دانشکده فیزیک

پایان نامه کارشناسی ارشد

فیزیک ذرات بنیادی

تصحیح خطای کوانتومی

استاد راهنما:

دکتر حسین موحدیان

ارائه دهنده:

فاطمه شیردل

شهریور ۱۳۸۶

بسم الله الرحمن الرحيم

با تشکر از استاد عزیزم جناب آقای
دکتر موحدیان که مرا در انجام این پروژه
یاری نموده‌اند

چکیده:

در محاسبات کوانتومی برای محافظت از اطلاعات کوانتـومی در برابـر خطاهـای نـویزی، تـصحیح خطای کوانتومی انجام می شود. فرض می کنیم خطاها مستقل هستند و بـا احتمـال p رخ مـی- دهد.

پیتر شر اولین کسی بود که با ذخیره کردن اطلاعـات یـک کیوبیـت در حالـت در هـم تنیـده نـه کیوبیتی کدهای تصحیح خطای کوانتومی را فرمول بندی کرد. کدهای تصحیح خطـای کوانتـومی اطلاعات کوانتومی را در برابر خطاها محافظت می کند.

در تصحیح خطای کلاسیکی نشانه خطا را بـرای مـشخص نمـودن نـوع خطـایی کـه روی حالـت کدگذاری شده رخ داده است، به کار می گیریم. سپس عمل بازیافت را انجام می دهـیم. تـصحیح خطای کوانتومی نیز مشابه مورد کلاسیکی است . ما یک اندازه گیری انجام می دهیم که اطلاعات کوانتومی را در حالت کدگذاری شده، بهم نمی زند.نشانه خطا تعیین می کند که آیا خطـایی روی یک کیوبیت رخ داده است و اگر چنین باشد کدام کیوبیت دچار خطا شده است. در بیـشتر کـدها خطاها یا بیت برگردان است یا فاز برگردان و یا هر دوی آنها (متناظر با ماتریسهای پائولی X و Z و Y).

کدهای CSS نوع وسیعی از کدهای کوانتومی هستند. بهترین کد کوانتومی CSS شناخته شده کد استین است که خطاهای روی یک کیوبیت را تصحیح می کند. اکثر کدهای کوانتومی را می تـوان بر اساس کدهای تثبیت کننده توضیح داد.

بنابراین اگر ما بخواهیم از یک حالت کوانتومی محافظت کنیم وقتـی کـه بخـواهیم آن را از درون یک کانال ارتباطی عبور دهیم، تنها می توانیم حالت را با استفاده از کدهای کوانتومی کد گـذاری کنیم و در نهایت آن را کدگشایی کنیم.

فهرست

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فصل چهارم:تصحیح خطای کوانتومی و کلاسیکی

فهرست اشکال

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

پیشگفتار:

هر کامپیوتر معمولی محاسبات را بر اساس واحد های اطلاعاتی به نام بیت انجام می دهد که می‌تواند مقدار صفر و یا یک داشته باشد. کامپیوتر های کوانتومی از حافظه هایی که بیت کوانتومی یا کیوبیت نامیده می شود، استفاده می کنند.

وقتی که بیت های کلاسیک از یک کانال کلاسیک عبور می کنند همواره ممکن است دچار خطا شوند. این خطا ها هنگام پردازش اطلاعات در یک کامپیوتر کلاسیک نیز می تواند رخ دهند. این اتفاق برای کیوبیت ها نیز می تواند رخ دهد یعنی کیوبیت ها نیز وقتی از یک کانال کوانتومی عبور می کنند ممکن است دچار خطا شوند. یک کامپیوتر کوانتومی وقتی می تواند به خوبی کار کند که بتوانیم خطا های ایجاد شده در کیوبیت ها را آشکار ساخته و تصحیح کنیم .

پژوهش حاضر یک نظریه کامل برای آشکار سازی و تصحیح خطای کوانتومی را مورد بحث و بررسی قرار می دهد.

فصل اول :مبانی مکانیک کوانتومی

۱ـ۱ـ مقدمه

بنابر اصول موضوع نظریه کوانتومی حالت یک سیستم بسته با یک بردار در یک فضای هیلبرت تعیین می شود.این بردار توسط یک عملگر یکانی در طول زمان تحول می یابد و اندازه گیری هر مشاهده پذیر، این بردار را به ویژه بردارهای آن عملگر متناظر با آن مشاهده پذیر تصویر می کند.

در عمل یک سیستم کوانتومی بندرت می تواند از محیط اطراف خود مستقل باشد در بسیاری اوقات نیز، ما نه به کلیت یک سیستم کوانتومی بلکه به اجزای آن علاقمندیم؛ در حالیکه سیستم کوانتومی بسته با یک بردار حالت توصیف می شود، می خواهیم ببینیم که اجزای آن سیستم در چه حالتی هستند و چگونه می بایست آنها را توصیف کرد.

۱-۲- اصول مکانیک کوانتومی

نظریه کوانتومی یک مدل ریاضی از دنیای فیزیکی است، برای آشنایی با این مدل نیاز به تعریف اصول موضوعی مکانیک کوانتومی است.

۱ـ۲ـ۱ـ حالتها :

یک حالت توصیف کاملی از یک سیستم فیزیکی است که به صورت یک بردار در فضای هیلبرت بیان می شود. یک فضای ضرب داخلی را که کامل باشد فضای هیلبرت می نامیم.

۱ـ۲ـ۲ـ مشاهده پذیرها :

یک مشاهده پذیرخاصیت سیستم فیزیکی است که در اصل می تواند اندازه گیری شود. در مکانیک کوانتومی یک مشاهده پذیر عملگر خود الحاقی است؛عملگر یک نگاشت خطی است که بردار رابه بردار تبدیل می کند. اگر عملگر را با A نمایش دهیم و بردار را با $|\psi\rangle$؛($\langle\psi|$ علامت کت دیراک) آنگاه:

$$A:|\psi\rangle \to A|\psi\rangle \qquad (۱-۱)$$

توجه شود اگر اندازه گیری بلافاصله تکرار شود سپس مطابق با این تعاریف همان نتیجه با احتمال یک دوباره بدست می آید.

۱ـ۲ـ۴ـ دینامیک

دینامیک کوانتومی را می توان با اتکا بر اصول و یا فرض های بسیار ساده ای بدست آورد. فرض کنید بردار حالت یک دستگاه کوانتومی درلحظه t را با $|\psi(t)\rangle$ نمایش می دهیم.در اثر هر نوع بر هم کنش این بردار حالت در لحظه t' عبارت خواهد بود از $|\psi(t')\rangle$.

فرض اساسی دینامیک کوانتومی آن است که این بردار حالت جدید را می توان با یک عملگر خطی از بردار حالت قدیمی بدست آورد؛ یعنی :

$$|\psi(t')\rangle = u(t',t)|\psi(t)\rangle \qquad (۹-۱)$$

از آنجا که هر دو بردار باید نرمالیزه باشند این شرط حکم می کند که عملگرها باید یک عملگر یکانی باشد بنابراین :

$$u(t',t)\ u(t',t)' = I \qquad (۱۰-۱)$$

هم چنین با استفاده از دوتحول پی در پی از زمان t تا t' و سپس اززمان t' تا t'' بدست می آوریم.

$$u(t'',t')\ u(t',t) = u(t'',t) \qquad (۱۱-۱)$$

علاوه بر این واضح است که :

$$u(t,t) = I \qquad (۱۲-۱)$$

هر گاه تحول فقط به اندازه زمان بی نهایت کوچکی مثل $\in$ انجام شود می توان $u(t+\in,t)$ را برحسب $\in$ بسط دارد و نوشت :

$$u(t+\in,t) = I - i\in H(t) + O(\in') \approx e^{-i\in H(t)} \qquad (۱۳-۱)$$

عملگر تحول رابرای هر بازه زمانی نوشت؛ خواهیم داشت.

یکانی بودن u الزام می کند که H هرمیتی باشد. حال با استفاده از رابطه (۱ـ۱۰) می توان نوشت:

$$u(t',t) = e^{-i\varepsilon H(t+(N-1)\varepsilon)} e^{-i\varepsilon H(t+(N-2)\varepsilon)} \ldots e^{-i\varepsilon H(t)} \qquad (۱۴-۱)$$

و یا در حد $N \to \infty, \varepsilon \to 0$ با شرط $N\varepsilon = (t'-t)$

$$u(t',t)=\lim_{N\to\infty}\prod_{i=0}^{N-1}e^{-i\varepsilon H(t+i\varepsilon)}=T'\left(e^{-i\int_t^{t'}H(T)dT}\right) \qquad (۱-۱۵)$$

که آخرین عبارت در سمت راست با عبارت نمایی مرتب شده است و به صورت حد طرف چپ تعریف می شود مهمترین حالت خالص، حالتی که H تاریع زمان نباشد. به این صورت همه عبارتهای نمایی با هم جمع می شوند و می توان نمادهای آنها را با هم جمع کرد و نوشت :

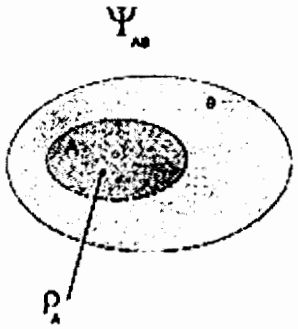
$$u(t',t)=e^{-i(t-t')H} \qquad (۱-۱۶)$$

۱ـ۳ـ ماتریس چگالی [1]

فرض کنید یک سیستم مرکب دو بخشی داریم. فضای هیلبرت سیستم دو بخشی $H_A\otimes H_B$ می باشد که کل سیستم به دو بخش A و B تقسیم شده است.

$$H_{A,B}=H_A\otimes H_B \qquad (۱\_۱۷)$$

به این معنی که اگر $\{|i\rangle_A\}$ یک پایه متعامد برای H_A و $\{|\mu_B>\}$ یک پایه متعامد برای H_B با شد پس $\{|i>_A\otimes|\mu>_B\}$ یک پایه متعامد برای $H_A\otimes H_B$ می باشد.



شکل ۱ـ۱ـ یک سیستم بسته با یک بردار حالت توصیف می شود ولی اجرای آن با یک ماتریس چگالی

در این صورت یک حالت کلی از سیستم AB توسط بردار حالت زیر داده می شود.

$$|\psi\rangle_{AB}=\sum_{i,\mu}a_{i\mu}|i\rangle_A|\mu\rangle_B \qquad (۱\_۱۷)$$

1-Density matrix

که $\sum_{i,\mu} |a_{i\mu}|^2 = 1$ مقدار انتظاری از یک مشاهده پذیر M_A با تعریف $M_A \otimes I_B$ که تنها روی سیستم A اثر می گذارد، (چون M_A یک عملگر خود الحاقی است که تنها روی A اثر می گذارد و I_B عملگر همانی است که روی B اثر می گذارد.) به این صورت است :

$$\begin{aligned}\langle M_A \rangle &= {}_{AB}\langle \psi | M_A \otimes I_B | \psi \rangle_{AB} \\ &= \sum_{j,\nu} a^*_{j\nu} \left({}_A\langle j| \otimes {}_B\langle \nu| \right) \left(M_A \otimes I_B \right) \sum_{i,\mu} a_{i\mu} \left(|i\rangle_A \otimes |\mu\rangle_B \right) \\ &= \sum_{ij\nu} a^*_{j\nu} a_{i\nu} \; {}_A\langle j | M_A | i \rangle_A \\ &= tr(M_A \rho_A)\end{aligned} \qquad (۱-۱۸)$$

$$\begin{aligned}\rho_A &= tr_B \left(|\psi\rangle_{AB} \; {}_{AB}\langle \psi| \right) \\ &= \sum_{i,j,\mu} a_{i\mu} a_{ju}^* \; |i\rangle_A \; {}_A\langle j|\end{aligned} \qquad (۱-۱۹)$$

ρ_A را عملگر چگالی برای سیستم A تعریف می کنیم. که از طریق رد گیری جزئی روی سیستم B برای سیستم مرکب AB به دست آمد.

به این ترتیب هر عنصر ماتریس روی دستگاه A را می توان به صورت $(tr(M\rho))$ نوشت که در آن ρ ازرابطه بالا به دست می آید و جانشین حالت کوانتومی دستگاه A است. به طریق مشابه ماتریس چگالی دستگاه B را با رابطه $\rho_B = tr_A(|\psi\rangle_{AB} \; {}_{AB}\langle\psi|)$ داده می شود.

از تعریف معادله (۱ـ۱۹) می توانیم اشاره کنیم که ρ_A ویژگی های زیر را دارد.

۱ـ ρ_A خود الحاقی است :

$$\rho_A = \rho_A^{\dagger}$$

۲ ـ ρ_A مثبت است، یعنی به ازاء هر ${}_A|\psi\rangle$ داریم :

$${}_A\langle\psi|\rho_A|\psi\rangle_A = \sum_{\mu} \left| \sum_i a_{i\mu} \, {}_A\langle j|i\rangle_A \right|^2 \geq 0$$

۳ـ $tr(\rho_A) = 1$. چون $|\psi\rangle_{AB}$ نرمالیزه است پس

$$tr(\rho_A) = \sum_{i,\mu} |a_{i\mu}|^2 = 1$$

حال که با مفهوم ماتریس چگالی آشنا شدیم می توانیم اصول موضوع مربوط به حالت و اندازه گیری را بدین صورت بیان کرد :

اصل اول : حالت یک سیستم در یک فضای هیلبرت یک ماتریس هرمیتی مثبت با رد واحد است که ماتریس چگالی نامیده می شود و معمولا با ρ نشان داده می شود.

اصل دوم : اندازه گیری تصویری : هر گاه یک اندازه گیری تصویری با عملگر های تصویرگر $\{P_m\}$ روی این حالت انجام دهیم حالت ρ به حالت زیر تبدیل می شود :

$$\rho := \sum_{im} P_m \rho P_m = \sum_{im} p(m)\rho_m \qquad (۲۰\_۱)$$

که $\rho_m = \frac{P_m \rho P_m}{tr(P_m \rho P_m)}$ یک ماتریس چگالی و $P(m) = tr(P_m \rho P_m)$ یک احتمال است؛ معنای این رابطه آن است که عمل اندازه گیری، احتمال به دست آمدن نتیجه m را p(m) بیان می کند. این رابطه در بخشهای بعدی اثبات می شود.

۱-۴-تجزیه اشمیت[1]

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

$$|\psi\rangle_{AB} = \sum_{i\mu} a_{i\mu} |i\rangle_A |\mu\rangle_B = \sum_i |i\rangle_A |\tilde{i}\rangle_B \qquad (۲۱\_۱)$$

که در آن $\{|i\rangle_A\}$ و $\{|\mu\rangle_B\}$ به ترتیب پایه های متعامد H_B و H_A هستند. می توان سیستم کوانتومی را به صورت تجزیه اشمیت به دست آورد که بسیار مفید و سودمند است. در زیر تجزیه اشمیت برای حالت خالص $|\psi\rangle_{AB}$ از سیستم مرکب را بدست می آوریم. برای بدست آوردن تساوی دوم تعریف می کنیم :

$$|\tilde{i}\rangle_B \equiv \sum_\mu a_{i\mu} |\mu\rangle_B \qquad (۲۲\_۱)$$

لازم نست که $|\tilde{i}\rangle_B$ از ابتدا متعامد یا نرمالیزه باشد. فرض می کنیم که $\{|i\rangle_A\}$ طوری انتخاب شده اند که ρ_A در آن پایه ها قطری باشد، یعنی :

---

[1]-Schmidt decomposition

$$\rho_A = \sum_i p_i |i\rangle_{AA}\langle i| \qquad (۲۳\_۱)$$

هم چنین می توان ρ_A را با گرفتن رد[1] جزئی بدست آورد :

$$\rho_A = tr_B\left(|\psi\rangle_{ABAB}\langle\psi|\right) \qquad (۲۴\_۱)$$

$$= tr\left(\sum_{ij}|i\rangle_{AA}\langle i|\otimes|\tilde{i}\rangle_{BB}\langle\tilde{j}|\right) = \sum_{ij}{}_B\langle\tilde{j}|\tilde{i}\rangle_B\left(|i\rangle_{AA}\langle i|\right) \qquad (۲۵\text{-}۱)$$

تساوی قبل را با توجه به این مسأله بدست آوریم که :

$$tr_B\left(|\tilde{i}\rangle_{BB}\langle\tilde{j}|\right) = \sum_K {}_B\langle k|\tilde{i}\rangle_{BB}\langle\tilde{j}|k\rangle_B \qquad (۲۶\text{-}۱)$$

$$= \sum_K {}_B\langle\tilde{j}|k\rangle_{BB}\langle k|\tilde{i}\rangle_B = {}_B\langle\tilde{j}|\tilde{i}\rangle_B$$

که $\{|K_B\rangle\}$ یک پایه متعامد برای H_B است. باقیاس معادلات (۱ــ۲۳) و (۱ــ۲۵) می بینیم که :

$${}_B\langle\tilde{j}|\tilde{i}\rangle_B = P_i\delta_{ij} \qquad (۲۷\text{-}۱)$$

بنابراین ثابت شد که $\{|i\rangle_B\}$ها روی هم رفته متعامد هستند. ما بردارهای متعامد را به صورت زیر باز نویسی می کنیم :

$$|i'\rangle_B = P_i^{-1/2}|i\rangle_B \qquad (۲۸\_۱)$$

(ممکن است فرض کنیم که $P_i \neq 0$)چون ما معادله فوق را تنها برای i های ظاهر شده در معادله ۱ـ۲۳ نیاز داریم، پس بسط زیر را بدست می آوریم :

$$|\psi_{AB}\rangle = \sum_i \sqrt{P_i}|i\rangle_A|i'\rangle_B \qquad (۲۹\_۱)$$

که بر حسب پایه های متعامد ویژه H_B و H_A است. معادله فوق تجزیه اشمیت از حالت خالص $|\psi\rangle_{AB}$ است.

1- trace

به بیان کاملتر می توان تجزیه اشمیت را به صورت زیر بیان کرد :

فرض کنید که $|\psi\rangle_{AB}$ یک حالت خالص از یک سیستم مرکب AB باشد برای $\{|i\rangle_A\}$ و $\{|i\rangle_B\}$ که بردارهای متعامد یکه هستند داریم :

$$|\psi\rangle_{AB} = \sum \lambda_i |i\rangle_A |i\rangle_B \qquad (۳۰\_۱)$$

به طوریکه λ_i ها اعداد حقیقی مثبت هستند که در شرط $\sum \lambda_i^2 = 1$ صدق می کنند و ضرایب اشمیت نامیده می شوند.

۱-۵- خالص سازی[1]

فرض کنید دستگاه A توسط یک ماتریس چگالی ρ توصیف شود، آیا می توان دستگاهی مثل B و حالتی از دستگاه مرکب AB مثل $|\psi\rangle_{AB}$ چنان یافت که :

$$\rho = tr_B(|\psi\rangle_{AB}\ {}_{AB}\langle\psi|)$$

اگر چنین حالتی پیدا کنیم حالت $|\psi\rangle_{AB}$ را حالت خالص شده ماتریس چگالی ρ می خوانیم. برای خالص شده یک ماتریس چگالی ρ_A با ویژه مقدار های ρ_i را پیدا کنیم به این ترتیب عمل می کنیم:

دستگاه B را دستگاهی می گیریم که بعد فضای هیلبرت آن یعنی H_B حداقل با بعد H_A یکی باشد هر گاه بردارهای $\{|i\rangle\}$ یک پایه متعامد برای دستگاه A باشد قرار می دهیم :

$$|\psi\rangle_{AB} = \sum_i \sqrt{P_i}|i\rangle\ |i'\rangle \qquad (۳۱\_۱)$$

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

1-purefication

۱ـ ۶ـ کره بلاخ[1]

کلی ترین حالت یک ذره با اسپین یک دوم و یا هر ذره دیگری که فضای هیلبرت آن دو بعدی است با یک ماتریس چگالی دو در دو داده می شود. این ماتریس را با ρ نشان می دهیم از آنجا که ماتریس های پائولی یک پایه برای فضای ماتریس های دو در دو تشکیل می دهند می توان این ماتریس را به شکل زیر نوشت :

$$\rho = 1/2(r_0 I + \vec{r}.\vec{\sigma}) = 1/2\begin{pmatrix} r_0 + z & x - iy \\ x + iy & r_o - z \end{pmatrix} \qquad (۳۲\_۱)$$

که $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ ماتریس های پائولی هستند؛ ضریب ۱/۲ بیرون کشیده شده است. می بینیم که :

۱ـ ρ هرمیتی است بنابراین ضرایب $\vec{r}, r$ حقیقی هستند.

۲ـ $tr(\rho) = 1$ بنابراین $r_0 = 1$.

۳ـ $\rho \geq 0$.

برای تأمین این شرایط می بایست ویژه مقدار های ρ را حساب کنیم. یک محاسبه ساده بیان می کند که ویژه مقدار های ρ عبارتند از :

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

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

شکل ۱ـ۲ـ کره بلاخ نقاط روی کره متاظر با حالت های خالص و نقاط درون کره متناظر با حالتهای آمیخته هستند.

1-Bloch sphere

بنابراین برای مثبت بودن کافی است که طول بردار $\vec{r}$ کمتر از یک باشد. یعنی $\vec{r} \leq 1$؛ به این ترتیب بین هر ماتریس چگالی و یک نقطه از یک کره به شعاع واحد یک تناظر یک به یک برقرار است. این کره، کره بلاخ نام دارد که در شکل ۱-۲ نشان داده شده است. نقاط روی سطح کره بلاخ نقاطی هستند که در آنها $r = 1$ بنابراین ویژه مقدار ρ برابر با یک و صفر هستند در نتیجه متناظر با حالت های خالص هستند.

در واقع می توان به راحتی نشان داد که هر گاه r=1، یعنی r برابر برداریکه n باشد آن گاه

$$\rho \equiv 1/2\left(I + \hat{n}.\vec{\sigma}\right) \qquad (۳۳\_۱)$$

که در خاصیت زیر صدق می کند.

$$\left(\vec{n}.\vec{\sigma}\right)\rho = \rho\left(\vec{n}.\vec{\sigma}\right) = \rho \qquad (۳۴\_۱)$$

به عنوان مثال پیشنهاد می شود که :

$$\rho = |\psi(\hat{n})\rangle\langle\psi(\hat{n})| \qquad (۳۵\_۱)$$

$\hat{n}$جهت امتدادی است که اسپین up را نشان می دهد؛ از عبارت زیر داریم.

$$|\psi(\theta,\phi)\rangle = \begin{pmatrix} e^{-i\phi/4} & \cos\theta/2 \\ e^{i\phi/2} & \sin\theta/2 \end{pmatrix}$$

$$\rho = |\psi(\theta,\phi)\rangle\langle\psi(\theta,\phi)| = 1/2\begin{pmatrix} \cos\theta/2 & \sin\theta e^{-i\phi} \\ \sin\theta e^{i\phi} & -\cos\theta/2 \end{pmatrix}$$

$$= 1/2(I + \vec{n}.\vec{\sigma})$$

که:

$$\hat{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta) \qquad (۳۶\_۱)$$

می توان (۱ـ۳۳)را بازنویسی کرد و نوشت :

$$\rho \equiv 1/2\left(I + \hat{n}.\vec{\sigma}\right) = |n\rangle\langle n| \qquad (۳۷\_۱)$$

که دران $|n\rangle$حالت یک ذره با اسپین در جهت برداریکه n است؛ از طرف دیگر مرکز کره یعنی r=0 متناظر با حالت کاملا مخلوط[1] ρ =1/2I است. هر چه از مرکز به طرف مرز پیش می رویم به درجه خلوص حالت ها اضافه می شود.

1-mixe

۱ـ۷ـ نکاتی در مورد مجموعه ماتریس های چگالی

یادآوری می کنیم که یک عملگر ρ که روی فضای هیلبرت H اثر می کند به عنوان یک عملگر چگالی تعبیر می شود اگرسه خاصیت زیر را داشته باشد.

۱ـ ρ عملگر خود الحاقی می باشد ۲ـ ρ غیر منفی باشد ۳ـ $tr(\rho)=1$

بلافاصله نتیجه می شود که اگر دو ماتریس چگالی ρ_1 و ρ_2 داشته باشیم می توان یک ماتریس چگالی را به عنوان ترکیب خطی محدب از این دو نوشت :

$$\rho(\lambda)=\lambda\rho_1+(1-\lambda)\rho_2 \qquad (۳۸\_۱)$$

البته بر ازاء هر λ که در شرط $0\le\lambda\le 1$ صدق کند، بر قرار است. به آسانی می بینیم که $\rho(\lambda)$ شرط ۱و۳ را برآورده می کند و ما برقراری شرط ۲ را بررسی می کنیم.

$$\langle\psi|\rho(\lambda)|\psi\rangle=\lambda\langle\psi|\rho_1|\psi\rangle+(1-\lambda)\langle\psi|\rho_2|\psi\rangle\ge 0 \qquad (۳۹\_۱)$$

$\langle\rho(\lambda)\rangle$ غیر منفی است چرا که $\langle\rho_2\rangle$ و $\langle\rho_1\rangle$ این چنین هستند. لذا نشان داده ایم که در یک فضای هیلبرت N بعدی H، عملگرهای چگالی یک زیر مجموعه محدب از فضای برداری ماتریس های هرمیتی N×N می باشند.

به یک زیر مجموعه از یک فضای برداری، محدب گفته می شود اگر مجموعه شامل بخش خطی مستقیم باشد که هر دو نقطه در مجموعه را به هم ارتباط می دهد.

بیشتر عملگرهای چگالی می توانند به عنوان یک مجموع ازعملگرهای چگالی دیگر به طرق مختلف بیان شوند. اما حالات خالص که دراین جا مورد توجهند نمی توانند در نتیجه یک جمع محدب از دو حالت دیگر بیان شوند.

تعریف : در یک زیر مجموعه محدب C از یک فضای برداری یک نقطه، نقطه اکسترمال است اگر نتوان آن را به صورت مجموع محدب دو نقطه از C نوشت.

قضیه: در فضای ماتریس های چگالی یک نقطه، نقطه اکسترمال است اگر و فقط اگر آن نقطه یک حالت خالص باشد.

اثبات: نخست فرض کنید که ρ یک نقطه اکسترمال باشد. حال تجزیه طیفی ρ را می نویسیم که بر مبنای آن :

$$\rho = \sum_i \lambda_i |i\rangle \langle i|$$

از آنجا که ρ یک نقطه اکسترمال است این امر بدان معناست که یکی از λ ها برابر با ۱ و بقیه برابر با صفرند و این چیزی نیست جز بیان خالص بودن ρ.

