محاسبات کوانتمی (۲۲۶۷۱) ترم بهار ۱۳۹۱-۱۳۹۰

مدرس: سلمان ابوالفتح بیگی نویسنده: سلمان ابوالفتح بیگی

جلسه ۱۴

با خلاصه‌ای از جلسه‌ی گذشته شروع می‌کنیم. G را گروه پاولی روی n کیوبیت گرفتیم و $S \subseteq G$ را زیرگروهی آبلی که شامل $-I$ نیست. کد P را برابر زیرفضای ویژه‌ی مشترک اعضای S با مقدار ویژه‌ی $+1$ گرفتیم. نشان دادیم که اگر $\{g_1, \dots, g_k\}$ یک مجموعه‌ی مولد مینیمال S باشد آنگاه $\mathrm{tr} P = 2^{n-k}$، یعنی P، $n-k$ کیوبیت را کد می‌کند.
همچنین تعریف کردیم

$$N(S) = \{h \in G : \quad \forall g \in S, \;\; gh = hg\}$$

و دیدیم که P مجموعه‌ی خطای $M \subseteq G$ را تصحیح می‌کند اگر و فقط اگر به ازای هر $E, E' \in M$ داشته باشیم $E^\dagger E' \notin N(S) \setminus S$.

در این جلسه می‌خواهیم ببینیم که چطور می‌توان مثال‌هایی عملی از S و P ساخت. همچنین چگونه می‌توان k و یا $N(S)$ را محاسبه کرد.

۱ گروه پاولی و $\mathbb{Z}_2^{2n}$

طبق تعریف ماتریس‌های پاولی داریم $X^2 = Y^2 = Z^2 = I$ و $XY = -YX$، $XZ = -ZX$ ، $ZY = -YZ$ و همچنین $Y = iXZ$. تناظر زیر را بین ماتریس‌های پاولی و بردارهای $\mathbb{Z}_2^2$ در نظر بگیرید:

$$\begin{aligned} I &\to (0 \quad 0), \quad X \to (1 \quad 0), \\ Z &\to (0 \quad 1), \quad Y \to (1 \quad 1). \end{aligned} \tag{۱}$$

توجه کنید که با در نظر نگرفتن فازها (برای مثال i در رابطه‌ی $Y = iXZ$) ضرب ماتریس‌های پاولی تحت این تناظر به جمع اعضای $\mathbb{Z}_2^2$ تبدیل می‌شود.

این تناظر را می‌توان به اعضای G تعمیم داد. توجه کنید که

$$G = \{c\sigma_1 \otimes \cdots \otimes \sigma_n : \quad c \in \{\pm 1, \pm i\}, \sigma_j \in \{I, X, Y, Z\}\}.$$

به ازای هر $c\sigma_1 \otimes \cdots \otimes \sigma_n \in G$ یک بردار در $\mathbb{Z}_2^{2n}$ به طول $2n$ نسبت می‌دهیم. این $2n$ تایی را به دو بخش n تایی تقسیم می‌کنیم. n تایی اول را بخش X و n تایی دوم را بخش Z می‌نامیم. هر $1 \leq i \leq n$ یک مولفه در بخش X دارد و یک مولفه در بخش Z که جمعا می‌شود دو مولفه. حال طبق (۱) می‌توانیم این دو مولفه را متناظر با σ_i تعریف کنیم.

تاکید می‌کنیم که در این تناظر مقدار $c \in \{\pm 1, \pm i\}$ مهم نیست. نکته‌ی دیگر این که حاصل‌ضرب ماتریس‌های پاولی تحت این تناظر به جمع بردارهای $\mathbb{Z}_2^{2n}$ تبدیل می‌شود.

مثال زیر تناظر فوق را واضح‌تر بیان می‌کند. فرض کنید $n = 3$ و قرار دهید $g = Y_1X_2Z_3$ و $h = X_1X_2X_2$. در تناظر فوق داریم

$$g \to (1\ 1\ 0\ |1\ 0\ 1),$$

$$h \to (1\ 1\ 1\ |0\ 0\ 0).$$

$gh = (Y_1X_2Z_3)(X_1X_2X_3) = (Y_1X_1)(X_2^2)(Z_3X_3) = (-iZ_1)(I_2)(-iY_3) = -Z_1Y_3,$ که متناظر است با بردار

$$-Z_1Y_3 \to (0\ 0\ 1\ |1\ 0\ 1) = (1\ 1\ 0\ |1\ 0\ 1) + (1\ 1\ 1\ |0\ 0\ 0).$$

توجه کنید که این تناظر در واقع یک یکریختی است بین گروه خارج قسمتی $G/\{\pm 1, \pm i\}$ و $\mathbb{Z}_2^{2n}$.

