‌گذارد.

به طور دقیق‌تر فرض کنید که یک خطای X روی کیوبیت اول رخ دهد، درست قبل از $CNot$ بین کیوبیت اول از هر گروه، که آنها را با کیوبیتهای ۱ تا ۸ نامگذاری می‌کنیم. اگر این گیت $CNot$ را با U نمایش دهیم، در این صورت عمل موثر

$$UX_1 = UX_1U^\dagger U = X_1X_8U \qquad (۲۳-۴)$$

می‌باشد، یعنی مثل این است که $CNot$ به طور صحیح اعمال شده باشد، اما یک خطای X روی کیوبیت اول هر دو دسته از کیوبیتهای کدگذاری شده رخ داده باشد. کمی متفاوت‌تر، فرض کنید یکی از گیتهای $CNot$، به سبب نویز موفق عمل نکند، در این صورت چه اتفاقی می‌افتد؟ فرض کنید که گیت $CNot$ نویزدارمان، عمل کوانتومی ε را اجرا کند. در این صورت می‌توان دوباره به این صورت بازنویسی کرد که:

$$\varepsilon = \varepsilon \circ u^{-1} \circ u \qquad (۲۴-۴)$$

به طوریکه u، یک عمل کوانتومی می‌باشد که گیت $CNot$ را به صورت صحیح اجرا می‌کند. بدین ترتیب گیت $CNot$ نویزدار، معادل با اعمال یک گیت بدون عیب $CNot$ به همراه عمل $\varepsilon \circ u^{-1}$ می‌باشد که به طور تقریبی همانی است در صورتیکه گیت نویزدار $CNot$ به طور معقولی خوب باشد و بتواند به صورت حاصلضربهای تانسوری خطاهای معمول مانند $X \otimes Z$ که روی دو کیوبیت با احتمال کم اتفاق می‌افتد، لحاظ شود.

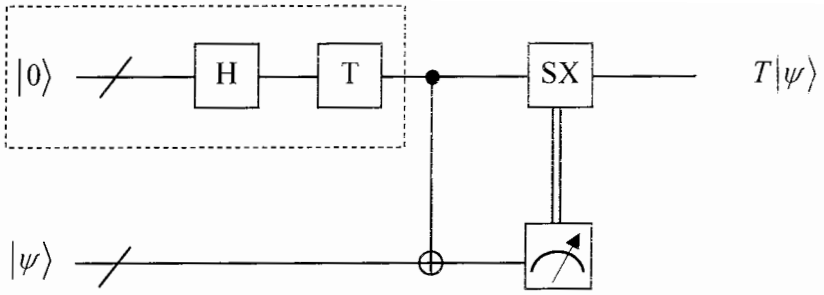
خوشبختانه زمانی که اینگونه خطاها دو کیوبیت را شامل می‌شوند، تنها یک تک کیوبیت در هر دسته از کیوبیتهای کدگذاری شده را در بر می‌گیرند. لذا شکست یک تک جزء در طول روند، انتشار می‌یابد و بیش از یک خطا در هر دسته از کیوبیتهای کدگذاری شده را سبب نمی‌شود و بدین ترتیب این اجرا از $CNot$ کدگذاری شده، FT می‌باشد.

۴-۴-۲- گیت FTی $\pi/8$

یک گیت دیگر که نیاز داریم تا مجموعه گیتهای استاندارد برای محاسبه کوانتومی جهانی را کامل کنیم، گیت $\frac{\pi}{8}$ می‌باشد.

متناوبا همانطور که قبلا گفته شد، با اضافه کردن یک گیت FTی تافولی به مجموعه گیتهای FTی هادامارد، فاز و $CNot$، یک مجموعه جهانی را خواهیم داشت که ما را قادر می‌سازد که همه گیتهای لازم توسط یک کامپیوتر کوانتومی را در یک حالت FT به کار ببریم. استراتژی اولیه ما در ایجاد گیت FTی $\frac{\pi}{8}$، تقسیم ساختار به ۳ بخش است. بخش اول ساختار، یک مدار ساده برای شبیه‌سازی گیت $\frac{\pi}{8}$ با استفاده از عناصری که ما از قبل می‌دانیم که چگونه به صورت FT عمل می‌کنند می‌باشند، مانند گیتهای $CNot$، فاز و X. دو بخش دیگر این مدار را هنوز نمی‌دانیم که چگونه FT بسازیم.

اولین بخش آماده سازی یک حالت کمکی برای قراردادن در مدار می‌باشد. برای اینکه این حالت کمکی کافی باشد، لازم است که شکست هر یک از اعضاء در طول آماده سازی حالت کمکی نهایتا منتهی به یک تک خطا در آن دسته از کیوبیتها که حالت کمکی را می‌سازند، شود. در این فصل توضیح خواهیم داد که چگونه یک چنین آماده‌سازی کمکی FT می‌تواند صورت گیرد. دومین عملی که نیاز داریم اندازه‌گیری می‌باشد. برای اینکه اندازه‌گیری را FT بسازیم لازم است که شکست یک تک عضو در طول روند، برای اندازه‌گیری روی خروجی اندازه‌گیری اثری نگذارد. در غیر این صورت خطا انتشار می‌یابد و خطاهایی را روی تعداد زیادی از کیوبیتها در دسته اول سبب می‌شود. اینکه عمل SX کدگذاری شده، اعمال می‌شود یا نه توسط نتیجه اندازه‌گیری مشخص می‌شود (به طور دقیق‌تر، برای اندازه‌گیری FT، که ممکن است خروجی اندازه‌گیری واقعا با احتمال $O\left(p^2\right)$ ناصحیح باشد، به طوریکه p احتمال شکست یک تک عضو می‌باشد. ما در اینجا از این چشمپوشی می‌کنیم).



شکل (۴-۱۵): مدار کوانتومی که به صورت FT یک گیت $\pi/8$ را اجرا می‌کند. مستطیل نقطه چین شده روند آماده سازی (FT نیست) برای حالت کمکی $\left(|0\rangle+\exp(i\pi/4)|1\rangle\right)/\sqrt{2}$ را نشان می‌دهد. علامت اِسلش روی سیم، معرف یک دسته هفت کیوبیتی می‌باشد و سیم دو خطی بیت کلاسیکی که از اندازه‌گیری ناشی می‌شود را نشان می‌دهد. توجه کنید که عمل نهایی SX توسط نتیجه‌ی اندازه‌گیری کنترل می‌شود.

