CSS коди. Реалізація кодування та вимірювань стабілізаторних кодів.

Лекція 12

2 травня 2023

CSS коди

CSS коди (Calderbank-Shor-Steane) це різновид стабілізаторних кодів, у яких провірочна матриця має вигляд

$$\left[\begin{array}{c|c} A & 0 \\ 0 & B \end{array}\right]$$

Іншими словами, це стабілізаторний код у якого частина генераторів складаються лише з генераторів типу

$$X_{i_1} \otimes X_{i_2} \otimes \cdots \otimes X_{i_k},$$

а інша частина з генераторів типу

$$Z_{j_1} \otimes Z_{j_2} \otimes \cdots \otimes Z_{j_l}.$$

Такі коди не є оптимальними (5-ти кубітний оптимальний код типу $[5, 1]$ не є CSS), але завдяки простоті конструкції мають інші переваги.
До того ж їх можна будувати із класичних лінійних кодів, коли A, B будуються по матрицям парності цих кодів.

Приклади CSS кодів

3х кубітний bit flip код можна розуміти як CSS код з наступними генераторами, логічними $\bar{X}, \bar{Z}$ та провірочною матрицею:

$$g_1 = \mathtt{ZZI}$$
$$g_2 = \mathtt{ZIZ}$$
$$\bar{Z} = \mathtt{ZII}$$
$$\bar{X} = \mathtt{XXX}$$

$$\left[\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

Оскільки g_1, g_2 стабілізують $\mathrm{span}\{|000\rangle, |111\rangle\}$ то це і буде підпростором, що стабілізується $\langle g_1, g_2\rangle$.
Стан $|000\rangle$ стабільний відносно $\bar{Z}$, тож він стабілізується $\langle g_1, g_2, \bar{Z}\rangle$. А $|111\rangle$ стабільний відносно $-\bar{Z}$, тож його код $\langle g_1, g_2, -\bar{Z}\rangle$.
Маємо, що $\bar{X}$ комутує з g_1, g_2 і антикомутує з $\bar{Z}$, тож при дії на стан з кодом $\langle g_1, g_2, \bar{Z}\rangle$ як раз вийде $\langle g_1, g_2, -\bar{Z}\rangle$.

Приклади CSS кодів

Відповідний 3х кубітний phase flip код так само CSS код, який можна зобразити як

$$
\begin{aligned}
g_1 &= \mathtt{XXI} \\
g_2 &= \mathtt{XIX} \\
\bar{Z} &= \mathtt{XII} \\
\bar{X} &= \mathtt{ZZZ}
\end{aligned}
\qquad
\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{array}\right]
$$

Тут g_1, g_2 стабілізують $\mathrm{span}\{|+++\rangle, |---\rangle\}$ а значить і $\langle g_1, g_2\rangle$ його стабілізує.
Стан $|+++\rangle$ стабільний відносно $\bar{Z}$, а значить має код $\langle g_1, g_2, \bar{Z}\rangle$. Відповідно $|---\rangle$ має код $\langle g_1, g_2, -\bar{Z}\rangle$.
Так само, $\bar{X}$ комутує з g_1, g_2 і антикомутує з $\bar{Z}$, тож

$$\bar{X}\,|0\rangle_L = \bar{X}\,|+++\rangle = |---\rangle = |1\rangle_L\,.$$

Приклади CSS кодів

9ти кубітний код Шора можна зобразити як

$$
\begin{aligned}
g_1 &= \mathtt{ZZIIIIIII} \\
g_2 &= \mathtt{ZIZIIIIII} \qquad & g_7 &= \mathtt{XXXXXXIII} \\
g_3 &= \mathtt{IIIZZIIII} & g_8 &= \mathtt{XXXIIIXXX} \\
g_4 &= \mathtt{IIIZIZIII} & \bar{Z} &= \mathtt{XXXXXXXXX} \\
g_5 &= \mathtt{IIIIIZZI} & \bar{X} &= \mathtt{ZZZZZZZZZ} \\
g_6 &= \mathtt{IIIIIZIZ}
\end{aligned}
$$