نه تنها ضرب ماتریس‌های پاولی، بلکه اطلاعات مربوط به جابجا شدن و یا نشدن آنها نیز تحت این نگاشت حفظ می‌شود. با همان مثال بالا شروع می‌کنیم. داریم

$$\begin{aligned} gh &= (Y_1X_2Z_3)(X_1X_2X_3) &&= (Y_1X_1)(X_2^2)(Z_3X_3), \\ hg &= (X_1X_2X_3)(Y_1X_2Z_3) &&= (X_1Y_1)(X_2^2)(X_3Z_3) = (-Y_1X_1)(X_2^2)(-Z_3X_3). \end{aligned}$$

پس $gh = hg$. در واقع در حاصل‌ضرب مولفه به مولفه‌ی g و h، مولفه‌های اول و سوم با هم جابجا نمی‌شوند و لذا به ازای هر یک از آنها یک فاکتور -1 خواهیم داشت. این دو -1 هم‌دیگر را خنثی می‌کنند و در نتیجه g و h جابجا می‌شوند.

در حالت کلی برای تشخیص جابجا شدن یا نشدن دو ماتریس پاولی کافی است به مولفه‌های اول تا n-ام آنها نگاه کرد و تعداد فاکتورهای -1 متناظر را شمرد. اگر تعداد آنها زوج بود دو عملگر جابجا می‌شوند و در غیر این صورت جابجا نمی‌شوند. در واقع اگر

$$g \to (v_1^x \dots v_n^x | v_1^z \dots v_n^z) = (v^x|v^z)$$

$$h \to (w_1^x \dots w_n^x | w_1^z \dots w_n^z) = (w^x|w^z)$$

زوجیت و یا فردیت تعداد فاکتورهای -1 از عبارت

$$\sum_i v_i^x w_i^z + v_i^z w_i^x = v^x \cdot w^z + v^z \cdot w^x = (v^x|v^z)\Lambda(w^x|w^z)^T$$

به دست می‌آید که

$$\Lambda = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

به طور خلاصه دو ماتریس پاولی g, h جابجا می‌شوند اگر بردارهای متناظر آنها $(v^x|v^z)$ و $(w^x|w^z)$ تحت Λ «عمود»[1] باشند: $(v^x|v^z)\Lambda(w^x|w^z)^T = 0 (\mod 2)$. توجه کنید که برای هر $(v^x|v^z)$ داریم $(v^x|v^z)\Lambda(v^x|v^z)^T = 0$.

[1] در این‌جا واژه‌ی عمود معنای هندسی معمول را ندارد زیرا $\mathbb{Z}_2^{2n}$ یک فضای برداری حقیقی یا مختلط نیست. برای مثال هر برداری با این تعریف بر خودش عمود است. با این حال ترجیح می‌دهیم برای راحتی از همان واژه‌ی عمود استفاده کنیم.

۲ کدهای کوانتمی جمعی و زیرفضاهای $\mathbb{Z}_2^{2n}$

به بحث کدهای جمعی[۲] برگردیم. $S \subseteq G$ تحت تناظر فوق به مجموعه‌ی $W \subseteq \mathbb{Z}_2^{2n}$ نگاشته می‌شود. از آنجا که S تحت ضرب بسته است، W تحت جمع بسته است. در واقع اگر $\mathbb{Z}_2^{2n}$ را یک فضای برداری با بعد $2n$ روی میدان $\mathbb{Z}_2$ بگیریم، W یک زیرفضای آن خواهد شد.

چون S آبلی است، W تحت Λ بر خود عمود است:

$$\forall v, w \in W : \qquad v\Lambda w^T = 0 (\mod 2).$$

همچنین $-I \notin S$ پس تناظر بین اعضای S و W یک به یک است. در واقع اگر $g \in S$ و $c \neq 1$ آنگاه $cg \in S$ نتیجه می‌دهد $cI \in S$ که تناقض است.

به راحتی قابل بررسی است که $\{g_1, \ldots, g_k\}$ یعنی مجموعه‌ی مولد مینیمال S متناظر با پایه‌ای برای W است: $k = \dim W$. به عبارت دیگر برای یافتن یک مجموعه‌ی مولد مینیمال کافی است یک پایه برای W بیابیم.