برعکس، ρ یک حالت خالص مثل $|\psi\rangle \langle\psi|$ باشد، نشان می دهیم که نمی توانیم این حالت را به صورت مجموع محدب دو ماتریس چگالی دیگر نوشت و به همین معنا واقعا این حالت، یک حالت خالص است. ازبرهان خلف استفاده می کنیم، فرض می کنیم که بتوان نوشت :

$$|\psi\rangle \langle\psi| = \lambda\rho_1 + (1-\lambda)\rho_2 \qquad (۴۰-۱)$$

حال بردار مثل $|\psi_\perp\rangle$ را در نظر گرفته که بر بردار $|\psi\rangle$ عمود است. پس $\langle\psi_\perp|\psi\rangle = 0$ داریم :

$$\langle\psi_\perp|\psi\rangle \langle\psi|\psi_\perp\rangle = 0 = \lambda\langle\psi_\perp|\rho_1|\psi_\perp\rangle + (1-\lambda)\langle\psi_\perp|\rho_2|\psi_\perp\rangle \qquad (۴۱\_۱)$$

از آنجا که سمت راست تساوی، مجموع دو جمله غیر منفی است و با توجه به اینکه مجموع صفر شده است لذا هر دو جمله باید صفر باشند، اگر λ مخالف صفر یا یک باشد نتیجه می گیریم که ρ_1 و ρ_2 بر $|\psi_\perp\rangle$ عمود هستند اما از آنجا که $|\psi_\perp\rangle$ می تواند هر برداری عمود بر $|\psi\rangle$ باشد لذا باید :

$$\rho_1 = \rho_2 = \rho \qquad (۴۲-۱)$$

نشان دادیم که حالت خالص نقاط اکسترمال مجموعه ای از ماتریس های چگالی هستند به علاوه تنها نقاط خالص نقاط اکسترمال هستند زیرا هر حالت ترکیبی می تواند به صورت $\rho = \sum_i \rho_i |i\rangle \langle i|$ بر این اساس که قطری است نوشته شود و بنابراین یک جمع محدب از حالات خالص است.

حال به مرز مجموعه ماتریس های چگالی نگاه می کنیم. این مرز جایی است که یکی یا بیشتر از ویژه مقدارهای ماتریس چگالی صفر می شود. زیرا بیرون ازاین مرز، جایی است که ماتریس های هرمیتی ولی منفی قرار گرفته اند.

درکره بلاخ نقاط اکسترمال نقاطی هستند که روی مرز کره هستند و این خاصیت مختص ۲ بعد است. بنابراین مثال در سه بعد یک ماتریس چگالی که تجزیه طیفی آن برابر با $\rho = 1/2(|1\rangle\langle 1| + |2\rangle\langle 2|)$ است، روی مرز قرار دارد ولی یک حالت خالص نیست.

۱ـ۸ـ آنسامبلهای حالت کوانتومی

یک آنسامل خالص اجتماعی از سیتمهای فیزیکی است به گونه ای که همه اعضاء آن با کت یکسان $|\psi\rangle$ مشخص می شوند؛ به عکس در یک آنسامبل آمیخته کسری از اعضاء با جمعیت نسبی ρ_1 با $|\psi^{(1)}\rangle$ مشخص می شود و کسر دیگری با جمعیت نسبی ρ_2 با $|\psi^{(2)}\rangle$ و...، که آنسامبل آمیخته نام دارد، جمعیت های نسبی مقیدند که در شرط بهنجارش زیر صدق می کند:

$$\sum_i \rho_i = 1 \qquad (۴۳\text{ـ}۱)$$

زبان عملگر چگالی شکل مناسب برای توصیف سیستم های کوانتومی که حالات آنها به طور کامل شناخته شده نیست؛ ایجاد می کند.

فرض کنید یک سیستم کوانتومی دریکی از حالات $|\psi_i\rangle$ باشد با احتمالات p_i ما می توانیم $\{P_i|\psi_i\rangle\}$ را یک آنسامبل از حالتهای خالص بنامیم عملگرچگالی برای سیستم با معادله زیر مشخص می شود.

$$\rho \equiv \sum_i p_i|\psi_i\rangle\ \langle\psi_i| \qquad (۴۴\text{-}۱)$$

حالات چنین دستگاهی به جای اینکه با بردار حالت مشخص شود با یک ماتریس چگالی مشخص شد. این ماتریس چگالی در بردارنده تمام اطلاعاتی است که ما می توانیم از دستگاه کوانتومی کسب کنیم.

دقت شود که معادله (۱ـ۴۴) یک تجزیه طیفی نیست و به همین دلیل بردارهای $|\psi_i\rangle$ یک مجموعه متعامد تشکیل نمی دهند و تعداد آنها هیچ ربطی به بعد ماتریس ندارد.

حال ببینیم فرضیات مکانیک کوانتومی بر حسب عملگر چگالی چگونه بیان می شود.

برای مثال فرض کنید که تحول یک سیستم کوانتومی بسته با عملگر یونیتاری u توصیف می شود. اگر سیستم در ابتدا در حالت $|\psi_i\rangle$ با احتمال p_i باشد بدین ترتیب تحول عملگر با معادله زیر توصیف می شود.

$$\rho \equiv \sum p_i|\psi_i\rangle\langle\psi_i| \to \sum p_i u|\psi_i\rangle\langle\psi_i|u' = u\rho u' \qquad (۴۵\text{-}۱)$$

اندازه گیریها نیز به آسانی به زبان عملگر چگالی توصیف می شود. فرض کنید ما یک اندازه گیری توسط عملگرهای اندازه گیری M_m اعمال می کنیم. اگر حالت اولیه $|\psi_i\rangle$ باشد در این صورت اعمال گرفتن نتیجه m است.

$$p(m|i) = \langle \psi_i | M_m^\dagger M_m | \psi_i \rangle = tr\left(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\right) \qquad (۴۶-۱)$$

و با استفاده از قانون جمع احتمالها، احتمال به دست آوردن نتیجه m خواهد شد:

$$\begin{aligned} p(m) &= \sum p(m|i) p_i \\ &= \sum p_i tr\left(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\right) \\ &= tr\left(M_m^\dagger M_m \rho\right) \end{aligned} \qquad (۴۷-۱)$$

حال می خواهیم ببنیم بعد از اعمال اندازه گیری عملگر چگالی چه خواهد شد :

اگر حالت اولیه $|\psi_i\rangle$ باشد بعد از به دست آوردن نتیجه m داریم:

$$|\psi_i^m\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}} \qquad (۴۸-۱)$$

بدین ترتیب بعد از یک اندازه گیری که نتیجه m را می دهد، ما یک آنسامبل از حالات $|\psi_i^m\rangle$ با احتمالات $P(i|m)$ داریم. عملگر چگالی مطابق با آن که با ρ_m بیان می شود بدین ترتیب خواهد بود :

$$\rho_m = \sum p(i|\ m)|\psi_i^m\rangle\langle\psi_i^m| = \sum P(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger M_{mm}|\psi_i\rangle} \qquad (۴۹-۱)$$

با استفاده از قضیه احتمالات بنیادی که بیان می کند :

$$p(i|m) = \frac{p(m|i)p_i}{p(m)} \qquad (۵۰-۱)$$

و با جانشینی معادلات (۱ـ۴۷)ـ (۱ـ۴۸) داریم:

$$\rho_m = \sum p_i \frac{M_{im}|\psi_i\rangle\langle\psi_i|M_m'}{tr\left(M_{im}'M_{im}\rho\right)} = \frac{M_{im}\rho M_m'}{tr\left(M_m'M_m\rho\right)} \qquad (۵۱\_۱)$$

حالت ρ یک حالت خالص است اگر و فقط اگر $tr\left(\rho^2\right)=1$ در حالیکه برای حالت آمیخته $tr\left(\rho^2\right)<1$ می باشد.

۱-۹- ارتباط آنسامبلهای مختلف

اصل موضوع اندازه گیری به ما می گوید که اندازه گیر ی یک حالت کوانتومی (حتی حالت خالص) را معمولا به یک حالت آمیخته تبدیل می کند، یعنی در اثر اندازه گیری $\{p_m\}$ حالت $|\psi\rangle$ تبدیل به حالت مخلوط $\rho = \sum_m p_m|\psi\rangle\langle\psi|p_m$ می شود. بنابراین ساده ترین راه برای تهیه حالت های مخلوط از حالت های خالص انجام یک عمل اندازه گیری است. برای درک ارتباط بین آنسامبلهای مختلف یا به عبارت دیگر تجزیه های متفاوت از یک ماتریس چگالی، ماتریس چگالی را به صورت زیر می نویسیم:

$$\rho = \sum_{i=1}^{N} \lambda_i|\psi_i\rangle\langle\psi_i| = \sum_{i=1}^{N}|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| \qquad (۵۲-۱)$$

$$|\tilde{\psi}_i\rangle = \sqrt{\lambda_i}|\psi_i\rangle \qquad (۵۳-۱)$$

که حالت های غیر بهنجار است. با قضیه زیر ارتباط زیر بین آنسامبلها را بیان میکنیم.

قضیه : فرض کنید که یک حالت ρ به صورت زیر تجزیه می شود.

$$\rho = \sum_{i=1}^{n}|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{j=1}^{N}|\tilde{Q}_j\rangle\langle\tilde{Q}_j| \qquad (۵۴-۱)$$

که در آن تعداد بردارهای هر دو آنسامبل را یکی گرفتیم چون همواره با افزودن احتمالات برابر با صفر، تعداد بردارهای به کار رفته در دو آنسامبل را مساوی گرفت.

در این صورت حتما یک ماتریس یکانی u وجود دارد به طوری که:

$$|\tilde{\psi}_i\rangle = \sum_{j=1}^{N} u|\tilde{Q}_i\rangle \qquad (۵۵-۱)$$

بالعکس، فرض کنید شرط فوق برقرار است آن گاه مخلوط هـای ناشـی از ایـن دو آنـسامبل یکـی است.

اثبات: نخست قسمت دوم قضیه را ثابت می کنیم، می نویسیم :

$$\rho = \sum_{i=1}^{N} |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{i,j,k=1}^{N} u_{ij}u_{jk}^{*}|\tilde{Q}_j\rangle\langle\tilde{Q}_j|$$

$$= \sum_{j,k} \delta_{j,k}|\tilde{Q}_j\rangle\langle\tilde{Q}_k|$$

$$= \sum_{j=1}^{N}|\tilde{Q}_j\rangle\langle\tilde{Q}_j| \qquad (۵۶-۱)$$

حال قسمت اول را اثبات می کنیم :

می دانیم که ρ یک تجزیه طیفی دارد یعنی

$$\rho = \sum_{r=1}^{n} k_r|k_r\rangle\langle k_r| = \sum_{r=1}^{n}|\tilde{k}_r\rangle\langle\tilde{k}_r| \qquad (۵۷-۱)$$

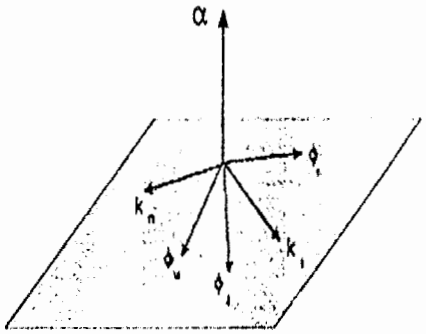
که در آن $\{|\tilde{k}_r\rangle, r = 1.....n\}$ها یک پایه متعامد ولی نه لزوما یکه را تشکیل می دهد. بـاز هـم در این جا می توان بعد n را مساوی N گرفت، به این معنی که اگر $N \le n$ باشد با افزودن وزن های صفر به آنسامبلها این کـار را مـی کنـیم. و اگـر $N\langle n$ باشـد بردارهـای $|k_n\rangle$,....,$|k_{n+1}\rangle$ را بـا ویـژه مقدارهای صفر به تجزیه طیفی اضافه می کنیم.

حال بردارهای مثل $|\alpha\rangle$ را در نظر می گیریم که بر بردارها ی $|k_r\rangle$ عمود باشد در این صورت

$$0 = \sum_{r}\langle\alpha|\tilde{k}_r\rangle\langle\tilde{k}_r\|\alpha\rangle = \sum_{i}\langle\alpha|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|\alpha\rangle \qquad (۵۸-۱)$$

از این رابطه نتیجه می گیریم که بردار $\langle\alpha|$ برهمه بردارهای $|\tilde{\psi}_i\rangle$ عمود است.

با استدلال مشابه نتیجه میگیریم که هر برداری که بر بردارهای $|\tilde{\psi}_i\rangle$ عمودباشد. بر بردارهای $|\tilde{k}_r\rangle$ عمود اسـت بنـابراین بردارهـای $\langle\tilde{\psi}_i|$ و بردارهـای $|\tilde{k}_r\rangle$ در یـک صـفحه قراردارنـد و مـی تـوان بردارهای $\langle\tilde{\psi}_i|$ را برحسب بربردارهای $|\tilde{k}_r\rangle$ بسط داد :



شکل ۱-۳-هر برداری مثل $|\alpha\rangle$ که بر بردارهای $|k\rangle$ عمود باشد بر بردارهای $|\phi\rangle$ نیز عمود است.
پس $|k\rangle$ و $|\phi\rangle$ در یک صفحه هستند.

$$|\tilde{\psi}_i\rangle = \sum_{r=1}^{n} u_{ir}|\tilde{k}_r\rangle \qquad (۱\_۵۹)$$

می توان همین استدلال را در مورد $|Q_j\rangle$ هم نوشت:

$$|\tilde{Q}_j\rangle = \sum_{r=1}^{n} V_{jr}|\tilde{k}_r\rangle \qquad (۱\_۶۰)$$

$$\rho = \sum_{i=1}^{n} |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{j=1}^{n} |\tilde{Q}_j\rangle\langle\tilde{Q}_j| = \sum_{r=1}^{n} |\tilde{k}_r\rangle\langle\tilde{k}| \qquad (۱-۶۱)$$

$$vv^{\dagger} = I \text{ و } uu^{\dagger} = I$$

با توجه به یکانی بودن ماتریس های می توان از روابط ۱ــ۵۹ و ۱ــ۶۰ نوشت:

$$|\tilde{\psi}_i\rangle = \sum_{r=1}^{n} (uv^{\dagger})_{ij}|\tilde{Q}_j\rangle \qquad (۱\_۶۲)$$

و این همان چیزی که می خواستیم ثابت کنیم.

۱۰ــ۱ــ قضیه GHJW

قضیه GHJW بیان می کند تمام آنسامبل های مختلف را می توان با اندازه گیریهای مناسب بدست آورد. نام این قضیه از نام کاشفان آن یعنی Jozsa و Huns و Gisin و Notters گرفته شده است.

ماتریس چگالی ρ_A را در نظر بگیرید.

$$\rho_A = \sum p_i |\varphi_i\rangle_A \langle\varphi_i| \qquad , \qquad \sum P_i = 1$$

با توجه به تعریف خالص سازی خواهیم داشت.

$$|\varphi_i\rangle_{AB} = \sum \sqrt{p_i} |\varphi_i\rangle_A |\alpha_i\rangle_B \qquad (۶۳\_۱)$$

که بردار $|\alpha_i\rangle_B$ پایه متعامد برای سیستم B در فضای هیلبرت H_B است که دو به دو برهم عمودند و نرمالیزه هستند یعنی

$$_B\langle\alpha_i|\alpha_j\rangle_B = \delta_{ij} \qquad (۶۴\_۱)$$

در این صورت واضح است که :

$$tr_B(|\varphi_i\rangle_{AB\ AB}\langle\varphi_i|) = \rho_A \qquad (۶۵\_۱)$$

بطور کلی تر بحث می کنیم.

ماتریس چگالی ρ_A و دو آنسامبل مختلف از آن را به صورت زیر در نظر می گیریم.

$$\rho_A = \sum_{\mu=1}^{M} P_\mu |\varphi_\mu >< \varphi_\mu| \qquad (۶۶\_۱)$$

$$\rho_A = \sum_{\nu=1}^{N} P_\nu |\psi_\nu\rangle\langle\psi_\nu| \qquad (۶۷\_۱)$$

با خالص سازی برای این دو عملگر خواهیم داشت.

$$|E_1\rangle = \sum_{\mu=1}^{M} \sqrt{p_\mu} |\varphi_\mu\rangle |\alpha_\mu\rangle$$

$$|E_2\rangle = \sum_{\mu=1}^{M} \sqrt{q_\mu} |\psi_\mu\rangle |\beta_\mu\rangle \qquad (۶۸-۱)$$

طوری که

$$\rho_A = tr_B(|E_1\rangle\langle E_1|) = tr_B(|E_2\rangle\langle E_2|) \qquad (۶۹\_۱)$$

$$\langle\alpha_\mu|\alpha_\nu\rangle = \langle\beta_\mu|\beta_\nu\rangle = \delta_{\mu,\nu} \qquad (۷۰\_۱)$$

تجزیه اشمیت حالتهای فوق به صورت زیر است.

$$|E_1\rangle = \sum_{i=1}^{n} \sqrt{\lambda_i} |K_i\rangle |\tilde{k}_i\rangle$$

$$|E_2\rangle = \sum_{i=1}^{n} \sqrt{\lambda} |K_i\rangle |K_i'\rangle \qquad (۷۱\_۱)$$

که در آن $|K_i\rangle$ ها ویژه بردارهای ρ_A و n بعد این ماتریس است. هم چنین $|\tilde{k}_i\rangle$ ها یک پایه متعامد یکه برای فضای B، $|K_i'\rangle$ یک پایه متعامد دیگر برای همان فضای B هستند.

چگونه می توان $|E_1\rangle$ و $|E_2\rangle$ را به هم ربط داد؛ در حقیقت به آسانی می توان نشان داد:

$$|E_2\rangle = (I \otimes U_B)|E_1\rangle \qquad (۷۲ \_ ۱)$$

U_B ماتریس یکانی است، با توجه به رابطه فوق در رابط (۱ـ ۶۸) داریم.

$$\sum_{\mu=1}^{M} \sqrt{q_\mu} |\psi_\mu\rangle |\beta_\mu\rangle = \sum_{\mu=1}^{M} \sqrt{P_\mu} |\varphi_\mu\rangle |(U_B|\alpha_\mu\rangle) \qquad (۷۳ \_ ۱)$$

رابط فوق بیان می کند اگر یک بار اندازه گیری در پایه $|\beta_\mu\rangle$ انجام شود آنسامبل اول و اگر روی همان حالت خالص اندازه گیری در پایه $|\gamma_M >= U_B|\alpha_\mu >$ انجام شود آنسامبل دوم را بدست می آوریم، یعنی تمام آنسامبلهای مختلف را می توان با اندازه گیری در پایه های مختلف بدست آورد.

۱۱ـ۱ـ تحول عملگر چگالی

فرض می کنیم که هامیلتونی روی $H_A \otimes H_B$ به شکل زیر داده شود.

$$H_{AB} = H_A \otimes I_B + I_A \otimes H_B \qquad (۷۴\_۱)$$

تحت این فرضیات، هیچ جفت شدگی بین دو سیستم A و B وجود ندارد طوری که هر کدام بطور مستقل از همند، عملگر تحول زمانی برای سیستم ترکیب شده بصورت زیر تعریف می شود.

$$U_{AB}(t) = U_A(t) \otimes U_B(t) \qquad (۷۵\_۱)$$

که به دو عملگر تحول زمانی یونیتاری که روی هر سیستم جداگانه عمل می کند تقسیم شده است.

در تصویر شرودینگری دینامیک،حالت خالص اولیه $|\psi(0)\rangle_{AB}$ از سیستم دو بخشی داده شده است که توسط معادله

$$|\psi\rangle_{AB} = \sum_{i,\mu} a_{i\mu} |i\rangle_A |\mu\rangle_B \qquad (۷۶\_۱)$$

به شکل زیر ظاهر می شود :

$$|\psi(t)\rangle_{AB} = \sum_{i,\mu} a_{i\mu} |i(t)\rangle_A \otimes |\mu(t)\rangle_B \qquad (۷۷\_۱)$$

که.

$$|i(t)>_A = U_A(t)|i(0)>_A \qquad (۷۸\_۱)$$

$$|\mu(t)\rangle_B = U_B(t)|\mu(0)\rangle_B \qquad (۷۹\_۱)$$

پایه های متعامد جدید برای H_A و H_B تعریف می کنیم (چون $U_A(t)$ و $U_B(t)$ یونیتاری هستند) با گرفتن رد جزئی پیدا می کنیم.

$$\rho_A(t) = \sum_{ijM} a_{i\mu} a^*_{jr} |i(t)\rangle_{AA}\langle j(t)| = U_A(t)\rho_A(0)U_A(t)' \qquad (۸۰\_۱)$$

در پایه ای که $\rho_A(0)$ قطری است داریم :

$$\rho_A(t) = \sum_a P_a u(t)|\psi_a(0)>_{AA}<\psi_a(0)|U_A(t) \qquad (۸۱\_۱)$$

رابطه فوق بیان می کند که اگر هر حالت $|\psi_a(0)\rangle$ با احتمال P_a در زمان صفر اتفاق نیفتد پس $|\psi_a(t)\rangle$ با احتمال P_a در زمانهایی از t اتفاق می افتد.

واضح است که معادله فوق تنها در صورتی به کاربرده می شود که ما فرض کردیم که هامیلتونین سیستم ها به صورت هاملیتونین جفت نشده بیان شد.

۱۲ـ۱ـ موضعیت[1]

نتیجه یا احتمال یک نتیجه اندازه گیری که روی قسمتی از یک سیستم مرکب با حالت λ (سیستم A +سیستم B) انجام می شود مستقل از جنبه های مولفه های قسمت های دیگر است که آزمایشگر برای اندازه گیری انتخاب می کند. این به هیچ وجه به این معنی نیست که نتوان با بررسی سیستم A اطلاعاتی در مورد سیستم B بدست آورد.

حالت λ شامل اطلاعات مشترک مربوط به هر دو سیستم است و اندازه گیری روی یکی از این سیستم ها بخشی از این اطلاعات را آشکار می سازد.

1-locality

هم چنین اگر یک اندازه گیری روی یک قسمت از سیستم مرکب انجام شود باعث اغتشاش موضعی آن قسمت می گردد و این با موضعیت مغایرتی ندارد.

انچه که موضعیت بیان می کند اساساً این است که مقدار اندازه گیری شده یک کمیت در یک سیستم به طور علی نمی تواند متاثر از اندازه گیری یک کمیت روی سیستم دیگر باشد زیرا که وقتی اندازه گیری انجام می شود فاصله سیستم ها فضا گونه است.

۱۳ـ۱ـ کیوبیت [1]

واحد بخش ناپذیر اطلاعات کلاسیکی بیت[2] است که یکی از دو مقدار ممکن {۱ و ۰ } را می گیرد. واحد متناظر برای اطلاعات کوانتومی را بیت کوانتومی یا کیوبیت نامند که یک حالت در ساده ترین شکل ممکن از سیستم کونتومی را توصیف می کند کوچکترین فضای هیلبرت بهنجار، دو بعدی است؛ ممکن است پایه متعامد برای یک فضای برداری دو بعدی را مثل $\{|0\rangle,|1\rangle\}$ نشان دهیم، پس کلی ترین حالت بهنجار به صورت زیر بیان می شود.

$$a|0\rangle + b|1\rangle \qquad (۸۲\_۱)$$

که a و b اعداد مختلطی هستند که در رابطه $|a|^2 + |B|^2 = 1$ صدق می کنند یک کیوبیت حالتی دو بعدی در فضای هیلبرت است که می تواند هر مقدار از معادله (۱ـ۸۲) را بگیرد.

ما می توانیم یک اندازه گیری که کیوبیت را درون پایه های $\{|0\rangle,|1\rangle\}$ نشان می دهد، انجام دهیم که نتیجه $|0\rangle$ را با احتمال $|a|^2$ و نتیجه $|1\rangle$ را با احتمال $|b|^2$ بدست می آوریم بعلاوه به جز در مواردی که a=0 و b=0 باشد قطعاً اندازه گیری حالت را برهم می زند.

اگر در ابتدا مقدار کیوبیت را نمی دانیم هیچ راهی برای تعیین a و b تنها با یک اندازه گیری وجود ندارد با وجود این بعد از اندازه گیری، کیوبیت در یک حالت معلوم ـ یا $|0\rangle$ یا $|1\rangle$ -آشکار شده است که از حالت قبلیش متفاوت است.

از این روی، کیوبیت از بیت کلاسیکی متفاوت است، یک بیت کلاسیکی را بدون برهم زدن حالت سیستم می توان اندازه گیری کرد؛ فرض کنید که یک بیت کلاسیکی حقیقتاً یک مقدار معین (۰

1-qubit
2-bit

یا ۱) را دارد ولی این مقدار در آغاز برای ما معلوم نیست، بر اساس اطلاعات در دسترس تنها می توان گفت که احتمال آنکه بیت مقدار ۰ را بگیرد p و احتمال آنکه بیت مقدار ۱ را بگیرد P_1 است طوریکه $p_0 + p_1 = 1$ می باشد. وقتی بیت اندازه گیری می شود اطلاعات اصلی بدست می آید که بعداً مقدار آن را با ۱۰۰٪ اطمینان می گوییم.

برای فیزیکدانان عادی است که معادله (۱۱ـ ۸۲) را به عنوان حالت اسپینی یک شی ء با اسپین ۱/۲ تعبیر کند (مثل یک الکترون) که $|1\rangle$ و $|0\rangle$ حالتهای اسپینup $|\uparrow\rangle$ و اسپین down $|\downarrow\rangle$ در امتداد یک محور خاص مثل z می باشند. بنابراین مجازیم یک کیوبیت را به عنوان حالتی از شی ء با اسپین ۱/۲ انتخاب کنیم.

$$|\downarrow z\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad , \quad |\uparrow z\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad (۸۳\_۱)$$

که در روابط ارتونرمالی زیر صادق هستند.

$$\langle\uparrow|\uparrow\rangle = \langle\downarrow|\downarrow\rangle = 1 \qquad (۸۴\_۱)$$

$$\langle\uparrow|\downarrow\rangle = 0 \qquad (۸۵\_۱)$$

حال اگر در امتداد محور x ها اندازه گیری انجام شود خواهیم داشت.

$$|+\rangle = {}^{1}\!/_{\sqrt{2}}(|0\rangle + |1\rangle) \Rightarrow |\uparrow_x\rangle = {}^{1}\!/_{\sqrt{2}}\left(|\uparrow_z\rangle + |\downarrow_z\rangle\right) \qquad (۸۶\_۱)$$

$$|-\rangle = {}^{1}\!/_{\sqrt{2}}(|0\rangle - |1\rangle) \Rightarrow |\downarrow_x\rangle = {}^{1}\!/_{\sqrt{2}}\left(|\uparrow_z\rangle - |\downarrow_z\rangle\right) \qquad (۸۷\_۱)$$

برای هر کدام از این حالتها اگر اندازه گیریمان در امتداد محور z ها باشد با احتمال ۱/۲، $|\uparrow_z\rangle$ را بدست خواهیم آورد و با احتمال ۱/۲ ، $|\downarrow_z\rangle$ را بدست خواهیم آورد.

معادله (۱ـ۸۲) می تواند توصیف کننده سیستم دو حالته پلاریزاسیون نور باشد که در آن ۲ قطبش ممکن(۰)، عمودی ۹۰°) و (۴۵°، ۱۳۵°) معادل حالتهای اسپینup $|\uparrow\rangle$ و اسپین down $|\downarrow\rangle$ را به عنوان پایه های قطبش در نظر می گیریم.