Видно, що $g_1, \ldots, g_6$ стабілізують стани

$$(|000\rangle + (-1)^{b_1}|111\rangle)(|000\rangle + (-1)^{b_2}|111\rangle)(|000\rangle + (-1)^{b_3}|111\rangle)$$

та їх лінійні комбінації, що дає простір розмірності 2^3.
Генератори g_7, g_8 залишають ті, в яких $b_1 = b_2 = b_3 \mod 2$.
$\bar{Z}$ стабілізує коли $b_i = 0$, а $-\bar{Z}$ коли $b_i = 1$.

7ми кубітний код Стейна

Код Стейна це CSS код типу $[7, 1]$ в якого провірочна матриця

$$\left[\begin{array}{c|c} A & 0 \\ 0 & A \end{array}\right], \quad \text{де} \quad A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix},$$

тобто $g_1 = \texttt{XIIXXIX}$, $g_4 = \texttt{ZIIZZIZ}$, ..., а логічні оператори

$$\bar{Z} = \texttt{ZZZZZZZ} \qquad \bar{X} = \texttt{XXXXXXX}$$

Група генераторів $\langle g_1, \ldots, g_6 \rangle$ стабілізує стани

$$\begin{aligned} |0\rangle_L = &\frac{1}{\sqrt{8}}(|0^7\rangle + g_1 |0^7\rangle + g_2 |0^7\rangle + g_3 |0^7\rangle + \\ &+ g_1 g_2 |0^7\rangle + g_1 g_3 |0^7\rangle + g_2 g_3 |0^7\rangle + g_1 g_2 g_3 |0^7\rangle) \end{aligned}$$

та

$$|1\rangle_L = \bar{X}|0\rangle_L$$

Знаходження стабільних підпросторів

Взагалі, якщо є скінченна група G порядку m, що складається з унітарних операторів, то

$$P = \frac{1}{m} \sum_{U \in G} U$$

буде проєктором на підпростір, який стабілізується усіма U. Зокрема, для будь-якого $|\psi\rangle$ вектор $P|\psi\rangle$ буде стабільним відносно всіх $U \in G$.
Для стабілізаторної підгрупи $\langle g_1, \ldots, g_k \rangle \subset \Pi^n$ виходить, що

$$P = \frac{1}{2^k} \sum_{b_1 \ldots b_k \in \mathbf{B}^k} \prod_{i=1}^{k} g_i^{b_i} = \frac{1}{2^k} \prod_{i=1}^{k} (I + g_i)$$

буде відповідним проєктором на стабілізаторний підпростір.

В попередньому прикладі $P|0^7\rangle$ буде стабільним вектором для $\langle g_1, \ldots, g_6, \bar{Z} \rangle$, але ж $g_i|0^7\rangle = |0^7\rangle$ при $i = 4, 5, 6$ та $\bar{Z}|0^7\rangle = |0^7\rangle$, тож якраз виходить та формула для $|0\rangle_L$.

Централізатор та нормалізатор у групі

Централізатором підмножини S в групі G називають підгрупу $\mathcal{Z}(S) \leqslant G$ таку, що для будь-якого $g \in \mathcal{Z}(S)$ виконується

$$\forall s \in S : \quad gsg^{-1} = s.$$

Нормалізатором підмножини S в групі G називають підгрупу $\mathcal{N}(S) \leqslant G$ таку, що для будь-якого $g \in \mathcal{N}(S)$ виконується

$$\forall s \in S : \quad gsg^{-1} \in S.$$

Очевидно, що

$$\mathcal{Z}(S) \leqslant \mathcal{N}(S) \leqslant G.$$

Наприклад, група Кліфорда є нормалізатором групи Паулі у групі всіх унітарних операторів.

Для стабілізаторної групи $S = \langle g_1, \ldots, g_k \rangle$ її централізатор та нормалізатор в групі Паулі Π^n співпадають і відіграють важливу роль.