$N(S)$ برابر مجموعه‌ی ماتریس‌های پاولی‌ای است که با همه اعضای S جابجا می‌شوند. در نتیجه $N(S)$ (که خود یک زیرگروه است) متناظر است با زیرفضای

$$N(W) = \{(v^x|v^z) \in \mathbb{Z}_2^{2n} : \quad \forall (w^x|w^z) \in W, \ (v^x|v^z)\Lambda(w^x|w^z)^T = 0\}.$$

توجه کنید که $N(W)$ با تعدادی معادله‌ی خطی مشخص می‌شود و محاسبه‌ی آن کاری ساده است. $N(W)$ فضای عمود به W است که دارای بعد k است. بنابراین $\dim N(W) = 2n - k$.

مثال ۱: A را ماتریس مجاورت یک گراف n راسی بگیرید. در واقع A یک ماتریس $n \times n$ متقارن ($A^T = A$) با درایه‌های $0, 1$ است. W را برابر فضای تولید شده توسط n سطر ماتریس $n \times (2n)$

$$(I \ \mid A)$$

قرار دهید. از آنجا که $(I|A)$ یک زیر ماتریس همانی دارد رتبه‌اش برابر n است و سطرهایش مستقل خطی هستند. پس $k = \dim W = n$. از تقارن A نتیجه می‌شود که سطرهای $(I|A)$ تحت Λ بر هم عمودند. لذا اگر ماتریس‌های پاولی «هرمیتی» متناظر با سطرهای $(I|A)$ را در نظر گرفته و S را زیرگروه تولید شده توسط این n عضو بگیریم، زیرگروهی آبلی به دست می‌آید. این زیرگروه آبلی شامل $-I \in S$ نیست چون تولید شده توسط ماتریس‌های پاولی هرمیتی مستقل است که با هم جابجا می‌شوند. بنابراین می‌توان کد P متناظر با S را تشکیل داد. طبق روابط قبل داریم $\text{tr}P = 2^{n-k} = 1$. یعنی فقط یک حالت در فضای کد وجود دارد. به چنین حالتی، «حالت گرافی»[۳] می‌گویند.

---

[۲] Additive codes
[۳] Graph state

مثال ۲: W را فضای تولید شده توسط $k \leq n$ سطر اول ماتریس $(I|A)$ در مثال قبل بگیرید و S, P را مانند قبل تعریف کنید. در این صورت $\mathrm{tr}P = 2^{n-k}$ و این کد $n-k$ کیوبیت را کد می‌کند. به چنین کدی، «کد گرافی»[۴] گویند.

داریم $\dim N(W) = 2n-k = n+(n-k)$. n سطر $(I|A)$، n عضو پایه‌ای برای $N(W)$ را تشکیل می‌دهند. بقیه‌ی $(n-k)$ عضو چنین پایه‌ای برابرند با

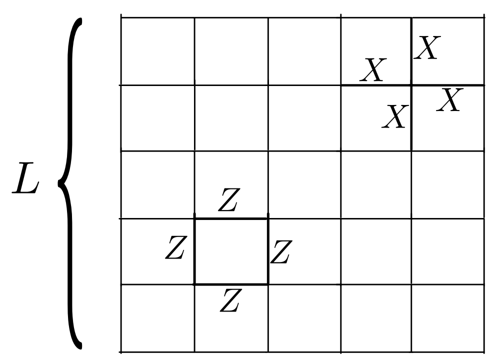
$$(\overbrace{0\ldots0}^{k}\overbrace{0\ldots1\ldots0}^{n-k}|\overbrace{0\ldots0}^{n}).$$

ثابت می‌شود که هر کد جمعی کوانتمی «معادل» با یک کد گرافی است.

۳ کدهای جمعی و همیلتونی‌های جابجایی

یک کد جمعی در نظر بگیرید که با مولدهای $g_1, \ldots, g_k$ تولید شده باشد. می‌دانیم g_i-ها هرمیتی هستند. پس می‌توانیم عملگر $H = -(g_1 + \cdots + g_k)$ را به عنوان یک همیلتونی در نظر بگیریم. در این صورت مینیمم انرژی یک سیستم با همیلتونی H (مینیمم مقدار ویژه‌ی H) برابر $-k$ است. از آنجا که g_i-ها جابجا می‌شوند، H یک همیلتونی جابجایی است. حالت‌های با انرژی $-k$ برابرند با حالت‌های $|\psi\rangle$ که برای هر i داشته باشیم $g_i|\psi\rangle = |\psi\rangle$. بنابراین یک کد جمعی کوانتمی معادل با فضای حالات با انرژی مینیمم[۵] یک هامیلتونی جابجایی است.