۱۴ـ۱ـ نمایش کره بلاخ برای تک کیوبیت

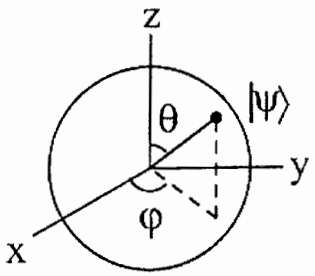
حالت زیر را برای نمایش تک کیوبیت در نظر می گیریم.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (۸۸-۱)$$

چون $|a^2| + |B|^2 = 1$ می توان پارامتر بندی زیر را انجام داد.

$$\alpha = \cos\theta/2 \qquad B = e^{i\varphi}\sin\theta/2 \qquad (0 \le \theta < \pi, 0 \le \varphi < 2\pi) \qquad (۸۹ـ۱)$$

زوایای θ و φ، زوایای قطبی و سمتی یک نقطه روی کره واحد هستند که در شکل نمـایش داده شده است.



شکل ۱ـ۴ ـ این نمایش کره بلاخ برای تک کیوبیتی می باشد.

حالتهـای پایـه محاسـباتی $|0\rangle, |1\rangle$ بـه ترتیـب بـا قطـب شـمال و جنـوب کـره نـشان داده می شوند. گیتهای[1] تک کیوبیتی با تبدیلات روی کـره بـلاخ متنـاظر هـستند، بـرای مثـال گیـت $X(NOT)$و گیت Z با چرخش π درجه حول محور x و حول محور z متناظرند.

ماتریس چگالی برای تک کیوبیت بصورت زیر نمایش داده می شود.

$$\rho = \frac{1}{2}(I + \vec{r}.\vec{\sigma}) \qquad (۹۰ـ۱)$$

I ماتریس واحد 2 × 2 است و σ ماتریس پائولی است و r یک بردار اختیاری است.

1-gate

۱۵ـ۱ـ درهم تنیدگی[1]

به هر حالت خالص $|\psi\rangle_{AB}$ برای سیستم مرکب متشکل از دو قسمت A+B، ممکن است ما یک عدد اشمیت حقیقی مثبت نسبت دهیم که این عدد تعداد مقادیر ویژه غیر صفر در ρ_A (یا ρ_B) می باشد. بنابراین تعداد جملات در تجزیه اشمیت از $|\psi\rangle_{AB}$ برحسب این عدد می باشد، می خواهیم معنی یک سیستم خالص دو طرفه درهم تنیده را بدانیم :

بنا به تعریف تجزیه اشمیت داشتیم :

$$|\psi_{AB}\rangle = \sum_i \lambda |i\rangle_A |i\rangle_B$$

$|\psi\rangle_{AB}$ یک حالت درهم تنیده است در صورتی که عدد اشمیت λ، بزرگتر از یک باشد و در غیر این صورت درهم تنیده می باشد.

بنابراین یک حالت خالص دو ذره ای را می توان به صورت حاصلضرب تانسوری مستقیم در فضاهای H_A و H_B به صورت زیر نمایش داد.

$$|\psi\rangle_{AB} = |\varphi\rangle_A \otimes |\chi\rangle_B \qquad (۹۱\_۱)$$

پس ماتریسهای چگالی تحول یافته ρ_A و ρ_B خالص هستند و شکل زیر را دارند.

$$\rho_A = |\varphi>_{AA}<\varphi| \quad , \quad \rho_B = |\chi>_{BB}<\chi| \qquad (۹۲\_۱)$$

هر حالتی را که نتوان به صورت حاصلضرب تانسوری مستقیم نشان داد درهم تنیده است و ماتریسهای چگالی ρ_A و ρ_B آن آمیخته هستند. [۱و۲و۳و۷]

1-entanglement

فصل دوم : گیتهای کلاسیکی و کوانتومی

۱ـ۲ـ تعریف

در کامپیوترهای کلاسیک تمام اطلاعات به شکل رشته ای از متغیرهای ۱ و۰ ذخیره می شوند و پردازش داده ها از هر نوع که باشد چیزی جز انجام اعمال منطقی روی این رشته ها نیست.

هر نوع پردازش اطلاعات چیزی جز یک سلسله توابع پشت سرهم که روی یک رشته ورودی انجام می شود نیست. تمام این توابع را می توان با ترکیب مقدماتی که تنها روی یک بیت یا دو بیت اثر می کند ساخت هر کدام از این توابع مقدماتی را اصطلاحاً گیت می نامند.

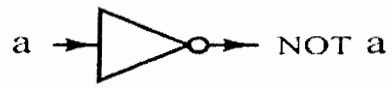
یک کامپیوتر الکترونیکی شامل صدها و هزارها میلیون گیت می باشد و هر کدام از این گیتها فرایند مربوط به خود را انجام می دهند. می توان گیتها را همانند جعبه های سیاه کوچک با ورودیهای خاص و خروجیهای متناسب فرض کرد.

۲ـ۲ـ گیت های کلاسیکی

گیت های کلاسیکی بر اساس تعداد ورودیهای طبقه بندی می شوند که شامل گیت های تک ورودی و گیت های دو ورودی هستند.

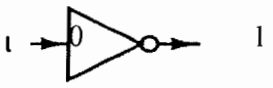
۱ـ۲ـ۲ـ گیت های تک ورودی :

۱ـ گیت NOT :



این گیت مقدار ورودی را از ۰ به ۱ و بالعکس تغییر می دهد.

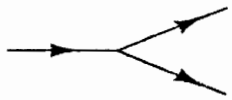
مثال :



$$NOT(0) = 1 \oplus 0 = \mathrm{mod}(\frac{0+1}{2}) = 1$$

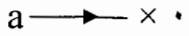
۲ـ گیت FANOUT (کپی) :

این گیت شامل یک ورودی و دو خروجی است که شاخه بیت ورودی را به دو شاخه بیت خروجی که حاصل دو بیت مشابه با بیت ورودی است، تبدیل می کند.



۳ـ گیت ERASE :

این گیت بیت ورودی را با صفر جایگزین می کند.



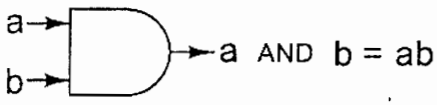
۲ـ۲ـ۲ـ گیت های دو ورودی :

۱ـ گیت AND :

شامل دو ورودی و یک خروجی است، خروجی یک است تنها اگر هر دو ورودی یک باشند در غیر این صورت، خروجی برابر صفر می باشد.

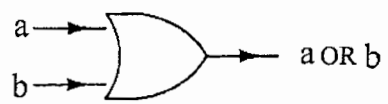
عملیات ریاضی آن مانند حاصلضرب است.

$$a \quad AND \quad b = ab$$



۲ـ گیت OR :

شامل دو ورودی و یک خروجی است. تنها اگر ورودیها هر دو صفر باشند. خروجی صفر است و در غیر این صورت خروجی برابر یک خواهد شد.



۳ـ گیت XOR :

عملیات ریاضی آن به شکل زیر است :

$$a \quad XOR \quad b = a \oplus b$$

بنابراین خروجی برابر یک خواهد شد اگر تنها یکی از ورودیها صفر و دیگری یک باشد یعنی ورودیها متفاوت باشند. در غیر این صورت خروجی صفر خواهد شد.

گیتهای دو ورودی را توسط جدول زیر می توان نمایش داد :

جدول ۲-۱-نمایش گیت ورودی

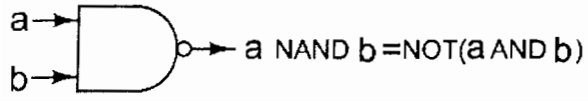
a	b	AND	OR	XOR
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

با استفاده از جدول فوق به راحتی می توان نشان داد که :

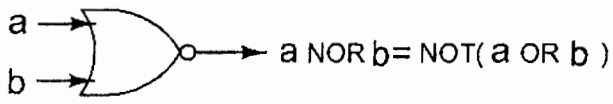
$$aORb = (aANDb)XOR(aXORb)$$

یعنی گیت OR می تواند بصورت ترکیبی از گیتهای AND و XOR ساخته شود.

۴ـ گیت NAND :



۵ـ گیت NOR :



محاسبات کلاسیکی با استفاده از گیت های فوق انجام می شود اما جالب توجه است بدانیم که برای محاسبات به همه گیتهای فوق نیاز نداریم چون می توان گیتهای دیگر را از گیتهای ERASE و FANOUT و NAND بدست آورد.

۳ـ۲ـ محاسبات برگشت پذیر [1]

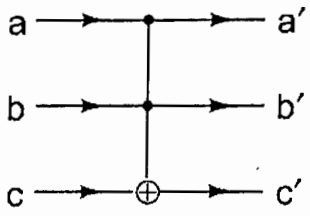
می توان ورودی گیت های FANOUT و NOT را از خروجیهای گیت بدست آورد. در حالیکه این عمل برای سایر گیت های کلاسیکی امکان پذیر نمی باشد. می توان گفت که گیت های NOT و FANOUT برگشت پذیرند و تنها گیت های کلاسیکی برگشت پذیر می باشند. در گیت های برگشت ناپذیر کلاسیکی خروجی یک بیت کمتر از ورودی دارد.

در قیاس گیت های کلاسیکی با کوانتومی باید گفت که همه گیت های کوانتومی برگشت پذیر هستند ما می توانیم گیت های کلاسیکی برگشت پذیر بسازیم. که ایده اصلی این کار، کپی کردن تعدادی از بیت های ورودی به بیت های خروجی است.

با گیت Toffoli می توان گیت های برگشت پذیر کلاسیکی را شبیه سازی کرد :

۱ـ۳ـ۲ گیت *Toffoli* :

این گیت شامل سه ورودی و سه خروجی است.



که $c' = c \oplus ab, b' = b, a' = a$

چون $a = a'$ و $b = b'$ و $c = c' \oplus a'b'$، بیت ورودی ممکن است با عقب برگشتن از بیت های خروجی ساخته شوند.

برای b=c=0 و $c' = 0$ یک گیت Toffoli مانند گیت برگشت پذیر ERASE عمل می کند.

1-revisable

به ازاء b=1 و c=0 و ، $c' = 0$ مشابه گیت FANOUT عمل می کند.

و اگر b=1 و c=1 و $c' = 1 \oplus a = NOTa$ که معادل با گیت NOT است.

به ازاء b=1 و $c' = c \oplus a = aXORc$ یک گیت برگشت پذیر XOR را داریم.

و نهایتاً به ازاء c=0 به $c' = ab = aANDb$ مشابه گیت برگشت پذیر AND عمل می کند.

۴ـ۲ـ گیت های کوانتومی

گیت های کوانتومی تبدیل کننده بیت های کوانتومی هستند درست مشابه گیت های کلاسیکی که بیت های کلاسیکی را تغییر می دهند.

مستلزم این عمل تحول زمانی سیستم کوانتومی است که بر طبق قوانین مکانیک کوانتومی این عمل با عملگر یکانی توصیف می شود. بنابراین هر گیت کوانتومی با یک عملگر (یکانی) یونیتاری u متناظر است.

چنانچه یک گیت کوانتومی روی یک حالت چند کیوبیتی اختیاری اثر کند داریم.

$$|\psi_{in}\rangle \rightarrow |\psi_{out}\rangle = U|\psi_{in}\rangle$$

گیت های کوانتومی همیشه برگشت پذیر هستند و حالتهای ورودی را می توان از حالتهای خروجی بازسازی کرد.

هر تحول یکانی برگشت پذیر است بنابراین :

$$|\psi_{in}\rangle = U^{+}|\psi_{out}\rangle$$

U عملگر یکانی است یعنی بزرگی و طول حالت را تغییر نمی دهد. بنابراین عملگر خطی و یکانی u به صورت یک گیت کوانتومی توصیف می شود که می تواند بر پایه های اصلی کیوبیت های منفرد $|0\rangle$ و $|1\rangle$ اعمال شود.

۱ـ۴ـ۲ـ گیت های کوانتومی منفرد :

۱ـ گیت کوانتومی NOT

مشابه گیت کلاسیکی NOT، برای گیت کوانتومی NOT داریم :

$$|0\rangle \rightarrow |1\rangle \quad , \quad |1\rangle \rightarrow |0\rangle$$

که ماتریس یکانی X را برای آن تعریف می کنیم.

$$X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

که بصورت زیر عمل می کند.

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

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

۲ـ گیت z :

برای گیت z داریم

$$|0\rangle \rightarrow |0\rangle \quad , \quad |1\rangle \rightarrow -|1\rangle$$

ماتریس یکانی آن به شکل زیر است :

$$Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

۳ـ گیت هادامارد[1] :

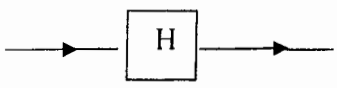
پایه های محاسباتی توسط عملگر گیت هادامارد بصورت زیر تعریف می شود :

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

ماتریس متناظر یکانی آن بصورت زیر است.

$$H=1/\sqrt{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

عموماً گیت هادامارد را با نماد زیر نمایش می دهیم.



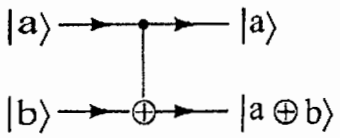
گیت z و گیت H هیچ گونه مشابه کلاسیکی ندارند.

1-hadamard gate

۲ـ۴ـ۲ـ گیت های کوانتومی دوتایی :

۱ـ گیت CONTROLLED NOT (C-NOT)

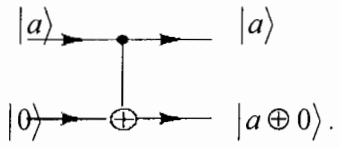
این گیت شامل دو کیوبیت ورودی است، کیوبیت ورودی بالایی را کیوبیت کنترل و کیوبیت ورودی پایینی را کیوبیت هدف نامند و نماد این گیت به شکل زیر است.



توجه شود که $a,b \in \{0,1\}$ هستند.

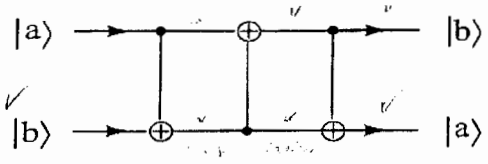
عمل ریاضی این گیت روی مدار فوق بیان شده است. ورودی هدف در صورتی که کنترل صفر باشد (a=0) تغییر نمی کند. اما اگر a=1 باشد، هدف تغییر می کند.

C-NOT یک گیت کوانتومی بسیار مهم است، اگر b=0 باشد گیت C-NOT به مانند کپی عمل می کند.



$$|a,o\rangle = |a\rangle|0\rangle = |a\rangle \otimes |0\rangle \xrightarrow{C\text{-}Not} |a\rangle|a\rangle = |a,a\rangle$$

یک نمونه از کاربردهای گیت C-NOT در زیر نشان داده شده است که یک جفت از بیت های کوانتومی را در پایه محاسباتی، عوض می کند.



عمل ریاضی به صورت زیر انجام شده است.

$$|a,b\rangle \to |a,a\oplus b\rangle \to |(a\oplus b)\oplus a, a\oplus b\rangle$$

$$= |b,(a+b)\rangle =\to |b,b+(a+b)\rangle = |b,a\rangle$$

بنابراین مکان a, b با هم عوض می شود.

ماتریس یکانی متناظر با عملگر گیت C-NOT به صورت زیر بیان می شود.

$$C=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

اگر کیوبیت کنترل یک حالت کوانتومی کلی باشد طوری که :

$$|\psi\rangle = \alpha|0\rangle + B|1\rangle \qquad a^2 + B^2 = 1$$

و کیوبیت هدف $|0\rangle$ باشد طبق تعریف کیت C-NOT خواهیم داشت :

$$|\psi\rangle|0\rangle = (\alpha|0\rangle + B|1\rangle)|0\rangle = \alpha|0,0\rangle + B|1,0\rangle \xrightarrow{C-NOT(gate)} \alpha|0,0\rangle + B|1,1\rangle$$

حال اگر کیوبیت هدف هم یک حالت کلی مانند $|\psi\rangle$ باشد :

$$|\psi\rangle|\psi\rangle = \alpha^2|0,0\rangle + \beta^2|1,1\rangle + \alpha\beta|0,1\rangle + \beta\alpha|1,0\rangle$$

این در صورتی مشابه حالت پیش است که $\alpha = 0$ یا $\beta = 0$ باشد، یعنی اگر کیوبیت هـای ورودی، حالتهای پایه محاسباتی باشد.

با این وجود نمی توان مدارها و گیتهای پیچیده تر را برای کپی کردن یک حالت کوانتومی دلخواه به کار ببریم که این نتیجه به عنوان قضیه no- cloning مطرح می شود.

بنابراین قضیه کپی شدن برای حالت های پایه راست هنجار امکان پذیر است نه بـرای هـر حالـت کوانتومی دلخواه.

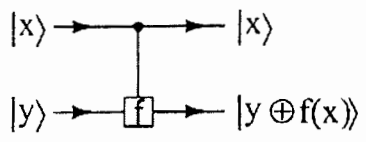
مثال :

$$|\psi\rangle = {}^{1}\!\!\diagup\!\!{}_{\sqrt{2}}\,(|0\rangle + |1\rangle)$$

$$|\psi\rangle = |0\rangle_x$$

۲ـ گیت Fanction (f-gatu)

گیت کوانتومی دوتایی مهم دیگری است که شامل دو ورودی و دو خروجی است.



تعمیمی از گیت C-NOT است و مانند C-NOT عمل می کند. با این تفاوت که کیوبیت هدف بـا تابعی از کیوبیت کنترل، مدول ۲ می شود.

$$f:\{0,1\}\to\{0,1\}$$
$$|x,y\rangle\to|x,y\oplus f(x)\rangle$$

اگر f(x)=x باشد با گیت C-NOT متناظر است.

به ازاء y=0 خواهیم داشت.

$$|x,0\rangle\xrightarrow{f-gate}|x,f(x)\rangle$$

۵ـ۲ـ قضیه No – Cloning

یک ویژگی حالتهای کوانتومی که مفاهیم تعمیمی را در محاسبات کوانتومی بـه همـراه دارد No-cloning می باشد. به این معنی که نمی توان از یک حالت کوانتومی E نشناخته، کپی گرفت و یـا به عبارتی همانندسازی انجام داد که از نتایج خطی بودن مکانیک کوانتومی بدست می آید.

برای اثبات آن کافی است فرض کنیم که یک حالت را روی خودش نگاشت بدهیم در این صـورت برای حالت دلخواه $|\psi\rangle$داریم :

$$|\psi\rangle\to|\psi\rangle\otimes|\psi\rangle$$

و همین طور برای حالت دلخواه $|\varphi\rangle$ هم بدست خواهیم آورد :

$$|\varphi\rangle\to|\varphi\rangle\otimes|\varphi\rangle$$

چون تبدیل باید خطی باشد بنابراین نشان می دهد که :

$$|\psi\rangle\oplus|\varphi\rangle\to|\psi\rangle\otimes|\psi\rangle+|\varphi\rangle\otimes|\varphi\rangle$$

از طرفی $|\varphi\rangle+|\psi\rangle$ را می شود معادل یک حالت کلی $|\chi\rangle$ در نظر گرفت که طبق آن داریم :

$$|\chi\rangle=|\psi\rangle+|\varphi\rangle$$
$$\rightarrow|\chi\rangle\rightarrow|\chi\rangle\otimes|\chi\rangle=(|\psi\rangle+|\varphi\rangle)\otimes(|\psi\rangle+|\varphi\rangle)$$

با توجه به دو فرمول فوق داریم.

$$|\psi\rangle\otimes|\psi\rangle+|\psi\rangle\otimes|\varphi\rangle\neq(|\psi\rangle+|\varphi\rangle)\otimes(|\psi\rangle+|\varphi\rangle)$$

بنابراین کپی کردن از $|\psi\rangle+|\varphi\rangle$ مردود اعلام می شود. در کل حالتهای متعامد را جدا می کنیم، می توان از حالتهای پایه کپی بدست بیاوریم اما از بر هم نهی حالتهای پایه نمی توان کپی برداشت.

در این صورت یا روی سیستم اولیه اندازه گیری خواهیم داشت که در این صورت برهم نهی از بین خواهد رفت یا اینکه حالتی را تولید می کنیم که حالت اولیه و کپی در هم تنیده می شود. [۱و۹]

فصل سوم : نویزهای کلاسیکی و نویزهای کوانتومی

۱ـ۳ـ مقدمه

معمولاً در مکانیک کوانتومی سیستمهای ایزوله مورد مطالعه قرار می گیرند، یعنی سیستمهایی که با محیط برهم کنشهای ناخواسته ندارند، اما سیستمهای حقیقی چنین برهم کنشهایی را دارند و با توجه به اینکه در دنیای واقعی، سیستم های کاملاً ایزوله نداریم، مشاهدات ما با این برهم کنشها آمیخته می شود.

این برهم کنشهای ناخواسته در سیستم های پردازشگر اطلاعات کوانتوی نویز[1] نام دارد. به منظور ساختن سیستم های اطلاعات،کامپیوترهای کوانتومی مفید نیاز به کنترل چنین نویزها می باشد.

در حقیقت هیچ سیستم کوانتومی کاملاً ایزوله وجود ندارد، بالخصوص در مورد کامپیوترهای کوانتومی؛ چون این کامپیوترها بطور کاملاً ظریف توسط یک سیستم خارجی برای انجام دادن مجموعه عملیاتی مورد نظر برنامه ریزی می شود، بطور مثال اگر حالت یک کیوبیت با دو موقعیت الکترون نمایش داده شود، آن الکترون ممکن است با ذرات بار دار دیگر برهم کنش کند که این برهم کنش مانند منبع نویز غیر قابل کنترل که بر روی کیوبیت است، اثر می گذارد.

عملگرهای کوانتومی ابزاری برای توصیف دینامیک سیستمهای بازکوانتومی است.

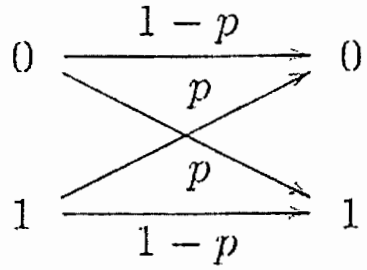
۲ـ۳ـ نویزهای کلاسیکی

وقتی که یک بیت کلاسیک از یک کانال کلاسیکی عبور می کند همواره ممکن است دچار خطا شود، این خطاها هنگام پردازش اطلاعات در یک کامپیوتر کلاسیک نیز می توانند رخ دهند، بنابراین لفظ کانال در این جا به یک معنای عام به کار می رود که الزاما به معنای آن نیست که بیت یک فاصله مکان طولانی را طی کند.

1-noise

به عنوان مثال فرض کنید بیتی از یک مکان به یک مکان دیگر از طریق یک کانال نویز ارسال شود. اما بعد از مدت زمان طولانی مشابه اینکه میدان مغناطیسی باعث درهم ریختن حالت شود، حالت بیت عوض می شود. بدون وجود نویز حالت بیت به صورت ۰ و ۱ خارج می شود اما با وجود نویز حالت صفر به حالت یک تبدیل می شود و بالعکس؛

فرض می کنیم با احتمال p بیت تغییر حالت می دهد و با احتمال (p ـ ۱) بیت حالتش تغییر نمی کند، که در شکل زیر نشان می دهیم.



شکل ۳ـ ۱ بعد از یک زمان طولانی بیت با احتمال p تغییر حالت می دهد

حال نمونه پیچیده تری از نویزها را در سیستم های کلاسیکی مطالعه می کنیم.فرض کنید ما یک مدار کلاسیکی را جهت انجام دادن بعضی اعمال محاسباتی ساخته ایم. متاسفانه بعضی مولفه های اشتباه برای ساختن مدار به کار رفته است. مدار نسبتا غیر واقعی ما، شامل بیت ورو دی X است که دو گیت پی در پی NOT را به کار می برد و بیت میانی Y را تولید می کند و نهایتاً بیت Z حاصل می شود.

منطقی است فرض کنیم گیت دوم NOT بطور مستقل از گیت اولی NOT عمل می کند. یعنی اینکه گیت دوم هم بطور صحیح کار می کند مستقل از اینکه آیا گیت اول درست عمل کرده یا نه؛ فرایند چند مرحله ای $X \to Y \to Z$ با فرض موجود، یک فرایند Markov نام دارد.

برای یک فرایند تک مرحله ای، احتمال خروجی بیت $\vec{q}$ و احتمال ورودی $\vec{p}$ با معادله زیر داده می شود.

$$\vec{q} = E\vec{p} \qquad (۱\_۳)$$

که E یک ماتریس تحول است.

بنابراین حالت نهایی سیستم بطور خطی با حالت اولیه در ارتباط است. خصوصیت خطی بودن در توصیف نویزهای کوانتومی نیز بیان می شود با این تفاوت که ماتریس چگالی جایگزین توصیف احتمالاتی می شود.

۳ـ۳ـ عملهای کوانتومی[1]

مشابه حالتهای کلاسیکی که توسط بردارهای احتمال توصیف می شود، سیستمهای کوانتومی را بر حسب عملگرهای چگالی ρ توصیف می کنیم و مشابه فرمول (۳ـ ۱) که تبدیلات حالتهای کلاسیکی را بیان می کند، تبدیلات حالتهای کوانتومی با فرمول زیر بیان می شود.

$$\rho' = \xi(\rho) \qquad (۲\_۳)$$

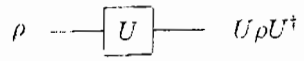
که در اینجا ξ یک عملگر کوانتومی است؛ دو مثال ساده از عملگرهای کوانتومی تبدیلات یونیتاری و اندازه گیریها هستند که به ترتیب داریم.

$$\xi(\rho) = U\rho U^{+} \qquad ;\xi_m(\rho) = M_m \rho M_m^{+} \qquad (۳\_۳)$$

ρ حالت اولیه قبل فرایند است و $\xi(\rho)$ حالت نهایی بعد از اعمال فرایند می باشد.

فرض می کنیم سیستم با محیط برهم کنش داشته باشد. ρ را عملگر چگالی سیستم نامیم و عملگر چگالی محیط را با ρ_{env} نشان می دهیم. پس حالت اولیه سیستم ـ محیط یک حالت ضربی مثل $\rho \otimes \rho_{env}$ می باشد.

دینامیک سیستم های ایزوله با تبدیل یونیتاری بیان می شود. تصور ما از تبدیل یونیتاری همچون جعبه ای است که حالت ورودی وارد می شود و حالت خروجی، خارج می شود که به شکل زیر نشان داده ایم.

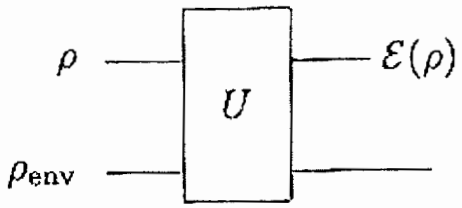


شکل ۲ـ۳ـ سیستم بسته

1-quantum operations

کار درونی جعبه، مورد توجه ما نیست که می توانیم به وسیله یک مدار کوانتومی یا تعدادی سیستم هامیلتونی و یا هر چیز دیگری انجام شود.

برای توصیف سیستم کوانتومی باز می توان گفت که یک برهم کنش بین سیستم مورد نظر که سیستم اصلی[1] نامیده می شود با محیط داریم؛ مانند شکل زیر.



شکل ۳ـ۳ـ سیستم باز

$\xi(\rho)$حالت نهایی سیستم است و برای سیستم باز داریم.

$$\xi(\rho) = tr_{env}\left[U(\rho \otimes \rho_{env})U^{\dagger}\right] \qquad (۴\_۳)$$

برای مثال فرض کنید یک کیوبیت واحد که A نامگذاری می کنیم در حالت ρ است و یک سیستم کوانتومی که B نام داده ایم، در حالت استاندارد $|0\rangle$ ظاهر شده است و با سیستم A از طریق عملگر یونیتاری U برهم کنش می کند که این عمل باعث می شود سیستم ضربی[2] به حالت $U(\rho \otimes |0\rangle\langle 0|)U^{\dagger}$ تبدیل شود.

