# تصحیح خطای کوانتومی ـ بخش اول

وحید کریمی پور، دانشکده فیزیک، دانشگاه صنعتی شریف

۲۵ آبان ۱۴۰۱

## ۱ مقدمه

وقتی که بیت های کلاسیک از یک کانال کلاسیک عبور می کنند همواره ممکن است دچار خطا شوند. این خطاها هنگام پردازش اطلاعات در یک کامپیوتر کلاسیک نیز می توانند رخ دهند. بنابراین لفظ کانال دراین جا به یک معنای عام به کار می رود که الزاماً به معنای آن نیست که بیت یک فاصله مکانی طولانی را طی می کند. این اتفاق برای کیوبیت ها نیز می توانند رخ دهد یعنی کیوبیت ها نیز وقتی که از یک کانال کوانتومی عبور می کنند ممکن است دچار خطا شوند. یک کامپیوتر کوانتومی وقتی می تواند به خوبی کار کند که بتوانیم خطاهای ایجاد شده در کیوبیت ها را آشکار ساخته و تصحیح کنیم. این امر هم چنین برای ارسال اطلاعات کوانتومی توسط کیوبیت ها ضرورت دارد. از این به بعد لفظ کانال کلاسیک یا کانال کوانتومی را همواره به یک معنای عام به کار می بریم. چند تفاوت مهم بین خطاهای کلاسیک و کوانتومی وجود دارد و به نظر می رسد که خطاهای کوانتومی را واقعاً نمی توان آشکار و تصحیح کرد:

۱ ـ یک بیت کلاسیک می تواند ولتاژ یک نقطه و یا جریان عبور کننده از یک نقطه و یا مغناطش یک حوزه مغناطیسی باشد و اگر چه از نظر ماکروسکوپی کوچک است ولی از نظر میکروسکوپی هنوز از میلیارد ها اتم تشکیل شده است و امکان بروز خطا در آن بسیار کم است . در حالیکه یک کیوبیت واقعاً میکروسکوپی است و نشان دهنده حالت یک اتم یا اسپین یا یون است و براحتی می تواند دچار خطا شود.

۲ ـ خطای ایجاد شده در یک بیت کلاسیک یک خطای گسسته است که در آن مقدار $0(1)$ به مقدار $1(0)$ تبدیل می شود و حال آنکه خطای ایجاد شده در یک کیوبیت پیوسته است و بردار حالت بیت کوانتومی می تواند به طور پیوسته تغییر کند.

۳ ــ می توان یک بیت کلاسیک را مشاهده کرد و از خطای ایجاد شده در آن آگاهی یافت ولی یک بیت کوانتومی را براحتی نمی توان مشاهده کرد زیرا مشاهده‌ی آن عموماً منجر به کاهش تابع حالت و از بین رفتن حالت اولیه می شود.

۴ ــ و بالاخره می توان نسخه‌های متعددی از یک بیت کلاسیک را تهیه کرد که در صورت بروز خطا در یکی یا چند تا از آنها با استفاده از قانون اکثریت بتوان به بروز خطا در آن ها پی برد و حال آنکه بنابر قضیه عدم تکثیر $No\ cloning\ theorem$ نمی توان یک حالت کوانتومی را تکثیر کرد و نسخه های متعددی از آن درست کرد.

تفاوت های بالا یا به عبارت بهتر موانع بالا در سالهای اولیه طرح نظریه کامپیوتر ها و اطلاعات کوانتومی باعث شده بود که عده‌ای فکر کنند کامپیوترهای کوانتومی یا مخابره اطلاعات کوانتومی هرگز به عمل نزدیک نخواهد شد زیر هرگز نمی توان خطاهای کوانتومی را تصحیح کرد. خوشبختانه امروزه یک نظریه کامل برای آشکارسازی و تصحیح خطاهای کوانتومی تدوین شده است که می تواند بر تمام موانع بالا غلبه کند و محاسبه و مخابره اطلاعات کوانتومی را به طوری که از خطا مصون باشد، امکان پذیر کند. هدف ما در این درس آن است که با این نظریه آشنا شویم. نخست سعی می کنیم نشان دهیم که موانع یادشده در بالا را واقعا می توان پشت سر گذاشت. این کار را با مثالهای ساده توضیح می دهیم. این مثال ها فقط اصول کلی را نشان می دهند ولی به ما نمی گویند که چگونه می توان به طور سیستماتیک کدهای تصحیح خطای کوانتومی نوشت. برای این کار ما سعی می کنیم نخست نظریه تصحیح خطای کلاسیک را یاد بگیریم و سپس از آن استفاده کنیم و چگونگی ایجاد کدهای تصحیح خطای کوانتومی را بفهمیم.

## ۲ چگونگی غلبه بر موانع تصحیح خطای کوانتومی ـ توضیحات کلی

دیدیم که خطاهای کوانتومی یک تفاوت بزرگ با خطاهای کلاسیک دارند و آن این است که این خطاها پیوسته هستند. یعنی حالتِ $|\psi\rangle = a|0\rangle + b|1\rangle$ می تواند در اثر برهم کنش با محیط تبدیل به حالتِ $|\psi'\rangle = a'|0\rangle + b'|1\rangle$ شود که تنها تفاوت اندکی با حالت قبلی دارد. این تفاوت های اندک می توانند انباشته شده و باعث شوند که حالت اولیه کاملا تغییر کند. به هرحال آنچه که مهم است این است که این خطاها پیوسته هستند. می خواهیم ببینیم چگونه این خطاها را می توانیم تصحیح کنیم؟

پاسخ این است که اگر تنها بتوانیم خطاهای بیت-برگردان، فازبرگردان و بیت-فاز-برگردان یعنی خطاهای پاوولی را اصلاح کنیم آنگاه هر نوع خطایی حتی خطاهای پیوسته را نیز می توانیم اصلاح کنیم. برای فهم این موضوع یک کیوبیت را در نظر بگیرید که در حالت $|\psi\rangle$ قرار گرفته است. در ابتدا این کیوبیت و محیط اطرافش در حالت $|\psi\rangle|e\rangle$ قرار گرفته اند. دقت کنید که همواره می توان محیط را آنقدر بزرگ گرفت که کیوبیت و محیط آن در یک حالت خالص قرار بگیرند. حال در اثر برهم کنش محیط و کیوبیت که با یک عملگر یکانی مشخص می شود حالت کیوبیت و محیط به ترتیب زیر تغییر می کند:

$$|\psi\rangle|e\rangle \longrightarrow U(|\psi\rangle|e\rangle) \tag{۱}$$

عملگر $U$ روی کیوبیت و محیط اثر می کند. می توان آن را روی فضای دو بعدی کیوبیت بسط داد. عملگرهای پاوولی و عملگر واحد یک پایه برای تمام ماتریس ها یا عملگرهای فضای دوبعدی کیوبیت می سازند و بنابراین می توان نوشت:

$$U = I\otimes U_0 + X\otimes U_1 + Y\otimes U_2 + Z\otimes U_3, \tag{۲}$$

که درآن عملگرهای $U_i$ عملگرهایی هستند که روی محیط اثر می کنند و نه متعامدند نه بهنجار . در واقع هیچ شرط ویژه ای روی این عملگرها نیست به جز این که در حالت کلی ما هیچ اطلاعی در باره آنها نداریم. عملگرهای پاوولی نیز این ها هستند که عملگر $I$ را هم جزء آنها قرار داده ایم که یک پایه کامل برای عملگرهای فضای یک کیوبیت تشکیل دهند:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{۳}$$

دقت کنید که تعریف ما از $Y$ با تعریف متعارف تفاوت دارد. این تفاوت هم بدلیلی که خواهیم دید اهمیت ندارد. به این ترتیب حالت کیوبیت و محیط به ترتیب زیر تغییر می کند:

$$\begin{aligned} |\psi\rangle\otimes|e\rangle \quad &\longrightarrow \quad I|\psi\rangle\otimes U_0|e\rangle + X|\psi\rangle\otimes U_1|e\rangle + Y|\psi\rangle\otimes U_2|e\rangle + Z|\psi\rangle\otimes U_3|e\rangle \\ &\equiv \quad I\,|\psi\rangle\otimes|e_0\rangle + X\,|\psi\rangle\otimes|e_1\rangle + Y\,|\psi\rangle\otimes|e_2\rangle + Z\,|\psi\rangle\otimes|e_3\rangle, \end{aligned} \tag{۴}$$

که در آن حالت های چهارگانه بالا برای محیط نه بهنجارهستند و نه متعامد. در واقع هیچ گونه اطلاع خاصی از این حالت ها نداریم. در واقع هیچ گونه کنترلی نیز روی این حالت ها نداریم زیرا هیچ گونه کنترلی نیز روی محیط نداریم. ما فقط می توانیم روی حالت کیوبیت اندازه گیری انجام

دهیم و آن را کنترل کنیم و در صورت لزوم اصلاح کنیم. حال اگر حالت های چهارگانه بر یکدیگر عمود باشند می توانیم با یک اندازه گیری آنها را از هم تمییز دهیم و تعیین کنیم که چه نوع خطایی روی حالت اولیه رخ داده و آن را با اعمال عملگر وارونِ مناسب به حالت اولیه برگردانیم

$$|\psi\rangle, \qquad X|\psi\rangle, \qquad Y|\psi\rangle, \qquad Z|\psi\rangle. \tag{۵}$$

برای یک کیوبیت اگر آن را کد نکنیم البته چنین اتفاقی نمی افتد. تمام نکته کدهای کوانتومی این است که چگونه حالت یک کیوبیت را کد کنیم تا حالت های فوق برهم عمود باشند و بتوانیم آن ها را از هم تمیز دهیم. اگر بتوانیم این کار را بکنیم در واقع می توانیم بگوییم که روی حالت اولیه یا خطای $I$ اتفاق افتاده است یا خطای $X$ یا خطای $Y$ و یا خطای $Z$. بنابراین اثر عملگر پیوسته $U$ و خطای پیوسته آن تبدیل به چهار خطای گسسته شده است. تمام پیوستگی $U$ به حالت های $|e_i\rangle$ و در واقع به احتمال وقوع خطاهای گسسته چهارگانه فوق منتقل شده است، چرا که داریم:

$$P(I) = \langle e_0|e_0\rangle, \qquad P(X) = \langle e_1|e_1\rangle, \qquad P(Y) = \langle e_2|e_2\rangle, \qquad P(Z) = \langle e_3|e_3\rangle. \tag{۶}$$

البته خطا می تواند روی دو کیوبیت یا بیشتر رخ دهد ولی در صورتی که کیوبیت ها به خوبی از اثر محیط محافظت شوند احتمال خطا روی دو کیوبیت از خطا روی یک کیوبیت کمتر است و همین طور احتمال خطا روی تعداد بیشتری از کیوبیت ها ناچیز خواهد بود . هرگاه خطا روی دو کیوبیت اثر کند بازهم می توانیم عملگر کلی خطا را برحسب عملگرهای پایه روی فضای هیلبرت دو کیوبیت بسط دهیم و بنویسیم:

$$U = \sum_{i,j=0}^{3} \sigma^i \otimes \sigma^j \otimes U_{ij}, \tag{۷}$$

و در نتیجه

$$U|\psi\rangle|e\rangle = \sum_{i,j=0}^{3} (\sigma^i \otimes \sigma^j)|\psi\rangle \otimes |e_{ij}\rangle \tag{۸}$$

که به این معناست که بارهم یک خطای کلی دو کیوبیتی به خطاهای گسسته پاوولی تجزیه می شود. در کلی ترین حالت ، یک خطا حاصلضرب عملگرهای مختلف پاوولی در کیوبیت های مختلف است.

