تصحیح خطای کوانتومی ـ بخش دوم

وحید کریمی پور، دانشکده فیزیک، دانشگاه صنعتی شریف

۲۵ اسفند ۱۴۰۳

۱ مقدمه

می دانیم که هرنوع اطلاعات کلاسیک را می توان به صورت رشته ای از علائم 0 و 1 کُد کرد. این نوع کُد کردن اصطلاحاً کُد کردن منبع یا $Source\ Coding$ نامیده می شود و قبل از ارسال اطلاعات به درون کانال انجام می شود و هدف آن تنها این است که اطلاعاتی که به صورت متن، صدا یا تصویر است به صورت رشته ای از علائم ساده و قابل حمل دربیت های کلاسیک درآید. در کُد کردن منبع مسئله‌ای به نام تصحیح خطا وجود ندارد زیرا هنوز اطلاعات به درون کانال که جایی است که خطاها در آن صورت می گیرد، ارسال نشده‌است. به عنوان مثال فرض کنید که منبع ما تنها از چهار حرف A ، B ، C و D تشکیل شده است. یک راه برای کد کردن منبع آن است که این حروف را به رشته های زیر کُد کنیم:

$$\begin{aligned} A &\longrightarrow 00 \\ B &\longrightarrow 01 \\ C &\longrightarrow 10 \\ D &\longrightarrow 11. \end{aligned} \qquad (۱)$$

در مقصد نیز وقتی که این رشته ها به دست گیرنده می رسد او نیز همین روش را برای گشودن کد به کار می برد که به آن $Source\ Decoding$ می گوییم. در حالت ساده بالا این عمل به صورت زیر انجام می شود:

$$\begin{aligned} 00 &\longrightarrow A \\ 01 &\longrightarrow B \end{aligned}$$

$$10 \longrightarrow C$$
$$11 \longrightarrow D. \qquad (۲)$$

اما وقتی که همین رشته ها را به درون کانال می فرستیم می توانند دچار خطا شوند. به عنوان مثال رشته 01 می تواند دراثر بروز یک خطا در بیت اول تبدیل به 11 شود که در مقصد به صورت حرف D تعبیر خواهد شد. بنابراین برای تصحیح این گونه خطاها که در کانال اتفاق می افتد می بایست در ابتدای کانال یک نوع کد گذاری به کار برد که به آن کدگذاری کانال $ChannelEncoding$ می گوییم . به عنوان مثال یک نوع ساده از کد گذاری کانال آن است که رشته های چهار گانه فوق را به صورت زیر کد کنیم:

$$00 \longrightarrow 0000$$
$$01 \longrightarrow 0101$$
$$10 \longrightarrow 1010$$
$$11 \longrightarrow 1111. \qquad (۳)$$

در گیرنده نیز می بایست این رشته ها را به صورت زیر بگشاییم که به آن $ChannelDecoding$ می گوییم:

$$0000 \longrightarrow 00$$
$$0101 \longrightarrow 01$$
$$1010 \longrightarrow 10$$
$$1111 \longrightarrow 11. \qquad (۴)$$

اینکه چگونه حروف را به صورت رشته های از علایم صفر و یک کد کنیم که هم حداقل بیت ها را به کار ببریم و هم هیچ گونه اطلاعاتی را از دست ندهیم موضوعی است که در فصل های آینده به آن خواهیم پرداخت. در این فصل کار ما این است که تنها امکان بروز خطا و شیوه تصحیح آن را مطالعه کنیم. این که چرا پس از معرفی خطاهای کوانتومی و شیوه تصحیح آنها به بررسی خطاهای کلاسیک و تصحیح خطای کلاسیک می پردازیم، سوالی طبیعی است که ممکن است برای خواننده پیش بیاید. پاسخ اش این است که نظریه کدهای تصحیح خطای کلاسیک به دلیل قدمت آن نظریه ای بسیار غنی است که از جهات گوناگون گسترش یافته است. بخشی از این گسترش با شاخه های کاملا نوینی از ریاضیات نیز تلاقی می کند. علاوه بر این دسته وسیعی از کدهای کوانتومی مبتنی بر ایده هایی هستند که از نظریه کدهای کلاسیک الهام گرفته اند. بعلاوه بر این آشنایی با کدهای کلاسیک ما را با مفاهیم بنیادی ای آشنا می کند که در کدهای کوانتومی نیز معنا و مفهوم دارند. در این درس نخست با مفاهیم پایه در کدهای کلاسیک آشنا می شویم و سپس به کدهای کوانتومی مبتنی بر آنها می پردازیم. با این مقدمه می توانیم تعریف کلی کدهای کلاسیک را ارائه دهیم. قبل از آن می بایست نماد گذاری خود را روشن کنیم.

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

$$Z_2^n := \{x = x_1x_2x_3\cdots x_n, |x_i = 0,1\}. \qquad (۵)$$

دقت کنید که در نوشتن عناصر Z_2^n، نمادِ $x_1x_2x_3\cdots x_n$ را بجای نمادِ $(x_1, x_2, x_3, \cdots x_n)$ به کار برده‌ایم. به هر عضو از Z_2^n یک کلمه [۱] می گوییم. تعداد کلمه های Z_2^n برابر است با 2^n .

این مجموعه در ضمن یک فضای برداری روی میدان Z_2 است، یعنی می توان هر کلمه ای را در صفر یا یک ضرب کرد و می توان هر دو کلمه ای را نیز با هم جمع کرد. بنابراین اگر x و y دو عضو از Z_2^n هستند، آنگاه $x + y$ نیز عضوی از Z_2^n است.

■ تعریف : هرگاه $e \in Z_2^n$ یک کلمه‌ی n بیتی باشد، وزن همینگ آن [۲] برابر است با تعداد ۱ های آن. این وزن را با $w(e)$ نشان می دهیم. بنابراین کلمه $e = 001110$ دارای وزن 3 است، یا $w(e) = 3$.

■ تعریف : هرگاه $x, y \in Z_2^n$ دو کلمه‌ی n بیتی باشند، فاصله همینگ آنها برابر است با تعداد بیت هایی که با یک دیگر تفاوت دارند. به عبارت دیگر $d(x, y) := w(x - y)$. این فاصله با $d(x, y)$ نشان داده می شود و می توان نوشت:

$$d(x, y) = \sum_{i=1}^{n} |x_i - y_i| = \sum_{i=1}^{n} (x_i - y_i)^2. \qquad (۶)$$

براحتی می توان نشان داد که فاصله همینگ تمام خصوصیات فاصله را دارد یعنی:

$$\begin{aligned} &d(x, y) \geq 0 \ , \ \ x = y \longrightarrow d(x, y) = 0 \ , \ \ d(x, y) = 0 \longrightarrow x = y, \\ &d(x, y) = d(y, x) \\ &d(x, y) \leq d(x, z) + d(z, y). \end{aligned} \qquad (۷)$$

فرض کنید که کلمه ای مثل v دچار خطای e شود و تبدیل به کلمه $v' = v + e$ شود. دراین صورت تعداد خطاهای صورت گرفته دراین کلمه برابر است با تعداد 1 های درون e که برابراست با $w(e)$. دقت کنید که به ازای هر 1 در e یک خطا روی v ایجاد می شود. به عنوان مثال هرگاه $e = 00110101$ باشد به این معناست که در مکان های ۳ ، ۴ ، ۶ و ۸ کلمه v دچار خطا شده است.

هرگاه احتمال وقوع یک خطا در یک بیت برابر با p باشد و فرض کنیم که خطاهای بیت های مختلف از هم مستقل هستند آنگاه می توان احتمال وقوع یک خطای e را حساب کرد. این خطا برابراست با

$$P(e) = p^{w(e)}(1 - p)^{n-w(e)} \approx p^{w(e)}. \qquad (۸)$$

[۱] word
[۲] Hamming Weigth

که در تساوی تقریبی آخر از این استفاده کرده‌ایم که p معمولا عدد بسیار کوچکی است.

هرگاه $x \in Z_2^n$ یک کلمه‌ی n بیتی باشد، کره هامینگ به شعاع d به مرکز x شامل تمام نقاطی است که فاصله آنها از x مساوی یا کمتراز d است. این کره را با $B_d(x)$ نشان می دهیم:

$$B_d(x) := \{y \in Z_2^n | d(x,y) \leq d\}. \quad (۹)$$

تعداد اعضای درون این کره یعنی تعداد کلمه هایی که در $1, 2, \cdots$ یا d بیت با x اختلاف دارند. بنابراین تعداد اعضای درون این کره برابر است با:

$$|B_d(x)| = \sum_{i=0}^{d} \begin{pmatrix} n \\ i \end{pmatrix} = 1 + n + \frac{n(n-1)}{2} + \cdots + \begin{pmatrix} n \\ d \end{pmatrix}. \quad (۱۰)$$

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

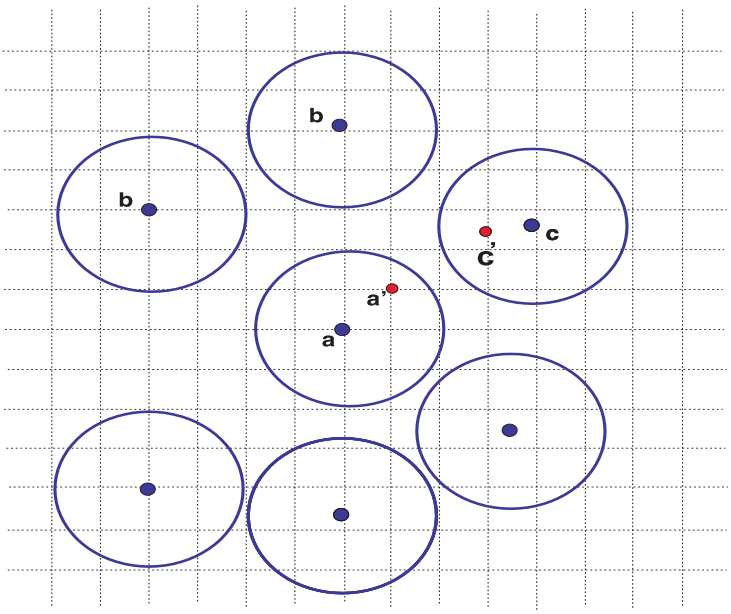
- تعریف : یک کد عبارت است از یک زیر مجموعه از Z_2^n. این زیر مجموعه را با C نشان می دهیم و تعداد اعضای آن را برابر با 2^k می گیریم. به هر عضو C یک کدـ کلمه یا $Codeword$ می گوییم. بنابراین می گوییم که کدـ کلمه های C ، کلمه های k بیتی یا به طور کلی k بیت را کد می کنند، چون تعدادشان برابر با 2^k است.

- تعریف : فاصله یک کدِ C که آن را با $d(C)$ یا d نشان می دهیم برابر است با کمترین فاصله ای که بین کلمات آن وجود دارد. به عبارت دیگر

$$d(C) := min_{x,y \in C} d(x,y). \quad (۱۱)$$

نمادگذاری: کدی را که در فضای Z_2^n نوشته می شود وبرای کد کردن k بیت به کار می رود، و فاصله آن برابر با d است با نمادِ $[n,k,d]$ نشان می دهند.

یک نحوه تصحیح خطاها در یک کد کلاسیک در شکل 1 نشان داده شده است. هرگاه فاصله کد برابر با $d = 2t+1$ باشد، حول هر کدـ کلمه یک کره هامینگ به شعاع t رسم می کنیم. دراین صورت هرگاه نقطه ای دریافت کنیم که متعلق به C نباشد به این معناست که خطایی صورت گرفته است و آن را به صورت کلمه‌ای که نزدیک ترین فاصله را با آن دارد تصحیح می کنیم. به عنوان مثال در شکل 1 کلمه های دریافتی a' و c' متعلق به C نیستند و به کلمه های a و c تصحیح می شوند. به این ترتیب می گوییم که کدی که فاصله آن برابر با $d = 2t+1$ است قادر است که خطاهای با وزن t یا اصطلاحاً t خطا را تصحیح کند.



شکل ۱: نحوه تشخیص و خنثی کردن خطا. اگر کلمه a' را دریافت کنیم آن را به a برمی گردانیم زیرا با احتمال بسیار زیاد این کلمه a بوده است که به a' تبدیل شده است.