مثال ۳: یک شبکه‌ی $L \times L$ در نظر بگیرید و روی هر یک از اضلاع شبکه یک کیوبیت قرار دهید. تعداد کوبیت‌ها برابر است با $n = 2L(L+1)$.



به ازای هر خانه از این شبکه یک ماتریس پاولی تعریف کنید که برابر حاصل‌ضرب Z روی چهار کیوبیت اطراف آن خانه است. همچنین به ازای هر راس از شبکه یک ماتریس پاولی تعریف کنید که برابر حاصل‌ضرب X روی کوبیت‌های اطراف آن راس است. توجه کنید تعداد این کیوبیت‌ها ممکن است $2, 3$ و یا 4 باشد. تعداد ماتریس‌های پاولی متناظر با خانه‌ها و

[۴] Graph code
[۵] Ground space

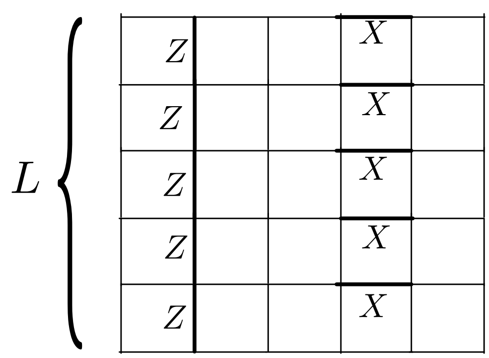
راس‌ها به ترتیب برابر L^2 و $(L+1)^2$ است. همچنین به راحتی قابل بررسی است که همه این $L^2+(L+1)^2$ ماتریس پاولی هرمیتی بوده و با هم جابجا می‌شوند. پس S را زیرگروه تولید شده توسط آنها بگیرید و کد P متناظر را تعریف کنید.

برای یافتن بعد فضای کد باید ببینیم چه تعداد از این $L^2+(L+1)^2$ مولد S مستقل هستند و یک مجموعه‌ی مولد مینیمال تشکیل می‌دهند. واضح است که مولدهای نوع X مستقل از مولدهای نوع Z هستند. همچنین Z-ها مستقل‌اند. ولی حاصل‌ضرب همه مول‌های نوع X برابر همانی است پس می‌توان یکی از آنها را حذف کرد. بنابراین تعداد مولدهای مستقل برابر است با $k = L^2+(L+1)^2-1$. پس بعد فضای کد می‌شود $2^{n-k}=1$. در نتیجه P یک بعدی است و متناظر با یک حالت.

مثال ۴: همان شبکه‌ی مثال قبل را در نظر بگیرید ولی این بار آن را شبکه‌ای روی چنبره در نظر بگیرید. یعنی اضلاع مقابل شبکه را با هم یکی کنید. پس تعداد کیوبیت‌ها در این حالت برابر است با $n = 2L(L+1) - 2L = 2L^2$. ماتریس‌های پاولی نوع X و Z را مانند حالت قبل تعریف کنید. حاصل‌ضرب همه مول‌های نوع X و همچنین حاصل‌ضرب همه مول‌های نوع Z برابر همانی است. پس دو عدد از این مولدها را می‌توان حذف کرد. تعداد مولدهای مستقل می‌شود $k = 2(L^2-1)$. بنابراین بعد فضای کد برابر است با $2^{n-k} = 2^2$. یعنی این کد که آن را کد چنبره‌ای[۶] می‌گویند، دو کیوبیت را کد می‌کند.

$$\dim N(W) = 2n - k = k + 2(n-k) = k + 4$$

یعنی $N(S)$ غیر از k مولد S دارای 4 مولد دیگر است. دو مولد از این چهار مولد در شکل زیر نمایش داده شده‌اند. دو مولد دیگر به همین صورت ولی در راستای افقی به دست می‌آیند.



این چهار مولد از ساختار گروه بنیادی چنبره به دست می‌آیند. از آنجا که گروه بنیادی صفحه بدیهی است، وقتی کد را روی چنبره در نظر گرفتیم فضای کد یک بعدی شد. در حالت کلی اگر همین کد را روی یک چنبره با ℓ سوراخ در نظر بگیریم فضای کد $2^{2\ell}$ بعدی می‌شود چون گروه بنیادی چنبره‌ی ℓ–سوراخه با 2ℓ مولد تولید می‌شود. چنین پدیده‌ای را نمی‌توان در ساختارهای کلاسیک مشاهده کرد.

[۶] Toric code