در انتها باید از خود بپرسیم که چرا تنها کافی است که خطاهای $X$ و $Z$ را تصحیح کنیم و نه خطای $Y$ را ؟ برای پاسخ به این سوال فرض کنید که کدی نوشته شده که خطای $X$ و $Z$ را مثلا در یک کیوبیت معین تصحیح کند. در این صورت می دانیم که اگر $|\psi\rangle$ یک حالت در فضای کد باشد آنگاه حالت های

$$|\psi\rangle, \quad X|\psi\rangle, \quad Z|\psi\rangle$$

بر هم دو به دو عمودند. معنای این حرف این است که روابط زیر برقرارند:

$$\langle\psi|X|\psi\rangle = 0, \qquad \langle\psi|Z|\psi\rangle = 0, \qquad \langle\psi|XZ|\psi\rangle = 0 \tag{۹}$$

اما از آنجا که منهای یک فازکلی روابط

$$XY = Z, \quad XZ = Y, \quad YZ = X$$

برقرارند، پس روابط زیر هم برقراند:

$$\langle\psi|Y|\psi\rangle = 0, \qquad \langle\psi|XY|\psi\rangle = 0, \qquad \langle\psi|YZ|\psi\rangle = 0. \tag{۱۰}$$

به این ترتیب روابط (۹) و (۱۰) روی هم نشان می دهند که تمام خطاهای پاوولی و در نتیجه تمام خطاهای پیوسته روی آن کیوبیت قابل تصحیح اند.

## ۳ مثال های ساده از کدهای کوانتومی

پس از این مقدمه می توانیم کد های کوانتومی را مطالعه کنیم. همانطور که در مقدمه گفتیم خطاهای کوانتومی و نحوه اصلاح آنها بکلی متفاوت با خطاهای کلاسیک هستند و به همین جهت در ابتدای امر گمان می شد که کامپیوترهای کوانتومی هرگز ساخته نخواهند شد زیرا هیچ روشی برای شناسایی و اصلاح خطاهای ناگزیری که درآنها وجود دارد شناخته شده نبود. امروزه معلوم شده است که یک نظریه جامع و کامل برای آشکارسازی و اصلاح خطاهای کوانتومی وجود دارد که ساخت عملی کامپیوترهای کوانتومی را امکان پذیر می کند. اندیشه هایی که مبنای این نظریه قرار گرفته اند اساساً از همان نظریه کلاسیک الهام گرفته شده‌اند ولی در تدوین آنها تمام محدودیت های مکانیک کوانتومی نظیر عدم امکان اندازه گیری های دلخواه و یا عدم امکان تکثیر حالت ها مورد ملاحظه قرار گرفته‌اند. کاری که ما دراین بخش می کنیم آن است که نخست کدهای ساده‌ای را معرفی می کنیم که قادرند خطاهای معینی را آشکار و اصلاح کنند. سپس به تدریج که این کد ها را بسط می دهیم اصول اساسی نظریه اصلاح خطاهای کوانتومی را نیز دریک چارچوب کلی شرح خواهیم داد.

## ۱.۳ اصلاح خطاهای بیت ـ برگردان

فرض کنید که تنها امکانی که برای خطا وجود دارد برگردان یک کیوبیت است به این معنا که در طول کانال ممکن است عملگر $X$ (یاهمان $\sigma_x$ ) روی یک کیوبیت اثر کند. دراین صورت هرگاه یک کیوبیت در ابتدای کانال به صورت $|\psi\rangle = a|0\rangle + b|1\rangle$ ارسال شده باشد، در اثر خطای احتمالی ممکن است به صورت $X|\psi\rangle = a|1\rangle + b|0\rangle$ دریافت شود.

برای آشکارسازی این نوع خطا یک راه این است که کیوبیت های $|0\rangle$ و $|1\rangle$ را به صورت زیر کُد کنیم:

$$|0\rangle \longrightarrow |0\rangle_E = |00\rangle, \qquad |1\rangle \longrightarrow |1\rangle_E = |11\rangle, \tag{۱۱}$$

که در آن علامتِ $E$ از کلمه $Encoding$ گرفته شده است. دقت کنید که این امر نقض کننده قضیه عدم تکثیر حالت نیست، زیرا حالت های $|0\rangle$ و $|1\rangle$ برهم عمودند و دو حالت دلخواه نیستند. درنتیجه حالتِ یک کیوبیت به صورت زیر کد می شود:

$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow |\psi\rangle_E = a|00\rangle + b|11\rangle. \tag{۱۲}$$

این حالت ویژه بردار عملگر $Z_1Z_2$ با ویژه مقدار یک است.

حال اگر یک خطای $X_1$ ، $X_2$ رخ دهد حالت $|\psi\rangle_E$ تبدیل به حالت های زیر می شود:

$$\begin{aligned} X_1|\psi\rangle_E &= a|10\rangle + b|01\rangle \\ X_2|\psi\rangle_E &= a|01\rangle + b|10\rangle \end{aligned} \tag{۱۳}$$

براحتی می توان این دو حالت را از حالت اولیه تشخیص داد و نتیجه گرفت که خطایی رخ داده است . این کار را با اندازه گیری مشاهده پذیر $Z_1Z_2$ انجام می دهیم که مقدارش برای هر دو حالت بالا برابر با منهای یک است و اندازه گیری اش باعث رمبش حالت نمی شود. اما اشکال این کد این است که تنها می توان وقوع خطا را تشخیص داد ولی نمی توان آن را تصحیح کرد زیر معلوم نیست که آیا خطای بیت برگردان در کیوبیت اول رخ داده است یا کیوبیت دوم. برای رفع این اشکال نیاز به یک کد بهتر داریم.

برای آشکارسازی و تصحیح خطای بیت برگردان کیوبیت های $|0\rangle$ و $|1\rangle$ را به صورت زیر کُد می کنیم:

$$|0\rangle \longrightarrow |0\rangle_E = |000\rangle, \qquad |1\rangle \longrightarrow |1\rangle_E = |111\rangle, \tag{۱۴}$$

که در آن علامتِ $E$ از کلمه $Encoding$ گرفته شده است. دقت کنید که این امر نقض کننده قضیه عدم تکثیر حالت نیست، زیرا حالت های

$|0\rangle$ و $|1\rangle$ برهم عمودند و دو حالت دلخواه نیستند. درنتیجه حالتِ یک کیوبیت به صورت زیر کد می شود:

$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow |\psi\rangle_E = a|000\rangle + b|111\rangle. \quad (۱۵)$$

این حالت ویژه حالت مشترک عملگرهای $Z_1Z_2$ و $Z_1Z_3$ با مقادیر ویژه ۱ است. به عبارت دیگر

$$Z_1Z_2|\psi\rangle_E = |\psi\rangle_E, \qquad Z_1Z_3|\psi\rangle_E = |\psi\rangle_E. \quad (۱۶)$$

حال اگر یک خطای $X_1$ ، $X_2$ یا $X_3$ رخ دهد حالت $|\psi\rangle_E$ تبدیل به حالتی می شود که ویژه مقدارش برای عملگرهای فوق تغییر خواهد کرد.

$$\begin{aligned}
I|\psi\rangle_E = a|000\rangle + b|111\rangle \qquad &\longrightarrow \qquad Z_1Z_2 = 1, \quad Z_1Z_3 = 1\\
X_1|\psi\rangle_E = a|100\rangle + b|011\rangle \qquad &\longrightarrow \qquad Z_1Z_2 = -1, \quad Z_1Z_3 = -1\\
X_2|\psi\rangle_E = a|010\rangle + b|101\rangle \qquad &\longrightarrow \qquad Z_1Z_2 = -1, \quad Z_1Z_3 = 1\\
X_3|\psi\rangle_E = a|001\rangle + b|110\rangle \qquad &\longrightarrow \qquad Z_1Z_2 = 1, \quad Z_1Z_3 = -1.
\end{aligned} \quad (۱۷)$$

در روابط بالا مقادیر ویژه عملگرهای $Z_1Z_2$ و $Z_1Z_3$ را نوشته ایم. این عملگرها که مقادیر ویژه آنها خطا را آشکار می کنند نشانه های خطا [۱] نامیده می شوند. شکل (۱ ) به یک ویژ گی مهم اشاره می کند و آن اینکه زیر فضای کد یعنی $C$ در اثر خطاهای متفاوت به زیر فضاهای متعامد نگاشته می شود و در نتیجه می توان با تعیین اینکه در کدام زیر فضا هستیم به خطای ایجاد شده پی برد.

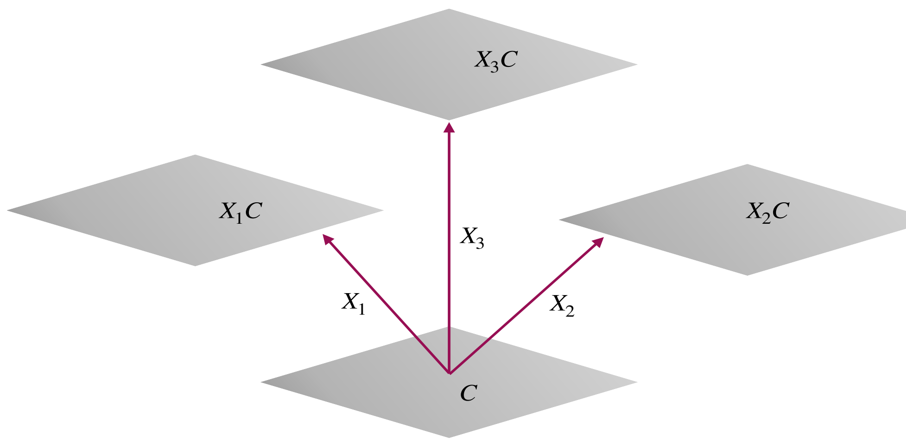
■ تمرین: کد زیر را در نظر بگیرید:

$$a|0\rangle + b|1\rangle \longrightarrow a|00\rangle + b|11\rangle. \quad (۱۸)$$

نشان دهید که این کد می تواند خطاهای بیت برگردان را تشخیص دهد ولی نمی تواند آنها را تصحیح کند. این ضعف را به ویژگی زیرفضای کد و زیرفضاهایی که در اثر ایجاد خطا پدیدار می شوند ربط دهید.

نکته مهم آن است که حالت دچار خطاشده همچنان ویژه بردار عملگرهای $Z_1Z_2$ و $Z_1Z_3$ باقی می ماند بنابراین اندازه گیری این دو عملگر باعث فروکاهش تابع موج نمی شود. بعد از اینکه معلوم شد خطای بیت برگردان در چه نقطه ای صورت گرفته است می توان با اعمال عملگر

[۱] Error Syndrome




شکل ۱: زیر فضای کد و زیرفضاهایی که در اثر خطا بوجود می آیند.