■ مثال ۱ : کد زیر را در نظر بگیرید:

$$C = \{000, 111\}. \tag{۱۲}$$

این کد که اصطلاحاً کد تکرار سه تایی نامیده می شود کدی است از نوع $[3, 1, 3]$ و می تواند یک خطا را تشخیص دهد و تصحیح کند.

■ مثال ۲ : کد زیر را در نظر بگیرید:

$$C = \{000000, 101010, 010101, 111111\}. \tag{۱۳}$$

این کد از نوع $[6, 2, 3]$ و می تواند یک خطا را تشخیص دهد و تصحیح کند. می توان این کد را برای کد کردن دو بیت به صورت زیر به کار برد:

$$\begin{aligned} 00 &\longrightarrow 000000 \\ 01 &\longrightarrow 010101 \\ 10 &\longrightarrow 101010 \\ 11 &\longrightarrow 111111. \end{aligned} \tag{۱۴}$$

■ یادآوری: توجه کنید که اگر چه خود مجموعه Z_2^n یک فضای برداری است، اما در حالت کلی یک کد تنها یک زیر مجموعه از این فضاست نه یک زیر فضا. در حالت خاصی که کد یک زیرفضاست اصطلاحا می گوییم که یک کد خطی ساخته ایم. این نوع کدها را در بخش های آینده همین درس مطالعه خواهیم کرد.

---

۲ حدهای حاکم بر کدهای تصحیح کننده خطاهای کلاسیک

برای نوشتن یک کد خوب می بایست بین دو خاصیت متناقض توازن برقرار کنیم. از یک طرف برای آنکه کد خطاهای هرچه بیشتری را تصحیح کند می بایست فاصله آن یعنی پارامتر d بزرگ باشد. به عبارت بهتر می بایست شعاع کره های همینگ ای که در اطراف هر کد کلمه ترسیم می شود زیاد باشد. اما این کار به معنای این است که تعداد کمی کد کلمه را در مجموعه کلمه های n بیتی انتخاب کنیم. به عبارت دیگر نسبت $R := \frac{k}{n}$ که همان نرخ کد است را کم کنیم. بنابراین افزایش فاصله کد با افزایش نرخ کد در تناقض است و یک کد خوب کدی است که این توازن را به بهترین وجهی ایجاد کند. برای این که این محدودیت ها را بفهمیم نخست سعی می کنیم که حد های حاکم بر یک کد دلخواه با مشخاصت $[n, k, d]$ را بفهمیم. این محدودیت ها در سه نامساوی مهم بیان می شوند که در زیر آنها را بیان و ثابت می کنیم. این کد ها را نخست روی بیت ها یعنی کدهایی که روی میدان $Z_2 = \{0, 1\}$ تعریف می شوند مطالعه می کنیم ولی تعمیم آنها به کدهایی که روی الفبای $Z_q = \{0, 1, 2, \cdots q-1\}$ تعریف می شوند نیز سرراست است.

۱.۲ حد همینگ

این حد نخستین بار توسط ریچارد همینگ [۳] مهندس آمریکایی معرفی شده است.

■ قضیه: در هر کد $[n, k, d]$ که روی Z_2 تعریف می شود، نامساوی زیر برقرار است که در آن $d = 2t + 1$:

$$2^k \leq \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}} \qquad (۱۵)$$

■ اثبات: به دور هر کد کلمه یک کره به شعاع t رسم می کنیم. از آنجا که فاصله کد برابراست با $2t+1$ این کره ها با یکدیگر هیچ اشتراکی ندارند. بنابراین اگر تعداد نقاط درون هر کره را حساب کنیم و در تعداد کره ها ضرب کنیم عدد حاصل می بایست از تعداد کل نقاط کمتر

[۳] Richard Hamming

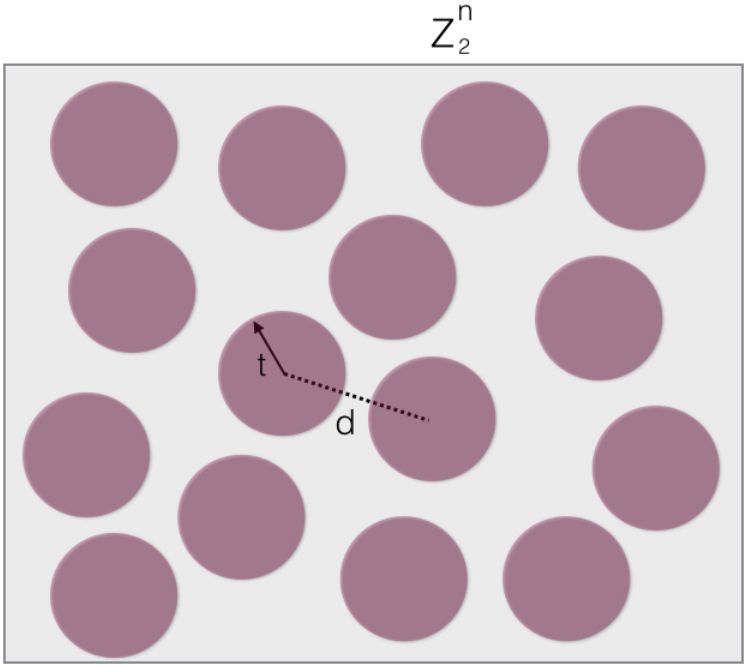
باشد. می دانیم که تعداد کل نقاط برابر است با 2^n. تعداد کل کد کلمه ها برابراست با 2^k . تعداد نقاط درون هر کره به شعاع t را با N_t نشان می دهیم. بنابراین نامساوی همینگ بیان می کند که شرط زیر می بایست برقرار باشد:

$$2^k N_t \leq 2^n. \tag{۱۶}$$

پس کافی است که N_t را محاسبه کنیم. اما محاسبه N_t راحت است و قبلا آن را محاسبه کرده ایم. در واقع :

$$N_t := \sum_{i=0}^{t} \begin{pmatrix} n \\ i \end{pmatrix} \tag{۱۷}$$

زیرا تعداد نقاطی که فاصله آنها برابر با i است برابر با تعداد کلماتی است که دقیقا در i نقطه از n نقطه با کلمه مرکزی تفاوت دارند. با ترکیب این رابطه با رابطه قبلی به حد همینگ می رسیم.



شکل ۲: روش بدست آوردن حد همینگ: برای تصحیح t خطا کره های با شعاع t نمی بایست با یکدیگر تلاقی کنند. فاصله کد برابر است با $d = 2t + 1$. برای توضیح بیشتر به متن مراجعه کنید.

۲.۲ حد گلیبرت ـ وارشاموف

حد همینگ نشان داد که تا چه اندازه می توانیم در فضای Z_2^n کد کلمه ها را بچپانیم. این حد نشان می داد که اگر بخواهیم فاصله کدکلمه ها از یک دیگر زیاد باشد یک حد بالا برای چپاندن این کلمه ها (یا به عبارت بهتر) کره های اطراف انها در فضای Z_2^n وجود دارد. ما همیشه می بایست این حد را رعایت کنیم. مسلم است که با قرار دادن تعداد کمی کره در فضای Z_2^n حد همینگ را رعایت کرده ایم. اما از کجا می توانیم مطمئن باشیم که به صورت بهینه عمل کرده ایم؟ ملاک بهینه بودن یک کد توسط یک نامساوی داده می شود که به آن حد گیلبرت_وارشاموف [۴] می گوییم.

- قضیه: یک کد $[n, k, d]$ که روی Z_2 تعریف می شود، وقتی بهینه است که نامساوی زیر برقرار باشد :

$$2^n \leq 2^k \times \sum_{i=0}^{d-1} \begin{pmatrix} n \\ i \end{pmatrix}. \qquad (۱۸)$$

به عبارت بهتر هر گاه که این نامساوی نقض شود به این این معناست که ما هنوز می توانیم کدکلمه های دیگری را در فضای Z_2^n قرار دهیم و کد بهتری با نرخ بیشتری بدست بیاوریم. این کار را می توانیم تا آنجا ادامه دهیم تا این نامساوی نقض شود.

- اثبات: فرض کنید که n مقدار معینی دارد. می دانیم که برای اینکه یک کد خوب بنویسیم یعنی کدی که فاصله اش زیاد باشد، می بایست تعداد کد کلمه ها را پایین بیاوریم زیرا می خواهیم فاصله کدکلمه ها از هم زیاد باشد. این همان حدی است که توسط نامسای همینگ داده می شود که بر مبنای آن k نمی بایست از یک حدی بیشتر باشد. اما ما نمی خواهیم که k را خیلی کم بگیریم زیرا در این صورت نرخ کد یعنی $R = \frac{k}{n}$ پایین می آید . برای آنکه یک کد بهینه داشته باشیم می بایست به اندازه کافی کد کلمه در فضای Z_2^n اختیار کنیم و فضای خالی بیهوده ای در آن به جای نگذاریم. این حد توسط گیلبرت ـ وارشاموف [۵] داده می شود. از برهان خلف استفاده می کنیم یعنی فرض می کنیم که این نامساوی نقض شود و داشته باشیم

$$\sum_{i=0}^{d-1} \begin{pmatrix} n \\ i \end{pmatrix} \times 2^k < 2^n. \qquad (۱۹)$$

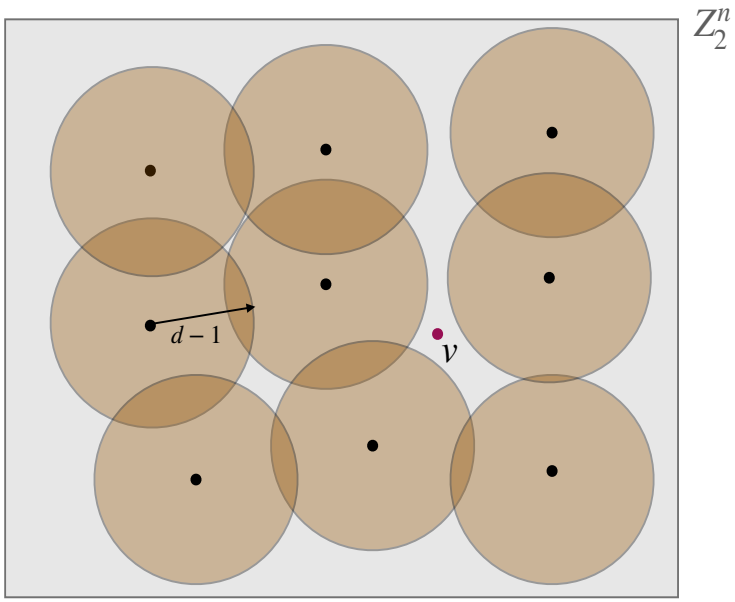
معنای این رابطه این است که کره هایی دور هر کد کلمه به شعاع $d-1$ کشیده شده و مجموع تمام نقاط درون این کره ها بازهم از تمام نقاط درون Z_2^n کمتر است. (دقت کنید که از آنجا که فاصله کد برابر با d است معلوم است که خیلی از کره ها با هم تلاقی پیدا می کنند.) اما از آنجا که بنابر فرض برهان خلف ، کلمه هایی وجود دارند که در درون هیچ کدام از کره ها جای نمی گیرند، پس نتیجه می گیریم که کلمه ای می توان یافت که فاصله اش از همه کلمات دیگر از $d-1$ بیشتر است یا اینکه کلمه ای وجود دارد که فاصله اش از همه کلمات دیگر بزرگتر یا مساوی با d است. پس این کلمه را نیز می توان به کد اضافه کرد بدون اینکه فاصله کد کم شود. یعنی کدی که نامساوی گیلبرت ـ وارشاموف را نقض کند نمی تواند یک کد بهینه باشد. به بیان دیگر ما همواره می توانیم آنقدر کلمه به کد اضافه کنیم تا جایی که این نامساوی نقض شود. [۶]

---

[۴] Gilbert-Varshamov

[۵] Gilbert-Varshamov

[۶] این بیان از حد گیلبرت ـ وارشاموف را مرهون یک بحث با خانم دکتر آسوده هستم.



شکل ۳: روش بدست آوردن حد گیلبرت_وارماشوف با برهان خلف. اگر حد گیلبرت_وارماشوف نقض شود، به این معناست که می توان نقطه ای یا کلمه ای (که با رنگ قرمز مشخص شده) پیدا کرد که فاصله اش با بقیه کلمه های کد C حداقل برابر باچd باشد. در نتیجه می توان این کلمه را هم به کد C اضافه کرد و کد بهتری بدست آورد.