با کنار گذاشتن سیستم A، سیستم B در حالت نهایت ρ است :

$$\xi(\rho) = \rho' = tr_A(U(\rho \otimes |0\rangle\langle 0|)U^{\dagger}) \qquad (۵\_۳)$$

توجه شود که ξ عملگر چگالی ورودی A را به عملگر چگالی سیستم خروجی B می نگارد.

1-prenciple system
2-joint

۳ـ۴ـ عملگر Sum

برای آنکه دینامیک کلی سیستم را بررسی کنیم فرض می کنیم که در لحظه اولیه سیستم در یک حالت ρ_A و محیط در یک حالت خالص $|e_0\rangle$ قرار دارد، تحت این شرایط ماتریس چگالی سیستم و محیط برابر خواهد بود با :

$$\rho = U(\rho_A \otimes |e.\rangle\langle e.|)U^{\dagger} \qquad (۷\_۳)$$

$$\rho_{env} = |e_0\rangle\langle e_0| \qquad (۸\_۳)$$

چنانچه بیان شد U عملگر تحول سیستم و محیط است. ماتریس چگالی سیستم با محاسبه رد جزئی روی محیط بدست می آید :

$$\rho'_A = \xi(\rho) = tr_{env}\left[U(\rho_A \otimes |e_0\rangle\langle e_0|)U^{\dagger}\right] \qquad (۹\_۳)$$

می توان معادله فوق را بازنویسی کرد :

$$\xi(\rho) = \sum_k < e_k \mid U\left[\rho \otimes |e_0\rangle\langle e_0|\right]U^{\dagger} \mid e_k > \qquad (۱۰\_۳)$$

که در آن :

$$= \sum_k E_k \rho E_k^{\dagger} \qquad (۱۱\_۳)$$

$$E_k \equiv \langle e_k | U | e_0 \rangle \qquad (۱۲\_۳)$$

E_k یک عملگر روی سیستم اصلی است و $|e_k\rangle$ یک پایه متعامد برای فضای حالت محیط با بعد محدود است. عملگرهای E_k عملگر sum نامیده می شوند و بدین ترتیب دینامیک عمومی سیستم کوانتومی بدست آمد.

تعداد عملگرهای E_k حداکثر برابر با بعد فضای هیلبرت محیط است. به راحتی می توان نشان داد که عملگر sum خاصیت زیر را دارد.

$$\sum_k E_k E_k^{\dagger} = I \qquad (۱۳\_۳)$$

عملگرهای $\{E_k\}$ عناصر ماتریسی عملگر E_k می باشد.

رابطه مکملیت در کلاسیک از خاصیت احتمال که باید به یک بهنجار باشد بدست می آید؛ در کوانتوم رابطه مکملیت از شرط مشابهی که رد $\xi(\rho)$ مساوی یک باشد، بدست می آید.

$$1 = tr(\xi(\rho)) \qquad (۱۴\_۳)$$

$$= tr(\sum_k E_k \rho E_k^\dagger) \qquad (۱۵\_۳)$$

$$= tr(\sum_k E_k^\dagger E_k \rho) \qquad (۱۶\_۳)$$

چون این روابط به ازاء همه ρ ها درست است ما خواهیم داشت که نگاشت E در رابطه

$$\sum_k E_k^\dagger E_k = I \qquad (۱۷\_۳)$$

چهار خاصیت زیر را دارد :

الف : خطی است

ب: ماتریس هرمیتی را به ماتریس هرمیتی می نگارد

ج: ماتریس مثبت را به ماتریس مثبت می نگارد.

د : رد ماتریس را حفظ می کند.

به چنین نگاشتی یک نگاشت مثبت و رد نگه دار[1] می گوییم.

فرض کنید که یک اندازه گیری روی محیط در پایه $|e_k\rangle$ بعد از اینکه تبدیل یونیتاری اعمال شد، انجام شود. در واقع با این فرض می توانیم هم تحول عمومی یک سیستم کوانتومی و هم اندازه گیری روی یک سیستم کوانتومی را در یک چارچوب واحد بگنجانیم. ρ_K حالت سیستم اصلی است که نتیجه k برای آن اتفاق می افتد.

$$P_k \propto tr_{env} |e_k\rangle\langle e_k| U(\rho \otimes |e.\rangle\langle e.|)U^\dagger |e_k\rangle\langle e_k|$$

$$= \langle e_k | U\rho \otimes |e.\rangle\langle e.| U^\dagger |e_k\rangle \qquad (۱۷\text{-}۳)$$

$$= E_k \rho E_k^\dagger \qquad (۱۸\_۳)$$

با نرمال کردن ρ_k

$$\rho_k = \frac{E_k \rho E_k^\dagger}{tr(E_k \rho E_k^\dagger)} \qquad (۱۹\_۳)$$

احتمال نتیجه k با فرمول زیر داده می شود :

1-trace-preserving

$$P(k) = tr|e_k\rangle\langle e_k|u(p\otimes|e.\rangle\langle e.|)u'|e_k\rangle\langle e_k| \qquad (۲۰\_۳)$$

$$= tr(E_k \rho E_k^{\dagger}) \qquad (۲۱\_۳)$$

$$\xi(p) = \sum_k P(k)\rho_k = \sum_k (E_k \rho E_k^{\dagger}) \qquad (۲۲\_۳)$$

حال می توان گفت که با احتمال P(k) عملگر E_k روی حالت ρ (از طریق اندازه گیری یا تحول زمانی) اثر کرده است و حالت نهایی $\xi(\rho)$ مخلوطی از تمام حالات مختلفی است که ممکن است در اثر فرایندهای مختلف به وجود آمده باشند.

۳ـ۵ـ مثالهایی از نویز کوانتومی و عملیات کوانتومی

در این بخش تعدادی از مثالهای نویز کوانتومی و عملیات کوانتومی را بررسی می کنیم که در فهم اثرات تجربی نویز روی سیستمهای کوانتومی و چگونگی کنترل این نویزها توسط روش تصحیح خطای کوانتومی مهم می باشد.

شکل های هندسی توصیف شده در زیر می توانند برای نشان دادن بعضی از عملیات کوانتومی مهم روی تک کیوبیتها استفاده شوند که بعداً در نظریه تصحیح غلط کوانتومی کاربرد دارند.

۳ـ۵ـ۱ـ کانال بیت برگردان[1]

کانال بیت برگردان حالت یک کیوبیت را از $|0\rangle$ به $|1\rangle$ و بالعکس با احتمال p تبدیل می کند. یعنی با احتمال p عملگر $X = \sigma_x$ روی کیوبیت اثر می کند و کیوبیت را برمی گرداند.

اثر عملگر پائولی X روی یک کیوبیت چنین است :

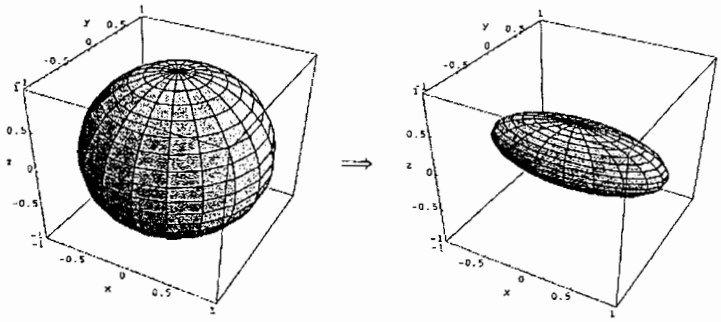
$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle \qquad (۲۳\_۳)$$

عناصر عملگر sum برای آن عبارتند از :

$$E_1 = \sqrt{P}\sigma_x = \sqrt{p}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad E_0 = \sqrt{1-p}I = \sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad (۲۴\_۳)$$

عمل این کانال بیت برگردان در شکل ۳-۴ نشان داده شده است.

1-bit flipe channels



شکل ۳ـ۴ـ اثر کانال بیت برگردان روی کره بلاخ به ازای p=0/3

به راحتی معلوم می شود که این کانال یک حالت با بردار $r=(x,y,z)$ در کره بلاخ را بـه حـالتی دیگر با بردار r می نگارد. یعنی :

$$\mathcal{E}(x,y,z)\to(x,(1-2p)y,(1-2p)z) \qquad (۲۵\_۳)$$

بنابراین کانال بیت برگردان کره بلاخ را در امتداد صفحه عمود بر محور x به طور یکسان با ضریب (p ۲ـ۱) فشرده می کند. اگر p =۱/۲ باشد آن گاه ضریب فشرده سازی صفر می شود و کره بـلاخ تبدیل به یک پاره خط در امتداد محور x می شود و تمامی اطلاعات در جهات دیگـر از بـین مـی رود.

۳ـ۵ـ۲ـ کانال فاز برگردان[1]

در این کانال خطای تغییر فاز رخ می دهد و بـا احتمـال p خطـا انجـام مـی شـود، یعنـی عملگـر $Z=\sigma_z$ روی کیوبیت اثر می کند و فاز را تغییر می دهد. عناصر عملگر sum برای آن عبارتند از:

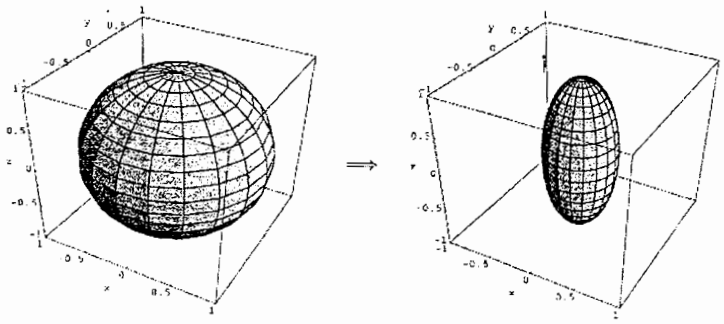
$$E_0=\sqrt{p}\sigma_z=\sqrt{p}\begin{bmatrix}1&0\\0&-1\end{bmatrix}\quad,\quad \mathcal{E}1=\sqrt{1-p}I=\sqrt{1-p}\begin{bmatrix}1&0\\0&1\end{bmatrix} \qquad (۲۶\_۲)$$

و با نگاشت زیر مشخص می شود:

$$\xi(\rho)=(1-p)\rho+pz\rho z$$

اثر این کانال در شکل ۳-۵ نشان داده شده است.

1-phase flip channel



شکل ۳ـ۵ـ اثر کانال فاز برگردان بر روی کره بلاخ به ازای p=0/3

کانال فاز برگردان کره بلاخ را در امتداد صفحه عمود بر Z به طور یکسان با ضریب (p ۲ـ ۱) فشرده می کند. به عنوان یک حالت خاص اگر p =۱/۲ باشد کره بلاخ تبدیل به یک پاره خط در امتداد محور z می شود.

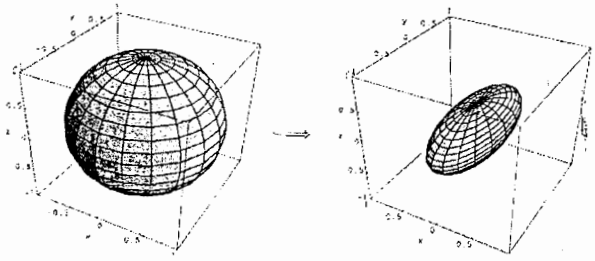
$$p=1/2:(r_x,r_y,r_z)\rightarrow(0,0,rz) \qquad (۲۷\_۳)$$

۳ـ۵ـ۳ـ کانال بیت فاز برگردان[1]

همان طور که از نام این کانال پیداست، این کانال ترکیبی از یک کانال فاز برگردان و یک کانال بیت برگردان است و عناصر عملگر sum عبارتند از :

$$E_0=\sqrt{1-p}I \qquad E_1=\sqrt{p}Y=\sqrt{p}\begin{bmatrix}0 & -i\\ -i & 0\end{bmatrix} \qquad Y=iXZ \qquad (۲۸\_۳)$$

عمل کانال بیت فاز برگردان در شکل ۳-۶ نمایش داده شده است.



شکل ۳ـ۶ـ اثر کانال بیت فاز برگردان برروی کره بلاخ به ازای p=0/3

1-bit flipe and phase flip channel

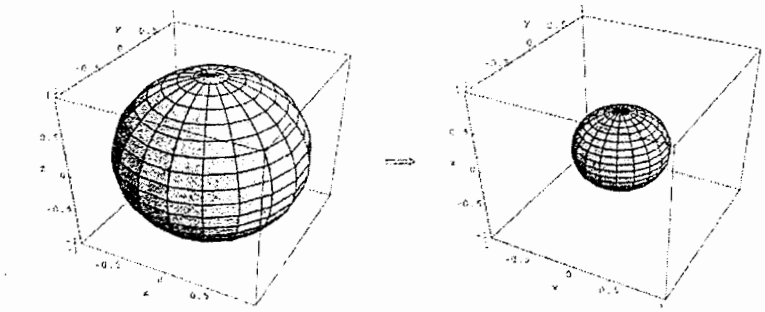
کانال بیت ـ فاز برگردان کره بلاخ را در امتداد صفحه عمود بر محور y به طور یکسان با ضریب (2p ـ ۱) فشرده می کند.

۳ـ۵ـ۴ـ کانال واقطبش[1]

فرض کنید یک تک کیوبیت در اختیار داریم که با احتمال p آن کیوبیت واقطبیده می شود. یعنی توسط یک حالت کاملاً آمیخته جایگزین می شود و با احتمال p ـ ۱ بدون تغییر باقی می ماند. اثر کانال به صورت زیر است :

$$\xi(\rho) = P\frac{I}{2} + (1-p)\rho \qquad (۲۹\_۳)$$

اثر کانال روی شکل ۳-۷ شرح داده شده است.



شکل ۳ـ۷ـ اثر کانال واقطبش بر روی کره بلاخ به ازاء p=0/5

کانال واقطبش کره بلاخ را به طور همسانگرد در تمام جهات به اندازه (p ـ ۱) فشرده می سازد. اثر این کانال به صورت زیر روی کره است.

برای یافتن عملگرهای sum از اتحاد زیر استفاده می کنیم.

$$\varepsilon : r \to (1-p)r$$

$$I/2 = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4} \qquad (۳۱\_۳)$$

و سپس I/2 را در فرمول (۲۹ـ۳) جایگزین می کنیم.

1-depolarizing channel

$$\xi(\rho) = (1-\frac{3p}{4})\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z) \qquad (۳۲\_۳)$$

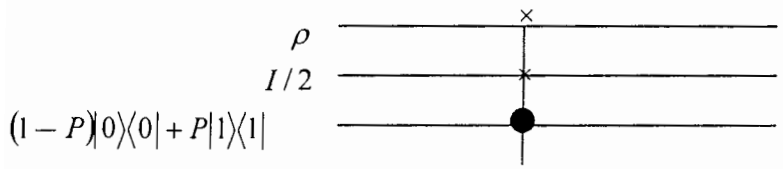
بنابراین :

$$E_0 = \sqrt{\frac{1-3p}{4}}I \qquad E_1 = \sqrt{p}\,X/2 \qquad E_2 = \sqrt{p}\,Y/2$$

$$E_3 = \sqrt{p}\,Z/2 \qquad (۳۳\_۳)$$

بنابراین در کانال واقطبش هر سه خطای X , Y , Z با احتمال یکسان رخ می دهند.

مدار کوانتومی که حالت واقطبش را نشان می دهد به شکل زیر است.



شکل ۳ـ۸ـ مدار کوانتومی حالت واقطبش

۳ـ۵ـ۶ـ کانال میراکنده دامنه [1]

فرض کنید یک تک مد نوری شامل حالت کوانتومی $|0\rangle + b|1\rangle$ را داریم که می خواهیم از یک نقطه به نقطه دیگر از طریق فیبر نوری یا هوا بفرستیم. در بین راه ممکن است این مد نوری جذب محیط شده؛ فرض می کنیم محیط حالت زیر را داشته باشد.

$$|\psi\rangle_{env} = |0\rangle \qquad (۳۴\_۳)$$

بنابراین حالت سیستم بعلاوه محیط می شود.

$$|\psi\rangle_{p,env} = (a|0\rangle + b|1\rangle) \otimes |0\rangle \qquad (۳۵\text{-}۳)$$

$$= a|0,0\rangle + b|1,0\rangle \qquad (۳۶\_۳)$$

فرض می کنیم عملگر یکانی زیر روی سیستم و محیط اثر کند :

$$|0,0\rangle \rightarrow |0,0\rangle$$

$$|0,1\rangle \rightarrow \cos\theta|0,1\rangle - \sin\theta|1,0\rangle \qquad (۳۷\text{-}۳)$$

1-Amplitude damping

$$|1,0\rangle \rightarrow \sin\theta|0,1\rangle + \cos\theta|1,0\rangle$$

$$|1,1\rangle \rightarrow |1,1\rangle$$

پس حالت نهایی سیستم و محیط می شود :

$$|\psi\rangle_{p,env} = a|0,0\rangle + b\sin\theta|0,1\rangle + b\cos\theta|1,0\rangle \qquad (۳۸\_۳)$$

شکل صریح حالت اولیه بصورت زیر است.

$$\rho_A = \begin{pmatrix} a\bar{a} & a\bar{b} \\ b\bar{a} & b\bar{b} \end{pmatrix} \qquad (۳۹\_۳)$$

چون

$$|\psi_A\rangle = a\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix} \qquad ,\rho_A = |\psi\rangle\langle\psi| \qquad (۴۰\_۳)$$

و شکل صریح حالت نهایی برابر است با :

$$\rho'_A = tr_{env}(|\psi\rangle_{\rho,env\ \ \rho,env}\langle\psi|)$$

$$= \begin{pmatrix} a\bar{a} + b\bar{b}\sin^2\theta & ab\cos\theta \\ b\bar{a}\sin\theta & b\bar{b}\cos^2\theta \end{pmatrix} \qquad (۴۱\text{-}۲)$$

پس عملگرهای sum عبارتند از :

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \cos\theta \end{pmatrix} \qquad , \qquad E_1 = \begin{pmatrix} 0 & \sin\theta \\ 0 & 0 \end{pmatrix} \qquad (۴۲\text{-}۳)$$

چون در این کانال فوتون سیستم جذب شده و شدت نور کاهش می یابد به آن کانـال میراکننـده دامنه گویند.

۳ـ۵ـ۷ـ کانال میراکننده فاز [1]

یک مدل بسیار ساده را برای این نویز کوانتومی بیان می کنیم. فرض می کنیم که یک کیوبیت در حالت $|\psi\rangle = a|0\rangle + b|1\rangle$ می باشد؛ برای مدل سازی این کانال فرض می کنیم که عملگر چـرخش

1-Phase damping

$R_z(\theta)$ روی حالات ورودی $|0\rangle$ و $|1|$ اختلاف فاز θ ایجاد می کند. حالت خروجی از این فرایند توسط ماتریس چگالی که از میانگین گیری روی θ بدست می آید داده می شود:

$$\xi(p) = {}^{1}\!/_{\sqrt{4\pi\lambda}} \int_{-\infty}^{+\infty} R_z(\theta)|\psi\rangle\langle\psi|R_z^{\dagger}(\theta)e^{-\theta^2/4\lambda}d\theta \qquad (۴۳\_۳)$$

ماتریس چگالی حالت ورودی را محاسبه می کنیم :

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \qquad p = |\psi\rangle\langle\psi| = \begin{pmatrix} a\bar{a} & a\bar{b} \\ b\bar{a} & a\bar{b} \end{pmatrix} \qquad (۴۴\_۳)$$

و داریم :

$$R_z(\theta)\rho R_z(\theta)^{\dagger} = \begin{pmatrix} a\bar{a} & a\bar{b}e^{i\theta} \\ b\bar{b}e^{-i\theta} & b\bar{b} \end{pmatrix} \qquad (۴۵\_۳)$$

با محاسبه آنتگرال بدست می آوریم

$$\xi(\rho) = {}^{1}\!/_{\sqrt{4\pi\lambda}} \int_{-\infty}^{+\infty} \begin{pmatrix} a\bar{a} & a\bar{b}e^{i\theta} \\ b\bar{a}e^{-i\theta} & b\bar{b} \end{pmatrix} \quad e^{-\theta^2/4\lambda}d\theta \qquad (۴۶\_۳)$$

$$= \begin{pmatrix} a\bar{a} & a\bar{b}e^{-\lambda} \\ b\bar{a}e^{-\lambda} & b\bar{b} \end{pmatrix} \qquad (۴۷\_۳)$$

با مقایسه ρ و $\xi(\rho)$متوجه می شویم که جملات غیر قطری با پارامتر $e^{-\lambda}$ دچار میرایی شده اند.

۶ـ۳ـ اندازه گیریهای فاصله ای[1]

منظور از اینکه می گوییم دو بخش اطلاعاتی مشابه هستند یا اطلاعات در طول یک فرایند حفظ می شوند چیست ؟

اینها پرسشهایی اصلی در نظریه پردازش اطلاعات کوانتومی است که پاسخ دادن به این سوالات، بسط اندازه گیریهای فاصله ای کمیتهای داده شده و نهایتاً دو نوع جامع از اندازه گیری فاصله را پیشنهاد می کند:

۱ـ اندازه گیری استاتیکی

۲ـ اندازه گیری دینامیکی

1-Distance measurees

اندازه گیری استاتیکی مشابهت دو حالت کوانتومی را مشخص می کند در حالیکه اندازه گیری دینامیکی چگونگی حفظ اطلاعات در طی یک فرایند دینامیکی را تعیین می کند.

۳ـ۷ـ اندازه گیری فاصله ای برای اطلاعات کلاسیکی

دو رشته بیت ۰۰۰۱۰ و ۱۰۰۱۱ را در نظر می گیریم، یکی از روش های تعیین فاصله بین این دو بیت، فاصله همینگ[1] است؛ تعداد مکانهایی را که در دو رشته بیت، بیتها با هم متفاوت هستند را فاصله همینگ نامند. در مثال فوق تنها در جایگاه اول و آخر بیتها متفاوتند، پس فاصله همینگ برای این دو رشته بیت ۲ است.

متاسفانه فاصله همینگ بین دو شی ء صرفاً یک موضوع برچسب خورده است و چون در مکانیک کوانتومی یک مکان را نمی توان با قطعیت کامل مشخص نمود بهترین روش برای تفسیر فاصله همنیگ و تعیین آن مقایسه بین توزیع های احتمال می باشد.

۳ـ۷ـ۱ـ اندازه گیری استاتیکی

مجموعه ای مانند x را در نظر می گیریم. هر عضو آن با یک توزیع احتمال p_x مشخص می شود برای همان عضو می توان توزیع احتمال دیگری مانند q_x نیز تعریف کرد.

$$X = \{X_1, X_2, ...\} \qquad (۴۸\_۳)$$

برای تشخیص بهترین جواب ابتدا معیار فاصله ردی[2] و سپس معیار ضریب اطمینان را شرح می-دهیم.

فاصله ردی با رابطه زیر تعریف می شود.

$$D(p_x, q_x) = \tfrac{1}{2}\sum_x |p_x - q_x| \qquad (۴۸\_۳)$$

فاصله ردی گاهی اوقات تحت Komogorov یا فاصله L_1 شناخته می شود؛ فاصله ردی متریک می باشد چون:

1-hamming distance
2-trace distance

۱ـ متقارن است

$$D(x,y) = D(y,x) \qquad (۴۹\_۳)$$

۲ـ در نامساوی زیر صدق می کند.

$$D(y,z) \le D(x,y) + D(y,z) \qquad (۵۰\_۳)$$

معیار دوم بین توزیع های احتمال q_x و p_x ضریب اطمینان[1] است که به صورت زیر تعریف می شود.

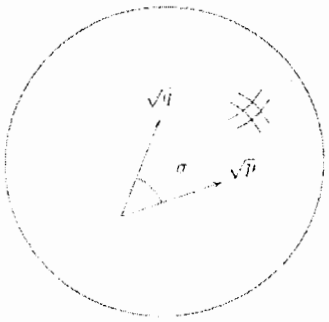
$$F(p_x,q_x) = \sum_x \sqrt{p_x q_x} \qquad (۵۱\_۳)$$

تفاوت عمده ضریب اطمینان با فاصله ردی در متریک نبودن آن است گرچه خروجی ضریب اطمینان کمیتی متریک است.

اگر دو توزیع احتمال $\{p_x\}$ و $\{q_x\}$ مساوی باشند داریم :

$$F(p_x,q_x) = \sum_x \sqrt{p_x}\sqrt{p_x} = \sum_x \sqrt{p_x} = 1 \qquad (۵۲\_۳)$$

می بینیم که ضریب اطمینان ۱ می شود.



شکل ۳ـ۹ـ توصیف هندسی ضریب اطمینان به عنوان حاصلضرب داخلی بین بردارهای $\sqrt{q_x}, \sqrt{p_x}$

1-fidelity

از لحاظ هندسی می توان گفت که ضریب اطمینان، حاصلضرب داخلی بین مولفه های $\sqrt{p_x}$ و $\sqrt{q_x}$ است که روی یک کره به شعاع واحد قرار می گیرد،که در شکل ۳-۹ نشان داده شده است.

تا اینجا دو معیار اندازه گیری استاتیکی فاصله ردی و ضریب اطمینان را برای مقیاس توزیع های احتمال در مکانهای مشخص و ثابتی بکار بردیم. حال معیار سوم اندازه گیری دینامیکی فاصله را شرح می دهیم که تعیین کننده چگونگی حفظ اطلاعات در بستر زمان است

۳ـ۷ـ۲ـ اندازه گیری دینامیکی

فرض کنید یک متغیر کاتوره ای X بدرون یک کانال نویزی فرستاده شده است، خروجی یک متغیر تصادفی دیگری مثل Y است که یک فرایند مارکو است.

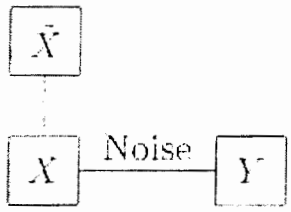
$$X \to Y$$

مناسب تر است که فرض کنیم X و Y رنجی مساوی از مقادیر که با X نشان داده می شوند را دارند. سپس با احتمال اینکه x با y متفاوت باشد $P(X \neq Y)$؛ نشان می دهیم که این معیار خوبی برای نشان دادن میزان اطلاعاتی است که حفظ شده اند.

تصور کنید که متغیر کاتوره ای x به شما داده شده و شما یک کپی از x را می سازید، ساختن یک متغیر کاتوره ای جدید با شرط زیر را داریم :

$$X = \widetilde{X}$$

اکنون متغیر تصادفی x از کانال نویز عبور کرده و حالت خروجی Y است. مطابق شکل ۳-۱۰ .



شکل ۳ـ۱۰ـ فرایندی که نشان می دهد قبل از اینکه x از کانال نویزی عبور کند و به y تبدیل شود یک کپی از آن گرفته شده است.

$\tilde{X}$ کپی X است و نزد خودمان نگه می داریم.