شکل (۴-۱۵) یک مدار که یک گیت را اجرا می‌کند نشان می‌دهد. همه اعضای این مدار می‌توانند به صورت FT اجرا شوند به جز شاید اندازه‌گیری و آنهایی که با یک مستطیل متمایز شده‌اند. مدار با دو کیوبیتِ کدگذاری شده شروع می‌شود که یکی از آنها کیوبیت $|\psi\rangle=a|0\rangle+b|1\rangle$ می‌باشد (در اینجا $|0\rangle$ و $|1\rangle$ حالتهای منطقی را نمایش می‌دهند).کیوبیت دیگر به صورت زیر آماده می‌شود:

$$|\Theta\rangle=\frac{|0\rangle+\exp(i\pi/4)|1\rangle}{\sqrt{2}} \qquad (۲۵-۴)$$

که حالتی است که توسط مدار در قسمتهای نقطه‌چین شده، ایجاد می‌شود. توضیح می‌دهیم که چگونه این مرحله آماده سازی کمکی در یک لحظه به صورت FT انجام می‌شود. سپس یک عمل FTی $CNot$ اعمال می‌کنیم:

$$\begin{aligned}&\frac{1}{\sqrt{2}}\left[|0\rangle\left(a|0\rangle+b|1\rangle\right)+\exp(i\pi/4)|1\rangle\left(a|1\rangle+b|0\rangle\right)\right]\\&=\frac{1}{\sqrt{2}}\left[\left(a|0\rangle+b\exp(i\pi/4)|1\rangle\right)|0\rangle+\left(b|0\rangle+a\exp(i\pi/4)|1\rangle\right)|1\rangle\right]\end{aligned} \qquad (۲۶-۴)$$

در پایان، کیوبیت دوم را اندازه می‌گیریم و اگر 0 باشد حالت مورد نظر آماده شده است، در غیر این صورت عمل زیر را به کیوبیت باقی مانده اعمال می‌کنیم:

$$SX = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad (۲۷-۴)$$

لذا با حالت $a|0\rangle + b\exp(i\pi/4)|1\rangle$، همانطور که برای یک گیت $\pi/8$ لازم بود، مواجه می‌شویم. این نتیجه ممکن است عجیب به نظر برسد که از هیچ جایی نیامده است، اما در حقیقت نتیجه یک ساختار متقارن می‌باشد.

ساختار گیت FTی $\pi/8$ ، یک روش FT برای ایجاد حالت کمکی $|\Theta\rangle$ را نیاز دارد. این آماده‌سازی می‌تواند با استفاده از تکنیکهایی برای اندازه‌گیری‌های FT به دست بیاید. در اینجا ارتباط آن با اندازه-گیری FT توضیح می‌دهیم. همانطور که در شکل (۴-۱۵) نشان داده شده است، $|\Theta\rangle$ با اعمال یک گیت هادامارد و سپس $\pi/8$ بر حالت $|0\rangle$ ایجاد می‌شود. حالت $|0\rangle$، یک ویژه حالت $+1$ از Z می-باشد، پس نتیجه می‌دهد که $|\Theta\rangle$ یک ویژه حالت از $THZHT^\dagger = TXT^\dagger = e^{-i\pi/4}SX$ می‌باشد. بنابراین $|\Theta\rangle$ می‌تواند با آماده سازی یک $|0\rangle$ کدگذاری شده و سپس اندازه‌گیری $e^{-i\pi/4}SX$ به صورت FT، حاضر شود. اگر نتیجه -1 به دست آمد، ما یکی از این ۲ انتخاب را داریم: می‌توانیم تا زمانی که اندازه‌گیری FTی $e^{-i\pi/4}SX$، نتیجه $+1$ را بدهد، روند را تکرار کنیم و یا اینکه از آنجائیکه $ZSXZ = -SX$، می‌توانیم با اعمال یک عمل FTی Z ، حالت را از ویژه حالت -1 برای $e^{-i\pi/4}SX$، به ویژه حالت $+1$ برای $e^{-i\pi/4}SX$، تغییر دهیم، یعنی به حالت $|\Theta\rangle$. هر کدام از این روشها به کار برده شوند، یک تک شکست در هر جایی از روند یک خطا را نهایتا در یک کیوبیت در حالت کمکی $|\Theta\rangle$ ایجاد می‌کند.

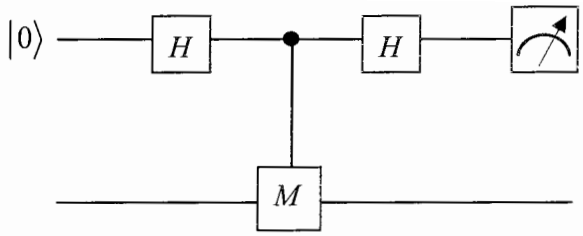
به آسانی می‌توان دید که روندی که ما توضیح دادیم در کل یک FT است. در هر صورت با یک مثال روشن این مسئله مشخص می‌شود. فرض کنید شکست یک تک عضوی در طول ساختار کمکی رخ دهد، منتهی به یک خطا روی یک تک کیوبیت در کمکی شود. این خطا در طول گیت $CNot$

کدگذاری شده منتشر می‌شود و یک خطا در هر دسته اول و دوم از کیوبیتها را سبب می‌شود. خوشبختانه یک خطا روی یک تک کیوبیت کدگذاری شده دوم، روی نتیجه روند اندازه‌گیری FT ما اثری نمی‌گذارد، بنابراین SX (با توجه به اقتضاء) یا اعمال می‌شود و یا اعمال نمی‌شود و بدین ترتیب خطا روی دسته اول از کیوبیتها انتشار می‌یابد تا یک تک خطا در خروجی از گیت کدگذاری شده را سبب شود.

۴-۴-۳- اندازه گیری FT

ابزار مهم و بسیار سودمند در ساختار مدارهای FT، توانایی برای اندازه‌گیری یک عملگر M می‌باشد. اندازه‌گیریها برای انجام کدگذاری، خواندن نتیجه یک محاسبه، تشخیص نشانه در تصحیح خطا و انجام آماده سازی حالت کمکی در ساختار گیتهای FTی تافولی و $\pi/8$ استفاده می‌شود و بدین ترتیب نقش کاملا تعیین کننده برای محاسبه کوانتومی FT را دارند.