۳.۲ حد منفرد

- قضیه: در هر کد $[n, k, d]$ نامساوی زیر برقرار است:

$$k \leq n - d + 1. \qquad (۲۰)$$

این نامساوی که به حد منفرد [۷] مشهور است به سادگی قید روی فاصله، و نرخ کد را مشخص می کند. با وجود اینکه صورت این نامساوی خیلی ساده است ولی اثبات آن نسبت به نامساوی های قبلی احتیاج به فکر و دقت بیشتری دارد.

- اثبات: یک کد کلمه دلخواه مثل $w = (s_1, s_2, \cdots s_{d-1}, s_d, s_{d+1}, \cdots s_n)$ را در نظر بگیرید. تعداد این کد کلمه ها برابر است با 2^k . همه کد کلمه ها چنین ساختاری دارند و فاصله هر دوتای آنها از d بیشتر یا مساوی با آن است. به بیان دیگر هر دو کد کلمه در بیشتر یا مساوی با d حرف با هم تفاوت دارند. پس اگر $d-1$ تا حرف اول را نیز از همه کدکلمه ها پاک کنیم بازهم کد کلمه ها ی جدید برهم منطبق نمی شوند چون که حداقل در یک حرف با هم متفاوت هستند. کلمه های جدید تعداد $n-d+1$ بیت دارند، زیرا $d-1$

[۷] Singleton Bound

تا از بیت های آنها حذف شده است. بنابراین ما تنها با استفاده کردن از $n-d+1$ بیت توانسته ایم 2^k کلمه متفاوت درست کنیم. پس معنایش این است که شرط

$$2^k \leq 2^{n-d+1}$$

برقرار است که چیزی نیست جز همان حد منفرد. به این ترتیب اثبات این حد نیز کامل می شود.

■ مثال : کد زیر را در نظر بگیرید:

$$C = \{000, 011, 101, 110\}. \qquad (۲۱)$$

در این کد بیت سوم که به بیت پاریته موسوم است پاریته دو بیت اول را تعیین می کند به این معنا که اگر مجموع این دو بیت برابر با صفر باشد مقدار این بیت برابر با صفر و درغیر این صورت مقدار آن برابر با ۱ است. به عبارت دیگر در هر کلمه این کد داریم $x_3 = x_1 + x_2$. با این حساب خواهیم داشت $x_1 + x_2 + x_3 = 0$، یعنی پاریته مجموع سه عدد برابر با صفر خواهد بود. به این تر تیب این کد می تواند یک خطا را آشکار کند، زیرا وقوع یک خطا پاریته کلمه را تغییر خواهد داد. اما این کد تنها می تواند این خطا را آشکار کند و قادر به تصحیح آن نیست . مثلاً معلوم نیست که کلمه دریافتی 111 کدام یک از سه کلمه ارسالی $110, 101, 011$ بوده است که دچار خطا شده است. کمی دقت نشان می دهد که فاصله این کد برابراست با 2 و به همین دلیل است که نمی تواند تشخیص دهد که یک کلمه معیوب ناشی از ایجاد خطا بر روی کدام کلمه کد بوده است زیرا کره های همینگ به شعاع یک برای سه کلمه فوق همگی نقطه‌ی 111 را در بردارند.

■ **مثال:** کد زیر را در نظر بگیرید:

$$C = \{00000, 01011, 01110, 10011, 10110, 11000, 11101\}$$

این کد از نوع $[6, 2, 3]$ و می تواند یک خطا را تشخیص دهد و تصحیح کند. می توان این کد را برای کد کردن دو بیت به کار برد:

$$\begin{aligned} 00 &\longrightarrow 000000 \\ 01 &\longrightarrow 010101 \\ 10 &\longrightarrow 101010 \\ 11 &\longrightarrow 111111. \end{aligned} \qquad (۲۲)$$

احتمالاً اگر سعی کرده باشید که کدی از نوع $[5, 2, 3]$ نویسید متوجه شده‌اید که نوشتن کد ها چندان آسان نیست و قاعده‌ی سرراستی برای ساختن آنها وجود ندارد. کدهای خطی [۸] دسته‌ای از کد ها هستند که خواص بسیار ساده و جالبی دارند و راه و روشی سیستماتیک برای نوشتن کد ها بدست می دهند. در بخش بعدی این کد ها را معرفی می کنیم.

[۸] Linear codes

۳ کد های خطی

می دانیم که مجموعه Z_2^n یک ساختار خطی دارد و می توان آن را به عنوان یک فضای برداری روی میدان Z_2 در نظر گرفت. هرگاه $\mathbf{x} = x_1x_2\cdots x_n \in Z_2^n$ و $\mathbf{y} = y_1y_2\cdots y_n \in Z_2^n$ آنگاه جمع این دو بردار به شکل زیر تعریف می شود

$$\mathbf{x} + \mathbf{y} = z_1z_2\cdots z_n, \qquad (۲۳)$$

که درآن

$$z_i = x_i + y_i \qquad mod\ 2.$$

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

$$\langle \mathbf{x} \cdot \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i, \qquad (۲۴)$$

که در آن جمع به پیمانه ۲ حساب می شود. تعداد عناصر این فضای خطی محدود و برابر با 2^n است.

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

- تعریف : در فضای خطی Z_2^n یک کد خطی چیزی نیست جز یک زیر فضای C از Z_2^n. خاصیت مهم کدهای خطی این است که اگر $(x_1, x_2, \cdots x_n)$ و $(y_1, y_2, \cdots y_n)$ دو کد_کلمه باشند، آنگاه مجموع آنها یعنی $(x_1 + y_1, x_2 + y_2, \cdots x_n + y_n)$ نیز یک کد_کلمه است. هرگاه این زیر فضا یعنی C k بعدی باشد آن را به شکل زیر برای کد کردن k بیت به کار می بریم. چون کد خطی است طبیعی است که همه کد_کلمه ها را بر حسب بردارهای پایه فضای کد بنویسیم. فرض کنید که $B = \{\mathbf{g}_1, \mathbf{g}_2, \cdots \mathbf{g}_k\}$ یک پایه برای C و $\alpha = \alpha_1\alpha_2\cdots\alpha_k \in Z_2^k$ یک کلمه k بیتی باشد. دراین صورت این کلمه را به صورت زیر در n بیت کد می کنیم:

$$\alpha \longrightarrow \mathbf{g}(\alpha) = \alpha_1\mathbf{g}_1 + \alpha_2\mathbf{g}_2 + \cdots \alpha_k\mathbf{g}_k. \qquad (۲۵)$$

در چنین مواردی می نویسیم

$$C = \langle \mathbf{g}_1, \mathbf{g}_2, \cdots \mathbf{g}_k \rangle. \qquad (۲۶)$$

بنابراین فضای کدِ خطی دارای بعدِ k است و دارای 2^k عضو متفاوت است.

دقت کنید که بردارهای $\{\mathbf{g}_1,\ \mathbf{g}_2, \cdots \mathbf{g}_k\}$ می بایست مستقل خطی باشند که با توجه به اینکه میدان این فضای برداری $Z_2 = \{0, 1\}$ است، به این معناست که مجموع آنها برابر با صفر نیست. بنابراین برای کد $C = \{0000, 1100, 0011, 1111\}$ نمی توان نوشت: $C = \langle 1100, 0011, 1111\rangle$ زیرا مجموع سه بردار بالا صفر است و مستقل نیستند، بلکه باید نوشت: $C = \langle 1100, 0011\rangle$

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

$$\alpha \longrightarrow \mathbf{g}(\alpha) = \alpha_1(00111) + \alpha_2(11000) + \alpha_3(10001) = (\alpha_2 + \alpha_3, \alpha_2, \alpha_1, \alpha_1, \alpha_1 + \alpha_3). \qquad (۲۷)$$

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

$$\begin{aligned}
000 &\longrightarrow 00000\\
001 &\longrightarrow 10001\\
010 &\longrightarrow 11000\\
011 &\longrightarrow 01001\\
100 &\longrightarrow 00111\\
101 &\longrightarrow 10110\\
110 &\longrightarrow 11111\\
111 &\longrightarrow 01110.
\end{aligned} \qquad (۲۸)$$

نوشتن کدهای خطی بسیار آسان است، کافی است که مجموعه‌ای از بردارهای مستقل از فضای Z_2^n در نظر گرفت و کلمات را به صورت ترکیب های خطی انها کد کرد. اما معلوم نیست که انتخاب ما انتخاب خوبی باشد یعنی این کد بتواند خطاها را تصحیح کند. بنابراین سوالی که با آن مواجه هستیم آن است که چگونه می توان خواص کد های خطی نظیر فاصله را تعیین کرد و این که آیا راه ساده‌ای برای تشخیص و تصحیح خطاها توسط این کدها وجود دارد یا نه؟ در واقع بااستفاده از ساختار خطی کد می بایست بتوانیم برای این سوال ها پاسخ های روشنی بیابیم. برای پاسخ به این سوال ها می بایست ساختار کد های خطی را بهتر بشناسیم. این کاری است که در زیر بخش بعدی انجام می دهیم.

۴ ساختار کد های خطی

فرض کنید که یک کد خطی با پایه $B_C = \{\mathbf{g}_1, \mathbf{g}_2, \cdots \mathbf{g}_k\}$ تعریف شده باشد. دراین صورت هر کلمه‌ی α به صورت $\mathbf{g}(\alpha)$ کد می شود که درآن

$$\mathbf{g}(\alpha) = \alpha_1\mathbf{g}_1 + \alpha_2\mathbf{g}_2 + \cdots \alpha_k\mathbf{g}_k = (\alpha_1, \alpha_2, \cdots \alpha_k) \begin{pmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \cdots \\ \mathbf{g}_k \end{pmatrix}. \quad (۲۹)$$

با تعریف ماتریس

$$G = \begin{pmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \cdots \\ \mathbf{g}_k \end{pmatrix} \quad (۳۰)$$

که بعدِ $k \times n$ دارد می توانیم رابطه بالا را به شکل فشرده زیر بنویسیم:

$$\mathbf{w}(\alpha) = \alpha G. \quad (۳۱)$$

دقت کنید که ماتریس G یک ماتریس با رتبه‌ی k است زیرا همه سطرهای آن مستقل خطی اند. ماتریس G ماتریس مولد [۹] نام دارد.

مثال: کد خطی C با پایه $B_C = \{1000, 1010, 0101\}$ دارای عناصر زیر است:

$$\{0000, 1000, 1010, 0101, 0010, 1101, 1111, 0111\}. \quad (۳۲)$$

ماتریس مولد این کد عبارت است از:

$$G = \begin{pmatrix} 1000 \\ 1010 \\ 0101 \end{pmatrix}. \quad (۳۳)$$

می دانیم که یک کد خطی C با یک زیر فضا در فضای برداری Z_2^n مشخص می شود، شکل 4. این کد برای نوشتن سه بیت در ۴ بیت به کار می رود. هر کلمه سه بیتی مثل $\alpha = \alpha_1\alpha_2\alpha_3$ به صورت زیر به یک کلمه چهاربیتی کد می شود:

[۹] Generator Matrix

$$\alpha \longrightarrow \mathbf{w}(\alpha) = (\alpha_1, \alpha_2, \alpha_3) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 + \alpha_2 & \alpha_3 & \alpha_2 & a_3 \end{pmatrix} \quad (۳۴)$$

ماتریس مولد یک ماتریس $k \times n$ است که سطرهایش از هم مستقل است یعنی ماتریس است با رتبه k.