حال می خواهیم بینیم که زوج اولیه (X و $\tilde{X}$) چقدر به زوج نهایی (Y و X) شبیه است ؟

با استفاده از معیار فاصله ردی و بعضی روابط جبری ساده بدست می آوریم :

$$\mathcal{D}(p_x, q_x) = \tfrac{1}{2}\sum_x |p_x - q_x| \qquad (۵۳\_۳)$$

$$\mathcal{D}(\tilde{x}, x), (x, y) = \tfrac{1}{2}\left[\left|\sum_{x,x'} (p(x = x', x = x) - p(\tilde{x} = x)(Y = x')\right|\right] \qquad (۵۴\_۳)$$

$$= \tfrac{1}{2}\sum_{x,x'} \left|\delta_{xx'}, P(X = x) - p(\tilde{X} = x, Y = x')\right| \qquad (۵۵\_۳)$$

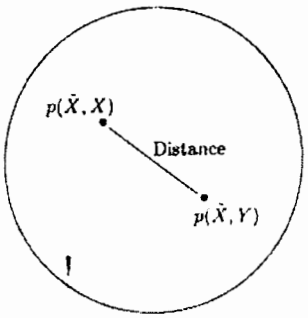
$$= \tfrac{1}{2}\sum_{\substack{x \\ x \neq x'}} \left|p(\tilde{X} = x, Y = x')\right| + \tfrac{1}{2}\sum_x \left|p(X = x) - p(\tilde{X} = x, Y = x)\right| \qquad (۵۶\_۳)$$

$$= \tfrac{1}{z}\left[P(\tilde{X} \neq Y) + 1 - p(\tilde{X} = Y)\right] \qquad (۵۷\_۳)$$

از طرفی $P(\tilde{X} \neq Y) + p(\tilde{X} = Y) = 1$ بنابراین :

$$\mathcal{D}((\overline{X}, x), (X, Y)) = P(\tilde{X} \neq Y) \qquad (۵۸\_۳)$$

بنابراین احتمال خطا در یک کانال برابر است با فاصله ردی بین توزیع های احتمال برای (X , Y) و ($X, \tilde{X}$).



شکل ۳ـ۱۱ـ احتمال خطا درکانال مساوی است با فاصله ردی بین توزیع های احتمالی(**x,y**) و ($X, \tilde{X}$).

۳ـ۸ـ دو حالت کوانتومی چقدر شبیه یکدیگر هستند؟

تا اینجا اندازه گیری فاصله ای برای حالتهای کلاسیکی را بدست آوریم. اکنون تعمیمی کوانتومی از روابط کلاسیکی فاصله ردی و ضریب اطمینان را بدست می آوریم.

۳ـ۸ـ۱ـ معادل کوانتومی فاصله ردی

با تعریف فاصله ردی برای دو حالت کوانتومی ρ و σ آغاز می کنیم.

$$D(\rho,\sigma) \equiv \tfrac{1}{2} tr|\rho-\sigma| \qquad (۵۹\_۳)$$

چون ρ و σ جابه جاپذیرند می توان بصورت قطری در پایه های یکسانی تعریف می کنیم که $|i\rangle$ پایه های متعامد است.

$$\rho = \sum_i r_i |i\rangle\langle i| \qquad (۶۰\_۳)$$

$$\sigma = \sum_i s_i |i\rangle\langle i| \qquad (۶۱\_۳)$$

بنابراین :

$$D(\rho,\sigma) = \tfrac{1}{2} tr\left[\sum_i r_i |i\rangle\langle i| - \Sigma s_i |i\rangle\langle i|\right] \qquad (۶۲\_۳)$$

$$= \tfrac{1}{2} tr\left(\sum_i (r_i - s_i)|i\rangle\langle i|\right) = D(r_i, s_i) \qquad (۶۲\_۳)$$

۳ـ۸ـ۲ـ ضریب اطمینان کوانتومی

ضریب اطمینان با حالتهای ρ و σ مطابق زیر تعریف می شد.

$$F(\rho,\sigma) = tr\sqrt{p^{1/2}\sigma\rho^{1/2}} \qquad (۶۴\_۳)$$

اگر ρ و σ جابه جاپذیرند در پایه های یکسان قطری اند.

$$\rho = \sum_i r_i |i\rangle\langle i| \qquad (۶۵\_۳)$$

$$\sigma = \sum_i s_i |i\rangle\langle i| \qquad (۶۶\_۳)$$

برای بعضی از پایه های متعامد $|i\rangle$؛

با توجه به تعریف ضریب اطمینان خواهیم داشت :

$$F(\rho,\sigma) = tr\left[\sqrt{\left(\sum_i r_i |i\rangle\langle i|\right)\left(\sum_i s_i |i\rangle\langle i|\right)}\right] \quad (۶۷\_۳)$$

$$= tr\sqrt{\sum_i r_i s_i |i\rangle\langle i\| i\rangle\langle i|} \quad (۶۸\_۳)$$

$$= tr\sqrt{\sum_i r_i s_i |i\rangle\langle i|} \quad (۶۹\_۳)$$

$$= \sum \sqrt{r_i s_i}\sqrt{tr\sum_i |i\rangle\langle i|} = \quad (۷۰\_۳)$$

$$= \sum_i \sqrt{r_i s_i} \quad (۷۱\_۳)$$

$$= F(r_i, s_i) \quad (۷۲\_۳)$$

$$\Rightarrow F(\rho,\sigma) = F(r_i, s_i) \quad (۷۳\_۳)$$

یعنی وقتی ρ و σ جابجاپذیر باشند ضریب اطمینان کوانتومی به ضریب اطمینان کلاسیکی با توزیع مقادیر ویژه r_i و s_i از ρ و σ تبدیل می شوند.

مثال دوم را برای محاسبه ضریب اطمینان بین حالتهای خالص $|\psi\rangle$ و یک حالت اختیاری ρ بحث می کنیم؛ با توجه به تعریف ضریب اطمینان :

$$F(|\psi\rangle,\rho) = tr\sqrt{\langle\psi|\rho|\psi\rangle|\psi\rangle\langle\psi|} \quad (۷۴\_۳)$$

$$= \sqrt{\langle\psi|\rho|\psi\rangle} \quad (۷۵\_۳)$$

.[۵،۷،۴،۲]

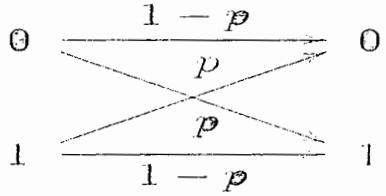
فصل چهارم:تصحیح خطای کوانتومی و کلاسیکی

۴-۱- مقدمه

وقتی که بیتها از درون یک کانال کلاسیکی عبور می کنند ممکن است دچار خطا شوند، به همین خاطر قبل از ارسال اطلاعات به درون کانال، اطلاعات کدگذاری می شوند و در پایان پس از دریافت اطلاعات آنها را کدگشایی می کنند.

نظریه اساسی برای حفظ اطلاعات و دریافت صحیح آنها، افزودن اطلاعات به پیغام اصلی است که روش تکرار نام دارد. به عنوان مثال فرض می کنیم که می خواهیم بیتی را از مکانی به مکان دیگر از طریق یک کانال کلاسیکی نویز بفرستیم، اثر نویز در کانال چنین است که بیت صفر را به یک تبدیل می کند و بالعکس.

با احتمال $p > 0$ بیت تغییر حالت می دهد و با احتمال 1-p بدون تغییر باقی می ماند و ارسال بدون خطا انجام می شود. این کانال را کانال متقارن باینری[1] نامیم که در شکل زیر نشان داده ایم.



شکل ۴-۱-کانال متقارن باینری

یک روش متداول در این کانال برای کد گذاری این است که به جای اینکه فقط یک بیت ارسال شود سه بیت ارسال می کنیم، در واقع سه کپی از بیت ارسالی را داریم یعنی:

$$0 \to 000 \qquad (۱-۴)$$

$$1 \to 111 \qquad (۲-۴)$$

1-binary symmetric channel

رشته بیت های 000 و 111 را بیت های منطقی 0 و 1 می نامیم چون این رشته بیت ها به جـای تک بیت ها عمل می کنند و به جای یک بیت 1 ،سه تا بیت 1 ارسال شده است.حال این سه بیت به درون کانال ارسال می شود. در پایان گیرنده سه بیت را دریافت می کند و باید بیـت ارسـالی را تشخیص دهد.

اگر رشته بیت ارسالی 000 باشد و بیتها در کانال دچار خطا شود بیت خروجی یکی از شکل هـای زیر را دارد.

$$000 \rightarrow 100,001,010,110,101,011,111 \qquad (۳-۴)$$

فرض می کنیم بیت خروجی 001 باشد، دریافت کننده با توجه بـه بیـت خروجـی مـی بینـد کـه احتمالP زیاد بالا نیست، پس تشخیص می دهد که بیت سوم دچار خطا شده است. پس بنـابراین بعد از تشخیص خطا می فهمد که بیت ارسالی صفر است.

آن دسته از بیتهایی قابل قبولند که بیشترین احتمال را دارند، در این مثال بیتهایی قابل قبولند که فقط یکی از بیتها در کانال دچار خطا شده اسـت. ایـن نـوع تـشخیص بیـت ارسـالی را روش رای اکثریت نامند. احتمال اینکه ۲ بیت یا بیشتر از ۲ بیت تغییر حالت دهند، می باشد:

$$p_e = 3p^2(1-p) + p^3 \qquad (۴-۴)$$

این نتیجه از محاسبه زیر حاصل می شود:

فرض می کنیم هر سه بیت تغییر حالت داده اند.

$$\begin{cases} 0 \xrightarrow{p} 1 \\ 0 \xrightarrow{p} 1 \\ 0 \xrightarrow{p} 1 \end{cases} \qquad (۵-۴)$$

پس هر بیت با احتمال p^3 تبدیل شده اند.

حال اگر دو بیت تغییر حالت دهند، حالتهای زیر را داریم:

$$\begin{cases} 0 \xrightarrow{1-p} 0 & 0 \xrightarrow{p} 1 & 0 \xrightarrow{p} 1 \\ 0 \xrightarrow{p} 1 & 0 \xrightarrow{1-p} 0 & 0 \xrightarrow{p} 1 \\ 0 \xrightarrow{p} 1 & 0 \xrightarrow{p} 1 & 0 \xrightarrow{1-p} 0 \end{cases} \qquad (۶-۴)$$

پس احتمال اینکه دو بیت تبدیل شوند، $3p^2(1-p)$ می باشد.

پس با جمع دو رابطه اخیر بدست می آوریم:

$$p_e = 3p^2(1-p) + p^3 \qquad (۷-۴)$$

با ساده سازی رابطه فوق بدست می آوریم.

$$p_e = 3p^2 - 2p^3 \qquad (۸-۴)$$

اگر کد گذاری انجام نمی شد و یک بیت ارسال می شد احتمال خطا p بود.اما در جایی که سه بیت ارسال کردیم احتمال خطا $p_e = 3p^2 - 2p^3$ است می بینیم اگر p<1/2 باشد، $p_e < p$ این نوع کد گذاری را روش تکرار[1] نامند.

۴-۲-کد بیت بر گردان سه کیوبیتی

برای محافظت حالتهای کوانتومی در برابر نویزها تصحیح خطای کوانتومی را با اصول مشابه کلاسیکی بدست می آوریم. تفاوت های مهم عمده ای بین اطلاعات کلاسیکی و اطلاعات کوانتومی وجود دارد که نیاز به تصحیح جهت بیان ایده های جدید دارد تا کدهای تصحیح خطای کوانتومی را بدست آوریم. بالخصوص روش کد گذاری فوق که در کلاسیک قابل انجام است در کوانتوم با سه مشکل عمده روبه رو می باشد :

۱- No-Cloning

در روش تکرار، کپی هایی از یک بیت کلاسیک تهیه کردیم که در صورت بروز خطا از روش رای اکثریت به وجود آن پی می بردیم. حال آنکه بنا به قضیه No-Cloning نمی توان از حالت کوانتومی کپی تهیه کرد و یک حالت را به سه حالت یا بیشتر تبدیل کرد حتی اگر No-Cloning هم ممکن بود، اندازه گیری کردن و مقایسه چند حالت کوانتومی خروجی از یک حالت ممکن نخواهد بود.

۲- پیوستگی خطا:

خطای ایجاد شده در یک بیت کلاسیک یک خطای گسسته است که در آن بیت 0 به 1 تبدیل می شود و بالعکس،حال آنکه خطای ایجاد شده در یک کیوبیت، پیوسته است و برای تعیین کردن

1-repetition

خطاها و تصحیح کردن آن به یک دقت نا محدود نیاز داریم.

۳- از بین بردن اطلاعات کوانتومی در اثر اندازه گیری :

یک بیت کلاسیک را می توان مشاهده کرد و از خطای ایجاد شده در آن آگاهی یافت، ولی یک کیوبیت را نمی توان به راحتی مشاهده نمود. زیرا در مکانیک کوانتومی مشاهده،حالت کوانتومی را بر هم می زند و باعث از بین رفتن حالت اولیه می شود و بازیافت حالت اولیه را غیر ممکن می سازد.

خوشبختانه هیچ کدام از این سه مشکل غیر قابل حل نیستند. فرض کنید که کیوبیت را از درون یک کانال نویزی عبور داده ایم که با احتمال p حالت کیوبیت را تغییر می دهد و با احتمال $p-1$کیوبیت بدون تغییر باقی می ماند.با توجه به تعریف کانال بیت بر گردان، یعنی با احتمال p ،حالت $|\psi\rangle$ به حالت $X|\psi\rangle$ تبدیل می شود.که X عملگر ماتریس پائولی است.

می خواهیم که بیت برگردان را توضیح دهیم که جهت محافظت کیوبیتها در برابر اثرات نویزها در این کانال، استفاده می شود.

فرض کنید ما تک کیوبیت با حالت $a|0\rangle+b|1\rangle$ را در سه تا کیوبیت کد گذاری کرده ایم مثل:

$$a|000\rangle+b|111\rangle \qquad (۹-۴)$$

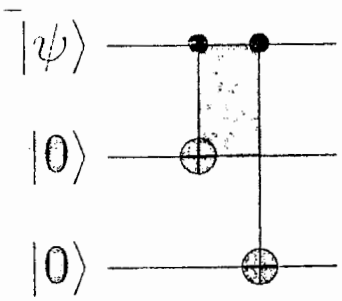
یک روش مناسب برای نوشتن این نوع کد گذاری به شکل زیر است:

$$|o\rangle\rightarrow|o_{\mathcal{L}}\rangle\equiv|000\rangle \qquad (۱۰-۴)$$

$$|1\rangle\rightarrow|1_{\mathcal{L}}\rangle\equiv|111\rangle \qquad (۱۱-۴)$$

که بر هم نهی را حفظ کرده است.

$|0_{\mathcal{L}}\rangle$ و $|1_{\mathcal{L}}\rangle$ به ترتیب نمایانگر حالتهای منطقی $|0\rangle$ و $|1\rangle$ هستند. مداری که این نوع کدگذاری را انجام می دهد در شکل ۲-۴ نشان داده است.



شکل ۴-۲- مدار کد گذاری کد بیت بر گردان سه کیوبیت

نهایتا توسط مدار شکل ۴-۲، $|\psi\rangle$ به حالت $|000\rangle+|111\rangle$ تبدیل می شود.

$$|\psi\rangle|0\rangle=(a|0\rangle+b|1\rangle)|0\rangle=a|0\rangle|0\rangle+b|1\rangle|0\rangle \qquad (۱۲-۴)$$

$$\begin{aligned} a|0\rangle|0\oplus 0\rangle+b|1\rangle|1\oplus 0\rangle &= a|0\rangle|0\rangle+b|1\rangle|1\rangle \\ &= a|00\rangle+b|11\rangle \end{aligned} \qquad (۱۳-۴)$$

$$\begin{aligned} &(a|00\rangle+b|11\rangle)|0\rangle=a|00\rangle|0\rangle+b|11\rangle|0\rangle \\ &a|00\rangle|0\oplus 0\rangle+b|11\rangle|1\oplus 0\rangle=a|000\rangle+b|111\rangle \end{aligned} \qquad (۱۴-۴)$$

اگر خطای وارون بیتی روی یکی از کیوبیت ها اتفاق بیفتد دو مرحله جهت تصحیح خطا وجود دارد: ۱-آشکارسازی خطا ۲-بازیافت

۴-۲-۱- آشکارسازی خطا

وقتی اندازه گیری انجام می شود نوع خطا مشخص می شود. نتیجه اندازه گیری تشخیص خطا نامیده می شود. برای کانال بیت برگردان چهار تشخیص خطا داریم که با چهار عملگرتصویرگر متناظر است:

بدون خطا $P_0 \equiv |000\rangle\langle 000|+|111\rangle\langle 111|$ (۱۵-۴)

بیت برگردان روی کیوبیت اول $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$ (۱۶-۴)

بیت برگردان روی کیوبیت دوم $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$ (۱۷-۴)

بیت برگردان روی کیوبیت سوم $P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$ (۱۸-۴)

p_i ها عملگر تصویرگر هستند. برای مثال فرض کنید که بیت برگردان برای کیوبیت اول اتفاق افتاده است پس حالت تغییر کرده عبارت است از:

$$a|100\rangle + b|011\rangle \quad (۱۹-۴)$$

بنابراین در این حالت :

$$\langle\psi|P_1|\psi\rangle = 1 \quad (۲۰-۴)$$

اندازه گیری حالت را تغییر نمی دهد و قبل و بعد از اندازه گیری حالت $a|100\rangle + b|011\rangle$ می باشد، اندازه گیری فقط نوع خطا را مشخص می کند و چیزی در مورد a,b نمی گوید.

۴-۲-۲-بازیافت

مقدار بدست آمده برای تشخیص خطا را جهت تعیین فرایند مورد نظر برای بازیافت حالت اولیه به کار می بریم.

به طور مثال اگر تشخیص خطا یک باشد کیوبیت اول تغییر حالت داده است پس با تصحیح کیوبیت اول به حالت اولیه $a|000\rangle + b|111\rangle$ می رسیم. با اعمال چهار عملگر تصویرگر نتایج زیر حاصل می شود که برای بازیافت استفاده می شود.

- اگر مقدار صفر باشد هیچ خطایی رخ نداده است.
- اگر مقدار یک باشد یعنی بیت برگردان روی کیوبیت اول انجام شده است
- اگر مقدار دو باشد یعنی کیوبیت دوم تغییر حالت داده است.
- اگر مقدار سه باشد یعنی بیت برگردان روی کیوبیت سوم انجام شده است و کافی است کیوبیت سوم را وارون کنیم تا حالت اولیه بدست آید.

این روش تصحیح خطا به خوبی نتیجه می دهد. احتمال اینکه بیت برگردان روی یک کیوبیت یا کمتر از یکی از سه کیوبیت انجام شود با رابطه ۴-۲۱ بیان می شود:

$$(1-p)^3+3p^2(1-p)=1-3p^2+2p^3 \qquad (۲۱-۴)$$

پس احتمال اینکه بیشتر از یک خطا داشته باشیم، $3p^2+2p^3$ است که مشابه این را برای کد تکرار کلاسیکی بدست آوردیم.

یک روش دیگر جهت تشخیص خطا وجود دارد که متفاوت با اندازه گیری از طریق عملگر تصویرگر است.

فرض کنید به جای اینکه انداره گیری با چهار عملگر تصویرگر انجام شود ما دو اندازه گیری را انجام می دهیم، اولین اندازه گیری را با عملگر Z_1Z_2 انجام می دهیم و دومین اندازه گیری را با عملگر Z_2Z_3 انجام داده.که $Z_1Z_2=Z\otimes Z\otimes I$ عملگر Z_1Z_2 روی کیوبیت اول و دوم اثر می گذارد و عملگر Z_2Z_3 روی کیوبیت دوم و سوم اعمال می شود. مقادیر ویژه این دو عملگر ± 1 است. عملگر Z_1Z_2 تجزیه طیفی زیر را دارد:

$$Z_1Z_2=\left(|00\rangle\langle 00|+|11\rangle\langle 11|\right)\otimes I-\left(|01\rangle\langle 01|+|10\rangle\langle 10|\right)\otimes I \qquad (۲۲-۴)$$

که با دو اندازه گیری توسط تصویر گرهای زیر متناظر است:

$$\left(|00\rangle\langle 00|+|11\rangle\langle 11|\right)\otimes I,\left(|01\rangle\langle 01|+|10\rangle\langle 10|\right)\otimes I$$

با اعمال Z_1Z_2 بر روی حالت خروجی اگر نتیجه (+۱) حاصل شد یعنی کیوبیت اول و دوم خروجی با کیوبیت متناظر ورودی یکسان هستند و اگر نتیجه (-۱) حاصل شود یکی از کیوبیت ها تغییر حالت داده است سپس عملگر Z_2Z_3 را روی حالت خروجی اعمال کرده، اگر نتیجه (+۱) حاصل شد کیوبیت دوم و سوم تغییر حالت نداده است و اگر نتیجه (-۱) حاصل شد یکی از کیوبیت های دوم یا سوم تغییر حالت داده است. با قیاس نتیجه اندازه گیری دو عملگر Z_1Z_2 و Z_2Z_3 می توان تصحیح خطا را انجام داد یعنی اگر نتیجه حاصله از هر دو اندازه گیری (+۱) باشد

خطا نداریم اما اگر نتیجه اندازه گیری Z_1Z_2، (+۱) و Z_2Z_3، (-۱) باشد پس کیوبیت سوم تغییر حالت داده است، و اگر نتیجه اندازه گیری Z_1Z_2، (-۱) و نتیجه اندازه گیری Z_2Z_3، (+۱) باشد کیوبیت اول تغییر حالت داده است و در نهایت اگر نتیجه اندازه گیری هر دو عملگر Z_1Z_2 و Z_2Z_3، (-۱) باشد کیوبیت دوم تغییر حالت داده است. بعد از اینکه کیوبیتی را که دچار خطا شده بود را یافتیم، با برگرداندن بیت به حالت اولیه تصحیح خطا انجام می شود.

این نوع روش تصحیح خطا برای کد گذاری سه کیوبیتی می باشد و در صورتی که حالت کوانتومی از کانال بیت برگردان عبور کرده باشد بعد از اندازه گیری ها و نتایج حاصله، تشخیص خطا انجام شده و در نهایت بیتی را که دچار خطا شده را وارون می کنیم و حالت اولیه را بازیافت می کنیم.

۴-۳-بهبود بخشیدن خطا

روش تشریح شده در بخش قبل یک روش کامل و کافی برای تصحیح خطا نمی باشد، چون خطاها و حالت ها در مکانیک کوانتومی با احتمال مساوی رخ نمی دهند و فضای که حالت های کوانتومی در آن هستند پیوسته است بنابراین ممکن است برای هر خطای ممکن، حالت به اندازه کوچکی تغییر کند و آن را بطور کامل آشفته سازد.

به عنوان مثال، کانال وارون بیتی روی حالت $1/\sqrt{2}(|0\rangle+|1\rangle)$ بطور کلی اثر ندارد، اما در واقع حالت $|0\rangle$ را به $|1\rangle$ تبدیل می کند و بالعکس. برای رفع این مشکل از ضریب اطمینان استفاده می کنیم. یادآوری می کنیم که ضریب اطمینان بین یک حالت خالص و آمیخته بصورت زیر تعریف می شود:

$$F(|\psi\rangle,\rho)=\sqrt{\langle\psi|\rho|\psi\rangle} \qquad (۲۳-۴)$$

بدون استفاده کردن از کد تصحیح خطا حالت کیوبیت بعد از عبور از کانال بصورت زیر است.

$$\rho=(1-p)|\psi\rangle\langle\psi|+pX|\psi\rangle\langle\psi|X \qquad (۲۴-۴)$$

بنابراین ضریب اطمینان می شود:

$$
\begin{aligned}
F(|\psi\rangle,\rho) &= \sqrt{\langle\psi|\rho|\psi\rangle} \\
&= \sqrt{\langle\psi|(1-p)|\psi\rangle\langle\psi| + pX|\psi\rangle\langle\psi|X|\psi\rangle} \\
&= \sqrt{(1-p)\langle\psi|\psi\rangle\langle\psi|\psi\rangle + p\langle\psi|X|\psi\rangle\langle\psi|X|\psi\rangle} \\
F(|\psi\rangle,\rho) &= \sqrt{(1-p) + p\langle\psi|X|\psi\rangle\langle\psi|X|\psi\rangle}
\end{aligned}
\qquad (۲۵-۴)
$$

جمله دوم زیر رادیکال معادله فوق تحت ریشه مربعی مثبت است و اگر $|\psi\rangle = |0\rangle$ باشد صفر می شود. بنابراین مینیمم مقدار ضریب اطمینان عبارت است از:

$$F = \sqrt{1-p} \qquad (۲۶-۴)$$

فرض کنید که کد تصحیح خطای سه کیوبیت استفاده شده است در این صورت داریم:

$$|\psi\rangle = a|o_{\angle}\rangle + b|1_{\angle}\rangle \qquad (۲۷-۴)$$

بعد از کد گذاری حالت، آن را از درون کانال عبور داده، با توجه به اینکه احتمال اثر بیت برگـردان روی یک کیوبیت $3P(1-p)^2$ است و احتمال اینکه هیچ کیوبیتی دچار خطا نشود $(1-p)^3$ است بعد از تصحیح خطا حالت نهایی حالت کوانتومی عبارت است از :

$$\rho = \left[(1-p)^3 + 3p(1-p)^2\right]|\psi\rangle\langle\psi| + \ldots \qquad (۲۸-۴)$$

و اگر دو کیوبیت یا بیشتر از آن دچار خطا شود جملات بعدی را می نویسیم. این جمـلات همگـی مثبت هستند پس ضریب اطمینان محاسباتی ما کران پایین خواهد داشت :

$$F = \sqrt{\langle\psi|\rho|\psi\rangle} \geq \sqrt{3p(1-p)^2 + (1-p)^3} \qquad (۲۹-۴)$$

یعنی مینیمم مقدار ضریب اطمینان $\sqrt{1-3p^2+2p^3}$ می باشد.

اکنون با قیاس دو رابطه (۲۸-۴)و (۲۹-۴)میبینیم که به ازا $p<1/2$ قدرت ضریب اطمینان در حالی که تصحیح خطا انجام شده است بالاتر است.

۴-۴-کد فاز بر گردان سه کیوبیتی

عملگرکانال فاز برگردان نوعی دیگر از خطای کوانتومی است،در این کانال حالت سیستم $|\psi\rangle = a|0\rangle + b|1\rangle$ سیستم به حالت $|\psi\rangle = a|0\rangle - b|1\rangle$ تبدیل می شود. با احتمال $1-p$ حالت کیوبیت ثابت است و با احتمال p حالت کیوبیت تغییر می کند. عملگر خطای فازی Z می باشد، هیچ معادل کلاسیکی برای این کانال وجود ندارد چون فاز، مشابهی در کلاسیک ندارد. بنابراین تحلیل مستقیم آن مشکل است و برای مطالعه آن، این کانال را به کانال بیت برگردان تبدیل می کنیم.

بنابراین در پایه های کیوبیتی $|+\rangle = 1/\sqrt{2}(|0\rangle+|1\rangle)$, $|-\rangle = 1/\sqrt{2}(|0\rangle-|1\rangle)$ کار می کنیم.