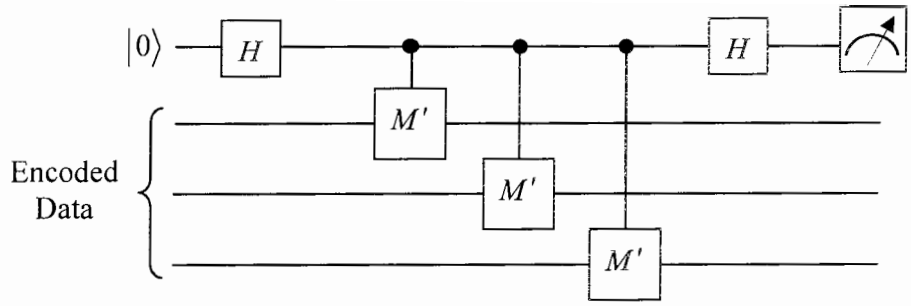
برای اینکه یک روند برای انجام یک اندازه‌گیری کدگذاری شده، FT باشد دو چیز نیاز داریم که برای جلوگیری از انتشار خطا صحیح می‌باشد. اول اینکه یک تک شکست در هر جای روند نهایتا به یک خطا در هر دسته از کیوبیتها در انتهای روند منجر شود. دوم اینکه، حتی اگر یک تک شکست در طول روند رخ دهد لازم است که نتیجه اندازه‌گیری با احتمال $1-O\left(p^2\right)$ صحیح باشد. این نیاز اخیر بسیار مهم می‌باشد، زیرا نتیجه اندازه‌گیری ممکن است برای کنترل بقیه عملها در کامپیوتر کوانتومی استفاده شود و اگر این نتیجه غیر صحیح باشد در این صورت ممکن است انتشار یابد و روی تعداد زیادی از کیوبیتها در دسته‌های دیگر کیوبیتهای کدگذاری شده اثر بگذارد.



شکل (۴-۱۶): مدار کوانتومی برای اندازه‌گیری یک عملگر تک کیوبیتی M با مقادیر ویژه‌ی ± 1. کیوبیت بالایی حالتی کمکی است که برای اندازه‌گیری استفاده می‌شود و کیوبیت پایینی در حال اندازه‌گیری شدن است.

یادآوری می‌کنیم که اندازه‌گیری یک مشاهده‌پذیر تک کیوبیتی M ممکن است با استفاده از مدار نشان داده شده در شکل(۴-۱۶) انجام شود. فرض کنید که M، یک اجرای عرضی کدگذاری شده روی یک کد کوانتومی به طوریکه گیت M' به صورت بیت به بیت روی هر کیوبیت کد عمل می‌کند. به عنوان مثال برای کد اِستین، $M = H$ می‌باشد، در حالیکه $M' = H$ به صورت بیت به بیت اعمال می‌شود اما اجرای عرضی $M = S$، گیت $M' = ZS$ را به صورت بیت به بیت روی هر کیوبیت اعمال می‌کند.

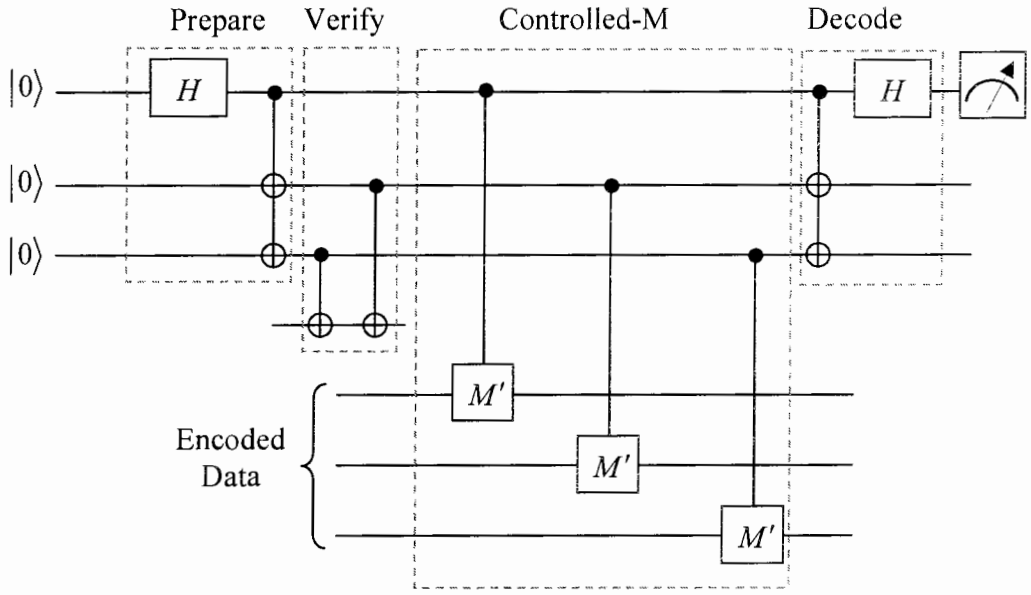
بدین ترتیب یک مدار ممکن را برای اندازه‌گیری M کدگذاری شده، روی داده‌ی کدگذاری شده همانطور که در شکل (۴-۱۷) نمایش داده شده است، پیشنهاد می‌شود. توجه کنید که یک کد کوانتومی واقعی مانند کد اِستین کیوبیتهای بیشتری نیاز دارد. متاسفانه مدار شکل (۴-۱۷) FT نمی-باشد. برای اثبات این مساله، تصور کنید که یک شکست در ابتدای مدار روی حالت کمکی رخ دهد، این شکست انتشار یافته و روی همه کیوبیتهای کدگذاری شده‌ی اثر می‌گذارد. بنابراین این مدار FT نیست.



شکل (۴-۱۷): روند شماتیک برای اجرای یک اندازه‌گیری از مشاهده‌پذیر کدگذاری شده‌ی M با یک اجرای عرضی با اعمال بیت به بیت M'. مدار FT نیست. توجه کنید که یک کد واقعی بیش از سه کیبویت نیاز دارد.

یک روش خوب برای اینکه مدار اندازه‌گیری را FT بسازیم، در شکل (۴-۱۸) نمایش داده شده است. برای ساده سازی، این شکل نشان می‌دهد که داده‌هایی که اندازه‌گیری می‌شوند تنها در ۳ کیوبیت کدگذاری شده‌اند. در عمل کیوبیتهای بیشتری به کاربرده می‌شود، مانند کد ۷ کیوبیتی اِستین. به علاوه برای هر کیوبیت داده‌ی کدگذاری شده، مدار یک کیوبیت کمکی وارد می‌کند به طوریکه در ابتدا هر کدام در حالت $|0\rangle$ هستند. مرحله اول، آماده‌سازی حالت کمکی در یک حالت «cat» است، $|00...0\rangle+|11...1\rangle$. مداری که این آماده سازی را انجام می‌دهد خودش FT نیست، زیرا یک تک شکست در طول مدار سبب خطا روی چندین کیوبیت در حالت cat می‌شود. با این وجود، این مسئله روی FT روند کل اثر نمی‌گذارد، زیرا آماده‌سازی کمکی به همراهی چندین مرحله بازبینی[۱] صورت می‌گیرد. در شکل (۴-۱۸) تنها یک مرحله از بازبینی نمایش داده شده است.