تصحیح کننده خطا را اصلاح کرد. دراین جا با چند سوال مواجه می شویم.

**۱:** چگونه می توان با یک مدار کوانتومی کدِ 11 را ایجاد کرد؟

**۲:** چگونه می توان عملگرهای نشانه‌ی خطا را اندازه گرفت؟ چگونه می توان این کار را به صورت منظمی انجام داد؟

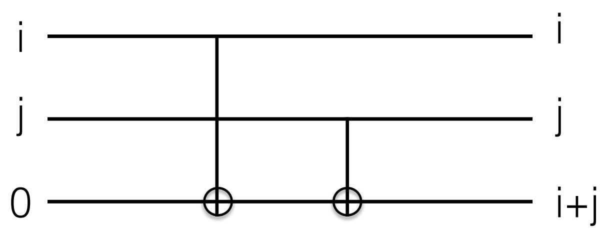
پاسخ سوال اول بسیار ساده است. این کار را می توان با استفاده از عملگر $CNOT$ انجام داد. از این به بعد برای یک عملگر $CNOT$ که بیت کنترلی اش $i$ و بیت هدف اش $j$ است، نمادِ $C_{ij}$ را به کار می بریم. درنتیجه خواهیم داشت:

$$C_{12}C_{13}(a|0\rangle + b|1\rangle)|00\rangle = a|000\rangle + b|111\rangle. \quad (۱۹)$$

مدار شکل 3 نشان می دهد که این کار چگونه انجام می شود.

برای سوال دوم نیز بهترین کار آن است که اطلاعات مربوط به نشانه های خطا در کیوبیت های جداگانه‌ای نوشته شود. این کیوبیت ها اصطلاحاً کیوبیت های خدمتکار [۲] نامیده می شوند. برای این کار باز هم از عملگر $CNOT$ استفاده می کنیم. فرض کنید که یک بیت خدمتکار

[۲] Ancilla qubit




شکل ۲: مداری که مساوی بودن یا مخالف بودن دو بیت را تشخیص می دهد.

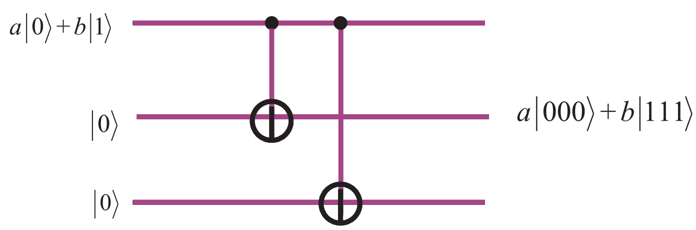
را در حالت $|0\rangle$ نگاه داشته باشیم. می خواهیم کاری کنیم که اگر در بیت های اول و دوم ِ کد یک بیت برگردانده شده باشد، مقدار این بیت خدمتکار به یک تغییر کند. کافی است که به رابطه زیر یا شکل (۲) توجه کنیم:

$$C_{1a}C_{2a}|ij\rangle|0\rangle_a = |ij\rangle|i+j\rangle_a. \qquad (۲۰)$$

دراین جا نماد $a$ برای بیت خدمتکار بکار می رود. بنابراین اگر $i$ و $j$ باهم مساوی باشند، مقدار بیت خدمتکار برابر با صفر و درغیر این صورت برابر با یک خواهد بود. مدار شکل 4 که در مقصد عمل می کند، نشان می دهد که این کار چگونه انجام می شود. دراین شکل حرف $M$ به معنای اندازه گیری و حرف $a$ به معنای بیت خدمتکار است.

از این مثال می توان به چند نکته اساسی که در همه کد های کوانتومی وجود دارد پی برد.

نکته‌اول: فضای برداری حالت های $n$ کیوبیت یک فضای $2^n$ بعدی است که آن را با $V = C_2^{\otimes n}$ نشان می دهیم که درآن فضای $C_2$، یک فضای دوبعدی مختلط با بردارهای پایه $|0\rangle$ و $|1\rangle$ است. یک کد چیزی نیست جز انتخاب یک زیر فضای مناسب از این فضا که آن را با $C \subset V$ نمایش می دهیم. هرگاه این زیرفضا دارای بعد $2^k$ باشد می گوییم کدِ مربوطه برای نوشتن $k$ کیوبیت در $n$ کیوبیت به کار رفته است. در




شکل ۳: مداری که کد اصلاح کننده بیت ـ برگردان را درست می کند

حالت کلی کدکردن به صورت زیراست:

$$|\psi\rangle = \sum_{x=0}^{2^k-1} \psi_x |x\rangle \longrightarrow |\psi\rangle_E = \sum_{x=0}^{2^k-1} \psi_x |x\rangle_E, \tag{۲۱}$$

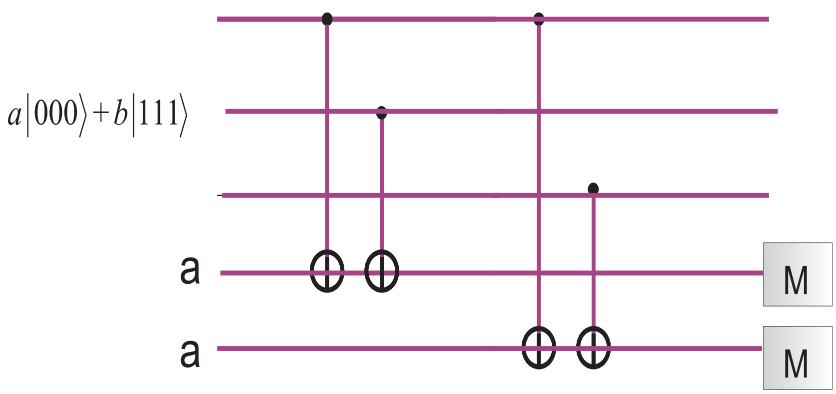
که درآن $\{|x\rangle_E\}$ پایه ای برای زیرفضای $C$ از $V$ است. در مثالی که در بالا ارایه کردیم فضای $V$ یک فضای ۸ بعدی است و زیر فضایی که انتخاب کرده‌ایم یک فضای دوبعدی است. بنابراین کدی نوشته ایم که یک کیوبیت را در سه کیوبیت می نویسد.

نکته دوم: برای تشخیص نشانه های خطا از بیت های خدمتکار استفاده کرده‌ایم. درحالت کلی اگر در طول راه، روی حالتِ $|\psi\rangle_E$ عملگر خطای $E_i$ اثر کرده باشد، مدارِ تشخیص خطا (درمقصد) کار زیر را انجام می دهد:

$$E_i|\psi\rangle_E|0\rangle_a \quad \longrightarrow \quad E_i|\psi\rangle_E|s_i\rangle_a, \tag{۲۲}$$

که درآن $s_i$ نشانه خطای $E_i$ است. دقت کنید که اطلاعاتی که در بیت های خدمتکار نوشته شده است تنها مربوط به نوع خطاست و هیچ اطلاعاتی از حالتِ $|\psi\rangle$ دراین بیت ها نوشته نشده‌است. بنابراین اندازه گیری این بیت ها تنها نوع خطا را مشخص می کند و نه خود حالت را به همین جهت همدوسی حالت دست نخورده باقی می ماند. پس از تعیین نوع خطا عملگرِ $E_i^\dagger$ که خنثی کننده خطاست روی حالت اثر داده می شود.

نکته سوم: هر کدی که می نویسیم تنها قادراست مجموعه‌ای از خطاها را خنثی کند. این مجموعه را خطاهای قابل تصحیح توسط کد می نامیم و با $\mathcal{E}_C = \{E_1, E_2, \cdots\}$ نمایش می دهیم. به عنوان مثال کدی که در بالا نوشته ایم تنها قادراست خطاهای تک بیتی $\mathcal{E}_C = \{X_1, X_2, X_3\}$




شکل ۴: مداری که نشانه های خطای بیت ـ برگردان را تشخیص می دهد

را خنثی می کند.

نکته چهارم: این کد، همانطور که قبلا گفتیم یک زیر فضای مشخص از فضای مربوط به سه کیوبیت است. این زیرفضای دو بعدی زیرفضایی است با ویژه مقدارهای یک برای دو عملگر $Z_1Z_2$ و $Z_1Z_3$ . به اصطلاح این زیرفضا توسط این دو عملگر پایدار می شود. این دو عملگر را عملگرهای پایدار ساز یا $Stabilizer$ های مربوط به این زیر فضا می خوانیم. در واقع می توان این زیر فضا را به این صورت تعریف کرد که زیر فضایی است که توسط این دو عملگر پایدار می شود.
توجه به یک نکته دراین جا مهم است و آن اینکه عملگر $Z_2Z_3$ نیز یک عملگر پایدارساز برای این زیر فضاست ولی مستقل از دو عملگر قبلی نیست. در واقع مجموعه عملگرهایی که یک زیر فضا را پایدار نگاه می دارند یک گروه تشکیل می دهد که به آن گروه پایدار ساز می گویند. در این جا گروه پایدار ساز عبارت است از

$$\mathcal{S} = \{Z_1Z_2, Z_1Z_3, Z_2Z_3, I\} \tag{۲۳}$$

■ تمرین: ثابت کنید که مجموعه عملگرهای مربوط به یک زیر فضا تشکیل یک گروه می دهند.

■ تمرین: زیر فضایی را که توسط دو عملگر $Z_1Z_2$ و $Z_1Z_3$ پایدار می شود بدست آوردید. فرض کنید که کل فضا مربوط به سه کیوبیت است. حال فرض کنید که کل فضا مربوط به چهار کیوبیت است و زیر فضایی را به دست آورید که توسط عملگرهای $Z_1Z_2$ ، $Z_2Z_3$ و $Z_3Z_4$ پایدار می شود.

■ تمرین: زیر فضایی را که توسط دو عملگر $X_1X_2$ و $X_1X_3$ پایدار می شود بدست آوردید. فرض کنید که کل فضا مربوط به سه کیوبیت است. حال فرض کنید که کل فضا مربوط به دو کیوبیت است و زیر فضایی را بدست آورید که توسط عملگرهای $X_1X_2$ ، $Z_1Z_2$ پایدار می شود.