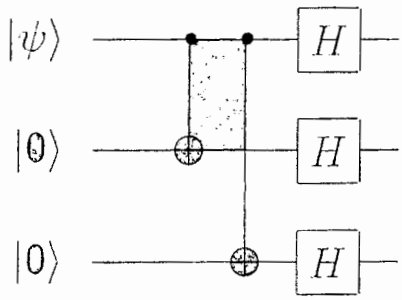
با این پایه ها عملگر Z ، $|+\rangle$ را به $|-\rangle$تبدیل می کند و بالعکس، درست مثل عملگر بیت برگردان که به جای $|0\rangle$ و $|1\rangle$ به ترتیب $|+\rangle$ و $|-\rangle$ به کار برده شده است.

می توان حالت های منطقی $|0_L\rangle \equiv |+++\rangle$ و $|1_L\rangle \equiv |---\rangle$ را برای محافظت در برابر خطای فاز برگردان استفاده کرد. تمام عملیات تصحیح خطا که برای کانال بیت گردان به کار برده ایم برای آشکار سازی و بازیافت خطای فازی نیز به کار می بریم. اما با این تفاوت که پایه های $|0\rangle,|1\rangle$جای خود را به پایه های $|+\rangle,|-\rangle$می دهند.

جهت تغییر پایه ها $|0\rangle$ و $|1\rangle$ به $|+\rangle$ و $|-\rangle$ از گیت ها دامارد استفاده می شود.

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad (۳۰-۴)$$

کد گذاری در کانال فاز برگردان در دو مرحله انجام می شود اول سه کیوبیت را مثل کانال بیت بر گردان رمز گذاری می کنیم و دوم اینکه مانند شکل ۴-۳ برای هر کیوبیت بعد از مرحله اول گیت هادامارد را به کار می بریم.



شکل۴-۳-مدار کدگذاری کد خطای فاز

تعیین خطا با بکارگیری اندازه گیری تصویری مانند قبل انجام می شود با این تفاوت که عملگر بکار رفته با گیت هادامارد ترکیب شده است:

$$P_j \to P_j' \equiv H^{\otimes 3} P_j H^{\otimes 3} \qquad (۳۱-۴)$$

تشخیص خطا را می توان با عملگرهای زیر بدست آورد.

$$H^{\otimes 3} Z_1 Z_2 H^{\otimes 3} = X_1 X_2 \qquad (۳۲-۴)$$

$$H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3 \qquad (۳۳-۴)$$

اعمال عملگر های $X_3 X_4$ و $X_1 X_2$ به ترتیب جهت قیاس علامت کیوبیت های اول و دوم و همچنین کیوبیت های دوم و سوم بکار می رود.

۴-۵-کد شر (shor code)

کد شر مثال ساده ای از کد تصحیح خطای کوانتومی است که می تواند یک کیوبیت را از اثر هر خطای دلخواه کوانتومی محافظت کند، این کد ترکیبی از کدهای بیت برگردان سه کیوبیتی و فاز برگردان سه کیوبیتی می باشد.

ابتدا با استفاده از کد فاز برگردان کیوبیتها را کد گذاری می کنیم. یعنی:

$$|0\rangle \to |+++\rangle \qquad (۳۴-۴)$$

$$|1\rangle \to |---\rangle \qquad (۳۵-۴)$$

در مرحله بعد هر کدام از این کیوبیت ها را با استفاده از کد بیت برگردان سه کیوبیتی کد گذاری می کنیم.

حالت $|+\rangle$ را تحت حالت $(|000\rangle+|111\rangle)/\sqrt{2}$ وحالت $|-\rangle$ را تحت حالت $(|000\rangle-|111\rangle)/\sqrt{2}$ می کنیم نتیجه حاصل یک کد ۹ کیوبیتی با کد-کلمه[1] زیر است:

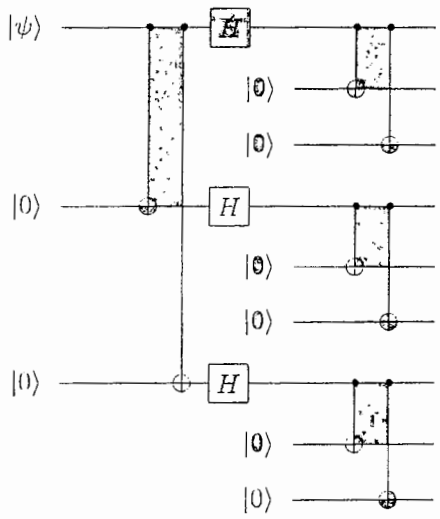
$$|0\rangle \to |0_L\rangle \equiv \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}} \qquad (۳۶-۴)$$

$$|1\rangle \to |1_L\rangle \equiv \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}} \qquad (۳۷-۴)$$

مدار کوانتومی کد شور در شکل ۴-۴ نشان داده شده است.

همان طور که قبلا هم بیان شد، قسمت اول مدار کد گذاری کیوبیت ها را با استفاده از کد فاز برگردان سه کیوبیتی انجام میدهند. دومین قسمت مدار، هر کدام از این کیوبیت ها را با استفاده از کد بیت برگردان کد گذاری می کند که سه کپی از مدار رمزگذاری کد بیت برگردان شکل۴-۴ را استفاده کرده ایم. این یک روش برای بدست آوردن کدهای جدید از کدهای قبلی بود.

1-code word



شکل ۴-۴-مدار کد گذاری نه کیوبیتی کد شر

کد شر قادر به محافظت هر کیوبیت در برابر خطاهای فازبرگردان و بیت برگردان است. برای اینکه این موضوع را بیشتر درک کنیم فرض کنید که کیوبیت اول دچار خطای بیت برگردان شده است؛ با اندازه گیری توسط عملگر Z_1Z_2 متوجه می شویم که یا کیوبیت اول دچار خطا شده است یا کیوبیت دوم؛ و با اعمال عملگر Z_2Z_3 کیوبیت دوم و سوم را قیاس می کنیم. مشاهده می شود که در کیوبیت دوم و سوم خطایی رخ نداده است. پس قطعا کیوبیت اول دچار خطا شده است.حال با وارون کردن کیوبیت اول، حالت اولیه را بازیافت می کنیم.

مشابه این روش می توان خطاهایی که در اثر خطای فاز برگردان نیز به وجود آمده اند را روی هر یک از کیوبیتها مشابه زیر تغییر می کند:

$$(|000\rangle + |111\rangle) \rightarrow (|000\rangle - |111\rangle) \qquad (۳۸-۴)$$

و یا بالعکس رابطه فوق؛

در واقع فاز برگردان روی هر کدام از سه کیوبیت اول این اثر را دارد و تصحیح خطا برای هر کدام از این کیوبیت ها انجام خواهد شد. با مقایسه علامت بلوک های اول و ذوم از سه کیوبیت اندازه گیری انجام می شود.

اگر هر دو خطای فاز برگردان و بیت برگردان برای کیوبیت اول رخ دهد یعنی عملگر Z_1X_1 روی آن کیوبیت اعمال شده است. پس به سادگی می توان دید که فرایند تشخیص خطای بیت برگردان یک خطای بیت برگردان را روی کیوبیت اول مشخص می کند و آن را تصحیح می کند و فرایند تشخیص خطای فاز برگردان خطای مربوط به کیوبیت اول را مشخص می کند. بنابراین کد شر قادر به تصحیح خطای ترکیبی از خطاهای بیت برگردان و فاز برگردان روی کیوبیت واحد می باشد.

برای ساده سازی تحلیل فوق فرض کنیم نویزی اختیاری روی کیوبیت اول رخ داده است و قبلا بیان کردیم که ξ را به شکل عملگر sum با عناصر ماتریسی $\{E_i\}$ بیان می کنیم.

فرض کنید حالت کیوبیت بعد از کد گذاری بصورت زیر باشد

$$|\psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle \qquad (۳۹-۴)$$

بعد از اعمال نویز حالت $|\psi\rangle$ به حالت زیر تبدیل شود :

$$\xi(|\psi\rangle\langle\psi|) = \sum_i E_i|\psi\rangle\langle\psi|E_i' \qquad (۴۰-۴)$$

برای تحلیل آثار تصحیح خطا ساده تر است تا اثر تصحیح خطا را روی یک جمله به جای جمع فوق متمرکز کنیم؛ یعنی:

$$E_i|\psi\rangle\langle\psi|E_i' \qquad (۴۱-۴)$$

آنگاه E_i عملگری است که تنها روی کیوبیت اول اعمال می شود و ممکن است بصورت ترکیب خطی از عملگر یکانی I وعملکر بیت برگردان X_1 و عملگر فاز برگردان Z_1 و عملگر ترکیبی از بیت برگردان و فاز برگردان X_1Z_1 می باشد.

$$E_i = e_{i1}I + e_{i1}X_1 + e_{i2}Z_1 + e_{i3}X_1Z_1 \qquad (۴۲-۴)$$

حالت کوانتومی $E_i|\psi\rangle$ بصورت بر هم نهی چهار حالت $|\psi\rangle, X_1|\psi\rangle, Z_1|\psi\rangle, X_1Z_1|\psi\rangle$ نوشته می شود. با اندازه گیری و تشخیص خطا،حالت بر هم نهی به یکی از این چهار حالت $X_1Z_1|\psi\rangle$ و $Z_1|\psi\rangle$ و $X_1|\psi\rangle$ و $|\psi\rangle$ تبدیل می شود و حالت اصلی آشفته می شود؛ با به کار بردن عملگر معکوس مناسب می توان حالت نهایی با عمل بازیافت به حالت اولیه تبدیل کرد.

۴-۶-نظریه تصحیح خطای کوانتومی

در این بخش یک چهار چوب کلی برای مطالعه تصحیح خطای کوانتومی ارائه می دهیم که شرایط تصحیح خطای کوانتومی را در بر می گیرد. ایده اصلی نظریه تصحیح خطای کوانتومی تعمیم یافته ایده معرفی شده در کد شر می باشد، حالت های کوانتومی با عملگر یونیتاری کد گذاری می شود؛ کد تصحیح خطای کوانتومی همانند زیر فضای C از فضای هیلبرت بزرگتر تعریف می شود. عملگر P را عملگر تصویرگر برای فضای C معرفی می کنیم که برای کد بیت برگردان سه کیوبیتی، P را بصورت زیر معرفی می کنیم.

$$P = |000\rangle\langle 000| + |111\rangle\langle 111| \qquad (۴۳-۴)$$

بعد از کد گذاری کردن، حالت کوانتومی در معرض نویز قرار می گیرد و به دنبال آن اندازه گیری خطا انجام می شود تا خطای رخ داده شده تشخیص داده شود و بعد عمل بازیافت را داریم تا حالت کوانتومی به حالت اولیه برگردد.

برای داشتن نظریه بهتر ما فرض های کلی تری را در نظر می گیریم. نویزها با یک عملگر کوانتومی ξ بیان می شود و فرایند تصحیح خطا با یک عمل کوانتومی رد نگه دار R که عمل تصحیح خطا می نامیم انجام می شود.

$$(R \circ \xi)\rho \propto \rho$$

عمل تصحیح خطا شامل دو مرحله آشکار سازی خطا و بازیافت حالت اولیه است. شرایط تصحیح خطای کوانتومی مجموعه ساده ای از معادلات است که کد تصحیح خطای کوانتومی را در برابر نوع خاصی از نویزهای ξ محافظت می کند.

۴-۵-۱- شرایط تصحیح خطای کوانتومی

با بیان قضیه (۴-۱) شرایط تصحیح خطای کوانتومی را شرح می دهیم.

قضیه(۴-۱) : فرض کنید که C یک کد کوانتومی و P عملگر تصویرگر برای C است، فرض کنید ξعمل کوانتومی با عناصر $\{E_i\}$ می باشد. شرط ضروری و کافی برای وجود یک عمل تصحیح خطای کوانتومی که خطای ξ را در C تصحیح می کند عبارت است از :

$$PE_i^{\dagger}E_jP=\alpha_{ij}P \qquad (۴۴-۴)$$

که α ماتریس هرمیتی از اعداد مختلط است.

تا اینجا محافظت از اطلاعات کوانتومی در برابر فرایند نویز های خاص ξ را بحث کردیم؛ اما بطور دقیق تر ما نمی دانیم که چه نوع نویزی روی سیستم کوانتومی تاثیر گذاشته است با استفاده قضیه زیر بیان می کنیم که عمل تصحیح خطای کوانتومی R قادر به تصحیح چه نویز های می باشد.

قضیه(۴-۲) : قبلا گفتیم که C یک کد کوانتومی است و R عمل تصحیح خطای کوانتومی است؛ فرض کنید که $\mathcal{F}$ یک عمل کوانتومی با عناصر $\{F_j\}$ است که ترکیب خطی از E_i می باشد یعنی:

$$F_j=\sum_i m_{ij}E_i \qquad (۴۵-۴)$$

بنابراین R اثرات فرایند نویز $\mathcal{F}$ روی C را نیز تصحیح می کند.(اثبات در [2] آمده است.)

۴-۷-کدهای تبهگن[1]

کدهای تصحیح کننده خطا در بسیاری از جهات، مشابه با کدهای کلاسیکی هستند. یک خطا با اندازه‌گیری 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 نمی-

1-Degenerate codes

باشند. این ایده به شکل بسیار راحتی برای کد شر توضیح داده می‌شود. اثر خطاهای Z_1 و Z_2 را روی کد–کلمه های کد شر در نظر بگیرید. همانطور که قبلا ملاحظه کردید، اثر این خطاها روی هر دو کد–کلمه مشابه می‌باشد. 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 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.

۴-۸- کران همینگ کوانتومی

در این بخش روشی را برای یافتن بهترین کد کوانتومی بیان می کنیم؛ با معرفی کران همینگ کوانتومی، یک کران پایین که اطلاعاتی در مورد کدهای کوانتومی به ما می دهد را بدست می-آوریم.

متاسفانه کران همینگ فقط در مورد کدهای غیر تبهگن به کار برده می شود؛ فرض کنید یک کد غیر تبهگن برای کد گذاری k کیوبیت از n کیوبیت داریم طوری که قادر است t کیوبیت یا کمتر را تصحیح کند.

اگر تعداد j خطا اتفاق بیفتد پس $j \le t$، تعداد موقعیت هایی که خطاها ممکن است اتفاق بیفتد از ترکیب زیر به دست می آید:

$$\binom{n}{j} \qquad (۴۶-۴)$$

در هر کدام از این موقعیت ها سه خطای ممکن اتفاق می افتد، سه عملگر X,Y,Z پس تعداد کل خطاهایی که روی یک موقعیت اتفاق می افتد 3^j خطای ممکن است.

نهایتا کل خطاها روی همه کیوبیت ها عبارت است از:

$$\sum_{j=0}^{i}\binom{n}{j}3^j \qquad (۴۷-۴)$$

توجه شود اگر j=0 باشد هیچ خطایی روی کیوبیت ها نداریم و عملگر I می تواند به عنوان خطا به حساب آید.

برای کد گذاری k کیوبیت ما از n کیوبیت توسط کد نا تبهگن هر کدام از این خطاها با یک زیر فضای 2^k بعدی متعامد، متناظر است.همه این زیر فضا ها با زیر فضای کلی 2^n بعدی برای n کیوبیت موجود متناسبند بنابراین نامساوی زیر را داریم:

$$\sum_{j=0}^{i}\binom{n}{j}3^j 2^k \le 2^n \qquad (۴۸-۴)$$

این یک کران همینگ است.

بطور مثال فرض کنید می خواهیم یک کیوبیت از n کیوبیت را در حالتی که خطاها روی یک کیوبیت اعمال شده اند را کد گذاری کنیم.در این مورد کران همینگ می شود:

$$\begin{cases} k=1 \\ j=0 \end{cases} \quad \Rightarrow \quad 2(1+3n) \le 2^n \qquad (۴۹-۴)$$

با تحقیق رابطه فوق، می بینیم رابطه به ازا ئ $n \le 4$ برقرار نیست و باید $n \ge 5$ باشد.بنابراین هیچ کد غیر تبهگن که یک کیوبیت را از میان کمتر از ۵ کیوبیت کد گذاری کند و از همه خطاهای ممکن روی یک کیوبیت محافظت کند وجود ندارد.

۴-۹- کدهای خطی کلاسیکی

کدهای تصحیح خطای کلاسیکی کاربرد های فنی مهمی دارد بسیاری از این فن ها مفاهیم مهمی را برای تصحیح خطاهای کوانتومی در بر دارد.

کد خطی C، k بیت از اطلاعات درون فضای کد n بیتی را کد گذاری می کند که این عمل با ماتریس مولد n× k بعدی G انجام می شود، G عضو گروه Z_2 است؛ عناصر Z_2 اعداد صحیح در مدول ۲ می باشند بنابراین فقط مقدار 0 یا ۱ را دارد، و پیام ها را به معادل کد گذاریشان می نگارد بنابراین پیام x با k بیت بصورت Gx کد گذاری می شود؛ پیام x به صورت یک بردار ستونی می باشد و عمل ضرب و تمام اعمال ریاضی دیگر در این مبحث در مدول ۲ محاسبه می شود.

به عنوان مثال برای ماتریس مولد G، کد تکرار را به خاطر آورید؛ کد تکرار تک بیت اولیه را به سه بیت که از تکرار تک بیت حاصل می شد، تبدیل می کرد. ماتریس مولد کد تکرار به صورت زیر است :

$$G=\begin{bmatrix}1\\1\\1\end{bmatrix} \qquad (۵۰-۴)$$

اگر پیغام ها بصورت 0 و ۱ باشد با اعمال G می شود:

$$x=0 \qquad \Rightarrow Gx=\begin{bmatrix}1\\1\\1\end{bmatrix}[0]=[0 \quad 0 \quad 0] \qquad (۵۱-۴)$$

$$x=1 \qquad \Rightarrow Gx=\begin{bmatrix}1\\1\\1\end{bmatrix}[1]=[1 \quad 1 \quad 1] \qquad (۵۲-۴)$$

کد n بیتی که برای کد گذاری k بیت از اطلاعات استفاده می شود به صورت [n,k] نمایش داده می شود. مثلا در مثال قبل کد [3,1] را داریم.

مثال دیگری از کد گذاری، کد گذاری ۲ بیت با سه بار تکرار برای هر بیت می باشد کد [6,2] است و ماتریس مولد آن به صورت زیر است:

$$G=\begin{bmatrix}1 & 0\\ 1 & 0\\ 1 & 0\\ 0 & 1\\ 0 & 1\\ 0 & 1\end{bmatrix} \qquad (۵۳-۴)$$

خواهیم دید:

$$\begin{aligned} &G(0,0) = (0,0,0,0,0,0)\\ &G(0.1) = (0,0,0,1,1,1)\\ &G(1,0) = (1,1,1,0,0,0)\\ &G(1,1) = (1,1,1,1,1,1) \end{aligned} \qquad (۵۴-۴)$$

برای درک بهتر کد های تصحیح خطای کوانتومی شکل استاندارد کد خطی بر حسب ماتریس کنترل پاریته را معرفی می کنیم. در این تعریف کد [n,k] تمام بردارهای x روی گروه Z_2 که x دارای n عنصر می باشد را در بر دارد طوری که:

$$Hx = 0 \qquad (۵۵-۴)$$

H ماتریس کنترل پاریته[1] است و یک ماتریس (n-k)×n بعدی است که همه عناصر آن 0,1 می باشند. برای تعریف کد بر حسب ماتریس کنترل پاریته نیاز به یک تعریف ریاضی داریم که در زیر شرح می دهیم:

تعریف کرنل[2]: دو فضای برداری V,W را در نظر می گیریم و H را به عنوان عملگر تبدیل خطی از V به

W تعریف می کنیم، در این صورت کرنل H به صورت زیر تعریف می شود :

$$\ker H = \{v \in V : Hv = o_W\} \qquad (۵۶-۴)$$

Hv به برداری در فضای W تبدیل می شود که اگر این بردار برابر صفر باشد آن کرنل بدست می آید.

1-check parity matrix
2-kernel

کد A که k بیت از n بیت را کد گذاری می کند 2^k کد- کلمه ممکن دارد بنابراین کرنل H باید k بعدی باشد. پس لازم است که ردیف های H مستقل خطی باشند. می توان کد را به صورت کرنل H تعریف کرد.

می توان ماتریس پاریته را از ماتریس مولد بدست آورد و بالعکس؛ اگر بخواهیم از ماتریس کنترل پاریته H ، ماتریس مولد را بدست آوریم بصورت زیر عمل می کنیم.

K بردارمستقل خطی را که $y_1, y_2, ..., y_k$ هستند را به گونه ای انتخاب می کنیم که کرنل H باشند و به صورت ستونی از $y_1, y_2, ..., y_k$ قرار میدهیم تا Gرا به دست اوریم:

$$G = [y_1, y_2, ... y_k] \qquad (۵۷-۴)$$

$y_1, y_2, ..., y_k$ هر کدام خود یک بردار ستونی هند.

اگر G را داشته باشیم در این صورت n-k بردار مستقل خطی $y_1, y_2, ..., y_{n-k}$ را جدا می کنیم که بر بردارهای ستونی G عمود باشند. آن گاه به صورت ردیفی در یک ماتریس قرار می دهیم که H را تشکیل می دهند.

$$y_1^T, y_2^T, ..., y_{n-k}^T$$

که $y_1^T, y_2^T, ..., y_{n-k}^T$ هر کدام خود یک بردار ردیفی هستند.

$$H = \begin{bmatrix} y_1^T \\ y^T{}_2 \\ \vdots \\ y^T{}_{n-k} \end{bmatrix} \qquad (۵۸-۴)$$

منظور از عمود بودن این است که حاصلضرب داخلی آنها در مدول ۲ برابر صفر است.

به عنوان مثال کد [3,1] را در نظر می گیریم؛ ماتریس مولد آن

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

می باشدکه n=3 , k=1 می باشد با توجه به اینکه $n-k=2$ ، بنابراین دو بردار مستقل خطی را که بر G عمود هستند را پیدا می کنیم:

$$\begin{bmatrix}1\\1\\0\end{bmatrix} \quad ; \quad \begin{bmatrix}0\\1\\1\end{bmatrix}$$

حال بردارهای عمود بر دو بردار فوق را بدست می آوریم:

$$y_1{}^T = [1 \quad 1 \quad 0] \quad ; \quad y_2{}^T = [0 \quad 1 \quad 1]$$

پس H بدست می آید:

$$H = \begin{bmatrix}1 & 1 & 0\\0 & 1 & 1\end{bmatrix}$$

به سادگی می توان تحقیق کرد که به ازائ کد-کلمه های $x = [1 \quad 1 \quad 1]; x = [0 \quad 0 \quad 0]$ ، $Hx = 0$ می شود:

$$Hx = \begin{bmatrix}1 & 1 & 0\\0 & 1 & 1\end{bmatrix}\begin{bmatrix}1\\1\\1\end{bmatrix} = \begin{bmatrix}1+1+0\\0+1+1\end{bmatrix} = \begin{bmatrix}0\\0\end{bmatrix}$$

حاصلضربها در مدول ۲ محاسبه می شود. با ماتریس کنترل پاریته، تصحیح خطا و بازیافت حالت اولیه امکان پذیر است.

فرض کنید که x را به صورت y=Gx کد گذاری کرده ایم، یک خطایe ، مربوط به نویز رخ می-دهد و اطلاعات نهایی دریافتی با حضور نویز به صورت زیر به دست می آید:

$$y' = y + e \qquad (۵۹-۴)$$

(توجه شود که علامت + ، علامت جمع بیت به بیت در مدول ۲ می باشد.)

چون Hy=0 به ازائ همه کد-کلمه ها برقرار است، بنابراین

$$Hy' = He \qquad (۶۰-۴)$$

Hy' را کرنل تشخیص خطا نامیم و نقشی مشابه نقش تشخیص خطای توضیح داده شده در تصحیح خطای کوانتومی را ایفا می کند. Hy' تابعی از فروپاشی حالت y' فقط به این عنوان که تشخیص خطای کوانتومی با اندازه گیری حالت کوانتومی تخریب شده بدست می آید و چون رابطه

$Hy' = He$ برقرار است تشخیص خطا اطلاعاتی در باره خطایی که رخ داده است می دهد و قـادر خواهیم بود کلمه رمز اولیه را بازیافت کنیم.

اگر خطایی رخ ندهد تشخیص خطا Hy' مساوی با صفر خواهد بود و زمانی که تنها یک خطا روی j امین بیت رخ دهد(j نمایانگر کیوبیتی است که خطا روی آن رخ داده است و اگر اولین کیوبیتی j=1 ، دومین بیت j=2 و...) تشخیص خطا $Hy' = He_j$ می باشـد. حـال اگـر بیـشتر از دو بیـت دچار خطا شود تشخیص خطای Hy' را محاسبه کرده و آن را با He_j قیاس می کنیم تا بیتـی را که دچار خطا شده بدست آوریم. تصحیح خطای کوانتومی ممکن است با یک کد خطی که با توجه به تعریف فاصله بدست می آید، انجام شود.

فرض کنید که x,y هر کدام کلمات n بیتی باشند، مسافت همینگ d(x,y) ، تعداد مکان های است که در آن بیت های x,y با هم متفاوت است.

$$\begin{matrix} x = (1,1,0,0) \\ y = (0,1,0,1) \end{matrix} \quad \Rightarrow \quad d\big((1,1,0,0),(0,1,0,1)\big) = 2$$

وزن همینگ x ، مسافتی است که در آن تعداد مکانی که x با پیغامی با همان طول که همه صفر هستند، در صفر تفاوت دارد؛ به طور مثال:

$$\begin{matrix} x = 1100 \\ I = 0000 \end{matrix} \quad \Rightarrow \quad d(x,y) = 2, wt(x) = 2$$

توجه کنید که

(۶۱-۴)

$$d(x,y) = wt(x \oplus y)$$

و در نتیجه :

$$d(y,y') = wt(e) \qquad (۶۲-۴)$$

برای درک مطلب فوق مثال زیر را در نظر بگیرید.

مثال: $[n,k]=[3,1]$, $0 \to 000$

حالت اولیه x تحت کد گذاری به حالت y تبدیل می شود $y=Gx$ اگر y دچار خطا شود پس $y'=y+e$ از میان خطاهای ممکن محتمل ترین خطا، یعنی خطای با کمترین وزن همینگ را در نظر می گیریم. اگر سیستم دچار خطا شده باشد $He \neq 0$ است و اگر خطا نداشته باشیم $He=0$ می باشد.

$$\underset{p(1-p)^2}{\begin{bmatrix}1\\0\\0\end{bmatrix}} \quad \underset{p(1-p)^2}{\begin{bmatrix}0\\1\\0\end{bmatrix}} \quad \underset{p(1-p)^2}{\begin{bmatrix}0\\0\\1\end{bmatrix}} \quad \underset{(1-p)^3}{\begin{bmatrix}0\\0\\0\end{bmatrix}}$$

$$3p(1-p)^2+(1-p)^3=2p^3+1-3p^2$$

$$\underset{p^2(1-p)}{\begin{bmatrix}1\\1\\0\end{bmatrix}} \quad \underset{p^2(1-p}{\begin{bmatrix}0\\1\\1\end{bmatrix}} \quad \underset{p^2(1-p)}{\begin{bmatrix}1\\0\\1\end{bmatrix}} \quad \underset{p^3}{\begin{bmatrix}1\\1\\1\end{bmatrix}}$$

$$p_e=3p^2(1-p)+p^3=3p^2-3p^3$$

برای p<1/2 خواهیم داشت که $p_e < p$.