فعلا از خطا و چگونگی تصحیح آن صرف نظر می کنیم و از خود می پرسیم که چگونه می بایست کلمه های اصلی را از کلمه های کدشده بازیابی کنیم. پاسخ این سوال ساده است. برای این کار کافی است که بردارهایی مثل

$$\{\mathbf{h}_1, \mathbf{h}_2, \cdots \mathbf{h}_{n-k}\} \quad (۳۵)$$

پیدا کنیم که دارای خاصیت زیر باشند:

$$\langle \mathbf{g}_i, \mathbf{h}_j \rangle = 0. \quad (۳۶)$$

این بردارها، بردارهای پایه فضای عمود بر فضای کد هستند. تعداد آنها نیز برابر است با $n-k$. می توانیم آنها را در سطرهای یک ماتریس مرتب کنیم و بنویسیم:

$$H = \begin{pmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \cdots \\ \mathbf{h}_{n-k} \end{pmatrix}. \quad (۳۷)$$

دراین صورت خواهیم داشت:

$$GH^T = 0. \quad (۳۸)$$

در اینجا با سوالات ساده ای مواجه می شویم: با در دست داشتن ماتریس G :

- چگونه خطاها را تشخیص می دهیم؟
- چگونه خطاها را تصحیح می کنیم؟
- فاصله کد را چگونه تعیین می کنیم؟

برای پاسخ به سوال اول می بایست روشی بیابیم که به کمک آن تشخیص دهیم آیا یک بردار از فضای کد خارج شده است یا نه؟ اگر به شکل 4 نگاه کنیم می توانیم یک راه ساده برای آن پیدا کنیم. می توان از یک نشانه خیلی ساده برای این کار استفاده کرد. این نشانه ساده ماتریس

چک‌ـپاریته [۱۰] خوانده می شود. مجموعه بردارهای عمود بر C را در نظر بگیریم و آن را با $C^{\perp}$ نشان می دهیم. یک پایه برای این فضا در نظر می گیریم. این پایه از $n-k$ بردار مستقل تشکیل شده است:

$$B_{C^{\perp}} = \{\mathbf{h}_1,\ \mathbf{h}_2,\ \cdots \mathbf{h}_{n-k}\}. \tag{۳۹}$$

این بردارها را در یک ماتریس H به صورت زیر می نویسیم:

$$H = \begin{pmatrix} \mathbf{h}_1 \\ \mathbf{h}_2, \\ \cdots \\ \mathbf{h}_{n-k} \end{pmatrix}_{n-k\times n} . \tag{۴۰}$$

به عبارت دیگر ماتریس H مولد زیر فضای $C^{\perp}$ است. از آنجا که همه بردارهای متعلق به C به صورت $\mathbf{v}(\alpha) = \alpha G$ هستند، نتیجه می گیریم که هر بردار متعلق به فضای C در رابطه $\mathbf{v}H^T = 0$ صدق می کند. حال اگر بردار $\mathbf{v}$ دچار خطا شود و تبدیل به برداری مثل $\mathbf{v}' = \mathbf{v} + \mathbf{e}$ شود، خواهیم داشت:

$$\mathbf{v}'H^T = (\mathbf{v} + \mathbf{e})H^T = \mathbf{e}H^T \neq 0. \tag{۴۱}$$

بنابراین صفر نشدن $\mathbf{v}'H^T$ به معنای آن است که بردارِ $\mathbf{v}'$ یک بردار متعلق به کد نیست و حتماً خطایی اتفاق افتاده است. ولی چگونه می توانیم نوع خطا را بفهمیم و در جهت تصحیح آن اقدام کنیم.

نکته‌ای که وجود دارد آن است که یک بردار معیوب مثل $\mathbf{v}'$ ممکن است به طرق مختلفی تولید شده باشد، بعنوان مثال این بردار حاصل خطای $\mathbf{e}_1$ بر بردار $\mathbf{v}_1$ یا خطای $\mathbf{e}_2$ بر بردار $\mathbf{v}_2$ باشد به نحوی که

$$\mathbf{v}_1 + \mathbf{e}_1 = \mathbf{v}_2 + \mathbf{e}_2 = \mathbf{v}'. \tag{۴۲}$$

از میان خطاهای ممکن می بایست محتمل ترین خطا یعنی خطای با کمترین وزن هامینگ در نظر گرفت و فرض کرد که $\mathbf{v} = \mathbf{v}_0 + \mathbf{e}_0$ که در آن $\mathbf{e}_0$ کمترین وزن ممکن را دارد و درنتیجه می بایست $\mathbf{v}$ را به شکل زیر تصحیح کرد:

$$\mathbf{v} \longrightarrow \mathbf{v} + \mathbf{e}_0 = \mathbf{v}_0. \tag{۴۳}$$

می توان مطالب بالا را به زبان دقیق و ریاضی نیز بیان کرد. اگر به شکل 4 نگاه کنیم متوجه می شویم که C یعنی خود کُد، یک زیر فضاست و بقیه صفحات در واقع یکسان با C هستند ولی زیر فضا نیستند زیرا شامل بردار 0 نیستند. برای پیشتر رفتن به تعاریف زیر احتیاج داریم.

---

[۱۰] Parity Check Matrix

■ تعریف : فرض کنید که V یک فضای برداری و C یک زیر فضای آن باشد. دراین صورت هردو بردار $\mathbf{v}_1, \mathbf{v}_2 \in V$ را هم ارز می گوییم هرگاه رابطه زیر برقرارباشد:

$$\mathbf{v}_1 - \mathbf{v}_2 \in C. \tag{۴۴}$$

خواننده براحتی می تواند ثابت کند که این رابطه یک رابطه هم ارزی است و بنابراین فضای V (دراینجا Z_2^n) توسط زیرفضای C (که دراینجا همان فضای کد-کلمه‌هاست) به زیرمجموعه هایی که عناصر آنها بایکدیگر هم ارز هستند افراز می شود [۱۱]:

هر کلاسِ هم ارز یک $Coset$ نامیده می شود. اگر به شکل 4 نگاه کنیم متوجه می شویم که از نظر هندسی هر هم مجموعه یک صفحه موازی با صفحه‌ی C است.

باید دقت کنیم که شکل 4 تنها تا حدودی به درک شهودی ما کمک می کند و از بعضی جهات می تواند گمراه کننده باشد، زیرا ما دراینجا با یک فضای برداری روی میدان $Z_2 = \{0, 1\}$ سروکار داریم نه یک فضای برداری حقیقی. به همین دلیل تعداد بردارهای کل فضا و هم چنین زیرفضای C و تمام کلاس های هم ارزی محدود است. فرض کنید که بردارهای فضای کد یعنی C را به صورت زیر نمایش دهیم:

$$C = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \cdots \mathbf{v}_K\} \tag{۴۵}$$

که درآن $K = 2^k$ (زیرا فرض کرده ایم که C یک فضای k بعدی است.). دراین صورت به ازای هر برداری مثل $\mathbf{e}_i$ که متعلق به C نباشد یک کلاس هم ارزی داریم که برابر است با:

$$[\mathbf{e}_i] \equiv \mathbf{e}_i + C = \{\mathbf{v}_1 + \mathbf{e}_i, \mathbf{v}_2 + \mathbf{e}_i, \mathbf{v}_3 + \mathbf{e}_i, \cdots \mathbf{v}_K + \mathbf{e}_i\}. \tag{۴۶}$$

به دو نکته باید دقت کرد:

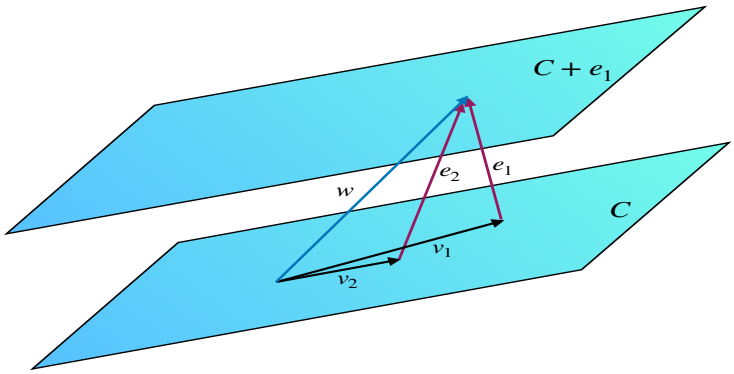
■ **نکته اول :**

برای تمام عناصر یک کلاس اثر H یکسان است، و برابر است با $\mathbf{e}_i H$. بنابراین تمام این کد-کلمه ها یک نشانه خطا دارند. با دریافت این کلمه ها بلافاصله می فهمیم که اشتباهی رخ داده است. البته این اشتباه می توانسته از راه های مختلفی رخ داده باشد. به طور قاطع نمی توانیم بگوییم که کدام خطا رخ داده است. تنها می توانیم بگوییم که محتمل ترین خطا یعنی خطایی با کمترین وزن هامینگ رخ داده و آن خطا را تصحیح کنیم.

بنابراین اثر H روی یک کد دریافتی تنها به کلاس هم ارزی بستگی دارد و می توان آن را به عنوان شناسنده کلاس هم ارزی یا نشانه خطا[۱۲] بکار برد.

[۱۱] از آنجا که در فضای برداری Z_2^n همه جمع ها به پیمانه 2 انجام می شود، $\mathbf{v}_1 - \mathbf{v}_2$ با $\mathbf{v}_1 + \mathbf{v}_2$ یکی است.

[۱۲] Error Syndrome



شکل ۴: وقتی که کلمه ای مثل $\mathbf{v}'$ یافته می شود می تواند ناشی از خطای $\mathbf{e}_1$ بر کلمه ی $\mathbf{v}_1$ یا ناشی از خطای $\mathbf{e}_2$ بر کلمه $\mathbf{v}_2$ باشد. فرض می کنیم که خطای با کمترین وزن یا کمترین طول همینگ یعنی $\mathbf{e}$ رخ داده است و آن را تصحیح می کنیم.

■ **نکته دوم :**

یک کلاس هم ارزی مثل کلاس 46 را می توان به صورت کلاس $[\mathbf{e}_i + \mathbf{v}_1]$ یا کلاس $[\mathbf{e}_i + \mathbf{v}_2]$ یا کلاس $[\mathbf{e}_i + \mathbf{v}_K]$ نیز نامید و در وهله اول هیچ ترجیحی در نامگذاری یک کلاس به یکی از این صورت ها نیست. از این به بعد نماینده کلاس را برداری می گیریم که کمترین وزن هامینگ را دارد. بنابراین وقتی می گوییم کلاس $[\mathbf{e}_i]$ یعنی بردار $\mathbf{e}_i$ دراین کلاس کمترین وزن هامینگ را دارد.

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

نحوه تصحیح خطا: هر بردار $\mathbf{w}$ که دریافت می شود، $\mathbf{w}H^T$ برای آن محاسبه می شود. اگر $\mathbf{w}H^T \neq 0$ می فهمیم که خطایی صورت گرفته است. مقدار $\mathbf{w}H$ در واقع نشانه خطاست و برای ما کلاس هم ارزی $[\mathbf{e}_1]$ را تعیین می کند، شکل (۴). دراین کلاس $\mathbf{e}_1$ کمترین وزن هامینگ را دارد و بنابراین محتمل ترین خطا همان $\mathbf{e}_1$ است . بنابراین کلمه دریافتی $\mathbf{w}$ را به صورت $\mathbf{w} \longrightarrow \mathbf{w}+\mathbf{e}_1 = \mathbf{v}_1$ تصحیح می کنیم.

■ **خطاهایی که قابل تصحیح نیستند:** ممکن است خطایی که رخ می دهد یک بردار درون صفحه C را به برداری در همان صفحه ببرد. در این صورت چنین خطاهایی هیچ نشانه ای ندارند و قابل تصحیح نیستند. این نوع خطاها یک کد کلمه را به یک کلمه دیگر تبدیل می کنند.

۱.۴ خواص بیشتری از کد های خطی

تا کنون خواص کد های خطی را بیان کرده ایم ولی هنوز نمی دانیم که چطور یک کد خطی را با خواص معین مثلا فاصله مشخص بسازیم. در این بخش این کار را انجام می دهیم. البته باید توجه کنیم که ساختن کد های خطی خوب، یعنی کدهایی که فاصله زیاد و در عین حال نرخ زیاد داشته باشند، یک کار آسان و بدیهی نیست. یک قضیه مهم به ما کمک می کند که فاصله کد را که یک پارامتر مهم از کد است ، را از روی ماتریس H تعیین کنیم.

۲.۴ فاصله در کدهای خطی

قضیه: هرگاه که هر $d-1$ ستون ماتریس H از هم مستقل خطی باشند، آنگاه فاصله کد برابر است با d.