[۱] verification



شکل (۴-۱۸): روند شماتیک برای اندازه‌گیری FT یک مشاهده‌پذیر M، که که روی داده‌ی کدگذاری شده اجرا می‌شود. این روند سه بار تکرار می‌شود و یک رای اکثریت از نتایج اندازه‌گیری گرفته می‌شود.

بازبینی به شکل زیر صورت می‌گیرد: هدف اساسی بازبینی این است که بررسی کنیم که آیا حالت، یک حالت cat است یا خیر. کافیست که نشان دهیم که اندازه‌گیری Z_iZ_j برای همه جفت کیوبیتهای i و j در حالت cat، 1 را خواهد داد. یعنی پاریته هر جفت از کیوبیتها در حالت cat، زوج است. برای بررسی این مسئله برای یک جفت ویژه Z_iZ_j (Z_2Z_3 در این مثال) ما یک کیوبیت اضافی وارد می‌کنیم که از ابتدا در حالت $|0\rangle$ است. پاریته دو کیوبیت در کمکی را با اجرای ۲ گیت $CNot$ با دو کیوبیت کمکی به عنوان کنترل و کیوبیت اضافه به عنوان هدف، قبل از اندازه‌گیری کیوبیت اضافی محاسبه می‌کنیم.

اگر پاریته اندازه‌گیری شده 1 باشد، در این صورت می‌دانیم که کمکی در حالت cat نیست، آن را کنار گذاشته و دوباره شروع می‌کنیم. فرض کنید که یک شکست تک عضوی در جایی در طول این بررسی پی در پی پاریته رخ دهد، این روند FT نیست زیرا به سادگی مشخص می‌شود که شکستهای تک

عضوی وجود دارد، به طوریکه منتهی به بیش از یک وارونی فاز در حالت کمکی می‌شود. به عنوان مثال اگر یک خطای Z روی کیوبیت اضافی بین گیتهای $CNot$ رخ دهد در این صورت می‌تواند انتشار یابد و سبب خطاهای Z روی دو کیوبیت کمکی شود. خوشبختانه به راحتی می‌توان نشان داد که چندین خطای Z در کیوبیتهای کمکی به داده‌ی کدگذاری شده انتشار نمی‌یابد، اگر چه ممکن است سبب شوند که نتیجه اندازه‌گیری نهایی غیر صحیح باشد. برای مقابله با این مشکل، و همانطور که در ادامه به طور جزئی‌تر توضیح داده خواهد شد ما این روند برای اندازه‌گیری را سه بار تکرار می‌کنیم و یک رأی اکثریت را انتخاب می‌کنیم. بنابراین احتمال اینکه اندازه‌گیری، دو یا بیش از دو بار در این روش غلط باشد، نهایتا $O\left(p^2\right)$ است، به طوریکه p احتمال شکست برای یک تک عضو می‌باشد. و اما خطای X و Y به چه صورت می‌باشند؟ این خطاها می‌توانند انتشار یابند و سبب خطاهایی در داده کدگذاری شده شوند. اما این حقیقت خوب است که یک تک شکست در طول آماده‌سازی حالت cat و بازبینی نهایتا یک خطای X و یا Y در کمکی را سبب می‌شوند (بعد بازبینی) و بدین ترتیب نهایتا یک خطا در داده کدگذاری شده، که این مسئله FT را تضمین بعد از اینکه حالت cat بازبینی شد، گیتهای $Controlled-M'$ بین کمکی‌ها و کیوبیتهای داده، اعمال می‌شوند به طوریکه هیچ کیوبیت کمکی بیش از یک بار به کار برده نمی‌شود. بدین ترتیب اگر کمکی در حالت $|00...0\rangle$ باشد، نتیجه می‌دهد که هیچ عملی روی داده کدگذاری شده صورت نمی‌گیرد، در حالیکه اگر کمکی در حالت $|11...1\rangle$ باشد عمل M کدگذاری شده روی داده اعمال می‌شود. مقدار حالت cat که مقداری است که تضمین می‌کند خطاها از یک گیت $Controlled-M'$ به دیگری انتشار نمی‌یابند، بنابراین یک تک خطا در مرحله بازبینی و یا در گیتهای $Controlled-M'$ که به صورت پی در پی اعمال می‌شوند، نهایتا یک تک خطا در داده کدگذاری شده را سبب می‌شوند. سرانجام نتیجه اندازه‌گیری با کدگشایی حالت cat به همراه یک مجموعه از گیتهای $CNot$ و یک گیت هادامارد به دست می‌آید.

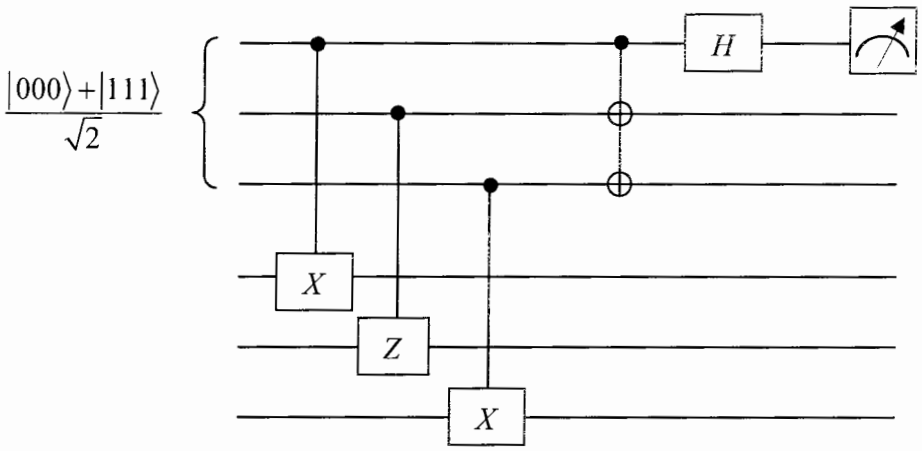
کیوبیت نتیجه 0 یا 1 می‌باشد و به مقدار ویژه‌ی داده، بستگی دارد. این گیتهای نهایی داده را در بر نمی‌گیرند و بدین ترتیب یک خطا در این گیتها به هیچ وجه رویِ داده اثری نمی‌گذارد. اما چه اتفاقی می‌افتد اگر یک خطا در این گیتهای نهایی یک نتیجه اندازه‌گیری ناصحیح بدهد؟ با سه بار تکرار روند اندازه‌گیری و گرفتن رای اکثریت، می‌توانیم تضمین کنیم که احتمال یک خطا در نتیجه اندازه‌گیری $O\left(p^2\right)$ می‌باشد، به طوریکه p احتمال شکست در یک عضو به صورت انفرادی است. ما روشی را توضیح داده‌ایم برای اعمال اندازه‌گیری‌های FT به طوریکه اندازه‌گیری یک نتیجه نادرست با احتمال $O\left(p^2\right)$ را بدهد به طوریکه p احتمال شکست برای اعضا به صورت انفرادی می‌باشد و یک تک شکست در هر جایی در روند، یک خطا روی نهایتا یک کیوبیت در داده کدگذاری شده را سبب شود. این ساختار می‌تواند برای هر مشاهده‌پذیر تک کیوبیتی M که می‌تواند عرضی اجرا شود، به کار می-شود. برای کد اِستین این ساختار شامل گیتهای هادامارد، فاز و پائولی می‌شود. برای اعمال عمل M روی کد اِستین (برای انتخاب مورد نظر)، ما گیتهای $Controlled-ZSX$ را به طور عرضی بین هر جفت از کیوبیتها در کمکی و کد وارد می‌کنیم، به همراه هفت گیت T که به طور عرضی بر کیوبیتهای کمکی اعمال می‌شوند.