تعریف: فاصله یک کد C که آن را با d(c) یا d نمایش می دهیم برابر است با کمترین فاصله که بین کلمات آن وجود دارد؛ به عبارت دیگر

$$d=d(c)=\min_{x,y\in c, x\neq y} d(x,y) \qquad (۶۳-۴)$$

اما d(x,y)=w(x+y) پس

$$d=d(c)=\min_{x\in c, x\neq 0} wt(x) \qquad (۶۴-۴)$$

کدی که برای کد کردن k بیت بکار می رود و فاصله آن برابر d است با نماد [n,k,d] نشان داده می شود.

کدی که فاصله آن برابر d=2t+1 باشد قادر است که t خطا را تصحیح کند. فاصله همینگ بیت y و بیت خطا یافته y' به صورت زیر تعریف می شود.

$$d(y, y') \le t \qquad (۴۵-۴)$$

۴-۱۰- کد همینگ

یک نوع خوب از کد تصحیح خطای خطی کد همینگ است. اگر $r \ge 2$ یک عدد صحیح باشد، H ماتریس کنترل پاریته کد است که ستونهای آن بردارهای غیر صفر با طول r هستند. یک کد همینگ به شکل $[2^r - 1, 2^r - r - 1, 3]$ تعریف می شود.

بطور مثال به ازای r=3 ، کد بصورت [7,4,3] است که ماتریس پاریته زیر را دارد.

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

هر دو ستون از ماتریس با هم متفاوتند، بنابراین مستقل خطی است.

۴-۱۱- کدهای دوگان[1]

فرض کنید کد C به صورت [n,k] است و ماتریس مولد آن G می باشد و ماتریس کنترل پاریته H را دارد. ما می توانیم یک کد دیگر تعریف کنیم که دوگان C نام دارد و با $C^{\perp}$ نشان می دهیم که به ترتیب دارای ماتریس مولد و کنترل پاریته $H^{\perp}$ و $G^{\perp}$ می باشد.

دوگان C شامل کد-کلمه های y است طوری که y بر همه کد-کلمه های درون C عمود است.

1-dual

می توان از ساختار کدهای خطی دوگان برای مطالعه تصحیح خطای کوانتومی استفاده کـرد و راه حلی برای ساختار نوع مهمی از کدهای کوانتومی شناخته شده به نام CSS می باشد.

می گوییم که یک کد، خود دوگان ضعیف[1] است اگر $C \subseteq C^{\perp}$ باشد و تعریف می کنیم که یک کد، خود دوگان قوی[2] است اگر $C = C^{\perp}$ باشد.

به طور مثال کد زیر یک کد خود دوگان قوی است.

$$\begin{cases} c = \{0000,0011,1100,1111\} \\ c^{\perp} = \{0000,0011,1100,111\} \end{cases} \Rightarrow c = c^{\perp} \qquad (۴۶-۴)$$

و کد زیر یک کد دوگان ضعیف است.

$$\begin{cases} c = \{0000,0011\} \\ c^{\perp} = \{0000,0011,1100,1111\} \end{cases} \Rightarrow c \subseteq c^{\perp} \qquad (۴۷-۴)$$

۴-۱۲-کدهای CSS (cladrbank-shor-steane)

کد کوانتـومی CSS از نـام کاشـفانه آن cladrbank-shor-steane گرفتـه شـده اسـت و یـک زیـر مجموعه از کدهای تثبیت کننده می باشد.

فرض کنید که C_1 و C_2 کدهای خطی کلاسیکی $[n,k_1]$ و $[n,k_2]$ هستند طوریکـه $C_2 \subset C_1$ و $C_1, C_2^{\perp}$ هر دو تعداد t خطا را تصحیح می کنند. ما کد کوانتومی $[n,k_1-k_2]$ را تعریف کرده کـه همان کد $CSS(C_1,C_2)$ است و توانایی تصحیح خطـای ایجـاد شـده روی t کیوبیـت را دارد .کـد CSS به صورت زیر تعریف می شود.

فرض کنید $x \in c_1$ و x یک کد کلمه در کد C_1 می باشد، سپس حالت کوانتومی زیـر را تعریـف می کنیم که حالت کد گذاری شده با CSS می باشد:

$$|x + c_2\rangle \equiv \frac{1}{|c_2|}\sum_{y \in c_2} |x + y\rangle \qquad (۴۸-۴)$$

که + جمع بیت به بیت در مدول ۲ می باشد.

فرض کنید x' یک عضو C_1 می باشد طوری که $x - x' \in C_2$ ، آن‌گاه:

۱-weakly self-dual
۲-strictly self-dusl

$$|x'+c_2\rangle \equiv \frac{1}{|c_2|}\sum_{y\in c_2}|x'+y\rangle \qquad (۶۹\text{-}۴)$$

$$|(x-x')+c_2\rangle \equiv \frac{1}{|c_2|}\sum_{y\in c_2}|(x-x')+y\rangle \Rightarrow$$

$$|(x-x')+c_2\rangle = \frac{1}{|c_2|}\left[\sum_{y\in c_2}|x+y\rangle - \sum_{y\in c_2}|x'+y\rangle\right] \qquad (۷۰\text{-}۴)$$

$$\begin{aligned}|(x-x')+c_2\rangle &= \frac{1}{|c_2|}\left[\sum_{y\in c_2}|x+y\rangle\right] - \frac{1}{|c_2|}\left[\sum_{y\in c_2}|x'+y\rangle\right] \\ &= |x+c_2\rangle - |x'+c_2\rangle\end{aligned} \qquad (۷۱\text{-}۴)$$

و چون $x-x'\in C_2$ بنابراین :

$$|(x-x')+c_2\rangle = \frac{1}{|c_2|}\sum_{y\in c_2}|(x-x')+y\rangle = 0 \qquad (۷۲\text{-}۴)$$

با توجه به رابطه (۷۱-۴) و (۷۲-۴) نتیجه می گیریم که:

$$|x+c_2\rangle = |x'+c_2\rangle \qquad (۷۳\text{-}۴)$$

بنابراین $|x+C_2\rangle$ تنها به هم مجموعه C_2 اگر x در C_1 است بستگی دارد. $|x+C_2\rangle$ هم مجموعه های C_2 در C_1 هستند.

اگر x',x مربوط به هم مجموعه های متفاوت C_2 باشند در این حالت به ازائ $y,y'\in C_2$ خواهیم داشت.

$$x+y = x'+y' \qquad (۷۴\text{-}۴)$$

در نتیجه $|x'+c_2\rangle$ و $|x+c_2\rangle$ حالتهای متعامد هستند.

کد $CSS(C_1,C_2)$ با فضای برداری که به وسیله بردارهای حالت $|x\oplus c_2\rangle$ که به ازائ تمام $x\in C_1$ به وجود می آید تعریف می شود.

تعداد هم مجموعه های C_2 در C_1 با $\frac{|C_1|}{|C_2|}$ تعریف می شود طوری که بعد کد CSS ، $|C_1|/|C_2| = 2^{k_1-k_2}$ می باشد بنابر این کد $CSS(C_1, C_2)$ یک کد کوانتومی $[n, k_1 - k_2]$ می باشد.

حال از ویژگی تصحیح کد کلاسیکی C_1 و $C_2^{\perp}$ برای تشخیص و تصحیح خطای کوانتومی استفاده می کنیم. در واقع می توان تصحیح خطا برای t بیت که دچار خطای بیت برگردان و خطای فاز برگردان است با کد CSS که به ترتیب با استفاده از ویژگی های کد C_1 و $C_2^{\perp}$ بدست می آید، انجام داد.

فرض کنید که خطای بیت برگردان با یک بردار n بیتی e_1 توصیف می شود، بردار e_1،در مکانهایی که بیت تغییر کرده یک می باشد و در باقی موارد صفر هست. خطای فاز برگردان با یک بردار n بیتی e_2 توصیف می شود. بردار e_2،در مکانهایی که فاز تغییر کرده یک می باشد و در باقی موارد صفر می باشد. اگر $|x + c_2\rangle$ حالت اولیه باشد پس حالت نهایی بعد از رخ دادن نویز

$$\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y).e_2}\left|x+y\ +e_1\right\rangle \qquad (۷۵-۴)$$

می باشد.

برای اینکه خطای بیت برگردان را آشکار کنیم $n-k_1$ تا حالت کمکی کیوبیتی را که در بردارنده کیوبیت های کافی برای ذخیره کردن تشخیص خطا در کد C_1 می باشد و همه آنها در حالت $|0\rangle$ باشند را در نظر می گیریم با بکار گیری ماتریس پاریته H_1 برای کد C_1 محاسبات برگشت پذیر را انجام می دهیم. ما به مداری نیاز داریم که عملیات زیر را انجام دهد:

$$\left|x+y\ +e_1\right\rangle|0\rangle \rightarrow \left|x+y\ +e_1\right\rangle|H(x+y+e_1)\rangle \qquad (۷۶-۴)$$

بنابراین

$$|H(x+y+e_1)\rangle = \left|x+y\ +e_1\right\rangle|He_1\rangle$$

چون $(x+y)\in C_1$ با ماتریس کنترل پاریته از بین می رود، که با استفاده از مدار C-NOT می توان این عملیات را نشان داد.

با تاثیراین عملیات حالت زیر را داریم :

$$\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y).e_2}\left|x+y\ +e_1\right\rangle\left|He_1\right\rangle \qquad (۷۷-۴)$$

آشکار سازی خطا برای خطای بیت برگردان با استفاده از حالت کمکی $|0\rangle$ و انـدازه گیـری آن و بدست آوردن نتیجه H_1e_1 و حذف حالت کمکی، بصورت زیر بدست می آید.

$$\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y).e_2}\left|x+y\ +e_1\right\rangle \qquad (۷۸-۴)$$

با یافتن H_1e_1 ، تشخیص خطا بدست می آید و از آنجا که C_1 ، تا t خطا را تصحیح می کند آشکار سازی خطا کامل می باشد؛ بازیافت خطا به آسانی با استفاده از گیـت NOT انجـام مـی شـود. بـا حذف خطاهای e_1 حالت به صورت زیر می باشد:

$$\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y).e_2}\left|x+y\right\rangle \qquad (۷۹-۴)$$

برای آشکار سازی خطای فاز برگردان، گیت هادامارد را روی کیوبیت ها اعمـال مـی کنـیم پـس حالت بعد از اعمال گیت هادامارد عبارت است از :

$$\begin{aligned}&\frac{1}{\sqrt{|C_2|2^n}}\sum_z\sum_{y\in C_2}(-1)^{(x+y)e_2+(x+y)z}\left|z\right\rangle\\&=\frac{1}{\sqrt{|C_2|2^n}}\sum_z\sum_{y\in C_2}(-1)^{(x+y)(e_2+z)}\left|z\right\rangle\end{aligned} \qquad (۸۰-۴)$$

که جمع روی همه مقادیر برای n حالت بیت با z بیان می شود.

اگر $z'=z+e$ آنگاه می توان حالت را به صورت زیر باز نویسی کرد :

$$\frac{1}{\sqrt{|C_2|2^n}}\sum_{z'}\sum_{y\in C_2}(-1)^{(x+y).z'}\left|z'+e_2\right\rangle \qquad (۸۱-۴)$$

قضیه: اگر C یک کد خطی باشد می توان نشان داد اگر $x\in C^{\perp}$ آنگـاه $\sum_{y\in C}(-1)^{x.y}=|C|$ و اگـر $x\notin C^{\perp}$ آنگاه $\sum_{y\in C}(-1)^{x.y}=0$

بنابر قضیه فوق داریم که اگر $z'\in C_2^{\perp}$ باشد داریم :

$$\sum_{y\in C_2}(-1)^{x.z'}=|C_2|$$

و اگر $z' \notin C_2^{\perp}$ آنگاه

$$\sum_{y \in C_2} (-1)^{x.z'} = 0$$

در نتیجه خواهیم داشت:

$$\frac{1}{\sqrt{\frac{2^n}{|C_2|}}} \sum_{z' \in C_2^{\perp}} (-1)^{x.z'} |z' + e_2\rangle \qquad (۸۲-۴)$$

می بینیم حالت نهایی به خطای بیت برگردان e_2 وابسته است.بنابراین برای آشکار سازی و بازیافت خطا درست مثل روند تشخیص خطای بیت برگردان عمل کرده یعنی از k_2 تا حالت کمکی $|0\rangle$ و با معرفی ماتریس پاریته H_2 برای $C_2^{\perp}$ تشخیص خطای $H_2 e_2$ بدست می آید. با تصحیح خطای بیت برگردان e_2 بدست می آورد:

$$\frac{1}{\sqrt{\frac{2^n}{|C_2|}}} \sum_{z' \in C_2^{\perp}} (-1)^{x.z'} |z'\rangle \qquad (۸۳-۴)$$

با دوباره بکار گیری گیت هادامارد تصحیح خطا بطور کامل انجام شده است تا به کیوبیت دست بیابیم و چون گیت هادامارد یک گیت self-inverse است، حالت نهایی بدون خطا به صورت زیر بدست می آید:

$$\frac{1}{|C_2|} \sum_{y \in C_2} |x + y\rangle \qquad (۸۴-۴)$$

که همان حالت کد گذاری شده اولیه اسشت.

۴-۱۲-۱- مدار تشخیص خطا در *css*

در این بخش نشان خواهیم داد که چگونه مدارهای تصحیح خطای کوانتومی از ماتریسهای کنترل پاریته H_1 و $H_2^{\perp}$ ساخته می شود.در بخش ۴-۱۲ نیاز به محاسبه تشخیص خطاهای $H_1(e_1)$ و $H_2^{\perp}(e_2)$ داشتیم. برای محاسبه تشخیص خطا به تعداد ردیفهای ماتریسهای کنترل پاریته،

حالتهای کمکی نیاز داریم. برای اندازه گیری تشخیص خطای بیت برگردان(عملگر X)، در صورتی که $H_1[j,i]=1$ باشد گیت C- NOT را روی j امین حالت کمکی و i امین کیوبیت داده شده اعمال می کنیم. حالت کمکی هدف گیت C- NOT می باشد. بعد از اعمال همه گیتهای $C-NOT$ حالتهای کمکی در پایه استاندارد اندازه گیری می شوند تا بیتی که دچار خطا شده را پیدا کنیم.

برای اندازه گیری تشخیص خطای فاز برگردان (عملگرZ) ، ابتدا گیت هادامارد بر هرکیوبیت داده شده اعمال می شود، سپس در صورتی که $H_2^{\perp}[j,i]=1$ باشد گیت C- NOT را روی j امین حالت کمکی و i امین کیوبیت داده شده اعمال می کنیم. حالتهای کمکی اندازه گیری می شوند و در نهایت گیت هادامارد دوباره بر کیوبیت داده شده اعمال می شود.

۴-۱۲-۲- کد استین

نمونه مهم کد CSS با استفاده از کد همینگ [7,4,3] که ماتریس پاریته آن به شکل زیر است ساخته می شود.

$$H=\begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix} \qquad (۸۵-۴)$$

این کد را با C نشان داده و تعریف می کنیم که $C_1 \equiv C, C_2 \equiv C^{\perp}$؛حال بررسی می کنیم که $C_2 \subseteq C_1$ باشد.ماتریس مولد C به صورت زیر میباشد:

$$G(C)=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\\0&1&1&1\\1&0&1&1\\1&1&0&1\end{bmatrix} \qquad (۸۶-۴)$$

یکی از ماتریسهای مولد C_2 به صورت زیر است:

$$G(C^{\perp}) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (۸۷-۴)$$

ستونهای $G(C^{\perp})$ مستقل خطی هستند و بر ستونهای $G(C)$ عمودند:می بینیم که:

$$\begin{aligned} G(C^{\perp})_1 &= G(C)_2 + G(C)_3 + G(C)_4 \\ G(C^{\perp})_2 &= G(C)_1 + G(C)_3 + G(C)_4 \\ G(C^{\perp})_3 &= G(C)_1 + G(C)_2 + G(C)_4 \end{aligned} \qquad (۸۸-۴)$$

که $G(C^{\perp})_1$ و $G(C)_1$ به ترتیب ستونهای ماتریسهای $G(C^{\perp})$ و $G(C)$ هستند.بنابراین هر بردار از $C^{\perp}$ را میتوان به صورت ترکیب خطی از بردارهای C نوشت،بنابراین $C_2 \subseteq C_1$. کد C_1 به شکل [7,4] است و کد C_2 به شکل [7,3] می باشد، بنابراین کد css یک کد کوانتومی [7,1] می باشد، این کد را کد استین نامند.

کد استین دو کد کلمه متفاوت دارد. کد کلمه اول $|0_L\rangle = |0000000 + C^{\perp}\rangle$ و کد کلمه دوم $|1_L\rangle$ می باشد و با یافتن x طوری که $x \notin C^{\perp}$ تعیین می شود. بردار (1,1,1,1,1,1,1) در این شرایط صدق می کند و به C تعلق دارد چون $G(C)(1,1,1,1)^T = (1,1,1,1,1,1,1)$، که بر خودش عمود نیست چون به $C^{\perp}$ تعلق ندارد. بنابراین $|1_L\rangle = |1111111 + C^{\perp}\rangle$؛ داریم:

$$\begin{aligned} |0_L\rangle = \frac{1}{\sqrt{8}}[&|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle] \end{aligned} \qquad (۸۹-۴)$$

$$\begin{aligned} |1_L\rangle = \frac{1}{\sqrt{8}}[&|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle] \end{aligned}$$

۴-۱۳-کدهای تثبیت کننده

کدهای تثبیت کننده را با نام کدهای جمع پذیرنیزمی شناسیم. این کدها نوع مهمی ازکدهای کوانتومی هستند که ساختاری مشابه کدهای خطی کلاسیکی دارندو توسط گاتسمن اختراع شدند. به منظور درک بهتر کدهای تثبیت کننده ابتدا فرمالیزم تثبیت کننده را شرح می دهیم فرمالیزم یک روش توانمند برای درک کردن نوع وسیعی از عملیات مکانیک کوانتوم است.

دیدگاه وسیع از فرمالیزم تثبیت کننده را با مثال زیر به سادگی بیان می کنیم. حالت EPR از دو کیوبیت را در نظر میگیریم:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad (۹۰-۴)$$

به آسانی می توان اثبات کرد که این حالت در روابطی مثل $X_1X_2|\psi\rangle = |\psi\rangle$ و $Z_1Z_2|\psi\rangle = |\psi\rangle$ صادق است. گفته می شود که حالت $|\psi\rangle$ با عملگرهای Z_1Z_2 و X_1X_2 تثبیت شده است.

کلید اصلی فرمالیزم تثبیت کننده در استفاده کردن از نظریه گروه است. برای n کیوبیت گروه پائولی G_n را تعریف می کنیم. به طور مثال برای یک کیوبیت واحد، گروه پائولی G_1 که شامل همه ماتریسهای پائولی با عامل های ضرب $\pm i$ و ± 1 است به صورت زیر تعریف می شود:

$$G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \qquad (۹۱-۴)$$

این مجموعه ماتریسی یک گروه درست عمل ضرب ماتریسی را تشکیل می دهد.

برای مثال کد شر را در نظر بگیرید، بردارهای $|1_L\rangle$ و $|0_L\rangle$ و همچنین برهمنهی اختیاریشان $\alpha|0_L\rangle + \beta|1_L\rangle$ توسط عملگرهای M_1 تا M_8 که در جدول ۴-۱ تعریف شده اند، تثبیت شده-اند.

عملگرهای M_1 تا M_8 همه عملگرهایی نیستند که کد شر را تثبیت می کنند. به طور مثال عملگر $M = Z \otimes I \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I = Z_1Z_3$ همه کدکلمه های کد شر را تثبیت می کند

M_1	Z	Z	I	I	I	I	I	I	I
M_2	I	Z	Z	I	I	I	I	I	I
M_3	I	I	I	Z	Z	I	I	I	I
M_4	I	I	I	I	Z	Z	I	I	I
M_5	I	I	I	I	I	I	Z	Z	I
M_6	I	I	I	I	I	I	I	Z	Z
M_7	X	X	X	X	X	X	I	I	I
M_8	I	I	I	X	X	X	X	X	X

جدول ۴-۲-مولدهای تثبیت کننده کد شر

فرض کنید S یک زیر گروه از G_n است و V_s مجموعه ای از حالتهای n کیوبیتی که با هر عنصر از S ثابت شده است. V_s را فضای برداری ثابت شده نامیم و S را تثبیت کننده فضای برداری V_s می گوییم.مجموعه عناصر $g_1,g_2,...,g_l$ در یک گروه G را مولد گروه G می نامیم و اگر هر عنصر از G را بتوان به صورت یک حاصلضرب از عناصر $g_1,g_2,...,g_l$ نوشت، نمایش می دهیم.

$$G=\langle g_1,g_2,g_3,...,g_l\rangle \qquad (۹۲-۴)$$

توجه شود که هر زیر گروه S ازگروه پائولی می تواند بعنوان تثبیت کننده، تنها برای یک فضای برداری غیر بدیهی استفاده شود.

برای مثال زیر گروهی از G_1 که شامل $S=\{\pm I,\pm X\}$ را در نظر بگیرید، به وضوح تنها جواب برای $(-I)|\psi\rangle=|\psi\rangle$ حالت $|\psi\rangle=0$ و بنابراین S تثبیت کننده فضای برداری بدیهی است.

پس باید شرایط S را برای تثبیت کننده فضای برداری غیر بدیهی با دو شرط زیر بیان کنیم:

شرط a) عناصر S جابجا پذیر باشند.

شرط b) I- عضو S نباشد.

نمی توان گفته های فوق را اثبات کرد اما می توان نشان داد که شرایط فوق کافی است تا V_s غیر بدیهی باشد:

فرض کنید V_s غیر بدیهی است به طوری که شامل بردار غیر صفر $|\psi\rangle$ است، M, N را عناصری از S در نظر بگیرید. برای اثبات شرط a) ما ازبرهان خلف استفاده می کنیم، فرض می کنیم که M و

N جابجا پذیر نیستند در این صورت مطابق توضیح زیر به تناقض می رسیم:

$$NM = -MN$$
$$\Rightarrow -|\psi\rangle = -NM|\psi\rangle = MN|\psi\rangle = |\psi\rangle$$
$$|\psi\rangle = -|\psi\rangle$$

رابطه فوق فقط به ازائ $|\psi\rangle = 0$ صادق است و این یک تناقض است پس M و N باید جابجا پذیر باشند.

برای اثبات شرط b) نیزبرهان خلف استفاده می کنیم. فرض می کنیم که I عنصری از S باشند:

$$(-I)|\psi\rangle = |\psi\rangle \qquad \Rightarrow \qquad |\psi\rangle = 0$$

که با فرض اولیه در تناقض است.

مفهوم ماتریس کنترل مولدها ابزار مناسبی برای بررسی تثبیت کنندها است. تثبیت کننده $S = \langle g_1, g_2, g_3, ..., g_l \rangle$ را در نظر بگیرید، ماتریس کنترل متناظر با S یک ماتریس $l \times 2n$ است که ردیفهای آن مولدهای g_1 تا g_l هستند. i امین ردیف ماتریس کنترل مطابق زیر ساخته میشود:

اگر g_i، روی j امین کیوبت I باشد پس ماتریس کنترل روی j امین و n+j امین ستون صفر است.

اگر g_i، روی j امین کیوبت X باشد پس ماتریس کنترل روی j امین ستون یک و روی n+j امین ستون صفر است. اگر g_i، روی j امین کیوبت Z باشد پس ماتریس کنترل روی j امین ستون صفر و روی n+j امین ستون یک است و در نهایت اگر g_i شامل عملگر Y روی j امین کیوبت باشد پس ماتریس کنترل روی j امین و n+j امین ستون یک است.

برای مثال ماتریس کنترل جدول ۴-۲ به صورت زیر است:

$$\left[\begin{array}{ccccccccc|ccccccccc}
0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0
\end{array}\right] \qquad (۹۳-۴)$$

ماتریس فوق هیچ گونه اطلاعاتی در مورد حاصلضرب g_i ندارد، با $r(g)$ نمایش ردیفی از عملگر g در ماتریس کنترل را نشان می دهیم. ماتریس Λ ، $2n\times 2n$ به صورت زیر تعریف می کنیم:

$$\Lambda=\begin{bmatrix}0_{n\times n} & I_{n\times n}\\ I_{n\times n} & 0_{n\times n}\end{bmatrix} \qquad (۹۴-۴)$$

به کمک دو لم زیر تعیین می کنیم که آیا یک مجموعه از مولدها مستقل هستند یا خیر.

لم ۴-۱-فرض کنید g و h عملگرهایی از G هستند، g و h جابجاپذیرند اگر و تنها اگر $r(g)\Lambda r(h)^T=0$. بنابراین مولدهای تثبیت کننده $S=\langle g_1,g_2,g_3,...,g_l\rangle$ متناظر با ماتریس کنترل M جابجاپذیرند اگر و تنها اگر $M\Lambda M=0$.

لم ۴-۲-فرض کنید $S=\langle g_1,g_2,g_3,...,g_l\rangle$ طوری که $-I\notin S$. مولد های $g_i, i=\{1,...,l\}$ مستقل هستند اگر و تنها اگر ردیف های متناظر ماتریس کنترل مستقل خطی باشند.

فرمالیزم تثبیت کننده برای توصیف فضای برداری را بحث کردیم. فرمالیزم می تواند برای توصیف دینامیک همین فضای برداری در فضای حالت استفاده می شود. فرض کنید ما یک عملگر یونیتاری U را برای یک فضای برداری V_s تثبیت شده توسط گروه S ، به کار می بریم، اگر $|\psi\rangle$ عنصری از V_s باشد بنابراین به ازائ هر عضو $g\in S$ داریم:

$$U|\psi\rangle=Ug|\psi\rangle=UgU^{\dagger}U|\psi\rangle \qquad (۹۵-۴)$$

بنا براین حالت $U|\psi\rangle$ با $UgU^{\dagger}$ تثبیت شده است. می توان نتیجه گرفت فضای برداری V_s U با گروه $USU^{\dagger}\equiv\{UgU_i|g\in S\}$ تثبیت شده است. چون $g_1,g_2,...,g_l$ ، S را تولید می کند

پس $Ug_1U^\dagger, Ug_2U^\dagger, ..., Ug_lU^\dagger$ گروه $USU^\dagger$ را تولید می کند و بیان می کند که برای دیدن چگونگی تغییرات کافی هست تغییرات مولدها را محاسبه کنیم.

بطور مثال با به کار بردن گیت هادامارد برای کیوبیت واحد:

$$HXH^\dagger = Z \qquad HYH^\dagger = -Y \qquad HZH^\dagger = X \tag{۹۶-۴}$$

. می بینیم با اعمال گیت هادامارد بر روی تثبیت کننده Z تثبیت کننده X را بدست می اوریم. بطور کلی اگر n کیوبیت با تثبیت کنندهای $\langle Z_1, Z_2, ..., Z_n \rangle$داریم به سادگی با به کارگیری گیت هادامارد میتوان n کیوبیت با تثبیت کننده های $\langle X_1, X_2, ..., X_n \rangle$ را یافت.