پس از این تمرین ها به توضیح نکته چهارم بازمی گردیم. در این کد خطاهایی که روی کیوبیت رخ می دهد سه نوع عملگر پاوولی $X_1, X_2, X_3$ هستند. این خطاها با عملگرهای پایدار ساز جابجا نمی شوند، بلکه با بعضی از آنها جابجا و با بعضی از آنها پاد جابجا می شوند و دقیقا همین رابطه پادجابجایی است که ویژه مقادیر عملگرهای پایدارکننده را از یک به منهای یک تبدیل می کند و باعث می شود که ما بتوانیم وقوع خطا را تشخیص بدهیم. فرض کنید که $S$ یک عملگر پایدارساز و $E$ یک خطاست که با $S$ پادجابجا می شود. هرگاه $|\psi\rangle$ یک حالت متعلق به کد باشد بنابر تعریف می دانیم که

$$S|\psi\rangle = |\psi\rangle, \qquad \longrightarrow \qquad S(E|\psi\rangle) = -E(S|\psi\rangle) = -E|\psi\rangle. \qquad (۲۴)$$

بنابراین وقتی که یک خطای $E$ رخ می دهد تمام عملگرهای پایدارسازی که با $E$ پادجابجا می شوند ویژه مقدارشان از یک به منهای یک تغییر می کند. جدول زیر رابطه جابجایی عملگرهای خطا و سندروم های خطا را نشان می دهد. علامت مثبت به معنای جابجایی و علامت منفی به معنای پادجابجایی است.

| $X_3$ | $X_2$ | $X_1$ | $I$ | |
|---|---|---|---|---|
| + | - | - | + | $Z_1Z_2$ |
| - | + | - | + | $Z_1Z_3$ |

همانطور که از جدول بالا پیداست، سندروم های مربوط به خطا ها همه با هم متفاوت اند و همین موضوع باعث تمیزدادن خطاها و در نتیجه تصحیح آنها می شود. در بخش بعدی یک کد کوانتومی خواهیم ساخت که خطاهای فاز-برگردان را تصحیح می کند.

## ۲.۳ اصلاح خطاهای فاز ـ برگردان

حال فرض کنید که تنها امکانی که برای خطا وجود دارد برگردان فاز یک کیوبیت است به این معنا که در طول کانال ممکن است عملگر $Z$ (یاهمان $\sigma_z$ ) روی یک کیوبیت اثر کند. دراین صورت هرگاه یک کیوبیت در ابتدای کانال به صورت $|\psi\rangle = a|0\rangle + b|1\rangle$ ارسال شده باشد، در اثر خطای احتمالی ممکن است به صورت $X|\psi\rangle = a|0\rangle - b|1\rangle$ دریافت شود. برای آشکارسازی این نوع خطا کیوبیت های $|0\rangle$ و $|1\rangle$ را به صورت زیر کُد می کنیم:

$$|0\rangle \longrightarrow |0\rangle_E = |+++\rangle, \qquad |1\rangle \longrightarrow |1\rangle_E = |---\rangle, \tag{۲۵}$$

که در آن علامتِ $E$ از کلمه $Encoding$ گرفته شده است. درنتیجه حالتِ یک کیوبیت به صورت زیر کد می شود:

$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow |\psi\rangle_E = a|+++\rangle + b|---\rangle. \tag{۲۶}$$

این حالت ویژه حالت مشترک عملگرهای $X_1X_2$ و $X_1X_3$ با مقادیر ویژه ۱ است. به عبارت دیگر

$$X_1X_2|\psi\rangle_E = |\psi\rangle_E, \qquad X_1X_3|\psi\rangle_E = |\psi\rangle_E. \tag{۲۷}$$

حال اگر یک خطای $Z_1$ ، $Z_2$ یا $Z_3$ رخ دهد حالت $|\psi\rangle_E$ تبدیل به حالتی می شود که ویژه مقدارش برای عملگرهای فوق تغییر خواهد کرد.

$$\begin{aligned}
I|\psi\rangle_E = a|+++\rangle + b|---\rangle \qquad &\longrightarrow \qquad X_1X_2 = 1, \quad X_1X_3 = 1 \\
Z_1|\psi\rangle_E = a|-++\rangle + b|+--\rangle \qquad &\longrightarrow \qquad X_1X_2 = -1, \quad X_1X_3 = -1 \\
Z_2|\psi\rangle_E = a|+-+\rangle + b|-+-\rangle \qquad &\longrightarrow \qquad X_1X_2 = -1, \quad X_1X_3 = 1 \\
Z_3|\psi\rangle_E = a|++-\rangle + b|--+\rangle \qquad &\longrightarrow \qquad X_1X_2 = 1, \quad X_1X_3 = -1.
\end{aligned} \tag{۲۸}$$

در روابط بالا مقادیر ویژه عملگرهای $X_1X_2$ و $X_1X_3$ را نوشته ایم. این عملگرها که مقادیر ویژه آنها خطا را آشکار می کنند نشانه های خطا [۳] نامیده می شوند. نکته مهم آن است که حالت دچار خطاشده همچنان ویژه بردار عملگرهای $X_1X_2$ و $X_1X_3$ باقی می ماند بنابراین اندازه گیری این دو عملگر باعث فروکاهش تابع موج نمی شود. بعد از اینکه معلوم شد خطای بیت برگردان در چه نقطه ای صورت گرفته است می توان با اعمال عملگر تصحیح کننده خطا را اصلاح کرد.

[۳] Error Syndrome

■ تمرین: گروه پایدار ساز این کد را مشخص کنید. جدول روابط جابجایی خطاها و سندورم های خطا ها را بسازید. مداری که کدگذاری را انجام می دهد و هم چنین مداری که سندروم های خطا را شناسایی می کند بسازید.

دیدیم که کدی که برای تصحیح خطای بیت_برگردان می نویسیم با کدی که برای تصحیح خطای فاز_برگردان می نویسیم متفاوت است. بنابراین هرکدام از این کد ها یک نوع خطا را تصحیح می کنند. حال سوال مهمی که پیش روی ماست این است که چه نوع کدی می تواند هر دو نوع خطا را تصحیح کند؟ به این سوال در بخش بعد پاسخ می دهیم. کدی که این کار را می کند کد شر $ShorCode$ نامیده می شود و توسط پیتر شر $PeterShor$ ساخته شده است.

## ۳.۳ کد ۹ کیوبیتی شُر _ اصلاح خطاهای فاز و بیت _ برگردان

حال فرض کنید که تنها امکانی که برای خطا وجود دارد برگردان یک کیوبیت یا برگردان فاز آن کیوبیت است. یعنی خطا می تواند از نوع $X$ یا $Z$باشد. واضح است که کدهای ساده قبلی نمی توانند هردو نوع خطا را آشکار کنند. هم چنین انتظار داریم که کدی که برای آشکارسازی این نوع خطا ها ساخته می شود از تعداد بیشتری کیوبیت استفاده کند. برای آشکارسازی این نوع خطا ها می توان به نوعی کدهای قبلی را با هم ترکیب کرد. این ترکیب به شکل زیر صورت می گیرد. حالت های $|+\rangle$ و $|-\rangle$ را به صورت زیر تعریف می کنیم:

$$|+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle). \tag{۲۹}$$

حال کیوبیت های $|0\rangle$ و $|1\rangle$ را به صورت زیر کُد می کنیم.

$$|0\rangle \longrightarrow |0\rangle_E = |+++\rangle, \qquad |1\rangle \longrightarrow |1\rangle_E = |---\rangle. \tag{۳۰}$$

به عبارت دیگر هر کیوبیت به ۹ کیوبیت کد می شود. به زبان کلاسیک نرخ این کد $\frac{1}{9}$ است که نرخ پایینی است ولی این بهایی است که برای تصحیح خطای کوانتومی باید بپردازیم. در واقع همانطور که بعدا نشان خواهیم داد این کد نه تنها خطاهای $X$ و $Z$ بلکه هر نوع خطایی حتی خطاهای پیوسته را می تواند تصحیح کند و با توجه به این مطلب بهایی که برای این تصحیح خطا پرداخته ایم قابل توجیه است. اما چگونه این کد خطاهای یادشده را تصحیح می کند؟ این کد از ۹ کیوبیت تشکیل شده است که در سه بلوک سه تایی مرتب شده اند. می خواهیم نشان دهیم که این کد خطاهای $X_1$ تا $X_9$ و هم چنین خطاهای $Z_1$ تا $Z_9$ را تصحیح می کند. نخست ببینیم که این کد توسط چه عملگرهایی پایدار می شود. عملگرهای زیر را در نظر بگیرید:

$$X_I = X_1X_2X_3, \qquad X_{II} = X_4X_5X_6, \qquad X_{III} = X_7X_8X_9. \tag{۳۱}$$

■ تمرین: الف: ثابت کنید که عملگرهای زیر کد شر را پایدار می کنند:

$$\{X_IX_{II},\ X_IX_{III},\ Z_1Z_2,\ Z_1Z_3,\ Z_4Z_5,\ Z_4Z_6,\ Z_7Z_8,\ Z_7Z_9\}. \tag{۳۲}$$

ب: نشان دهید که همه این عملگرها با هم جابجا می شوند. سپس نشان دهید که خطاهای $X_1$ تا $X_9$ هرکدام روابط پادجابجایی متفاوتی با پایدارکننده های فوق دارند و در نتیجه می توان با اندازه گیری این سندروم ها همه این خطا ها را از هم تمیز داد و آنها را تصحیح کرد.

پ: سپس نشان دهید که خطاهای فاز برگردانی که در هر بلوک رخ می دهد نیز سندروم های متفاوت دارند و قابل تشخیص و تصحیح هستند. دقت کنید که یک بلوک مثل بلوک یک، چندین خطای فازبرگردان مثل $Z_1, Z_2, Z_3$ دارد که در ظاهر متفاوت اند ولی اثرشان یکی است.

ت: مداری که عمل کد کردن را انجام می دهد رسم کنید. هم چنین مداری که سندروم ها را اندازه گیری می کند رسم کنید.

به این ترتیب کد شر می تواند هر نوع خطای بیت برگردان $X$ یا $Z$ را در هر کدام از ۹ کیوبیت کد تمیز داده و اصلاح کند. هروقت که علامت های خطاهای $X_i$ و $Z_i$ باهم روشن شوند به این معناست که خطای $Y_i$ رخ داده است. پس به این ترتیب کد شر می تواند خطاهای $X_i$ ، $Y_i$ و $Z_i$ را در تمام کیوبیت ها تشخیص داده و آنها را تصحیح کند.

با این مثال ها اکنون قانع شده ایم که می توان بر موانع اساسی تصحیح خطای کوانتومی غلبه کرد. کد شُر اگرچه تمام خطاهای یک کیوبیتی را تصحیح می کند ولی این عیب را دارد که از $n=9$ کیوبیت برای کد کردن $k=1$ کیوبیت منطقی استفاده می کند. به عبارت دیگر نرخ کد کردن برای کد شُر برابر است با $R := \frac{k}{n} = \frac{1}{9}$. سوال طبیعی این است که آیا می توان کدهای بهتری ابداع کرد که نرخ آنها بیشتر باشد؟ سوال های دیگری نیز مطرح هستند: مثلا تا چه حدی میتوان نرخ را افزایش داد؟ چه رابطه ای بین نرخ و توانایی یک کد برای تصحیح خطا وجود دارد؟ این ها و سوالات بنیادی دیگر را تنها در پرتو یک نظریه کامل تصحیح خطای کوانتومی می توان پاسخ گفت. سعی می کنیم که در ادامه این درس و در درس بعدی به این سوال ها پاسخ بدهیم.