۴-۴-۵- اندازه‌گیری مولدهای تثبیت کننده

روند اندازه‌گیری FT، زمانی که M مشاهده‌پذیر کدگذاری شده برای یک تک کیوبیت باشد، را توضیح دادیم و می‌توان این روشها را به حالتهای دیگر نیز تعمیم داد. کافیست قادر باشیم مولدهای تثبیت کننده (که به صورت حاصلضرب تانسوری از ماتریسهای پائولی می‌باشند) را اندازه‌گیری کنیم، یک چنین اندازه‌گیری‌هایی به ما اجازه می‌دهد که تصحیح خطای FT را اعمال کنیم (کدگذاری اولیه برای

کامپیوترهای کوانتومی) و عملگرهای Z کدگذاری شده را برای مرحله بازخوانی نهایی محاسبات اندازه‌گیری کنیم.

به عنوان یک مثال ساده، فرض کنید که می‌خواهیم یک عملگر مثل $X_1Z_2X_3$ را روی ۳ کیوبیت اول یک دسته هفت کیوبیتی کدگذاری شده با استفاده از کد اِستین، را اندازه بگیریم، همانطور که در شکل (۴-۱۹) نشان داده شده است.



شکل (۴-۱۹): روند شماتیک برای اجرای یک اندازه‌گیری FT از عملگر XZX روی سه کیوبیت.

یک بار دیگر ما حالت *cat* بازبینی شده را قبل از اعمال عملهای *Controlled* عرضی، روی داده کدگذاری شده اجرا می‌کنیم، تا به یک روند اندازه‌گیری FT برای عملگر $X_1Z_2X_3$ برسیم. با این توانایی که یکچنین مشاهده‌پذیرهایی را به صورت FT اندازه‌گیری کنیم به طور اتوماتیک قادر خواهیم بود که مراحل کدگذاری، اندازه‌گیری نشانه و اندازه‌گیری در پایه محاسباتی (منطقی) که برای اجرای محاسبات کوانتومی لازم می‌شود را اعمال کنیم. به منظور کدگذاری، برای محاسبه کوانتومی کافیست یک حالت کدگذاری شده $|0\rangle$ را آماده کنیم.

مهمترین موفقیت کدهای تصحیح خطای کوانتومی این است که مشروط بر آنکه نویز در گیتهای کوانتومی به طور انفرادی کمتر از یک مقدار آستانه‌ی ثابتِ مشخص باشد، این امکان وجود دارد تا به طور موثری یک محاسبات کوانتومی جامع اختیاری را اجرا کرده، به عبارت دیگر، نویز در اصل یک مشکل جدی برای محاسبات کوانتومی نمی‌باشد. ایده اساسی در طرح آستانه این است که عملهای FT را به طور مستقیم روی حالتهای کدگذاری شده اعمال کنیم. با قرار دادن مراحل تصحیح خطا که سبب کاهش احتمال خطا از p به $O(p^2)$ می‌شود. با چندین بار تسلسل کدها و ایجاد روندهای FT، احتمال خطا می‌تواند تا $O(p^4)$ و سپس $O(p^8)$ و ... و نهایتا تا حدی که می‌خواهیم کاهش یابد، به شرط آنکه خطای اصلی p از مقدار آستانه‌ی p_{th} کمتر باشد. با به کار بردن این روندها، ما یک آستانه تقریبی $p_{th} \sim 10^{-5} - 10^{-6}$ را تخمین میزنیم.

[۱۹,۱۸,۱۷,۱۶,۱۵,۱۴,۱۳,۱۲,۱۱,۱۰,۶,۵,۴,۳,۱]

فصل پنجم:
نتیجه‌گیری و پیشنهادات

نتیجه‌گیری و پیشنهادات

مدلهای خطایی که مورد بررسی قرار گرفتند، نسبتا ساده هستند و مطمئنا کامپیوترهای کوانتومی واقعی، انواع متنوعی از نویزها و خطاها را تجربه خواهند کرد. با این وجود تکنیکهای معرفی شده در اینجا، زمانی که با کدهای تصحیح خطای کوانتومی پیچیده‌تر و ابزارهای پیچیده‌تر جهت آنالیز مرتبط شوند، آستانه‌ای را برای محاسبه‌ی کوانتومی FT سبب می‌شوند که قابل کاربرد در شرایط متنوع‌تری نسبت به آنچه ما در اینجا توضیح دادیم، می‌باشد.

با توجه به آنچه گفته شد، به نظر می‌رسد در ساخت کامپیوترهای کوانتومی، پرداختن به موارد زیر موثر و مفید می‌باشد.

۱- نتیجه‌ی آستانه به درجه‌ی بالایی از توازی در مدارها نیاز دارد. حتی اگر تنها خواسته‌ی ما ذخیره‌ی اطلاعات کوانتومی در یک حافظه‌ی کوانتومی باشد، این عمل احتیاج به تصحیح خطای مکرر دارد که درجه‌ی بالایی از توازی را در مدارهایمان می‌طلبد. بدین ترتیب، طراحان کامپیوترهای کوانتومی باید ساختارهایی با این قابلیت ، طراحی و ایجاد کنند تا تکنیکهای محاسبه‌ی کوانتومی FT قابل اعمال باشند.