۴-۱۴- اندازه گیری در فرمالیزم تثبیت کننده

می توان اندازه گیری در پایه محاسباتی را به آسانی با فرمالیزم تثبیت کننده توصیف کرد، برای درک این مطلب تصور کنید که می توانیم $g \in G_n$ را اندازه گیری کنیم. (یاد آوری می شود که g یک عملگرد هرمیتی است بنابراین می تواند به عنوان یک مشاهده پذیر مورد توجه باشد).

برای سادگی، بدون از دست دادن کلیت مسئله، فرض می کنیم که g یک ماتریس پائولی است اما عامل ضربی $1, \pm i$ -1- را ندارد. فرض می کنیم که سیستم در حالت $|\psi\rangle$ باشد و تثبیت کننده های آن $g_1, ...g_n$ باشد. می خواهیم ببینیم تحت این اندازه گیری تثبیت کننده ها چگونه تغییر می کنند. دو امکان برای g_n, g وجود دارد:

۱- g با همه مولدهای تثبیت کننده جابجا پذیر است.

۲- g با یکی یا بیشتر مولدهای تثبیت کننده جابجا پذیر نمی باشد.

فرض کنید $g_1, ...g_l$مولدهای تثبیت کننده باشد، اگر g فقط با g_1 جابجا پذیر نباشد با $g_2, ...g_l$ جابجا پذیر است پس آن به آسانی ثابت می شود که g با g_1g_2 جابجا پذیر است و می توان مولدهای g_1 را با g_1g_2 جایگزین کرد.

ابتدا حالت ۱ را بررسی می کنیم:

در زیر نشان می دهیم که یکی از g یا g– عضوی از تثبیت کننده می باشد.

از آنجا که:

$$g_i g|\psi\rangle = g g_i|\psi\rangle = g|\psi\rangle \qquad (۹۷-۴)$$

پس $g|\psi\rangle$ توسط g_n تثبیت می شود پس $g|\psi\rangle$ با یک فضای بر داری v_s هستند.

$$g^2 = I \qquad \Rightarrow \qquad g|\psi\rangle = \pm|\psi\rangle \qquad (۹۸-۴)$$

بنابراین g یا g– باید عضو تثبیت کننده باشد. اگر g عضو تثبیت کننده باشد پس

$$g|\psi\rangle = |\psi\rangle \qquad (۹۹-۴)$$

بنابراین اندازه گیری از g ، نتیجه ۱+ را با احتمال یک می دهد و حالت سیستم را بهم نمی زند بنابراین تثبیت کننده ثابت باقی می ماند.

برای g– نیز بحث مشابه است. حال مورد ۲ را بررسی می کنیم.

توجه شود که g مقادیر ویژه ± 1 را دارد طوریکه تصویرگرها (projectors) برای نتایج اندازه گیری (± 1) با $(I \pm g)/2$ داده می شود و بنابراین احتمالات اندازه گیری با روابط زیر داده می شود:

$$P(+1) = tr(\frac{I+g}{2}|\psi\rangle\langle\psi|) \qquad (۱۰۰-۴)$$

$$P(-1) = tr(\frac{I-g}{2}|\psi\rangle\langle\psi|) \qquad (۱۰۱-۴)$$

با استفاده از اینکه g با g_1 جابجا پذیر نیست:

$$g_1|\psi\rangle = |\psi\rangle \qquad , \qquad g g_1 = -g_1 g \qquad (۱۰۲-۴)$$

$$\Rightarrow P(+1) = tr(\frac{I+g}{2} g_1|\psi\rangle\langle\psi|)$$

$$= tr(g_1 \frac{I-g}{2}|\psi\rangle\langle\psi|) \qquad (۱۰۳-۴)$$

$$= tr(\frac{I-g}{2}|\psi\rangle\langle\psi|g_1) \qquad (۱۰۴-۴)$$

و چون $g_1 = g_1'$

$$P(+1) = tr(\frac{I-g}{2}|\psi\rangle\langle\psi|g_1) = P(-1) \qquad (۱۰۵-۴)$$

و چون $p(+1)+p(-1)=1$ نتیجه می گیریم که:

$$P(+1)=P(-1)=\frac{1}{2} \qquad (۱۰۶-۴)$$

فرض کنید نتیجه ۱+ اتفاق بیفتد در این مورد حالت جدید سیستم

$$\left|\psi'\right\rangle \equiv (I+g)\frac{\left|\psi\right\rangle}{\sqrt{2}} \qquad (۱۰۷-۴)$$

است که تثبیت کننده های آن $\langle g, g_2,...g_n\rangle$ می باشد. با محاسبه مشابه برای نتیجه (-1) داریم:

$$\langle -g, g_2, g_3,..., g_n\rangle \qquad (۱۰۸-۴)$$

۴-۱۵- ساختار کد های تثبیت کننده

کد تثبیت کننده [n,k] به صورت فضای برداری V_s که با زیر گروه S از گروه G_n تعریف می شود طوری که $-I \notin S$ و S ، (n-k) تا مولد جابجا پذیر و مستقل دارد، S را به صورت زیر تعریف می کنیم:

$$S=\langle g_1, g_2, g_3,..., g_{n-k}\rangle \qquad (۱۰۹-۴)$$

کد تثبیت کننده را با C(s) نشان می دهیم. تثبیت کننده S، (n-k) تا مولد دارد ما می توانیم 2^k بردار متعامد در کد C(s) را به عنوان حالتهای پایه محاسباتی انتخاب کنیم.

فرض کنید که حالت با کد تثبیت کننده [n,k] که تثبیت کننده های آن $S=\langle g_1, g_2, g_3,..., g_{n-k}\rangle$ است کد گذاری شده است و خطای E حالت را بهم زده است؛ مراحل تحلیل نوع خطا و شناسایی آن و نهایتا بازیافت حالت اولیه را بصورت زیر می توان انجام داد.

ابتدا نوع خطای که روی فضای کد رخ داده است را جستجو می کنیم در مرحله دوم قضیه بیان می کنیم که به ما می گویید چه نوع خطایی را می توان آشکار سازی کرد و بعد توسط کدهای C(s) تصحیح کرد که بر اساس شرایط تصحیح خطای کوانتومی بیان می شود و مرحله سوم آشکار سازی خطا و بازیافت می باشد.

فرض می کنیم که کد C(s) با خطای $E\in G_n$ معیوب شده است اگر $E\in S$ باشد در واقع هیچ خطایی روی حالت اولیه رخ نداده است و اگر E با عناصر S جابه جا پذیر نباشد در این حالت E

کد C(s) را به زیر فضای متعامد می برد و می توان خطا را آشکار سازی و بازیافت کرد اما اگر E با عناصر S جابه جاپذیر باشد یعنی $gE = Eg$ به ازائ $g \in S$ طوری که $E \in G$ باشد این خطـا را تثبیت کننده S در G می نامند و با Z(s) نمایش میدهیم.

خطای نرمالیز کننده S را با N(s) نشان داده طوری که به ازائ

$$E \in G, g \in S \quad \rightarrow \quad EgE^{+} \in S$$

قضیه: شرایط تصحیح خطا برای کدهای تثبیت کننده؛

فرض کنید که S تثبیت کننده کد C(s) باشد و $\{E_j\}$ مجموعه عملگری در G_n است طوری کـه به ازائ همه k ها و j ها داریم:

$$E_j' E_k \notin N(s) - S$$

بنابراین $\{E_j\}$ یک مجموعه خطایی در C(s) است که قابل تصحیح کردن می باشد؛ می توان بدون از دست دادن کلیت مسئله خود را به خطاهایی محدود کرد :

$$E_j' = E_j \qquad (۱۱۰-۴)$$

که شرایط تصحیح خطای کد C(s) را مانند زیر تغییر می دهد:

$$E_j E_k \notin N(S) - S \qquad (۱۱۱-۴)$$

فرض کنید $g_1, g_2, g_3, \ldots, g_{n-k}$ مجموعه مولد های تثبیت کننده کد تثبیت کننده ی [n,k] است و $\{E_j\}$ مجموعه خطای تصحیح پذیری است که برای کد رخ داده است.شناسایی خطـا بـا انـدازه گیری کردن مولدهای تثبیت کننده انجام می شود و تشخیص خطا بدست می آید؛اگر نتایج اندازه گیری B_1 تا B_{n-k} باشد و خطای رخ داده شده E_j باشد پس تشخیص خطا B_l می باشد طوری که :

$$E_j' g_l E_j = B_l g_l \qquad (۱۱۲-۴)$$

که $B_l \in \{+1, -1\}$. اگر هیچ خطایی رخ نداده باشد پس همه $B_l = +1$، از طرفی اگر بعضی از B_j مساوی -1 باشند تصحیح خطا را انجام میدهیمدر صورتی که خطای E_j رخ داده باشد بازیافت بـه سادگی با اعمال E'_j حاصل می شود.

در موردی که دو خطای مجزا داشته باشیم یعنی E_j و $E_{j'}$ اما تشخیص خطای یکسانی را نتیجه می دهند یعنی $E_jPE'_j=E_{j'}PE'_{j'}$ که P عملگر تصویرگر در فضای کد گذاری می باشد بنابراین :

$$E_{l'}'E_lPE_{l'}'E_l = P \qquad (۱۱۳-۴)$$

که $E'_jE_{j'} \in S$

بنابراین با به کار بردن $E_{l'}'$ بعد از خطای $E_{l'}$ که تشخیص خطا را ممکن می سازد، عمل بازیافت را انجام می دهیم.

تعریف فاصله برای یک کد کوانتومی مشابه تعریف فاصله برای کدهای کلاسیکی می باشد؛ وزن خطا طوری تعریف می شود که در آن تعداد جملات متفاوت در ماتریس ضرب پائولی با ماتریس همانی مورد نظر می باشد.فاصله برای کد تثبیت کننده به صورت مینیمم وزن $N(s)-S$ تعریف می شود.

اگر قبلا C(s) به صورت [n,k] نمایش داده شد حال با تعریف d به عنوان فاصله کد C(s) را به صورت [n,k,d] نشان داده می شود.

کد C(s) با فاصله d=2t+1 قادر به تصحیح t خطای رخ داده شده روی کیوبیت می باشد؛ درست مثل مورد کلاسیک.

۴-۱۵-۱- مثالها

در اینجا چند مثال ساده از کدهای تثبیت کننده شامل کدهایی که قبلا در مورد آنها صحبت شد، به عنوان مثال کد ۹ کیوبیتی شر و کدهای CSS اما این بار از نقطه نظر فرمالیزم تثبیت کننده ارائه می‌دهیم.

کد بیت برگردان ۳ کیوبیتی: کد بیت برگردان ۳ کیوبیتی را که توسط حالتهای $|000\rangle$ و $|111\rangle$ محدود می‌شوند با تثبیت کننده ایجاد شده توسط Z_1Z_2 و Z_2Z_3، در نظر بگیرید. با بررسی و بازبینی، می‌بینیم که هر حاصلضرب ممکن از دو عنصر از مجموعه خطای $\{I,X_1,X_2,X_3\}-I$، با حداقل یکی از مولدهای تثبیت کننده (به جز I که در S می-

باشد) جابه جاپذیر است و بدین ترتیب با استفاده از قضیه ۴-۳، مجموعه $\{I, X_1, X_2, X_3\}$ یک مجموعه تصحیح‌پذیر از خطاها برای کد بیت برگردان ۳ کیوبیتی با تثبیت کننده $\langle Z_1Z_2, Z_2Z_3\rangle$ می‌باشد.

آشکارسازی خطا برای کد بیت برگردان با اندازه‌گیری مولدهای تثبیت کننده Z_1Z_2 و Z_2Z_3 صورت می‌گیرد. به عنوان مثال، اگر خطای X_1 اتفاق بیفتد، در این صورت تثبیت کننده به $\langle -Z_1Z_2, Z_2Z_3\rangle$ تبدیل می‌شود. بنابراین اندازه‌گیری نشانه، نتایج 1− و 1+ را می‌دهد. به طور مشابه خطای X_2، نشانه خطای 1− و 1− را می‌دهد، خطای X_3، نشانه خطای 1+ و 1− را می‌دهد و خطای بدیهی I، نشانه خطای 1+ و 1+ را می‌دهد. در هر نمونه عمل بازیابی به آسانی با به کار بردن عمل معکوس خطایی که توسط نشانه خطا مشخص شده، صورت می‌گیرد. عمل تصحیح خطا برای کد بیت برگردان درجدول ۲-۴ خلاصه شده است. البته روندی که ما ذکر کردیم دقیقا مشابه به آنچه که اخیرا برای کد بیت برگردان ۳ کیوبیتی توضیح دادیم، بود.

جدول ۴-۲- تصحیح خطا برای کد بیت برگردان ۳ کیوبیتی به زبان کدهای تثبیت کننده

Z_1Z_2	Z_2Z_3	نوع خطا	عمل تصحیح
+۱	+۱	خطایی صورت نگرفته	عملی صورت نمی‌گیرد
+۱	-۱	بیت سوم وارون شده	بیت ۳ را برمی‌گردانیم
-۱	-۱	بیت اول وارون شده	بیت ۱ را برمی‌گردانیم
-۱	L-۱	بیت دوم وارون شده	بیت ۲ را برمی‌گردانیم

کد شر ۹ کیوبیتی: تثبیت کننده برای کد شر، همان طور که در جدول ۲-۴ آمده است، ۸ مولد دارد. به آسانی می‌توان شرایط قضیه ۴-۳ را برای مجموعه خطای شامل I و همه خطاهای تک کیوبیتی بررسی کرد. به عنوان مثال خطاهای تک کیوبیتی مثل X_1 و Y_4 را در نظر بگیرید. حاصلضرب X_1Y_4 با Z_1Z_2 جابجاپذیر نیستند و بنابراین در $N(S)$ نمی‌باشد. به طور مشابه همه حاصلضرب‌های دیگر دو خطا از این مجموعه خطا یا در S هستند یا حداقل با یکی از عناصر S

جابجاپذیر نیستند و بدین ترتیب در $N(S)$ نیستند و دلالت بر این دارد که کد شر می‌تواند برای تصحیح یک خطای تک کیوبیتی اختیاری به کار برده شود.

عملهای $\bar{Z} = X_1X_2X_3X_4X_5X_6X_7X_8X_9$ و $\bar{X} = Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9$ به عنوان عملهای Z و X منطقی روی یک کیوبیت کد شر کدگذاری شده، عمل می‌کند. یعنی نشان می‌دهد که این $\bar{Z}$، مستقل ازمولدهای کد شر می‌باشد و با آنها جابه جاپذیر است و $\bar{X}$ مستقل از مولدهای کد شر می‌باشد و با مولدها جابه جاپذیرند و با $\bar{Z}$ جابه جاپذیر نیست.

جدول ۴-۳- ۴ مولد برای کد ۵ کیوبیتی و عملهای X منطقی و Z منطقی

نام	عملگر
g_1	$XZZXI$
g_2	$IXZZX$
g_3	$XIXZZ$
g_4	$ZXIXZ$
$\bar{Z}$	$ZZZZZ$
$\bar{X}$	$XXXXX$

کد ۵ کیوبیتی: کوچکترین سایز یک کد کوانتومی، که یک تک کیوبیت را کدگذاری می‌کند و هر خطایی را روی یک تک کیوبیت در حالت کدگذاری شده، می‌تواند آشکارسازی و تصحیح کند، یک کد ۵ کیوبیتی می‌باشد. تثبیت کننده برای یک کد ۵ کیوبیتی در جدول ۴-۳ داده‌شده است. از آنجائیکه کد ۵ کیوبیتی کوچکترین کدی است که قادر به محافظت در برابر یک تک خطا می‌باشد، به نظر می‌رسد که مفیدترین کد باشد. در هر صورت برای بسیاری از کاربردها بهتر است که از کد هفت کیوبیتی اِستین استفاده کنیم.

کد-کلمه‌های منطقی برای کد ۵ کیوبیتی به صورت زیر می‌باشند:

$$|0\rangle_{\mathcal{L}} = \frac{1}{4}[|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle] \quad (۱۱۴-۴)$$

$$|1_{\mathcal{L}}\rangle = [\frac{1}{4}|11111\rangle|01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle] \quad (۱۱۵-۴)$$

کدهای *CSS* و کدهای ۷ کیوبیتی: کدهای *CSS* یک مثال عالی ازیک دسته از کدهای تثبیت کننده می‌باشند. فرض کنید C_1 و C_2 کدهای خطی کلاسیکی $[n_1,k_1]$ و $[n_2,k_2]$ باشند به طوریکه $C_2 \subset C_1$، و C_1 $C_2^{\perp}$ هر دو قادر به تصحیح t خطا هستند. یک ماتریس کنترلی به شکل زیر تعریف می‌کنیم:

$$\begin{bmatrix} H(C_2^{\perp}) & 0 \\ 0 & H(C_1) \end{bmatrix} \quad (۱۱۶-۴)$$

برای اینکه ببینیم که این شکل یک کد تثبیت کننده را تعریف می‌کند، لازم است که ماتریس کنترلی، شرط جابجاپذیر بودن $H(C_2^{\perp})H(C_1)^T = 0$ را برآورده کند. اما داریم:

$$H(C_2^{\perp})H(C_1)^T = [H(C_1)G(C_2)]^T = 0 \quad (۱۱۷-۴)$$

زیرا فرض کردیم که $C_2 \subset C_1$ می‌باشد.

کد *Stean* هفت کیوبیتی یک مثال از کد *CSS* می‌باشد که ماتریس کنترلی پاریته آن را قبلا دیدیم. عملگرهای Z و X کدگذاری شده برای کد *stean* به صورت زیر تعریف می‌شوند.

$$\bar{Z} \equiv Z_1Z_2Z_3Z_4Z_5Z_6 \qquad \bar{X} \equiv X_1X_2X_3X_4X_5X_6 \quad (۱۱۸-۴)$$

[۲،۴،۵،۶،۸،۱۰]

۴-۱۶- پیشنهادات

با توجه به آنچه گفته شد برای انتقال اطلاعات کوانتومی از حالتهای کوانتومی مانند قطبش ، اسپین الکترون و یا نوترون و غیره استفاده می شود که می توان برای ایجاد شبکه های اطلاعاتی جهانی رسوخ ناپذیر و رایانه هایی که با سرعت مبهوت کننده کار می کنند، به کار بریم. ایجاد ارتباط بین حافظه های کوانتومی (حالتهای کوانتومی)، برای ساخت شبکه های پیچیده ای که از پدیده های کوانتومی (همانند در هم تنیدگی و برهمنهی) بهره می برند، ضروریست.

در تصحیح خطای کوانتومی از کد CSS جهت کد گذاری کیوبیت ها استفاده کردیم. در ساختن کد CSS کد های خطی دوگان را به کار بردیم که ابتدا یک کد خطی را تعیین کردیم و بعد کد دیگر را که بر کد اولی عمود بود بطور تصادفی انتخاب کردیم در نتیجه ضروری است که جفت بهتری از کد ها را طراحی کرده و ارزیابی کنیم.

شناخته شده ترین کد CSS کد استین می باشد که قابلیت تصحیح یک خطا روی یک کیوبیت را دارد . با استفاده از الگوریتم های احتمالی برای کد CSS توانسته اند کد [19,1,5] را پیدا کنند بنابراین یافتن کد ۱۷ یا ۱۸ کیوبیتی برای ساختن کد CSS که دو خطا را تصحیح می کند پیشرفت بزرگی در کامپیوترهای کوانتومی است .

به نظر می رسد که تصویرگرهای کدگذاری و کدگشایی یکانی برای گیتهای مورد نظر تجربی که مستقیما بر روی حاملهای اطلاعات اثر می کنند، مانند اجرای مستقیم گیت C-NOT روی فوتونهای قطبیده شده، برای ارتباطات کوانتومی بسیار مناسب باشند.

منابع :

[1] - Ashok chatterjee. 16 Dec 2003 . *Introduction to quantum computation.*

[2]-Michael A.Nielsen And Isaac L.Chuang.First published 2000.*Quantum Computation And Quantum Information.*

[3]- John Preskill. *Conseps Of Quantum Computation*

[4]- Peter Majek. 2005.*Quantum Error Correcting Codes.*

[5]- Maki Ohata and Kanta Matsuura.22 mar 2007.*Constructing CSS Codes with LDPC Codes for the BB84 Quantum Key Distribution Protocol.*

[6]- Artur ERKER, Patrick Hayden And Hitoshi Inamori.2 nov 2000. *Basic concepts in quantum computation.*

[7]- Sakurai, Jun John. Second Published 1999. *Modern Quantum Mechanics.*

[8]-A.R.Calderbank and Peter W.Shor.1996.*Good quantum error-correcting codes exist.*

[9]-Daniel Gottesman.28 may 1997.*Stabilizer Codes and Quantum Error Correction..*

[10]-Daniel Gottesman.1997.*A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound.*

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. 03

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.

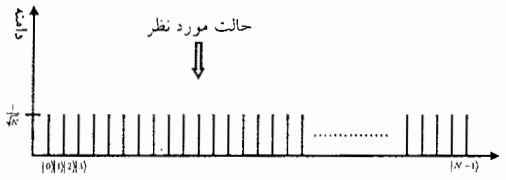
الگوریتم گراور

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 میباشد[1,3,5]:

1- 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 1).

$$W_{ij} = 2^{-N/2}(-1)^{i,j} \qquad i,j = 0,1,...,N$$



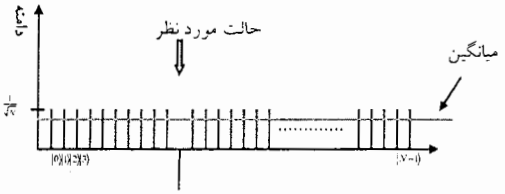
شکل 1: دامنه حالات سیستم بعد از اعمال ماتریس Walsh Hadamard

2- دو مرحله زیر را $O(\sqrt{N})$ بار تکرار می کنیم.

الف) اگر $C(S) = 1$ باشد (یعنی حالت مورد نظر)، در این صورت فاز را به اندازه π می چرخانیم، در غیر این صورت یعنی در حالتی که $C(S) = 0$ باشد، در آن تغییری ایجاد نمی‌کنیم. این کار توسط اپراتور Oracle انجام می‌شود که به صورت زیر نشان داده میشود:

$$O = \begin{bmatrix} e^{i\varphi_1} & 0 & 0 & 0 & 0 & \cdots \\ 0 & e^{i\varphi_2} & 0 & 0 & 0 & 0 \\ 0 & 0 & e^{i\varphi_3} & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{i\varphi_4} & 0 & 0 \\ 0 & 0 & 0 & 0 & e^{i\varphi_5} & 0 \\ \vdots & 0 & 0 & 0 & 0 & \ddots \end{bmatrix}$$

پس از اعمال این اپراتور حالت مورد نظر به اندازه π رادیان تغییر فاز پیدا کرده و بقیه حالات بدون تغییر باقی می مانند (شکل2).



شکل 2: 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 [2,4]، زیرا:

$$R = \begin{bmatrix} 1 & 0 & 0 & & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & & 0 \\ & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\begin{aligned} WRW &= W(2|0\rangle\langle 0| - I)W \\ &= 2W|0\rangle\langle 0|W - WIW \\ &= 2|\psi\rangle\langle\psi| - WIW \\ &= 2|\psi\rangle\langle\psi| - I \end{aligned}$$

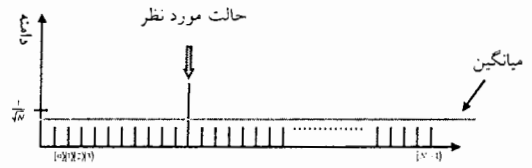
$$(|\psi\rangle\langle\psi|)|\alpha\rangle = \frac{1}{N}\begin{bmatrix} 1 & 1 & 1 & & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & & 1 \\ & \vdots & & \ddots & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \end{bmatrix}$$

$$WRW = 2|\psi\rangle\langle\psi| - I$$

$$WRW|\alpha\rangle = (2|\psi\rangle\langle\psi| - I\sum\alpha_n|n\rangle)$$

$$= \sum(2\bar{a} - \alpha_n|n\rangle)$$

که این همان عمل معکوس حول میانگین می باشد (شکل 3).



شکل 3: دامنه حالات سیستم بعد از اعمال ماتریس پراکندگی

3- سیستم را بررسی می کنیم. حالت مورد نظر با احتمالی بیش از $\frac{1}{2}$ به دست خواهد آمد.

مثالی برای یک سیستم 3 کیوبیتی

ابتدا از یک مثال کلاسیکی شروع می کنیم. فرض کنید که شما 8 توپ در اختیار دارید. حال بدون اطلاع به دوست خود، یکی از توپها را انتخاب کنید. در اینجا فرض می‌کنیم که شما توپ شماره 7 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 1 است؟
- خیر
- آیا توپ انتخابی شما، توپ شماره 2 است؟
- خیر
- ⋮
- آیا توپ انتخابی شما، توپ شماره 7 است؟
- بله

مشاهده می کنیم که برای دستیابی به پاسخ مورد نظر 7 سوال مطرح شد. مینیمم و ماکزیمم سوال‌هایی که برای یافتن یک توپ مطرح می‌شود به ترتیب 1 و 7 سوال می‌باشد، لذا به طور میانگین 4 سوال برای دست یابی به مورد انتخابی مطرح می شود. اما با به کار بردن الگوریتم کوانتومی گراور تنها با طرح 2 پرسش به پاسخ مورد نظر دست پیدا می کنیم!

برای یک سیستم 3 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.

$$W|000\rangle \rightarrow \frac{1}{\sqrt{2^3}}(|000\rangle+|100\rangle+|001\rangle+|010\rangle+|110\rangle+|101\rangle+|011\rangle+|111\rangle)$$

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 8 حالت است، لذا حلقه گراور باید از مرتبه $\sqrt{۸}$ بار(2 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 $\frac{11}{8\sqrt{2}}$ افزایش یافته و حالت مورد نظر با احتمال 94/53٪ ($(\frac{11}{8\sqrt{2}})^2 = ۰/۹٤٥۳$) که احتمال بسیار بالایی است، به دست می‌آید. برای یک سیستم 4 کیوبیتی نیز با به کاربردن ماتریسهای ۱٦×۱٦ و طی مراحل این الگوریتم، حالت مورد نظر با احتمال 96/14٪ 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 8 رکورد اعمال کردیم و مشاهده کردیم که الگوریتم کلاسیکی، بعد از طی به طور میانگین 4 مرحله با احتمال $\frac{1}{2}$، پاسخ مورد نظر را به ما می دهد، در صورتیکه با اعمال الگوریتم کوانتومی گراور بعد از طی 2 مرحله و با احتمال 94/53٪ 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

[1] Michael Nielsen and Isaac Chuang; *"Quantum Computation And Quantum Information"*;1th edition, Cambridge University Press, 2003.

[2] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings, 35 th Annual Symposium on Fundamentals of Comp. Science (FOCS), 1994, pp. 124-134.

[3] C.H. Bennett, E. Bernstein, G. Brassard & U.Vazirani, *Strengths and weaknesses of quantum computing*, to be published in the SIAM Journal on Computing.

[4] L.K. Grover, *A fast quantum mechanical algorithm for estimating the median*,lanl e-print quant-ph/9607024.

[5] M. Boyer, G. Brassard, P. Hoyer & A. Tapp; *"Tight bounds on quantum searching"*; Proceedings, PhysCo mp 1996 (lanl e-print quant-ph/9605034).