# ۴ نظریه کلی اصلاح خطاهای کوانتومی

پس از این مثال ها می توانیم به روش منظم تری کد های کوانتومی را مطالعه کنیم. همانطور که در مقدمه گفتیم خطاهای کوانتومی و نحوه اصلاح آنها بکلی متفاوت با خطاهای کلاسیک هستند و به همین جهت در ابتدای امر گمان می شد که کامپیوترهای کوانتومی هرگز ساخته نخواهند شد زیرا هیچ روشی برای شناسایی و اصلاح خطاهای ناگزیری که درآنها وجود دارد شناخته شده نبود. امروزه معلوم شده است که یک نظریه جامع و کامل برای آشکارسازی و اصلاح خطاهای کلاسیک وجود دارد که ساخت عملی کامپیوترهای کوانتومی را امکان پذیر می کند. اندیشه هایی که مبنای این نظریه قرار گرفته اند اساساً از همان نظریه کلاسیک الهام گرفته شده‌اند ولی در تدوین آنها تمام محدودیت های مکانیک کوانتومی نظیر عدم امکان اندازه گیری های دلخواه و یا عدم امکان تکثیر حالت ها مورد ملاحظه قرار گرفته‌اند. کاری که ما دراین بخش می کنیم آن است که نخست کدهای ساده‌ای را معرفی می کنیم که قادرند خطاهای معینی را آشکار و اصلاح کنند. سپس به تدریج که این کد ها را بسط می دهیم اصول اساسی نظریه اصلاح خطاهای کوانتومی را نیز دریک چارچوب کلی شرح خواهیم داد.

می دانیم که فضای هیلبرت یک کیوبیت یک فضای دوبعدی مختلط است که آن را با $C_2$ نشان می دهیم. فضای هیلبرت ِ $n$ کیوبیت را با $C_2^n$ نشان می دهیم. می دانیم که بعد این فضا برابر است با $2^n$ . این فضا برای کد کردن $n$ کیوبیت جا دارد ولی اگر این کار را بکنیم براحتی حالت ها به هم تبدیل می شوند ، آنهم توسط خطاهای با وزن یک ، یعنی خطاهایی که تنها بر یک کیوبیت اثر می گذارند و محتمل ترین خطا ها هستند. مشابه با حالت کلاسیک که تنها از تعداد کمی از نقاط موجود در فضای $Z_2^n$ برای کد کردن کلمه ها استفاده می کردیم، در این جا هم برای کد کردن حالت های کیوبیت ها از یک زیر فضای کم بعد از $C_2^n$ استفاده می کنیم. این زیر فضا را فضای کد یا $CodeSpace$ می نامیم و آن را با

$$\mathcal{C} \in C_2^n \tag{۳۳}$$

نشان می دهیم. بنابراین یک کد کوانتومی چیزی نیست جز یک زیر فضا از $C_2^n$ . اگر این زیر فضا بعد $2^k$ داشته باشد، می گوییم $k$ کیوبیت را در $n$ کیوبیت کد کرده ایم. درست مثل حالت کلاسیک ، یک کد کوانتومی یک مجموعه مشخص از خطاها را می تواند تصحیح کند. این مجموعه خطا را با

$$\mathcal{E} = \{E_a,\ E_b,\ E_c, \cdots E_n\} \tag{۳۴}$$

نشان می دهیم. سوال کلی ای که در این بخش با آن روبرو هستیم این است که اگر یک کد بخواهد این مجموعه خطا را اصلاح کند، چه شرایطی رابابد داشته باشد. خواهیم دید که یک کد در واقع می بایست یک شرط خیلی ساده را برآورده کند تا بتواند یک مجموعه از خطا را تصحیح کند. نخست شرط کافی را بیان می کنیم.

قضیه: شرط کافی برای آن که یک کد $\mathcal{C}$ بتواند یک مجموعه خطای $\mathcal{E}$ را اصلاح کند آن است که :

$$\langle\psi|E_a^\dagger E_b|\psi\rangle = 0, \qquad E_a \neq E_b \in \mathcal{E}, \qquad \forall\psi \in \mathcal{C}. \tag{۳۵}$$

اثبات: هرگاه شرط فوق برآورده شود، و حالت $|\psi\rangle \in \mathcal{C}$ به صورت زیر تحول پیدا کند:

$$|\psi\rangle \otimes |e\rangle \longrightarrow \sum_a E_a|\psi\rangle \otimes |e_a\rangle \tag{۳۶}$$

شرط فوق بیان می کند که حالت های متفاوت $E_a|\psi\rangle$ برهم عمودند و در نتیجه بایک اندازه گیری از هم قابل تمیزند. به عبارت دیگر فضاهای $E_a\mathcal{C}$ و$E_b\mathcal{C}$ و دیگر فضاهایی که از اثر خطاهای متعلق به $\mathcal{E}$ پدیدار می شوند ، همگی زیرفضاهای عمود برهم هستند :

$$E_a\mathcal{C} \perp E_b\mathcal{C} \qquad a \neq b. \tag{۳۷}$$

پس با یک اندازه گیری می توانیم تشخیص دهیم که در کدام زیر فضا هستیم و سپس با توجه به اینکه یک عملگر پاوولی براحتی معکوس پذیراست ، می توانیم اثر آن را روی حالت $|\psi\rangle$ خنثی کنیم و خطا را اصلاح کنیم. دقت کنید که دراین اندازه گیری ما فقط نتیجه می گیریم که در کدام زیرفضا هستیم و هیچ گونه اطلاعاتی در باره حالت اولیه بدست نمی آوریم چرا که بدست آوردن اطلاعات از حالت اولیه معادل با مختل کردن آن است و ما نمی خواهیم که این اتفاق بیفتد.

اما آیا این شرط لازم هم هست؟ پاسخ این است که واقعا این شرط لازم نیست. خواننده براحتی می تواند ببیند که در کد شر این شرط برآورده نمی شود. مثلا خطاهای $Z_1$ و $Z_2$ را در نظر بگیرید. این دو خطا در شرط ۳۵ صدق نمی کنند با این حال کد شر می تواند این خطاها را اصلاح کند.

■ تمرین: کد شر را در نظر بگیرید. جدولی تشکیل دهید که سندروم تمام خطاهای تک کیوبیتی یعنی $X_i, Y_i, Z_i$ را نشان دهد. آیا سندروم

همه خطا ها با هم متفاوت است؟ چرا کد شر می تواند همه خطاها ی تک کیوبیتی را تصحیح کند؟

■ تمرین: ضرب داخلی $\langle\psi|Z_iZ_j|\psi\rangle$ را برای همه $i,j=1,\cdots 9$ تشکیل دهید . ببنید که آیا شرط ۳۵ برای کد شُر برقرار است یا خیر؟

پس از این مثال و تمرین می توانیم قضیه اصلی نظریه اصلاح خطای کوانتومی را بیان کنیم.

قضیه: شرط لازم و کافی برای آنکه یک کد کوانتومی $\mathcal{C}$ بتواند یک مجموعه خطای $\mathcal{E}$ را اصلاح کند این است که :

$$\langle\psi|E_a^\dagger E_b|\psi\rangle=\Lambda_{ab},\qquad \forall\psi\in\mathcal{C},\qquad \forall E_a,\ \ E_b\in\mathcal{E}. \tag{۳۸}$$

دقت کنید که نکته اصلی این شرط این است که ماتریس $\Lambda$ مستقل از $|\psi\rangle$ است در غیر این صورت این رابطه هیچ محتوایی ندارد.

■ تمرین: صحت این شرط را برای کدی که خطای بیت_برگردان را اصلاح می کند بیازمایید. همین کار را برای کد شُر و کد پنج کیوبیتی نیز انجام دهید.

■ تمرین: نشان دهید که ماتریس $\Lambda$ هرمیتی است.

حال می توانیم به اثبات این قضیه بپردازیم.

اثبات: درست است که ماتریس $\Lambda$ قطری نیست، ولی ما می توانیم ترکیب جدیدی از عملگرهای $E_a$ را انتخاب کنیم به نحوی که این ماتریس قطری شود. در واقع قرار می دهیم:

$$F_a=\gamma_{ab}^*E_b, \tag{۳۹}$$

که در آن $\gamma_{ab}$ ها اعداد مختلط هستند. در نتیجه خواهیم داشت:

$$\langle\psi|F_a^\dagger F_b|\psi\rangle = \gamma_{ac}\gamma_{bd}^*\langle\psi|E_c^\dagger E_d|\psi\rangle = \gamma_{ac}\gamma_{bd}^*\Lambda_{cd} = (\gamma\Lambda\gamma^\dagger)_{ab} \quad (۴۰)$$

بنابراین اگر ضرایب $\gamma_{ab}$ را به طرز مناسب انتخاب کنیم خواهیم داشت:

$$\langle\psi|F_a^\dagger F_b|\psi\rangle = \omega_a\delta_{ab}. \quad (۴۱)$$

یعنی این که برای خطاهای جدید یعنی $F_a$ ها فضاهای مربوطه بازهم بر هم عمود هستند، یعنی اینکه $F_aC \perp F_bC$ . بنابراین با یک اندازه گیری می توانیم تشخیص دهیم که در کدام زیر فضا هستیم بدون اینکه از خود حالت اطلاعی بدست آوریم. هر زیرفضا نشانه یا سندروم خاص خود را دارد و پس از تشخیص نشانه می توانیم دو باره حالت را با اعمال مناسب یک عمل گر کوانتومی به حالت اولیه برگردانیم. ولی چرا خطاهای اولیه با این خطاهای جدید هم ارز هستند؟ پاسخ این سوال با توجه به رابطه زیر روشن می شود. زیرا می توانیم بنویسیم

$$|\psi\rangle\otimes|e\rangle \longrightarrow \sum_a E_a|\psi\rangle\otimes|e_a\rangle = \sum_{a,b}\gamma_{ba}F_b|\psi\rangle|e_a\rangle = \sum_b\left(F_b|\psi\rangle\right)\left(\gamma_{ba}|e_a\rangle\right) == \sum_b\left(F_b|\psi\rangle\right)\left(|\tilde{e_b}\rangle\right) \quad (۴۲)$$

این رابطه در واقع بیان می کند که هم می توان فرض کرد که خطاهای $E_a$ روی حالت $|\psi\rangle$ رخ داده است و هم می توان فرض کرد که خطاهای $F_a$ روی حالت رخ داده است . تفاوت این دو نوع بسط در حالت های محیط است که بکلی از دسترس ما خارج هستند ولی تا جایی که به سیستم و کیوبیت های کد شده مربوط است این دو نوع بسط هم ارز هستند.

■ تمرین: شرط ۳۸ را در نظر بگیرید. طرف راست این رابطه بستگی به حالت $|\psi\rangle$ ندارد. نشان دهید که اگر طرف راست به حالت بستگی داشته باشد، دیگر نمی توان ماتریس $\Lambda$ را با تغییر عملگرهای خطا قطری کرد.