۲- در ارائه‌ی مقدار آستانه، ما کاملا از مقادیر محاسبات و ارتباطات کلاسیکی که در طول آماده-سازی حالت، اندازه‌گیری نشانه و بازیابی انجام شدند، صرفنظر کردیم. این مقادیر، بالقوه می-توانند زیاد باشند. به عنوان مثال، برای انجام عمل بازیابی در بالاترین مراحل از کدهای زنجیره‌ای، نیاز به ارتباط بین همه‌ی قسمتهای سیستم کوانتومی می‌باشد. اگر این ارتباط نتواند سریعتر از زمانی که خطاها در سیستم رخ می‌دهند، انجام پذیرد، در این صورت خطاها شروع به بازگشت می‌کنند و اثر تصحیح خطا را خنثی می‌کنند. لذا یک مقدار ضمیمه در یک آستانه‌ی دقیق‌تر برای محاسبه‌ی کوانتومی وجود دارد.

۳- ساختارهای FT، استفاده از کیوبیتهای کمکی در حالت $|0\rangle$ را سبب می‌شوند. لذا یک منبع ثابت از اینگونه کیوبیتهای کمکی لازم می‌باشد و بدین ترتیب طراحان کامپیوترهای کوانتومی باید ساختارهایی را ایجاد کنند که نه تنها قابلیت توازی دارند، بلکه قادر به پرورش کیوبیتهای کمکی تازه و آماده در یک پایه‌ی معین باشند.

فهرست مراجع

[1] D. Gottesman, *"A theory of fault-tolerant quantum computation,"* (online preprint quant-ph/9702029, 1997).

[2] D. Gottesman, *"Stabilizer codes and quantum error correction,"*. Ph.D. thesis, California Institute of Technology (online preprint quant-ph/9705052, 1997).

[3] M. Nielsen and I. Chuang, *"Quantum Computation and Quantum Information,"* (Cambridge University Press, 2000).

[4] P. W. Shor, *"Fault-tolerant quantum computa- tion,"* Proc. 35th Ann. Symp. on Fundamentals of Computer Science (IEEE Press, Los Alamitos, 1996), pp. 56–65; quant-ph/9605011.

[5] J. Preskill, *"Introduction to Quantum Computation and Information,"*, (World Scientific, New Jersey, 1998).

[6] D. Gottesman, *"fault-tolerant quantum computation."* (online preprint quant-ph/07011120, 2007).

[7] E. Knill and R. Laflamme, *"A theory of quantum error-correcting codes,"* Phys. Rev. A 55 (1997), 900–911; quant-ph/9604034.

[8] A. R. Calderbank and P. W. Shor, *"Good quan- tum error-correcting codes exist,"* Phys. Rev. A 54 (1996), 1098–1105; quant-ph/9512032.

[9] D. Gottesman, *"An Introduction to Quantum Error Correction,"* in *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium* , ed. S. J. Lomonaco, Jr., pp. 221–235 (American Mathematical Society, Providence, Rhode Island, 2002), quant-ph/0004072.

[10] Y. C. Cheng and R. J. Silbey, *"A Study on the Noise Threshold of Fault-tolerant Quantum Error Correction,"* (online preprint quant-ph/0412168).

[11] D. Gottesman, *"Quantum Error Correction and Fault-Tolerance."* (online preprint quant-ph/0507174).

[12] D. Gottesman, *"Fault-Tolerant Quantum Computation with Local Gates."* (online preprint quant-ph/9903099).

[13] J. Preskill, *"Reliable Quantum Computers,"* Proc. Roy. Soc. Lond. A 454 (1998) 385–410, quant-ph/9705031.

[14] P. Aliferis, D. Gottesman, and J. Preskill, *"Quantum Accuracy Threshold for Concatenated Distance-3 Codes,"* Quantum Information and Computation 6, No. 2, 97–165 (2006), quant-ph/0504218.

[15] E. Knill, *"Quantum Computing with Realistically Noisy Devices,"* Nature 434, 39–44 (2005); E. Knill, "Fault-tolerant Postselected Quantum Computation: Schemes," quant-ph/0402171.

[16] B. Reichardt, *"Error-Detection-Based Quantum Fault Tolerance Against Discrete Pauli Noise,"* Berkeley Ph.D. thesis, 1996, quant-ph/0612004.

[17] K. M. Svore, D. P. DiVincenzo, and B. M. Terhal, *"Noise Threshold for a Fault-Tolerant Two-Dimensional Lattice Architecture,"* quant-ph/0604090.

[18] T. Szkopek, P. O. Boykin, H. Fan, V. Roychowdhury, E. Yablonovitch, G. Simms, M. Gyure, and B. Fong, *"Threshold Error Penalty for Fault Tolerant Computation with Nearest Neighbour Communication,"* IEEE Trans. Nano. 5, No. 1, pp. 42–49 (2006), quant-ph/0411111.

[19] A. M. Steane, *"Overhead and noise threshold of fault tolerant quantum error correction,"* Phys. Rev. A 68, 042322 (2003) [19 pages], quant-ph/0207119.

الگوریتم جستجوی کوانتومی گراور

نیکبخت، شهلا؛ شیردل، فاطمه؛ موحدیان، حسین

گروه فیزیک دانشگاه صنعتی شاهرود میدان هفتم تیر، شاهرود

چکیده

الگوریتم جستجوی کوانتومی، این اجازه را می دهد که یک بانک اطلاعاتی نامرتب، در مقایسه با روش کلاسیکی جستجو، در مراحل کمتری جستجو شود. به لحاظ کلاسیکی، جستجوی یک بانک اطلاعاتی نامرتب، مستلزم جستجوی خطی است که تعداد دفعات آن O(N) می باشد. الگوریتم گراور که نیاز به $O(\sqrt{N})$ مرحله دارد. برای جستجوی یک بانک اطلاعاتی نامرتب، سریعترین الگوریتم کوانتومی ممکن می باشد.

Grover Quantum Search Algorithm

Nikbakht, Shahla; Shirdel, Fatemeh ; Movahedian, Hossein
Physics Department, Shahrood University of Technology, Shahrood

Abstract

Quantum search algorithm allows an unsorted database to be searched in fewer steps compared to a classical way of searching. Classically, searching an unsorted database requires a linear search which is O(N) in time. Grover's algorithm which takes $O(\sqrt{N})$ time, is the fastest possible quantum algorithm for searching an unsorted database.

PACS No. ۰۳

مقدمه

جستجو در بانکهای اطلاعاتی بخش مهمی از الگوریتمهای کامپیوتری می‌باشد. با افزایش تعداد رکوردهای بانک اطلاعاتی، سرعت جستجو اهمیت پیدا می کند. به عنوان مثال جستجوهایی که در yahoo ، google و ... صورت می گیرد، امروزه با افزایش web page ها و اطلاعات موجود و با توجه به اینکه کامپیوترهای کلاسیکی سرعت بالایی نمی توانند داشته باشند، چرا که هر بیت آن فقط دو حالت می تواند داشته باشد، دچار مشکل می‌شوند. این مسئله ما را متوجه کامپیوترهای کوانتومی و الگوریتمهای کوانتومی می‌کند. الگوریتمهای کوانتومی این امکان را به ما می دهد که برای جستجو در یک بانک اطلاعاتی تعداد مراحل کمتری نسبت به سایر الگوریتمهای کلاسیکی طی کنیم.