Типи похибок відносно стабілізаторного коду

Нехай є стабілізаторна група $S = \langle g_1, \ldots, g_k \rangle \subset \Pi^n$.
Припустимо на стан $|\psi\rangle \in C(S)$, що стабільний відносно S, подіяла похибка $E \in \Pi^n$. Стан $E|\psi\rangle$ потрапить до підпростору стабільного відносно $\langle Eg_1E^\dagger, \ldots, Eg_kE^\dagger \rangle$.

Якщо E антикомутує з деякими g_i, то $E|\psi\rangle$ буде стабільним відносно $Eg_iE^\dagger = -g_i$. Тож синдромні вимірювання, що відповідають g_i, покажуть -1 і тоді можна застосувати операцію $R \in \Pi^n$, яка поверне $E|\psi\rangle$ у підпростір $C(S)$. В залежності від операції R логічне значення стану $RE|\psi\rangle$ може змінитися. Наприклад, у 3х кубітному біт-фліп коді може статися $E = X_1$. Для обидвох $R = X_1$ та $R = X_2X_3$ вийде $RE|\psi\rangle \in C(S)$, але у другому випадку логічний стан зміниться на протилежний (тобто подіє $\bar{X}$).

Загальний ідея - в якості R береться операція, яка діє на найменшу кількість кубітів (серед усіх R, що повертають $E|\psi\rangle$ у $C(S)$).

Типи похибок відносно стабілізаторного коду

Якщо похибка $E \in S$, то $E|\psi\rangle = |\psi\rangle$ і нічого виправляти не доведеться.
Якщо похибка $E \in \mathcal{N}(S)\backslash S$, то синдромні вимірювання нічого не покажуть, але знов таки, логічне значення стану $E|\psi\rangle$ може змінитися (наприклад, коли $E = XXX$ у біт-фліп коді).

Якщо є множина можливих похибок $\{E_i\} \subset \Pi^n$ (яку ми знаємо), то коректне виправлення можна або завжди зробити або ні. Наприклад, у біт-фліп коді множини похибок $\{X_1, X_2X_3\}$ чи $\{I, X_1X_2X_3\}$ виправити не можна - адже ми не зможемо відрізнити яка саме помилка сталася, а неправильне виправлення змінює логічний стан. А ось множина $\{I, X_1, X_2, X_3\}$ виправляється коректно.

Наступні умови є достатніми для того, щоб множину похибок $\{E_i\} \subset \Pi^n$ можна було завжди коректно виправляти:

$$E_j^\dagger E_k \notin \mathcal{N}(S)\backslash S.$$

Відстань стабілізаторного коду

Для оператору $E \in \Pi^n$ можна визначити вагу - це кількість кубітів, де E діє нетривіально. Наприклад, $E = X_1 Z_6 Y_2$ має вагу 3.

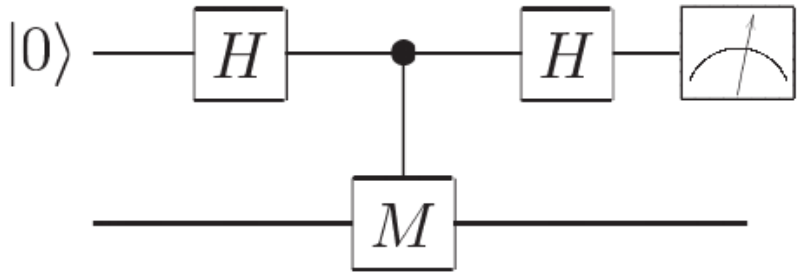
Відстанню d стабілізаторного коду S називають найменшу вагу елементу $E \in \mathcal{N}(S) \backslash S$. При цьому стабілізаторний код типу $[n, k]$ записують як $[n, k, d]$.

Не важко бачити, що якщо код має відстань $d = 2t + 1$, то множина похибок $\{E_i\} \subset \Pi^n$, де кожне E_i має вагу не більше за t, задовольняє достатнім умовам для коректного виправлення.