■ تمرین: شرط ۳۸ را در نظر بگیرید. اگر بردارهای پایه فضای کد یعنی $\mathcal{C}$ را با $v_1, v_2, \cdots v_k$ نشان دهیم ، ثابت کنید که این شرط با شرط زیر معادل است. دقت کنید که این معادل بودن را به صورت دو طرفه باید نشان دهید. یعنی نشان دهید که هرکدام از این رابطه ها، دیگری

را نتیجه می دهد.

$$\langle v_i|E_a^\dagger E_b|v_j\rangle = \tilde{\Lambda}_{ab}\delta_{ij}. \quad (۴۳)$$

این رابطه یک نتیجه فرعی ولی مهم و از نظر مفهومی روشن را در بر دارد. فرض کنید که $i \neq j$ باشد . در این صورت همواره روابط زیر برقرارند:

$$\begin{aligned} E_a|v_i\rangle &\perp E_a|v_j\rangle, \\ E_a|v_i\rangle &\perp E_b|v_j\rangle. \end{aligned} \quad (۴۴)$$

رابطه اول می گوید که امکان ندارد که دو بردار پایه متفاوت توسط یک خطا به بردارهای شبیه به هم نگاشته شود و این شرط مهمی است زیرا می گوید که بردارهای پایه متفاوت توسط یک خطا به زیر فضاهای متفاوت نگاشته می شوند. اگر این طور نبود نمی شد تشخیص داد که آیا برداری که بدست آورده ایم ناشی از خطای $E_a$ روی کدام یک از بردارهای پایه است. رابطه دوم بیان می کند که حتی خطاهای متفاوت نیز نمی توانند بردارهای پایه متفاوت را به بردارهایی تبدیل کنند که باهم اشتباه می شوند.

## ۵ فرمالیزم پایدارسازها

نظریه اصلاح خطای کوانتومی را به بهترین نحو می توان در فرمالیزم پایدارساز ها [۴] فهمید. این چارچوب نخستین بار توسط دانیل گوتسمان [۵] ارایه شده است. برای فهم این چارچوب می بایست بعضی مفاهیم مقدماتی را مرور کنیم. طبیعی است که مجموعه عملگرهای پاوولی در این فرمالیزم نقش مرکزی دارد. می دانیم که مجموعه عملگرهای پاوولی تشکیل یک گروه نمی دهند (این موضوع را بیازمایید) ولی اگر این مجموعه را در اعداد $\pm 1, \pm i$ ضرب کنیم آنگاه یک گروه تشکیل می دهند یعنی مجموعه 16 عضوی حاصل تحت عمل ضرب بسته است. این گروه را گروه پاوولی روی یک کیوبیت می نامیم. بنابراین داریم:

---

[۴] Stabilizer Formalism

[۵] Daniel Gottesmann

تعریف: گروه پاوولی روی یک کیوبیت عبارت است از مجموعه زیر :

$$P_1 = \{\pm 1, \pm i\} \times \{I, X, Y, Z\}, \qquad (۴۵)$$

مرتبه این گروه متناهی یعنی تعداد اعضای آن برابراست با $|P_1| = 16$ .

■ تمرین: گروه بودن این مجموعه را بیازمایید. خودتان را قانع کنید که اگر بعضی از ضرایب مثلا $\pm i$ را حذف کنیم، مجموعه حاصل دیگر گروه نخواهد بود.

به همین نحو می توانیم گروه پاوولی روی $n$ کیوبیت را تعریف کنیم. بازهم نیازمند این هستیم که ماتریس های پاوولی را که این بار روی $n$ کیوبیت اثر می کنند همراه با ضرایب چهارگانه فوق در نظر بگیریم تا مجموعه حاصل تشکیل یک گروه بدهد. بنابراین داریم:

■ تمرین: گروه پاوولی روی $n$ کیوبیت به صورت زیر تعریف می شود:

$$P_n = \{\pm 1, \pm i\} \times \{\sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \sigma_{i_n}, \quad | \quad i_1, i_2, \cdots i_n = 0, 1, 2, 3\}. \qquad (۴۶)$$

تعداد اعضای این گروه برابر است با $|P_n| = 4^{n+1}$ .

■ تمرین: نشان دهید که اگر $g$ و$g'$ دو عضو از گروه پاوولی باشند، آنگاه

$$gg' = \pm g'g, \qquad g^2 = \pm 1, g'^2 = \pm 1. \qquad (۴۷)$$

یعنی اینکه هر دو عضو گروه پاوولی یا باهم جابجا می شوند یا باهم پادجابجا می شوند. هم چنین مربع هر عضو گروه پاوولی یا برابر است با $1$ یا برابراست با $-1$.

تعریف: هر زیر گروه از گروه $P_n$ که عناصر آن ۱ـ هرمیتی باشند، ۲ـ باهم جابجا شوند و ۳ـ زیرگروه شامل عنصر $-1$ نباشد، یک گروه پایدارساز [6] خوانده می شود.

از این جا به بعد گروه پایدارساز را با $\mathcal{S}$ نمایش می دهیم. واضح است که گروه پایدارساز یک تعداد مولد دارد به این معنا که تمام عناصر گروه از حاصل ضرب های این مولدها ساخته می شود. اگر عناصر $s_1$ تا $s_r$ مولدهای یک گروه پایدارساز باشند می نویسیم:

$$\mathcal{S} = \langle s_1, s_2, \cdots s_r \rangle \quad (۴۸)$$

■ تمرین: کدام یک از مجموعه های زیر یک گروه پایدارساز تشکیل می دهند و کدام نمی دهند. در مواردی که پاسخ شما منفی است دلیل خود را ذکر کنید.

$$\begin{aligned}
\mathcal{S}_1 &= \{I, ZZZ\},\\
\mathcal{S}_2 &= \{I, ZZI, IZZ\},\\
\mathcal{S}_3 &= \{I, iZZZ\},\\
\mathcal{S}_4 &= \{I, XXX, ZZZ, YYY\},\\
\mathcal{S}_5 &= \{I, ZZZ, -I, -ZZZ\},\\
\mathcal{S}_6 &= \{I, XXI, IXX, XIX\}.
\end{aligned} \quad (۴۹)$$

■ تمرین: در هر کدام از موارد زیر تمامی اعضای گروه پایدارساز را بنویسید:

$$\begin{aligned}
\mathcal{S}_1 &= \langle XXZ, ZXX\rangle,\\
\mathcal{S}_2 &= \langle XXI, IXX\rangle,\\
\mathcal{S}_3 &= \langle ZZI, IZ\rangle,\\
\mathcal{S}_4 &= \langle ZII, IIZ\rangle,\\
\mathcal{S}_5 &= \langle ZYI, IYZ\rangle.
\end{aligned} \quad (۵۰)$$

■ تمرین: نشان دهید که در یک گروه پایدارساز مربع همه عناصر برابر با 1 است.

[6] Stabilizer Group

■ تعریف: هرگاه $\mathcal{S} \subset P_n$ یک گروه پایدارساز باشد، فضای پایدارشده توسط این گروه یعنی زیر فضایی از فضای $n$ کیوبیت که توسط عناصر این گروه پایدار می شود. این زیرفضا را با $\mathcal{C}_{\mathcal{S}}$ نشان می دهیم. به عبارت دقیق تر داریم:

$$\mathcal{C}_{\mathcal{S}} = \{|\psi\rangle \in C_2^{\otimes n} \ | \ s|\psi\rangle = |\psi\rangle, \qquad \forall s \in \mathcal{S}\} \tag{۵۱}$$

در ادامه برای سادگی نمادها از نوشتن زیرنویس $\mathcal{S}$ برای فضای $\mathcal{C}$ صرف نظر می کنیم و فضای پایدارشده را تنها به صورت $\mathcal{C}$ می نویسیم.

■ تمرین: در تمرین قبلی فضای پایدارشده توسط هر گروه را مشخص کنید. یک پایه برای این فضا بنویسید.

■ تمرین: یک کد کوانتومی در نظر بگیرید با گروه پایدارساز زیر:

$$G = \langle ZZZ \rangle. \tag{۵۲}$$

بردارهای پایه این کد را مشخص کنید. تعیین کنید که این کد چه خطاهایی را تشخیص می دهد . یک مجموعه از خطاهای قابل اصلاح برای این کد بنویسید.

آیا تعداد اعضای گروه پایدارساز ربطی به بعد فضای پایدارشده دارد؟ مسلم است که هرچه تعداد عناصر گروه پایدارساز بیشتر باشد قید های بیشتری روی فضای پایدارشده اعمال می شود و بنابراین بعد آن کمتر می شود ولی چقدر کمتر؟ دقیقا چه رابطه ای بین این دو وجود دارد. پاسخ آن در قضیه زیر داده می شود.

قضیه: هرگاه تعداد مولدهای گروه پایدارساز برابر با $r$ باشد، آنگاه بعد فضای پایدارشده برابراست با $2^{n-r}$.

اثبات: نخست دقت می کنیم که هرگاه $s \in \mathcal{G}$ یک عضو گروه پایدار ساز باشد، آنگاه $\frac{1}{2}(1+s)$ یک عملگرتصویری است که فضا را روی زیر فضایی که برای عملگر $s$ ویژه مقدار $+1$ دارد تصویر می کند. درنتیجه عملگرتصویری زیر که حاصلضرب عملگرهای تصویری

مربوط به همه مولدها ست دقیقا عملگر تصویری روی فضای کد است. بنابراین کافی است که بتوانیم رد آن را حساب کنیم تا بعد فضای کد بدست بیاید.

$$\prod_{\mathcal{C}} := \prod_{i=1}^{r} \frac{1}{2}(1+s_i) \tag{۵۳}$$

برای آنکه رد این عملگر را حساب کنیم آن را بسط می دهیم که به صورت زیر در می آید:

$$\prod_{\mathcal{C}} = \frac{1}{2^r}\sum_{s\in\mathcal{S}} s = \frac{1}{2^r}\left(1+\sum_{s\neq I\in\mathcal{S}} s\right) \tag{۵۴}$$

اما می دانیم که تمام عملگر های $S$ حتما شامل ماتریس های پاوولی هستند و بنابراین رد آنها برابر با صفراست. در نتیجه

$$tr(\prod_{\mathcal{C}}) = \frac{1}{2^r}tr(I) = \frac{2^n}{2^r} = 2^{n-r}. \tag{۵۵}$$

به این ترتیب قضیه ثابت می شود.

یک نکته در باره نمادها: معمولا بعد فضای کد را با $2^k$ نشان می دهیم که در نتیجه آن تعداد مولدهای گروه پایدارساز را با $n-k$ نمایش می دهیم. این انتخاب البته با قضیه بالا سازگار است.

## ۱.۵ تشخیص و اصلاح خطا در کدهای مبتنی بر پایدارسازها

حال که با پاوولی و زیر گروه پایدارساز آشنا شده ایم می خواهیم بفهمیم که قسمت های مختلف گروه پاوولی چه نقشی در تصحیح خطا به عهده دارند. عناصر زیرگروه پایدار ساز که نقش مشخصی دارند. آنها سندروم های خطا هستند و روی تمام فضای کد ویژه مقدار برابر با $+1$ دارند.