قبل از اثبات این قضیه بیایید اول نتایج آن را بفهمیم. فرض کنید که می خواهیم کدی بسازیم که یک خطا را آشکار و تصحیح کند. بنابراین فاصله این کد می بایست برابر با 3 باشد. بنابراین قضیه می بایست هر دو ستون ماتریس H از هم مستقل باشند. در فضای برداری ای که روی میدان Z_2 نوشته می شود، دو بردار وقتی مستقل خطی هستند که باهم یکی نباشند. (دقت کنید که این خاصیت فقط برای این نوع فضای برداری درست است.) بنابراین مسئله ما تبدیل می شود به ساختن ماتریسی با ابعاد $n-k \times n$ که هر دوستون اش با هم متفاوت باشند. یک کد خوب می بایست نرخ بالایی نیز داشته باشد به این معنا که k به n نزدیک باشد. بنابراین تعداد سطر های این ماتریس در مقایسه با ستون های آن می بایست هرچه کمتر باشد. این امر به این معناست که می خواهیم تعداد زیادی بردار با مولفه های کم داشته باشیم که همه از هم مستقل باشند و همین تقاضاست که کار ساختن یک کد خوب را دشوار و در عین حال جذاب می کند.

■ مثال:

کد هامینگ را در نظر بگیرید که با ماتریس زیر ساخته می شود:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (۴۷)$$

براحتی معلوم می شود که در این ماتریس هر دو ستونی مستقل خطی اند. علاوه بر این می توان سه ستون یافت که وابسته خطی باشند مثل ستون های ۳، ۴ و ۷. بنابراین فاصله این کد برابر است با 3. در نتیجه این کد با نماد $[7,4,3]$ نمایش داده می شود و دارای نرخ $R = \frac{4}{7}$ است. حال به اثبات قضیه ای که بیان کردیم می پردازیم.

■ **اثبات:** ایده اصلی را می توانیم با یک مثال توضیح دهیم بدون اینکه از کلیت مسئله کم کنیم. شرط $\mathbf{v}H^T = 0$ را به صورت $H\mathbf{v}^T = 0$

می نویسیم. حال فرض کنید که ماتریس H به صورت زیر باشد:

$$H = \begin{pmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \end{pmatrix} \tag{۴۸}$$

بنابراین شرط $H\mathbf{v}^T = 0$ به شکل زیر است:

$$H\mathbf{v}^T = \begin{pmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} h_{11}v_1 + h_{12}v_2 + h_{13}v_3 \\ h_{21}v_1 + h_{22}v_2 + h_{23}v_3 \end{pmatrix} \tag{۴۹}$$

صفر بودن این ماتریس به این معناست که:

$$v_1 \begin{pmatrix} h_{11} \\ h_{21} \end{pmatrix} + v_2 \begin{pmatrix} h_{12} \\ h_{22} \end{pmatrix} + v_3 \begin{pmatrix} h_{13} \\ h_{23} \end{pmatrix} = 0 \tag{۵۰}$$

بردارهای قید شده در معادله بالا همان ستون های ماتریس H هستند. بنابراین در حالت کلی این رابطه به شکل زیر است:

$$v_1\mathbf{h}_1 + v_2\mathbf{h}_2 + v_3\mathbf{h}_3 + \cdots + v_n\mathbf{h}_n = 0 \tag{۵۱}$$

که در آن $\mathbf{h}_i$ ها ستون های ماتریس H هستند. بنابرتعریف فاصله یک کُد کمترین مقدار فاصله همینگ بین کلمات آن است. در یک کد خطی فاصله برابر می شود با کمترین وزن همینگ برای بردارهای ناصفر در آن کد. در نتیجه هر برداری که از فضای کد در رابطه بالا قرار دهیم حتما تعداد مساوی یا بیشتری از d مولفه برابر با ۱ دارد. یعنی هر d تا ستون ماتریس H به هم وابسته خطی هستند. به همین ترتیب اگر هر $d-1$ تا ستون H از هم مستقل باشند یعنی هیچ کلمه ای با وزن $d-1$ در کد وجود ندارد و در نتیجه کمترین فاصله کد برابر است با d.

به این ترتیب یاد می گیریم که برای ساختن یک کد با مشخصات معین چه مسیری را باید به صورت سیستماتیک طی کنیم. فرض کنید که می خواهیم کدی بسازیم با فاصله 3 که طبیعتا یک خطا را آشکار و تصحیح کند. هم چنین می خواهیم یک بیت را کد کنیم. این به معنای این است که کد ما دارای مشخصات $[n, 1, 3]$ است. می خواهیم ببینیم با این فاصله یک بیت را می بایست حداقل در چند بیت کد کنیم. چون که $k = 1$ است پس می بایست ماتریس H بعد $n-1 \times n$ داشته باشد. از آنجا که فاصله کد برابر با $d = 3$ است، پس $d - 1 = 2$ است، یعنی هر دو ستون ماتریس H می بایست از هم مستقل یا در واقع با هم متفاوت باشند. پس مسئله ما ساختن ماتریسی $n-1 \times n$ است که هر دو ستون آن با هم مساوی باشند. با کمی فکر معلوم می شود که کمترین مقدار n برابر با 3 است و ماتریس H نیز برابر است با:

$$H = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}. \tag{۵۲}$$

در نتیجه ماتریس G یک ماتریس 1×3 است که می بایست در شرط GH^T صدق کند که تنها جواب اش این است که:

$$G = (1, 1, 1). \tag{۵۳}$$

به این ترتیب هر بیت مثل α در یک سه تایی کد می شود:

$$\alpha \longrightarrow a(1,1,1) = (\alpha, \alpha, \alpha). \qquad (۵۴)$$

حال اگر بخواهیم دو بیت را در چند بیت کد کنیم که همان فاصله $d = 3$ را داشته باشد باید ماتریس $H_{n-2\times n}$ را چنان پیدا کنیم که هر دو ستون آن از هم مستقل باشند.

۳.۴ دوگان یک کد

یک کد C دارای ماتریس مولد G و ماتریس چک‌ـپاریته H است که در شرط زیر صدق می کنند:

$$GH^T = 0. \qquad (۵۵)$$

بنابراین می نویسیم $C = code(G, H)$ که در آن منظور این است که این کد خطی توسط ماتریس G تولید می شود و توسط ماتریس H چک می شود.

حال اگر طرفین رابطه ۵۵ را ترانهاده کنیم به شرط زیر می رسیم

$$HG^T = 0. \qquad (۵۶)$$

این رابطه نشان می دهد که ما می توانیم یک کد دیگر تعریف کنیم که توسط H تولید شده و توسط G چک شود. این کد را دوگان کد C می نامیم و آن را با $C^\perp$ نشان می دهیم. بنابراین می نویسیم

$$C^\perp = code(H, G). \qquad (۵۷)$$

دقت کنید که هرگاه یک کلمه متعلق به کد C باشد، داریم:

$$v = \alpha\, G \longrightarrow vH^T = \alpha\, GH^T = 0. \qquad (۵۸)$$

برعکس هرگاه یک کد متعلق به کد $C^\perp$ باشد داریم

$$w = \beta H \longrightarrow wG^T = \beta HG^T = 0. \qquad (۵۹)$$

هم چنین داریم:

$$\langle w, v\rangle = wv^T = \beta HG^T\alpha = 0 \qquad \forall\, v \in C \qquad , w \in C^\perp. \qquad (۶۰)$$

به این ترتیب معلوم می شود که چرا کد دوگان را با $C^{\perp}$ نشان داده ایم.

- مثال: کدِ $[5,2,3]$ را در نظر می گیریم. از ما خواسته اند دوگان این کد را بدست آوریم و بگوییم که این کد چه نوع خطاهایی را تشخیص می دهد یا تصحیح می کند.

- حل: نخست توجه می کنیم که این کد می بایست دو بیت را در پنج بیت کد کند. بنابراین ماتریس پاریته آن دارای بعد 3×5 است. چون فاصله کد برابر با ۳ است پس می بایست هر دو سطر این ماتریس از هم مستقل باشند یا در واقع هر دو سطری از این ماتریس با هم متفاوت باشند. به این ترتیب یک انتخاب برای ماتریس H چنین است:

$$H_C = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}. \qquad (۶۱)$$

حال ماتریس G به آسانی بدست می آید:

$$G_C = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}. \qquad (۶۲)$$

بنابراین بدست می آوریم:

$$G_{C^{\perp}} = H_C = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \qquad (۶۳)$$

به این ترتیب این کد سه بیت را در پنج بیت کد می کند. سوال این است که این کد چه خطاهایی را تشخیص می دهد و تصحیح می کند. برای این کار می بایست ماتریس پاریته آن را تشکیل دهیم:

$$H_{C^{\perp}} = G_C == \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}. \qquad (۶۴)$$

اما این ماتریس بعضی از سطرهایش با هم یکسان هستند. به این ترتیب فاصله این کد ۳ نیست و از ۳ کمتر است. این کد فقط می تواند خطا در یک بیت را تشخیص دهد ولی نمی تواند آن را تصحیح کند.

- دوگان کد $[7,4,3]$ را بدست آورید و مشخصات آن را معلوم کنید.

مثال: در Z_2^4 قرار می دهیم:

$$C = \langle 0011, 1100 \rangle = \{0000, 0011, 1100, 1111\} \qquad (۶۵)$$

به آسانی معلوم می شود که

$$C^{\perp} = \{0000, 0011, 1100, 1111\} = C. \quad (۶۶)$$

چنین کدی را یک کدِ خود-دوگان می نامیم.

مثال: در Z_2^4 قرار می دهیم:

$$C = \langle 0011 \rangle = \{0000, 0011\}, \quad (۶۷)$$

دراین صورت داریم

$$C^{\perp} = \{0000, 0011, 1100, 1111\} \supset C. \quad (۶۸)$$

۱.۳.۴ کدهای خود-دوگان

هرگاه یک کد دارای این خاصیت باشد که $G = H$ باشد، آنگاه این کد را کد خود-دوگان [۱۳] می نامیم. برای چنین کدهایی داریم: $HH^T = 0$.

برای چنین کدهایی داریم $C = C^{\perp}$. یک نمونه از کدهای خود دوگان کد زیر است:

$$C = \langle 1100, 0011 \rangle = \{0000, 1100, 0011, 1111\} \quad (۶۹)$$

در چنین کدی همه بردارها بر هم، از جمله خودشان، عمودند.

■ نشان دهید که کد همینگ با مشخصات $[7, 4, 3]$ یک کد خود دوگان است. این خاصیت بعدها در ساختن یک نمونه از کدهای کوانتومی اهمیت پیدا می کند.

---

۵ ساختن کدهای کوانتومی از روی کدهای خطی کلاسیک

در ابتدای این درس وقتی که کدهای کلاسیک را مطالعه می کردیم به معرفی کدهای خطی پرداختیم و گفتیم که این کد ها دسته وسیعی از کدهای کلاسیک را تشکیل می دهند. آیا ممکن است که از این کدها ی خطی برای ساختن کدهای کوانتومی استفاده کنیم. این امکان، یک امکان جذاب و درعین حال منطقی است زیرا یک کد کوانتومی بنابر تعریف یک زیرفضای برداری خطی است و این همان چیزی است که در ساختمان

[۱۳] self-dual code

کدهای خطی از ابتدا وجود داشته است. در واقع می دانیم که کدهای کلاسیک خطی در واقع به صورت یک زیر فضا از فضای Z_2^n هستند. یعنی اینکه مجموع هر دو کد_کلمه ای خود یک کد_کلمه است. البته این مجموع با ضرایب 0 یا 1 صورت می گیرد. اگر یک کد خطی کلاسیک مثل C داشته باشیم با بردارهای پایه $\mathbf{g}_i,\ \ i = 1 \cdots k$ براحتی می توانیم یک کد کوانتومی خطی درست کنیم. نکته مهم این است که کد کوانتومی را نه از روی بردارهای پایه C بلکه از روی تمامی بردارهای آن یعنی از روی مجموعه $C = \{\mathbf{v}_i, \qquad i = 1 \cdots 2^k\}$ می سازیم. به این ترتیب که قرار می دهیم:

$$\mathcal{C}_q := \{|\psi\rangle = \sum_{i=1}^{2^k} \psi_i |\mathbf{v}_i\rangle, \quad \psi_i = \text{complex number}\}. \tag{۷۰}$$