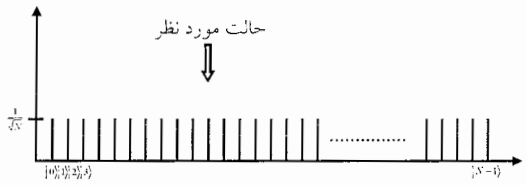
الگوریتم گراور

فرض کنید که یک سیستم n کیوبیتی داریم. در این صورت، این سیستم $N = 2^n$ حالت خواهد داشت که به صورت $S_1, S_2, S_3, ..., S_N$ بر چسب گذاری می‌شوند. اگر تنها یکی از این حالتها مثلا S_m در شرط مورد نظر ما صدق کند، یعنی $C(S_m) = 1$، و برای بقیه حالتها $C(S_i) = 0, i \neq m$، هدف یافتن S_m می‌باشد.

الگوریتمی که برای یافتن حالت مورد نظر (S_m) به کار می رود، الگوریتم کوانتومی گراور است که شامل سه مرحله می باشد:

۱- در ابتدا سیستم باید به صورت برهم نهی از همه حالتها با دامنه‌های برابر نرمالیزه شود. این کار با اعمال ماتریس Walsh Hadamard بر روی حالت اولیه سیستم، یعنی $\psi = |000...000\rangle$ صورت می گیرد(شکل ۱).

$$W_{ij} = 2^{-N/2}(-1)^{i.j} \qquad i, j = 0,1,...,N$$



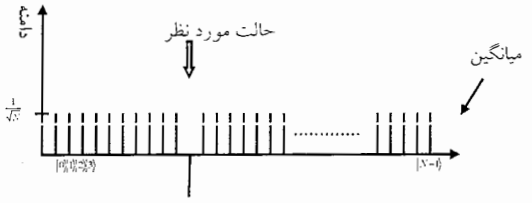
شکل ۱: دامنه حالات سیستم بعد از اعمال ماتریس Walsh Hadamard

۲- دو مرحله زیر را $O(\sqrt{N})$ بار تکرار می کنیم.

الف) اگر C(S)=۱ باشد (یعنی حالت مورد نظر)، در این صورت فاز را به اندازه π می چرخانیم، در غیر این صورت یعنی در حالتی که C(S)=۰ باشد، در آن تغییری ایجاد نمی‌کنیم. این کار توسط اپراتور Oracle انجام می‌شود که به صورت زیر نشان داده میشود:

$$O = \begin{bmatrix} e^{i\phi_1} & 0 & 0 & 0 & 0 & \cdots \\ 0 & e^{i\phi_2} & 0 & 0 & 0 & 0 \\ 0 & 0 & e^{i\phi_3} & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{i\phi_4} & 0 & 0 \\ 0 & 0 & 0 & 0 & e^{i\phi_5} & 0 \\ \vdots & 0 & 0 & 0 & 0 & \ddots \end{bmatrix}$$

پس از اعمال این اپراتور حالت مورد نظر به اندازه π رادیان تغییر فاز پیدا کرده و بقیه حالات بدون تغییر باقی می مانند (شکل۲).



شکل ۲: دامنه حالات سیستم بعد از اعمال اپراتور Oracle

ب) ماتریس پراکندگی(D) را اعمال میکنیم. ماتریس پراکندگی می تواند به صورت ترکیبWRW به کار برده شود که در آن W ماتریس Walsh Hadamard است و R ماتریس چرخش می باشد. ماتریس پراکندگی این ویژگی را دارد که عمل معکوس حول میانگین را انجام می‌دهد، زیرا:

$$R = \begin{bmatrix} 1 & 0 & 0 & & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & & 0 \\ & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\begin{aligned} WRW &= W(2|0\rangle\langle 0| - I)W \\ &= 2W|0\rangle\langle 0|W - WIW \\ &= 2|\psi\rangle\langle\psi| - WIW \\ &= 2|\psi\rangle\langle\psi| - I \end{aligned}$$

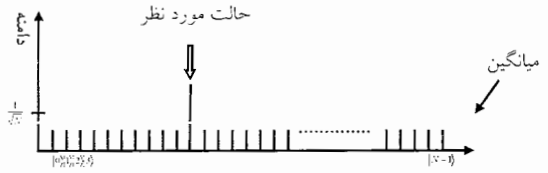
$$(|\psi\rangle\langle\psi|)|\alpha\rangle = \frac{1}{N}\begin{bmatrix} 1 & 1 & 1 & & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & & 1 \\ & \vdots & & \ddots & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \end{bmatrix}$$

$$WRW = 2|\psi\rangle\langle\psi| - I$$

$$WRW|\alpha\rangle = (2|\psi\rangle\langle\psi| - I\sum\alpha_n|n\rangle)$$

$$= \sum(2\bar{a} - \alpha_n|n\rangle)$$

که این همان عمل معکوس حول میانگین می باشد (شکل ۳).



شکل ۳: دامنه حالات سیستم بعد از اعمال ماتریس پراکندگی

۳- سیستم را بررسی می کنیم. حالت مورد نظر با احتمالی بیش از $\frac{۱}{۲}$ به دست خواهد آمد.

مثالی برای یک سیستم ۳ کیوبیتی

ابتدا از یک مثال کلاسیکی شروع می کنیم. فرض کنید که شما ۸ توپ در اختیار دارید. حال بدون اطلاع به دوست خود، یکی از توپها را انتخاب کنید. در اینجا فرض می‌کنیم که شما توپ شماره ۷ را انتخاب کرده‌اید. اکنون از دوست خود بخواهید که بگوید که شما کدام توپ را انتخاب کرده‌اید. او با طرح پرسش‌هایی به شکل زیر به پاسخ مورد نظر دست پیدا می کند. بدین ترتیب:

- آیا توپ انتخابی شما، توپ شماره ۱ است؟
- خیر
- آیا توپ انتخابی شما، توپ شماره ۲ است؟
- خیر
- ⋮
- آیا توپ انتخابی شما، توپ شماره ۷ است؟
- بله

مشاهده می کنیم که برای دستیابی به پاسخ مورد نظر ۷ سوال مطرح شد. مینیمم و ماکزیمم سوال‌هایی که برای یافتن یک توپ مطرح می‌شود به ترتیب ۱ و ۷ سوال می‌باشد، لذا به طور میانگین ٤ سوال برای دست یابی به مورد انتخابی مطرح می شود. اما با به کار بردن الگوریتم کوانتومی گراور تنها با طرح ۲ پرسش به پاسخ مورد نظر دست پیدا می کنیم!