حال به هر عضو دیگری در گروه پاوولی که نگاه کنیم با دوحالت بیشتر مواجه نمی شویم. یا اینکه این عضو با همه عناصر $S$ جابجا می شود یا اینکه با بعضی از عناصر $S$ جابجا نمی شود. آن دسته از عناصری که با همه اعضای $S$ جابجا می شوند در یک زیر مجموعه قرار می دهیم و آن را با $\mathcal{N}(S)$ نمایش می دهیم. به عبارت دیگر:

$$\mathcal{N}(S) := \{n \in P \quad ns_i = s_i n \ \ \forall \ \ s_i \in \ S\}. \tag{۵۶}$$

بقیه عناصر گروه پاوولی حتما با یک یا چند عضو از $S$ پادجابجا می شوند. واضح است که $\mathcal{N}(S)$ یک گروه است. هم چنین واضح است که $S \subset \mathcal{N}(S)$. خواهیم دید که با توجه به مفاهیم نظریه گروه تصویر منسجم و خیلی زیبایی از فضای کد و خطاهای قابل تشخیص و تصحیح بدست می آید. یک عضو مثل $n \in \mathcal{N}(S)$ را در نظر می گیریم. این عضو با همه مولدهای $S$ جابجا می شود. در این صورت برای یک بردار دلخواه در فضای کد داریم:

$$s_i(n|\psi\rangle) = n(s_i|\psi\rangle) = n|\psi\rangle. \tag{۵۷}$$

معنای این رابطه این است که $n$ ویژه مقدار $s_i$ ها را تغییر نمی دهد و در نتیجه $n|\psi\rangle$ یک حالت دیگر در فضای کد است که البته ممکن است با $|\psi\rangle$ متفاوت باشد. بنابراین $n$ یک خطای غیرقابل تشخیص است که مثل یک عملگر پاوولی کد شده روی فضای کد عمل می کند. برای وقتی که فضای کد فقط یک کیوبیت را کد کرده است، این عملگرهای پاوولی که گاهی آنها را عملگرهای منطقی [۷] نیز می خوانیم با نمادهای زیر نشان داده می شوند:

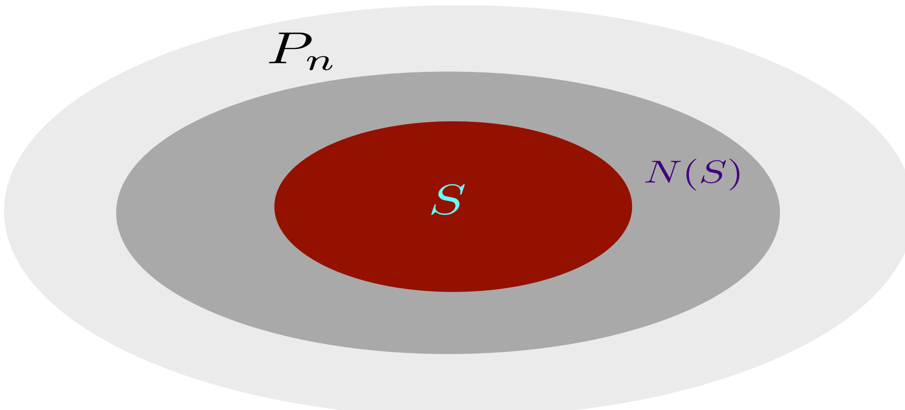
$$\overline{X} \qquad \overline{Y} \qquad \overline{Z}. \tag{۵۸}$$

برای وقتی که فضای کد ها چند کیوبیت را کد کرده باشد این عملگرهای منطقی با اندیس مربوطه مشخص می شوند. دقت کنید که چندین عملگر متفاوت در $N(S)$ می توانند یک نقش واحد ایفا کنند. به عنوان مثال در کد تکرار سه کیوبیتی $C = \{|000\rangle, |111\rangle\}$ دو عملگرِ $Z_1$ و سه $Z_1Z_2Z_3$ هر دو یک اثر دارند و این اثر چیزی نیست جز عملگر پاوولی کد شده یعنی $\overline{Z}$

$$\overline{Z}(a|000\rangle + b|111\rangle) = a|000\rangle - b|111\rangle. \tag{۵۹}$$

مثال : گروه پایدارساز $\mathcal{S} = \langle ZZI, IZZ\rangle$ را در نظر بگیرید. تمام عناصر این گروه عبارتند از $\mathcal{S} = \{I,\ ZZI,\ ZIZ,\ IZZ\}$ . عناصری مثل $XXX$ یا $YYY$ با تمام عناصر این گروه جابجا می شوند و در عین حال جز خود گروه نیستند. به عنوان یک تمرین تمام عناصر

[۷] Logical Operator




شکل ۵: گروه پاوولی، زیرگروه پایدارساز و گروه بهنجارساز این زیرگروه

مجموعه $\mathcal{N}(\mathcal{S})$ را بدست آورید.

مجموعه $\mathcal{N}(\mathcal{S})$ واقعا یک گروه است.

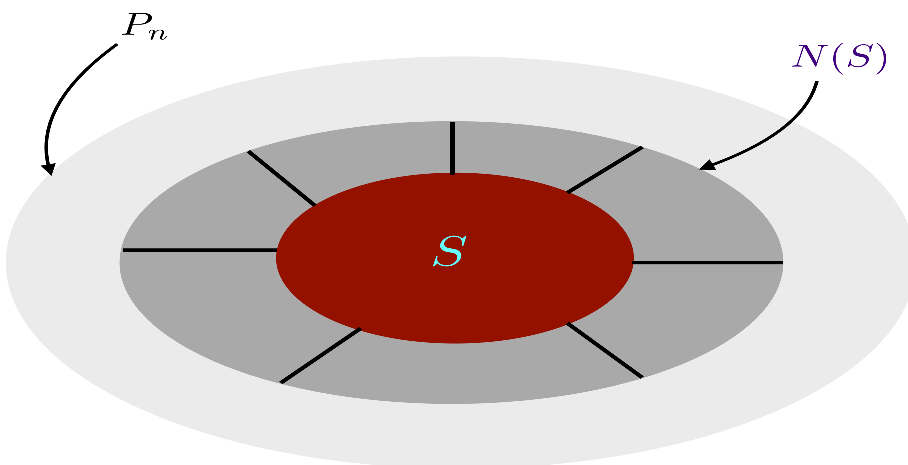
- تمرین: ثابت کنید که بهنجارساز ِ $\mathcal{S}$ تمام خواص یک گروه را دارد. دقت کنید که حتی اگر گروه $\mathcal{S}$ آبلی هم نبود، حتما بهنجارساز آن یک گروه می شد.
- تمرین: برای هرکدام از گروه های پایدارساز نشان داده شده در روابط ۵۰ گروه بهنجارساز را پیدا کنید.

حال دو عضو از گروه بهنجارساز مثل $n, n' \in \mathcal{N}(\mathcal{S})$ در نظر بگیرید به قسمی که

$$n' = nS, \quad for \;\; some \;\; S \in \mathcal{S} \tag{۶۰}$$

دراین صورت داریم

$$n'|\psi\rangle = nS|\psi\rangle = n|\psi\rangle,$$




شکل ۶: گروه پاوولی، زیرگروه پایدارساز و گروه بهنجارساز این زیرگروه

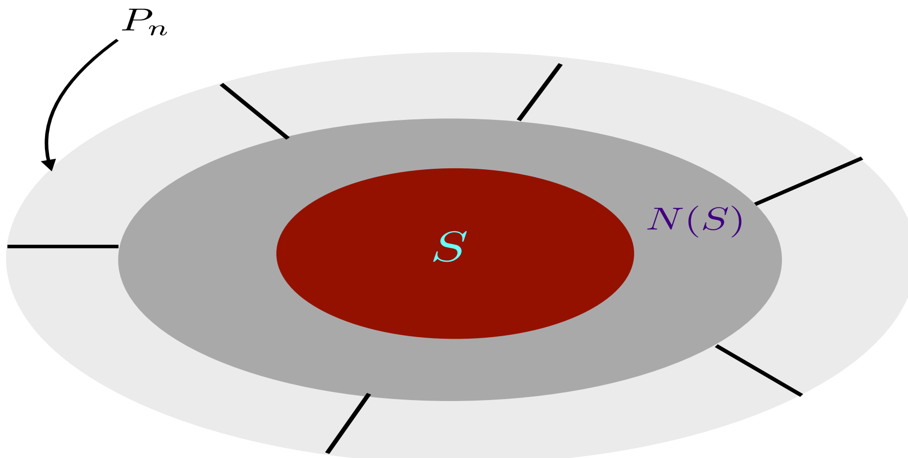
زیرا که $s$ حالت $|\psi\rangle$ را تغییر نمی دهد. در واقع هردو عناصر $n$ و $n'$ یک نوع خطا ایجاد می کنند. این موضوع به ما می گوید که می بایست $n$ و $n'$ را در ایجاد خطا هم ارز و یکسان بگیریم. به زبان ریاضی می گوییم که رابطه ۶۰ یک رابطه هم ارزی است و گروه $\mathcal{N}(\mathcal{S})$ را به کلاس های هم ارزی افراز می کند. هر کلاس هم ارزی را به صورت زیر نشان می دهیم:

$$[n] \equiv n\mathcal{S} = \{ns|, \qquad s \in \mathcal{S}\}. \tag{۶۱}$$

هرکلاس هم ارزی یک خطای خاص ایجاد می کند. تعداد کلاس های هم ارزی برابر است با $\frac{|\mathcal{N}(\mathcal{S})|}{|\mathcal{S}|}$.

تا کنون تکلیف دو قسمت از شکل (۵) را تعیین کرده ایم. حال به سراغ قسمت سوم می رویم یعنی قسمتی از گروه پاوولی که در $\mathcal{N}(S)$ نیست. این ها خطاهایی هستند که قابل تشخیص اند زیرا از خود نشانه (یا سندروم) باقی می گذارند. البته ممکن است دو خطای متفاوت سندورم یکسان داشته باشند و از یکدیگر تمیز داده نشوند. سوال این است که کدام خطاها از هم تمیز داده نمی شوند. برای پاسخ به این سوال دو خطای متفاوت مثل $E$ و $E'$ در نظر می گیریم به قسمی که

$$\exists\, n \in \mathcal{N}(S) \quad | \quad E' = En. \tag{۶۲}$$




شکل ۷: گروه پاوولی، زیرگروه پایدارساز و گروه بهنجارساز این زیرگروه

می خواهیم نشان دهیم که این دو خطا سندروم یکسان دارند. فرض کنید که $E$ با $s_i$ پادجابجا می شود. یعنی

$$Es_i = -s_iE$$

در این صورت خواهیم داشت:

$$E's_i = (En)s_i = E(ns_i) = E(s_in) = Es_in = -s_iEn = -s_iE'. \quad (۶۳)$$

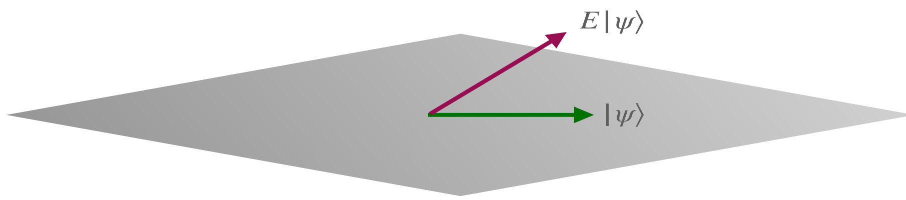
همین استدلال برای وقتی که خطای $E$ با یک عضو گروه پایدارساز جابجا می شود نیز درست است. حاصل کار این است که $E$ و $E'$ هر دو یک نشانه خطا دارند. برعکس تصور کنید که $E$ و $E'$ هر دو یک نشانه خطا دارند. می خواهیم نشان دهیم که هر دو به معنای فوق هم ارز هستند. برای این کار به ترتیب زیر عمل می کنیم.