تفاوت مهم این است که اگر چه بردارهای $\{\mathbf{v}_i\}$ به عنوان بردارهایی از فضای Z_2^n مستقل نیستند ولی بردارهای $\{|\mathbf{v}_i\rangle\}$ به عنوان بردارهایی در فضای برداری n کیوبیت همه از هم مستقل خطی اند. در واقع کد تکرار سه تایی که یک کوانتومی است دقیقا به همین شیوه از مشابه کلاسیکی آن ساخته شده است. اگر کد کلاسیک $\mathcal{C}$ خطاهای با وزن t را می تواند تصحیح کند، این کد کوانتومی نیز می تواند خطاهای بیت ـبرگردان با وزن t را تصحیح کند. دلیل این امر هم این است که یک خطای e به این صورت روی کدکلمه های کلاسیک و روی حالت های کوانتومی اثر می کند:

$$\begin{aligned} &Classical: \mathbf{v} = (v_1, v_2, \cdots v_n) \longrightarrow (v_1 + e_1, v_2 + e_2, \cdots v_n + e_n) = \mathbf{v} + \mathbf{e} \\ &Quantum\ Bit\ Flip: |\mathbf{v}\rangle = |v_1, v_2, \cdots v_n\rangle \longrightarrow |v_1 + e_1, v_2 + e_2, \cdots v_n + e_n\rangle = |\mathbf{v} + \mathbf{e}\rangle. \end{aligned} \tag{۷۱}$$

با چه نوع مدار کوانتومی می توان از روی یک کد خطی یک کد کوانتومی ساخت که خطاهای بیت برگردان را تصحیح کند؟ برای پاسخ به این سوال توجه می کنیم که کدهای خطی به صورت زیر تعریف می شوند:

$$\alpha_k \longrightarrow v_n = \alpha_k G_{k \times n}. \tag{۷۲}$$

که در آن اندیس ها نشان دهنده طول رشته ها هستن. متناظر با این کد کوانتومی باید به صورت زیر k کیوبیت را در n کیوبیت کد کند، یعنی کار زیر را انجام دهد:

$$|\alpha\rangle \longrightarrow |v\rangle = |\alpha G\rangle. \tag{۷۳}$$

برای ساختن چنین کدی با یک مدار کوانتومی که به صورت یک عملگر یکانی عمل می کند باید از کیوبیت های اضافه به صورت زیر استفاده کنیم:

$$|\alpha\rangle|0\rangle^{n-k} \longrightarrow |\alpha G\rangle. \tag{۷۴}$$

حال کافی است که یک عملگر یکانی داشته باشیم که سندروم هر خطایی را تشخیص دهد و این سندروم در حالت کلاسیک همان ماتریس چک_پاریته است و در حالت کوانتومی به شکل عملگریکانی زیر در می آید:

$$U_H : |\mathbf{v}\rangle|0\rangle \longrightarrow |\mathbf{v}\rangle|\mathbf{v}H^T\rangle. \tag{۷۵}$$

■ مثال: در یک کد پنج کیوبیتی ماتریس چک ـ پاریته به صورت زیر است.

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \tag{۷۶}$$

الف: ماتریس مولد این کد را پیدا کنید.

ب: یک مدار کوانتومی بسازید که حالت های پایه سه کیوبیتی $|\alpha\rangle = |\alpha_1, \alpha_2, \alpha_3\rangle$ را به حالت های پایه پنج کیوبیتی کد کند.

پ: یک مدار کوانتومی بسازید که نشانه های خطا را که با ماتریس پاریته بالا تعریف شده اند تشخیص دهد.

■ حل: الف: هر کلمه ای مثل $\mathbf{v} = (a,\ b,\ c,\ d,\ e)$ که عضوی از کد باشد باید در شرط $\mathbf{v}H^T = 0$ صدق کند. بنابراین چنین کلمه ای حتما می بایست به فرم زیر باشد:

$$\mathbf{v} = (a,\ b,\ a+e,\ b,\ e) \tag{۷۷}$$

باشد که به این معناست که فضای کد دارای سه بردار پایه است، یعنی

$$\mathbf{v} = a(1,0,1,0,0) + b(0,1,0,1,0) + e(0,0,1,0,1) \tag{۷۸}$$

این بردارهای پایه را در یک ماتریس مولد قرار می دهیم و بدست می آوریم:

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}. \tag{۷۹}$$

ب: مدار مولد کد می بایست کار زیر را انجام دهد:

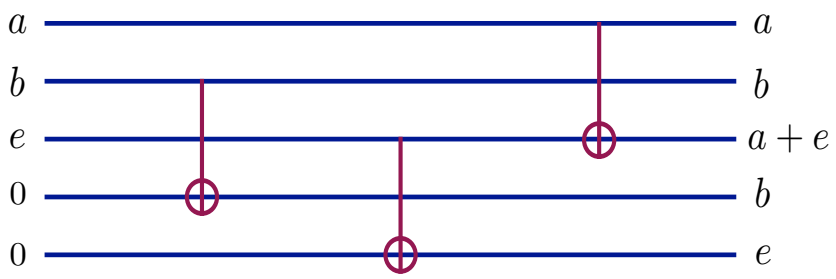
$$|a,b,e\rangle|0,0\rangle \longrightarrow |a,b,a+e,b,e\rangle \tag{۸۰}$$

براحتی دیده می شود که مدار (۵) این کار را انجام می دهد:

پ: با توجه به شکل ماتریس H این مدار باید کار زیر را انجام دهد:

$$|v_1,v_2,v_3,v_4,v_5\rangle|0,0\rangle \longrightarrow |v_1,v_2,v_3,v_4,v_5\rangle|v_2+v_4, v_1+v_3+v_5\rangle \tag{۸۱}$$

مدار کوانتومی مربوطه به راحتی ساخته می شود، شکل (۶).



شکل ۵: مدار مولد کد برای ماتریس (۷۶).

به این ترتیب اگر یک حالت دلخواه مثل $|\psi\rangle$ تحت تاثیر یک خطای بیت ـ برگردان قرار گیرد ، عملگر تشخیص سندروم یعنی U_H می تواند به ترتیب زیر خطا را تشخیص داده و اصلاح کند:

$$\begin{aligned}
&\text{Error :} \qquad X(\mathbf{e}) : |\psi\rangle = \sum_i \psi_i |\mathbf{v}_i\rangle \longrightarrow \sum_i \psi_i |\mathbf{v}_i + \mathbf{e}\rangle, \\
&\text{Error detection} \ : \sum_i \psi_i |\mathbf{v}_i + \mathbf{e}\rangle|0\rangle \longrightarrow \sum_i \psi_i |\mathbf{v}_i + \mathbf{e}\rangle|(\mathbf{v}_i + \mathbf{e})H^T\rangle = \sum_i \psi_i |\mathbf{v}_i + \mathbf{e}\rangle|\mathbf{e}H^T\rangle \\
&\text{Error correction :} \quad X(\mathbf{e}) : \sum_i \psi_i |\mathbf{v}_i + \mathbf{e}\rangle \longrightarrow \sum_i \psi_i |\mathbf{v}_i\rangle = |\psi\rangle. \qquad (۸۲)
\end{aligned}$$

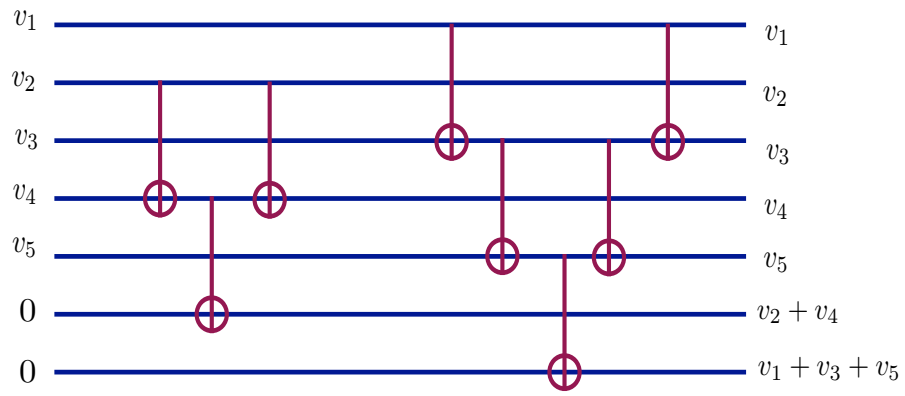
البته کد کوانتومی ای که ساخته ایم تنها می تواند خطاهای بیت‌ـبرگردان را اصلاح کند و توانایی اش برای اصلاح این خطاها به همان اندازه کد خطی است یعنی خطاهایی با همان وزن را که کد کلاسیک می توانست تصحیح کند این کد نیز می تواند تصحیح کند. چنین کدی را با نماد $[[n, k, d]]$ نشان می دهیم (وجود دو تا علامت براکت به معنای کوانتومی بودن کد است.)

- تمرین: الف: یک کد کلاسیک از نوع $[5, 2, 3]$ در نظر بگیرید. حالت $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ به چه حالتی کد می شود؟

  ب: مدار کوانتومی مولد این کد را بسازید.

- تمرین: الف: یک کد کلاسیک از نوع $[6, 3, 3]$ در نظر بگیرید. حالت های پایه سه کیوبیتی از نوع $(i, j, k) = 0, 1$ $|i, j, k\rangle$ به چه حالت هایی کد می شوند.

  ب: مدار کوانتومی مولد این کد را بسازید.



شکل ۶: مدار تشخیص نشانه خطا برای ماتریس (۷۶).

■ تمرین: یک کد کلاسیک از نوع $[7, 4, 3]$ در نظر بگیرید. حالت پایه این کد را وقتی که مطابق بالا آن را تبدیل به یک کد کوانتومی می کنید بدست آورید.

می توانیم پایدارسازهای این کد را نیز بدست آوریم. از آنجا که این کد تنها خطاهای بیت ـ برگردان را تصحیح می کند انتظار داریم که پایدارسازهای آن نیز از عملگر Z ساخته شوند. در واقع از آنجا که به ازای تمام کد کلمه های کلاسیک رابطه $vH^T = 0$ برقرار است می توانیم بنویسیم

$$\forall \ |\mathbf{v}\rangle \in \mathcal{C}_q, \quad (-1)^{\sum_i v_i H_{ji}} |\mathbf{v}\rangle = |\mathbf{v}\rangle, \quad \forall j. \tag{۸۳}$$

و یا

$$\forall \ |\mathbf{v}\rangle \in \mathcal{C}_q, \quad (-1)^{v_1 H_{j1}} (-1)^{v_2 H_{j2}} \cdots (-1)^{v_n H_{jn}} |\mathbf{v}\rangle = |\mathbf{v}\rangle, \quad \forall j. \tag{۸۴}$$

با استفاده از رابطه

$$Z|v\rangle = (-1)^v |v\rangle, \qquad v = 0, 1$$

می توانیم رابطه قبلی را به صورت زیر بازنویسی کنیم:

$$Z_1^{H_{j1}} Z_2^{H_{j2}} Z_3^{H_{j3}} \cdots Z_n^{H_{jn}} |\mathbf{v}\rangle = |\mathbf{v}\rangle, \quad j = 1, 2, \cdots n - k. \tag{۸۵}$$

اما حسن بزرگ این نوع نوشتن این است که حالا می توانیم بگوییم که این عملگر هر ترکیب خطی از این بردارها را نیز ثابت نگاه می دارد. به عبارت دیگر این عملگر یک پایدار ساز فضای کد است. به این ترتیب پایدارسازهای این کد را پیدا کرده ایم که برابرند با:

$$S_j := Z_1^{H_{j1}} Z_2^{H_{j2}} Z_3^{H_{j3}} \cdots Z_n^{H_{jn}}, \quad j = 1, 2, \cdots n-k. \tag{۸۶}$$

هر کد خطی ای که به این ترتیب می سازیم، تنها می تواند خطاهای بیت‌ـبرگردان را اصلاح کند و از اصلاح خطاهای فاز‌ـبرگردان و در نتیجه از اصلاح خطاهای کوانتومی ناتوان است. حال سوال این است که چگونه می توانیم کدی بسازیم که قادر به اصلاح هر دو نوع خطا باشد. این کدها که به طور سیستماتیک با استفاده از دو کد کوانتومی ساخته می شوند به کدهای CSS مشهورند که در بخش آینده به تفصیل آنها را شرح می دهیم.