برای یک سیستم ۳ کیوبیتی تعداد کل حالات برابر خواهد بود با $۸ = ۲^۳$. با فرض اینکه حالت مورد نظر(S_m) پنجمین حالت باشد و حالت ها از صفر نامگذاری شده باشند، مراحل ذکر شده در الگوریتم را به ترتیب اعمال می کنیم.

در ابتدای کار با اعمال ماتریس Walsh Hadamard بر روی حالت اولیه، سیستم به صورت برهم نهی از همه حالات در خواهد آمد.

$$W|000\rangle \rightarrow \frac{1}{\sqrt{2^3}}\left(|000\rangle+|100\rangle+|001\rangle+|010\rangle+|110\rangle+|101\rangle+|011\rangle+|111\rangle\right)$$

اپراتورهای Oracle ، Walsh Hadamard و چرخش (R) مورد نیاز برای این سیستم سه کیوبیتی در زیر آمده است:

$$O=\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&-1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{bmatrix}$$

$$W_8=\frac{1}{\sqrt{2^3}}\begin{bmatrix}1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\end{bmatrix}$$

$$R=\begin{bmatrix}1&0&0&0&0&0&0&0\\0&-1&0&0&0&0&0&0\\0&0&-1&0&0&0&0&0\\0&0&0&-1&0&0&0&0\\0&0&0&0&-1&0&0&0\\0&0&0&0&0&-1&0&0\\0&0&0&0&0&0&-1&0\\0&0&0&0&0&0&0&-1\end{bmatrix}$$

که در نهایت ماتریس پراکندگی که در واقع همان WRW است را به شکل زیر خواهیم داشت:

$$D=\begin{bmatrix}-3/4&1/4&1/4&1/4&1/4&1/4&1/4&1/4\\1/4&-3/4&1/4&1/4&1/4&1/4&1/4&1/4\\1/4&1/4&-3/4&1/4&1/4&1/4&1/4&1/4\\1/4&1/4&1/4&-3/4&1/4&1/4&1/4&1/4\\1/4&1/4&1/4&1/4&-3/4&1/4&1/4&1/4\\1/4&1/4&1/4&1/4&1/4&-3/4&1/4&1/4\\1/4&1/4&1/4&1/4&1/4&1/4&-3/4&1/4\\1/4&1/4&1/4&1/4&1/4&1/4&1/4&-3/4\end{bmatrix}$$

با توجه به اینکه سیستم مورد نظر دارای ۸ حالت است، لذا حلقه گراور باید از مرتبه $\sqrt{۸}$ بار(۲ بار) تکرار شود.

پس از یک بار اعمال حلقه گراور خواهیم داشت:

$$C = D \times O(oracle)$$

$$CW_8|000\rangle = \frac{1}{4\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 5 \\ 1 \\ 1 \end{pmatrix}$$

لذا دامنه حالت مورد نظر نسبت به سایر حالات بیشتر می‌شود و در پی آن احتمال این حالت نیز افزایش می یابد. با اعمال مجدد این حلقه خواهیم داشت:

$$(C)^2 W_8|000\rangle = \frac{1}{8\sqrt{2}} \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ 11 \\ -1 \\ -1 \end{pmatrix}$$

مشاهده می کنیم که دامنه حالت مورد نظر به $\frac{11}{8\sqrt{2}}$ افزایش‌یافته و حالت مورد نظر با احتمال ٪۹٤/۵۳ ($(\frac{11}{8\sqrt{2}})^2 = ۰/۹٤۵۳$) که احتمال بسیار بالایی است به دست می‌آید. برای یک سیستم ٤ کیوبیتی نیز با به کاربردن ماتریسهای ۱٦×۱٦ و طی مراحل این الگوریتم، حالت مورد نظر با احتمال ٪۹٦/۱٤ که این نیز احتمال بسیار بالایی است، قابل دستیابی است.

نتیجه گیری

در این مقاله ما الگوریتمهای کلاسیکی و کوانتومی را برای یک بانک اطلاعاتی، با ۸ رکورد اعمال کردیم و مشاهده کردیم که الگوریتم کلاسیکی، بعد از طی به طور میانگین ٤ مرحله با احتمال ٪۵۰ پاسخ مورد نظر را به ما می دهد، در صورتیکه با اعمال الگوریتم کوانتومی گراور بعد از طی ۲ مرحله و با احتمال ٪۹٤/۵۳ که بسیار قابل توجه است، پاسخ مورد نظر به دست می آید که برتری این الگوریتم را نسبت به سایر الگوریتمهای کلاسیکی نشان می دهد.

مراجع

[۱] Michael Nielsen and Isaac Chuang; *"Quantum Computation And Quantum Information"*; 1^{th} edition, Cambridge University Press, ۲۰۰۳.

[۲] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring,* Proceedings, ۳۵ th Annual Symposium on Fundamentals of Comp. Science (FOCS), ۱۹۹٤, pp. ۱۲٤-۱۳٤.

[۳] C.H. Bennett, E. Bernstein, G. Brassard & U.Vazirani, *Strengths and weaknesses of quantum computing*, to be published in the SIAM Journal on Computing.

[٤] L.K. Grover, *A fast quantum mechanical algorithm for estimating the median,* lanl e-print quant-ph/۹٦۰۷۰۲٤.

M. Boyer, G. Brassard, P. Hoyer & A.

[۵] Tapp; *"Tight bounds on quantum searching";* Proceedings, PhysComp ۱۹۹٦ (lanl e-print quant-ph/۹٦۰۵۰۳٤).

Abstract

The future prospects for quantum computing received a tremendous boost from the discovery that quantum error correction is really possible in principle. But this discovery in itself is not sufficient to ensure that a noisy quantum computer can perform reliably. To carry out a quantum error-correction protocol, we must first encode the quantum information we want to protect, and then repeatedly perform recovery operations that reverse the errors that accumulate. But encoding and recovery are themselves complex quantum computations and errors will inevitably occur while we perform these operations. Thus, we need to find methods for recovering from errors that are sufficiently robust to succeed with high reliability even when we make some errors during the recovery step.

Furthermore, to operate a quantum computer, we must do more than just store quantum information; we must process the information. We need to be able to perform quantum gates, in which two or more encoded qubits come together and interact with one another. If an error occurs in one qubit, and then that qubit interacts with another through the operation of a quantum gate, the error is likely to spread to the second qubit. We must design our gates to minimize the propagation of error.

A device that works effectively even when its elementary components are imperfect is said to be fault tolerant. This thesis is devoted to the theory of fault-tolerant quantum computation.