نشانه های خطای $E$ و $E'$ را با یک مولد دلخواه مثل $s_i$ با $\alpha_i$ نشان می دهیم. در این صورت داریم:

$$Es_i = \alpha_i s_i E, \qquad E's_i = \alpha_i s_i E'. \quad (۶۴)$$

از آنجا که $\alpha_i^2 = 1$ استِ، نتیجه می گیریم:

$$(E'^{-1}E)s_i = E'^{-1}(Es_i) = E'^{-1}(\alpha_i s_i E) = \alpha_i(E'^{-1}s_i)E = s_iE'^{-1}E. \quad (۶۵)$$




شکل ۸: خطاهای قابل شناسایی آنهایی هستند که حالت را از فضای کد خارج می کنند و از خود نشانه باقی می گذارند.

در نتیجه $E'^{-1}E$ می بایست عضو $\mathcal{N}(S)$ باشد.

در این جا هم یک رابطه هم ارزی می توان تعریف کرد به این معنا که

$$\forall\ E\ ,E' \in\ P, \quad E \sim E' \qquad iff E' = En \quad for\ some\ n \in \mathcal{N}(S). \tag{۶۶}$$

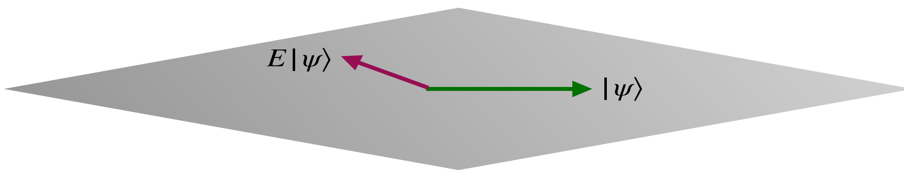
به این ترتیب گروه پاوولی نیز به کلاس های هم ارزی تبدیل می شود که در آنها سندروم تمام اعضای یک کلاس یکسان است و در نتیجه خطاهای این کلاس از هم تمیز پذیر نیستند ولی نشانه های کلاس های متفاوت تمیز پذیر و در نتیجه قابل اصلاح اند. در نتیجه مجموعه خطاهای اصلاح پذیر برابر است با تعداد کلاس های هم ارزی

$$P/\mathcal{N}(S).$$

هر کلاس هم ارزی عبارت است از:

$$[E] = \{En \qquad n \in \mathcal{N}\}. \tag{۶۷}$$

مجموعه تمام عناصر یک کلاس هم ارزی نشانه های یکسان دارند. هر دو کلاس هم ارزی نشانه های متفاوت دارند و بنابراین از یکدیگر قابل تمیز هستند. اندازه گیری نشانه های خطا معین می کند که خطای مربوط به کدام کلاس اتفاق افتاده است اما دقیقا نمی گوید که کدام خطا در آن کلاس اتفاق افتاده است. پس از اینکه تشخیص دادیم که خطای کدام کلاس اتفاق افتاده است برای تصحیح خطا فرض می کنیم که خطای




شکل ۹: خطاهای غیر قابل شناسایی آنهایی هستند که حالت را از فضای کد خارج نمی کنند و از خود نشانه ای باقی نمی گذارند.

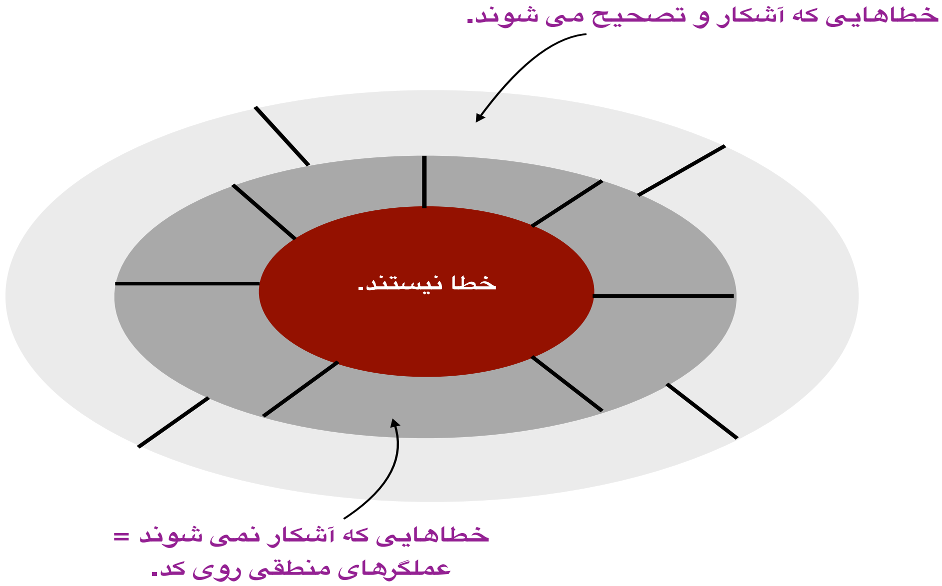
با بیشترین احتمال (یعنی خطای با کمترین وزن) اتفاق افتاده و سپس با اعمال معکوس آن عملگر (که البته با خود آن عملگر مساوی است) خطا را تصحیح می کنیم. منظور از وزن یک خطا تعداد عملگرهای پاوولی موجود در آن خطاست. به این ترتیب داریم:

$$\omega(X_1X_2) = 2 \qquad \omega(X_1X_2Z_3) = 3 \qquad \omega(Y_1Y_2Z_3Z_4) = 4. \tag{۶۸}$$

شکل (۱۰) تصویر کلی را در باره کدهای پایدارساز ها و رابطه آنها با خطاها نشان می دهد.

## ۲.۵ کد پنج کیوبیتی

دیدیم که کد شر یک کیوبیت منطقی را در ۹ کیوبیت کد می کند و این بهایی است که باید برای تصحیح تمام خطاها پرداخت. حال سوال این است که آیا نمی توان برای تصحیح همه خطاها بهای کمتری پرداخت؟ آیا ممکن است کدی بسازیم که یک کیوبیت منطقی را در تعداد کمتری کیوبیت فیزیکی کد کند و در نتیجه نرخ بالاتری داشته باشد؟ پاسخ این سوال مثبت است. در این بخش نشان می دهیم که می توان یک کیوبیت منطقی را در ۵ کیوبیت کد کرد و در نتیجه به نرخ $R = \frac{1}{5}$ دست یافت. هم چنین نشان می دهیم که بهتر از این نمی توان عمل کرد و یک کیوبیت را نمی توان در تعداد کمتری کیوبیت کد کرد. برای پاسخ به این سوال بهترین کار استفاده از عملگرهای پایدار کننده است. کد کردن یک کیوبیت در ۵ کیوبیت به این معناست که در فضای ۵ کیوبیتی که دارای بعد $2^5$ است یک زیر فضای $2^1$ را به عنوان فضا ی کد انتخاب می کنیم. بنابراین زیر فضای کد توسط چهار عملگر پایدار می شود. می بایست چهار عملگر پیدا کنیم که روی فضای ۵ کیوبیتی عمل می کنند و




شکل ۱۰: تصویر کلی در کدهای پایدارساز.

همه با هم جابجا می شوند و در عین حال برای تمام خطاهای بیت و فاز برگردان علامت های خطای متمایز دارند. می توانیم این کار را با سعی و خطا انجام دهیم. اما بعضی از اصول راهنما داریم که از همان ابتدا کار ساختن گروه پایدارساز را آسان می کنند. نخست باید بدانیم که کدی که می خواهیم بنویسیم می بایست خطاهای یک کیوبیتی را اصلاح کند. بنابراین هیچکدام از عملگرهای پاوولی که روی یک کیوبیت اثر می کنند مثل $X_1 \cdots X_5, Y_1 \cdots Y_5, Z_1 \cdots Z_5$ نمی بایست در $\mathcal{N}(S)$ وجود داشته باشند. به این ترتیب می توان بلافاصله انتخاب های ساده ای مثل

$$S_1 = \langle X_1, X_2, X_3, X_4 \rangle \quad (۶۹)$$

یا

$$\langle Z_1, Z_2, Z_3, Z_4 \rangle \quad (۷۰)$$

را کنار گذاشت، زیرا در اولی عملگر $X_5$ و در دومی $Z_5$ خطا هستند و قابل شناسایی نیستند. اگر با سعی و خطا پیش برویم به تدریج به مجموعه مولدهایی پیچیده تری می رسیم. یک نمونه می تواند به شکل زیر باشد:

$$
\begin{aligned}
S_1 &= Z\ Z\ X\ X\ X, \\
S_2 &= X\ Z\ Z\ X\ X, \\
S_3 &= X\ X\ Z\ Z\ X, \\
S_4 &= X\ X\ X\ Z\ Z.
\end{aligned} \tag{۷۱}
$$

■ تمرین: الف: نخست خودتان را قانع کنید که همه این عملگرها باهم جابجا می شوند.

ب: زیرفضایی را که توسط این عملگرها پایدار می شود بدست آورید.

پ: جدولی را که نشان دهنده روابط جابجایی عملگرهای خطای بیت و فاز برگردان با عملگر های پایدار کننده فوق است بدست آورید.

ت: با توجه به این جدول بگویید که آیا این کد واقعا می تواند همه خطاها را از هم تمیز دهد؟ کدام خطاها را باهم اشتباه می کند؟

اگر تمرین بالا را به درستی حل کرده باشید متوجه می شوید که کد بالا به یک کد کامل خیلی نزدیک شده است بنابراین می توانیم سعی خود را ادامه بدهیم و اشکالی را که در کد قبلی وجود داشت رفع کنیم. این بار پایدار کننده ها را به طریق زیر در نظر می گیریم:

$$
\begin{aligned}
S_1 &= I\ Z\ X\ X\ Z, \\
S_2 &= Z\ I\ Z\ X\ X, \\
S_3 &= X\ X\ Z\ I\ Z, \\
S_4 &= Z\ X\ X\ Z\ I.
\end{aligned} \tag{۷۲}
$$

■ تمرین: مراحل تمرین قبلی را برای این کد تکرار کنید و نشان دهید که این کد واقعا تمام خطاهای تک کیوبیتی را از هم تمیز داده و آن ها را اصلاح می کند.

## ۶ قدردانی

این درسنامه را آقای حسین محمدی دانشجوی دانشکده فیزیک در آبان ماه ۱۴۰۱ به دقت خوانده و اشکالات متعدد آن را به من یادآوری کردند. برای این لطف بزرگ از ایشان تشکر می کنم.