---

۶ کدهای CSS

در این بخش به معرفی کدهای CSS [۱۴] می پردازیم. این کدها نخستین بار توسط Calderbank, Steane, Shor معرفی شدند و نام خود را نیز از نام این سه نفر گرفته اند. راهی که طی می کنیم این است که به مجموعه پایدارسازهایی که در بخش قبل ساختیم و همگی از عملگرهای Z ساخته شده بودند (چون خطاهای بیت برگردان را تصحیح می کردند)، یک مجموعه پایدارساز اضافه می کنیم که همگی از عملگرهای X ساخته شده باشند (تا بتوانند خطاهای فازبرگردان را تصحیح کنند.) این پایدارسازها را می بایست به شکلی اضافه کنیم که با پایدارسازهای قبلی جابجا شوند. سپس فضایی را شناسایی می کنیم که توسط مجموعه کامل پایدارسازها پایدار باقی بماند. به این ترتیب است که نهایتا کدهای CSS ساخته می شود.

برای ساختن این کدها می بایست دو کد کلاسیک خطی در اختیار داشت. فرض کنید که $C = [n, k, d]$ و $C' = [n, k', d']$ دو کد کلاسیک خطی و $C_q = [[n, k, d]]$ و $C'_q = [[n, k', d']]$ کدهای کوانتومی ای باشند که به طریق ساده بالا از روی آنها ساخته شده اند.

کد C با ماتریس پاریته ی H مشخص می شود که ابعاد آن $(n-k) \times n$ است. به ازای هر سطر این ماتریس یک عملگر پایدارساز به شکل زیر تعریف می کنیم:

$$S_j := Z_1^{H_{j1}} \; Z_2^{H_{j2}} \; Z_3^{H_{j3}} \cdots Z_n^{H_{jn}} \qquad \forall j. \tag{۸۷}$$

تعداد این پایدارسازها برابر است با $n-k$. حال به کد C' توجه می کنیم. این کد با ماتریس پاریته H' مشخص می شود که ابعاد آن $(n-k') \times n$ است. به ازای هر سطر این ماتریس نیز یک عملگر پایدارساز به شکل زیر تعریف می کنیم:

[۱۴] Calderbank-Steane-Shor

$$S'_k := X_1^{H'_{k1}} X_2^{H'_{k2}} X_3^{H'_{k3}} \cdots X_n^{H'_{kn}} \qquad \forall k. \tag{۸۸}$$

طبیعی است که S_j ها بین خود جابجا می شوند و به عنوان سندورم تشخیص خطا ی با وزن $d-1$ به کار می روند. هم چنین S'_k ها بین خود جابجا می شوند و به عنوان سندروم خطای با وزن حداکثر $d'-1$ به کار می روند. ولی آیا می توان این عملگرهای پایدارساز را روی هم ریخت؟ پاسخ در صورتی مثبت است که باهم جابجا شوند. ولی شرط جابجا شدن این عملگرها بسیار ساده است.

با استفاده از رابطه جابجایی

$$Z^a X^b = (-1)^{ab} X^b Z^a$$

می توانیم بفهمیم که

$$S_j S'_k = (-1)^{\sum_i H_{ji} H'_{ki}} S'_k S_j, \tag{۸۹}$$

و یا

$$S_j S'_k = (-1)^{(HH'^T)_{j,k}} S'_k S_j. \tag{۹۰}$$

بنابراین پایدارسازهای ۸۷ و ۸۸ وقتی باهم جابجا می شوند که رابطه زیر برقرار باشد:

$$H' H^T = 0. \tag{۹۱}$$

اما این رابطه چه می گوید؟ یک عضو $x \in C'^{\perp}$ را در نظر بگیرید. این عضو توسط H' تولید می شود. بنابراین می توانیم بنویسیم:

$$x = \alpha H' \longrightarrow x H^T = (\alpha H') H^T = 0 \longrightarrow x \in C. \tag{۹۲}$$

بنابراین این رابطه بیان می کند که

$$C'^{\perp} \subset C. \tag{۹۳}$$

- تمرین: نشان دهید که رابطه زیر نیز برقرار است:

$$C^{\perp} \subset C'. \tag{۹۴}$$

- تمرین: با تجربه ای که از حل تمرین های قبلی (برای ساختن کدهای کلاسیک) پیدا کرده اید تحقیق کنید که آیا می توانید دو کد کلاسیک با $n=5$ پیدا کنید که در شرط $HH'^T = 0$ صدق کنند. با $n=6$ چطور؟ با $n=7$ چطور؟ در این مورد پاسخ مثبت است. این کد ها را به طور صریح بنویسید.

پس شرط جابجا شدن تمام عناصر پایدارسازی را که ساختیم پیدا کردیم. تعداد کل این عناصر پایدار ساز برابراست با: $(n-k)+(n-k')$. کد جدید چند تا کیوبیت را در n کیوبیت کد می کند؟ پاسخ برابر است با $n-(2n-k-k)=k+k'-n$. از آنجا که پایدارسازهای S_j تمام خطاهای بیت ـ برگردان تا وزن $d-1$ را شناسایی می کنند و پایدارسازهای S'_k تمام خطاهای فازـ برگردان تا وزن $d'-1$ را شناسایی می کنند، معلوم می شود که کد جدیدی که ساخته ایم حتما خطاهای کوانتومی را با وزن d شناسایی می کند که در آن

$$d \geq min(d, d'). \tag{۹۵}$$

بنابراین کد جدید که آن را با نماد $CSS(C,C')$ نشان می دهیم کدی است با مشخصات زیر:

$$CSS(C,C') = [[n, k+k'-n, d \geq min(d,d')]]. \tag{۹۶}$$

حال سوال می کنیم که حالت های این کد به طور صریح چه هستند؟ برای پاسخ دقت می کنیم که با توجه به رابطه ۹۴ فضای $C'^{\perp}$ زیرفضای C است. در نتیجه رابطه هم ارزی زیر را تعریف می کنیم:

$$\mathbf{v}, \mathbf{v}' \in C, \quad \mathbf{v} \sim \mathbf{v}' \quad if \quad \mathbf{v}-\mathbf{v}' \in C'^{\perp}. \tag{۹۷}$$

این رابطه هم ارزی تمام فضای C را مطابق با شکل ۷ به کلاس ها ی هم ارزی تبدیل می کند. به ازای هر کلاس هم ارزی که یک نماینده مثلv دارد، یک حالت به صورت زیر تعریف می کنیم:

$$|\overline{\mathbf{v}}\rangle = \sum_{\mathbf{x}\in C'^{\perp}} |\mathbf{v}+\mathbf{x}\rangle. \tag{۹۸}$$

این حالت ها را برای سادگی بهنجار نکرده ایم. در پایان بحث می توانیم با انتخاب ضرایب مناسب آنها را بهنجار کنیم. تعداد کلاس ها برابر است با: $\frac{|C|}{|C'^{\perp}|} = \frac{2^k}{2^{n-k'}} = 2^{k+k'-n}$ که همان مقداری است که انتظار داریم. حال ثابت می کنیم که این حالت ها واقعا توسط عملگرهای پایدارسازی که معرفی کرده ایم پایدار باقی می ماند. نخست می دانیم که به ازای هر بردار $|\mathbf{v}\rangle \in C$ داریم $S_j|\mathbf{v}\rangle = |\mathbf{v}\rangle$ ، در نتیجه واضح است که

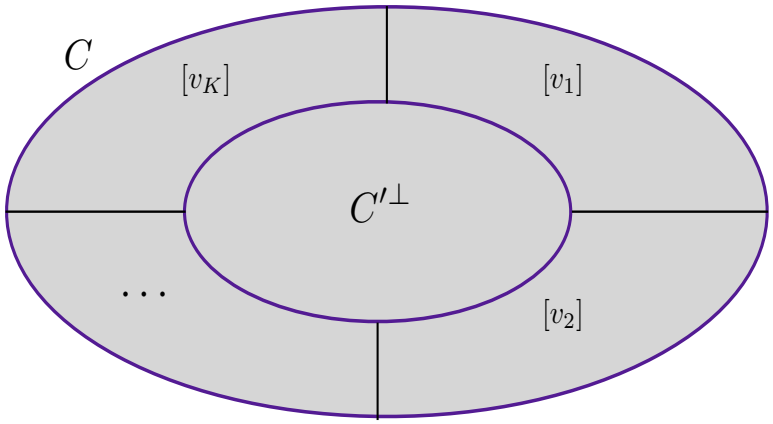
$$S_j|\overline{v}\rangle = |\overline{v}\rangle. \tag{۹۹}$$

حال به پایدارسازهایS'_k توجه می کنیم: با توجه به اینکه ماتریس H' مولد کد $C'^{\perp}$ است، داریم

$$S'_k|\overline{\mathbf{v}}\rangle = S'_k \sum_{\mathbf{x}\in C'^{\perp}} |\mathbf{v}+\mathbf{x}\rangle = X_1^{H'_{k1}} X_2^{H'_{k2}} X_3^{H'_{k3}} \cdots X_n^{H'_{kn}} \sum_{\mathbf{x}\in C'^{\perp}} |\mathbf{v}+\mathbf{x}\rangle \tag{۱۰۰}$$

اما می دانیم که ماتریس H' در واقع ماتریس مولد کد $C'^{\perp}$ است که به این معنا ست که سطرهای این ماتریس بردارهای پایه این کد هستند . این بردارهای پایه را با $\mathbf{e}_k$ نشان می دهیم. در نتیجه داریم

$$S'_k|\overline{\mathbf{v}}\rangle = S'_k \sum_{\mathbf{x}\in C'^{\perp}} |\mathbf{v}+\mathbf{x}\rangle = \sum_{\mathbf{x}\in C'^{\perp}} |\mathbf{v}+\mathbf{x}+\mathbf{e}_k\rangle = \sum_{\mathbf{x}'\in C'^{\perp}} |\mathbf{v}+\mathbf{x}'\rangle = |\overline{\mathbf{v}}\rangle. \tag{۱۰۱}$$



شکل ۷: کلاس های هم ارزی $C'^{\perp}$ (زیر فضای افقی) در C. هر کدام از هم مجموعه ها با یک نماینده از آنها مشخص شده است. کلاس $[v]$ شامل تمام کلمه هایی است که با v هم ارز هستند.

- تمرین: آیا می توانید کدی از نوع $[5, 2, 3]$ بنویسید؟

- تمرین: حالت های ۹۸ را بهنجار کنید.

- **مثال:** کد هامینگ یعنی کد کلاسیک $[7, 4, 3]$ را با $C_{Hamming}$ نشان می دهیم. می خواهیم برای این کد، مدار تولید کننده، و مدار تشخیص خطا را تعیین کنیم.

  حل: این کد از روی ماتریس پاریته هامینگ ساخته می شود. ماتریس پاریته برای این کد عبارت است از:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \qquad (۱۰۲)$$

مطابق آنچه که در مورد کدهای CSS یاد گرفتیم، پایدارسازها از روی سطرهای این ماتریس و ماتریس عمود بر آن ساخته می شود. اما این کد خاص، یک کد خوددوگان [۱۵] است، یعنی $HH^T = 0$. بنابراین هر دو نوع پایدارسازها از سطرهای ماتریس H ساخته می شود:

[۱۵] Self-Dual

$$
\begin{aligned}
S_1 &= Z_1Z_4Z_5Z_7\\
S_2 &= Z_2Z_4Z_6Z_7\\
S_3 &= Z_3Z_5Z_6Z_7\\
S'_1 &= X_1X_4X_5X_7\\
S'_2 &= X_2X_4X_6X_7\\
S'_3 &= X_3X_5X_6X_7. \qquad (۱۰۳)
\end{aligned}
$$

$|\psi\rangle = a|0\rangle + b|1\rangle$ بسازد از آنچه که در درس قبلی یاد گرفتیم کمک می گیریم. حالت های $|0\rangle$ و $|1\rangle$ را به صورت زیر و در یک مدار که شش کیوبیت دوم تا هفتم آن در حالت $|0\rangle$ قرار گرفته اند، به دو حالت متعامد هفت کیوبیتی تبدیل می کنیم:

$$
\begin{aligned}
|0\rangle|0,0,0,0,0,0\rangle &\longrightarrow |\overline{0}\rangle = (I+S'_1)(I+S'_2)(I+S'_3)|0,0,0,0,0,0,0\rangle,\\
|1\rangle|0,0,0,0,0,0\rangle &\longrightarrow |\overline{1}\rangle = (I+S'_1)(I+S'_2)(I+S'_3)|1,1,1,1,1,1,1\rangle. \qquad (۱۰۴)
\end{aligned}
$$

از آنجا که دو حالت

$$
|0,0,0,0,0,0,0,\rangle, \qquad |1,1,1,1,1,1,1\rangle
$$

برهم عمودند و گیت هایی که روی این حالت ها اثر می کنند (با در نظر گرفتن بهنجارش که فعلا از آن صرف نظر کرده ایم) یکانی هستند، دو حالت نهایی تولید شده نیز برهم عمود خواهند بود. اعمال گیت های $(I+S'_i)$ ساده است. این گیت ها در مدار (۸) نشان داده شده اند. اما این مدار با عمل روی حالت، $|0,0,0,0,0,0,0\rangle$ فقط حالت، $|\overline{0}\rangle$ را درست می کند. چگونه می توانیم با تغییر کوچکی در این مدار روی همین حالت ورودی حالت $|\overline{1}\rangle$ را نیز درست کنیم. برای این کار توجه می کنیم که با تعریف عملگر

$$
\mathbf{X} := X_1X_2X_3X_4X_5X_6X_7,
$$

می توانیم بنویسیم:

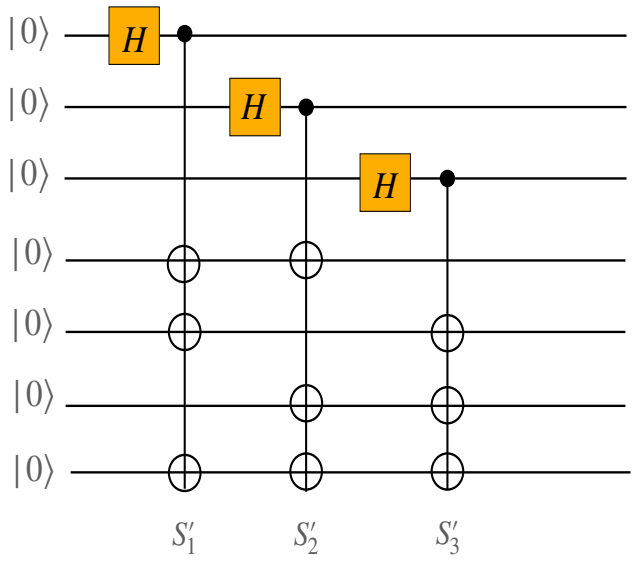
$$
|\overline{1}\rangle = (I+S'_1)(I+S'_2)(I+S'_3)\mathbf{X}|0,0,0,0,0,0,0\rangle \qquad (۱۰۵)
$$

حال دقت می کنیم که رابطه زیر نیز برقرار است:

$$
\mathbf{X} \equiv X_1X_2X_3X_4X_5X_6X_7 = X_1X_3X_5S'_2 \qquad (۱۰۶)
$$

و در نتیجه

به این ترتیب، عملگر S'_2 که یک پایدارساز است در یکی از پرانتزهای قبل از آن در عبارت (۱۰۵) جذب می شود و می توانیم بنویسیم:

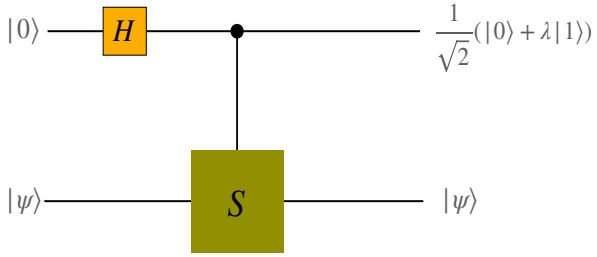


شکل ۸: مدار اولیه ای که حالت $|\bar{0}\rangle$ را از روی حالت، $|0,0,0,0,0,0,0\rangle$ درست می کند.

$$|\bar{1}\rangle = (I+S'_1)(I+S'_2)(I+S'_3)X_1X_3X_5|0,0,0,0,0,0,0\rangle. \qquad (۱۰۷)$$

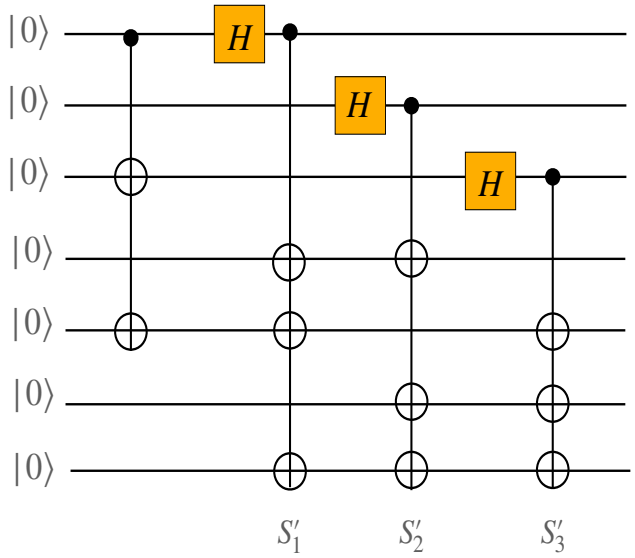
حال می بایست قبل از مدار شکل (۸) گیت های ساده ای قرار دهیم که وقتی که کیوبیت اول 0 است عمل نکند ولی وقتی که کیوبیت اول 1 است، گیت $X_4X_5X_6$ را اعمال کند. این کار با مدار شکل (۹) انجام می شود.

حال باید مداری را بسازیم که نشانه های خطا را تشخیص می دهد. اگر به شکل (۱۰) وضیح آن نگاه کنیم، براحتی متوجه می شویم که مدار تشخیص نشانه های خطا، آن چیزی است که در شکل (۱۱) رسم شده است.

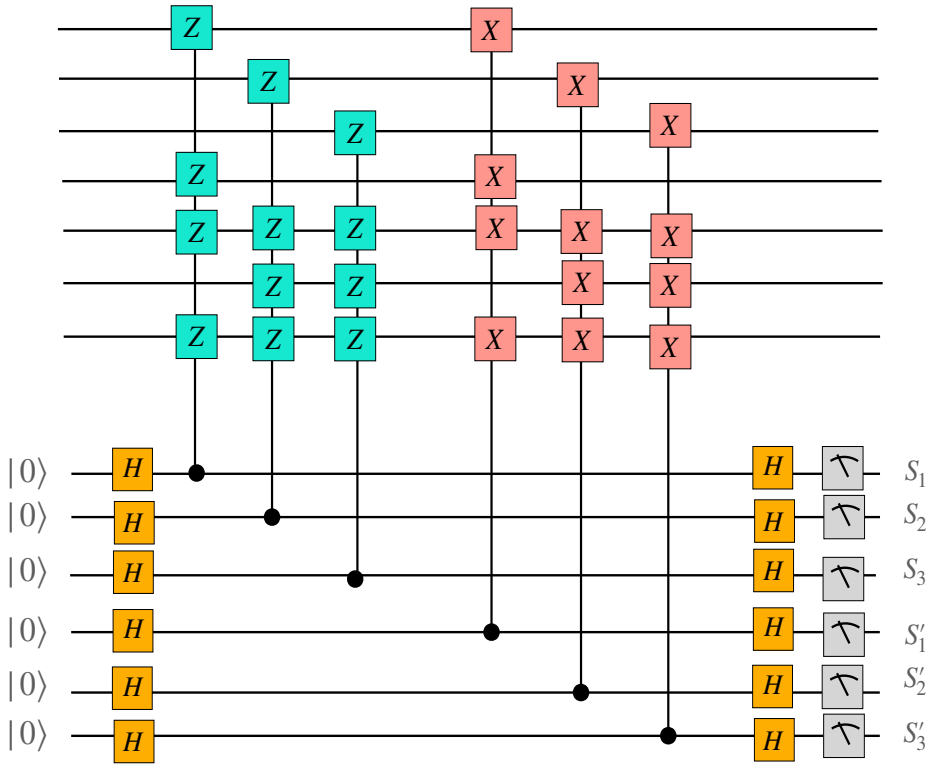


شکل ۱۰: یک مدار ساده که تشخیص می دهد آیا حالت $|\psi\rangle$ برای پایدارساز S که یک عملگر یکانی است ویژه مقدارش یک است یا منهای یک.

و ت



شکل ۹: دار اولیه ای که هر دو حالت $|\bar{0}\rangle$ و $|\bar{1}\rangle$ را از روی حالت، $|0,0,0,0,0,0,0\rangle$ درست می کند.



شکل ۱۱: مدار تشخیص خطا برای کد ۷ کیوبیتی.

۷ مسئله ها

- نشان دهید که تمام کد_کلمه های $C^{\perp}$ بر تمام کلمه های C عمود هستند. این تمرین نمادگذاری $C^{\perp}$ را برای دوگان یک کد توجیه می کند.

- نشان دهید که اگر کد C k بیت را در n بیت کد کند ، در این صورت $C^{\perp}$ تعداد $n-k$ بیت را درn بیت کد می کند.

- کوچکترین ماتریس از نوع بالا را پیدا کنید. سپس ماتریس G و شکل دقیق کدها را بنویسید.
- یک کد کلاسیک بنویسید که دارای مشخصات $[n,2,3]$ باشد. کوچکترین n را پیدا کنید. ماتریس های G و H را بدست آورید.
- یک کد کلاسیک بنویسید که دارای مشخصات $[n,3,3]$ باشد. کوچکترین n را پیدا کنید. ماتریس های G و H را بدست آورید.
- یک کد کلاسیک بنویسید که دارای مشخصات $[n,4,3]$ باشد. کوچکترین n را پیدا کنید. ماتریس های G و H را بدست آورید.
- از رابطه $\mathbf{g}(\alpha)=\alpha G$ استفاده کنید و ماتریس مولد کد زیر را پیدا کنید.

$$C=\{(a,b,a+b,b,a)\mid a,b=0,1\} \qquad (۱۰۸)$$

ماتریس H را برای این بنویسید.

- از رابطه $\mathbf{w}(\alpha)=\alpha G$ استفاده کنید و ماتریس مولد کد زیر را پیدا کنید.

$$C=\{(a,b,a+b,c,a+b+c,b+c)\mid a,b,c=0,1\} \qquad (۱۰۹)$$

ماتریس H را برای این کد بدست آورید.

- نشان دهید که $C^{\perp}$ یک زیرفضای برداری است. هم چنین نشان دهید که بعد این زیرفضا برابر با $n-k$ است.
- برای کدهای کوانتومی $[[7,4,3]]$,$[[6,3,3]]$,$[[5,2,3]]$ مولدهای پایدارساز را پیدا کنید:
- پایدارسازهای زیر را در نظر بگیرید:

$$X_1X_2, \qquad X_1X_3. \qquad (۱۱۰)$$

زیرفضایی از فضای سه کیوبیتی که توسط این عملگرها پایدار شود، چند بعد دارد؟ مداری رسم کنید که یک حالت یک کیوبیتی دلخواه را به یک حالت سه کیوبیتی با این پایدارسازها کد کند.

- پایدارسازهای زیر را در نظر بگیرید:

$$X_1X_2, \qquad X_1X_3, \qquad Z_1Z_2Z_3. \tag{۱۱۱}$$

آیا با یک استدلال ساده می توانید نشان دهید که این زیرفضا یک بعدی است و فقط یک حالت در آن قرار دارد؟ مداری رسم کنید که این حالت را تولید کند.

- پایدارسازهای زیر را در نظر بگیرید:

$$Z_1Z_2, \qquad Z_3Z_4, \qquad X_1X_2X_3X_4. \tag{۱۱۲}$$

زیرفضایی از فضای چهار کیوبیتی که توسط این عملگرها پایدار شود، چند بعد دارد؟ مداری رسم کنید که یک حالت یک کیوبیتی دلخواه را به یک حالت چهارکیوبیتی با این پایدارسازها کد کند.

- مداری بسازید که حالتِ $|\psi\rangle = a|0\rangle + b|1\rangle$ را به یک حالت سه کیوبیتی کد کند. این حالت سه کیوبیتی می بایست توسط عملگرهای $Z_1Z_2Z_3$ و X_1X_2 پایدار شود. (راهنمایی: نخست خود حالت سه کیوبیتی را بنویسید و از روی آن مدار را بسازید.)

- مداری بسازید که حالتِ $|\psi\rangle = a|0\rangle + b|1\rangle$ را به یک حالت سه کیوبیتی کد کند. این حالت سه کیوبیتی می بایست توسط عملگرهای $X_1X_2X_3$ و Z_1Z_2 پایدار شود. (راهنمایی: نخست خود حالت سه کیوبیتی را بنویسید و از روی آن مدار را بسازید.)

---

۸ 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.