Реалізація вимірювань

Нехай ми маємо оператор $M \in \Pi^n$, $M^2 = I$, $M \neq I$. Йому відповідає розбиття простору в пряму ортогональну суму двох підпросторів, що є власними підпросторами для власних значень $+1$ та -1 оператора M. Як реалізувати відповідне вимірювання стану $|\psi\rangle$?

Це можна зробити наступною схемою:



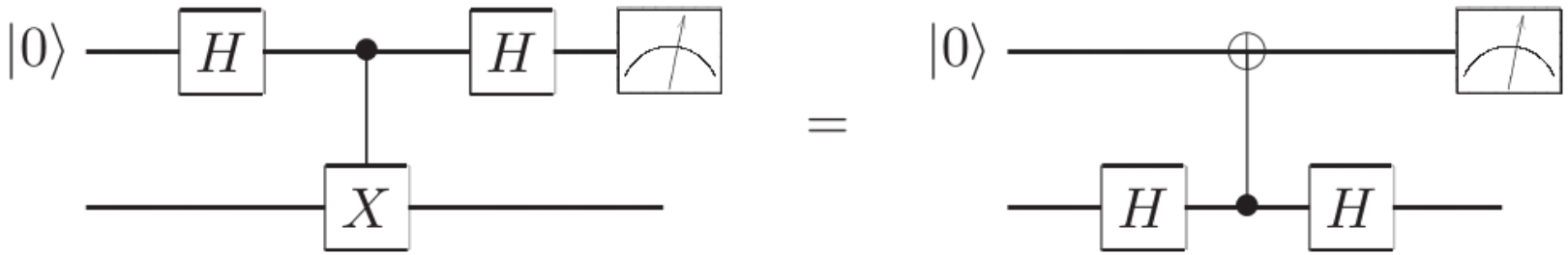
Як видно, результатом застосування схеми буде стан

$$(H \otimes I)\mathrm{C}(M)(H \otimes I)\,|0\rangle\,|\psi\rangle = (H \otimes I)\frac{1}{\sqrt{2}}(|0\rangle\,|\psi\rangle + |1\rangle\,M\,|\psi\rangle) =$$

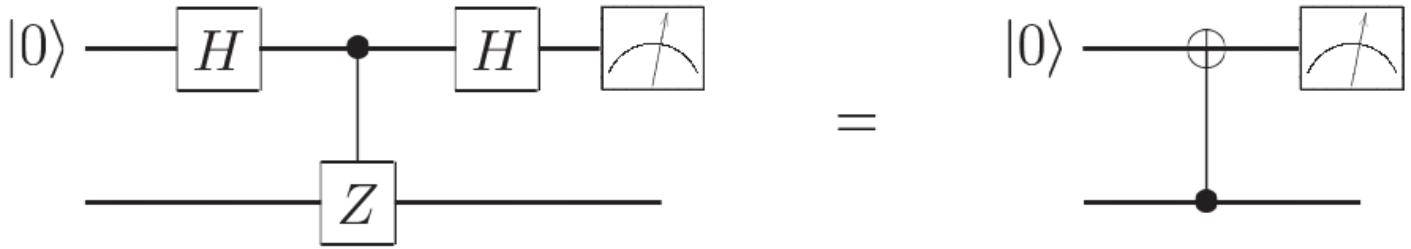
$$= \frac{1}{\sqrt{2}}(|+\rangle\,|\psi\rangle + |-\rangle\,M\,|\psi\rangle) = |0\rangle\,\frac{1}{2}(I+M)\,|\psi\rangle + |1\rangle\,\frac{1}{2}(I-M)\,|\psi\rangle\,.$$

Реалізація вимірювань

Наприклад, при $M = X$ схема буде



а при $M = Z$ буде



Реалізація вимірювань коду Стейна

Нагадаємо, що стандартна форма провірочної матриці коду має вигляд

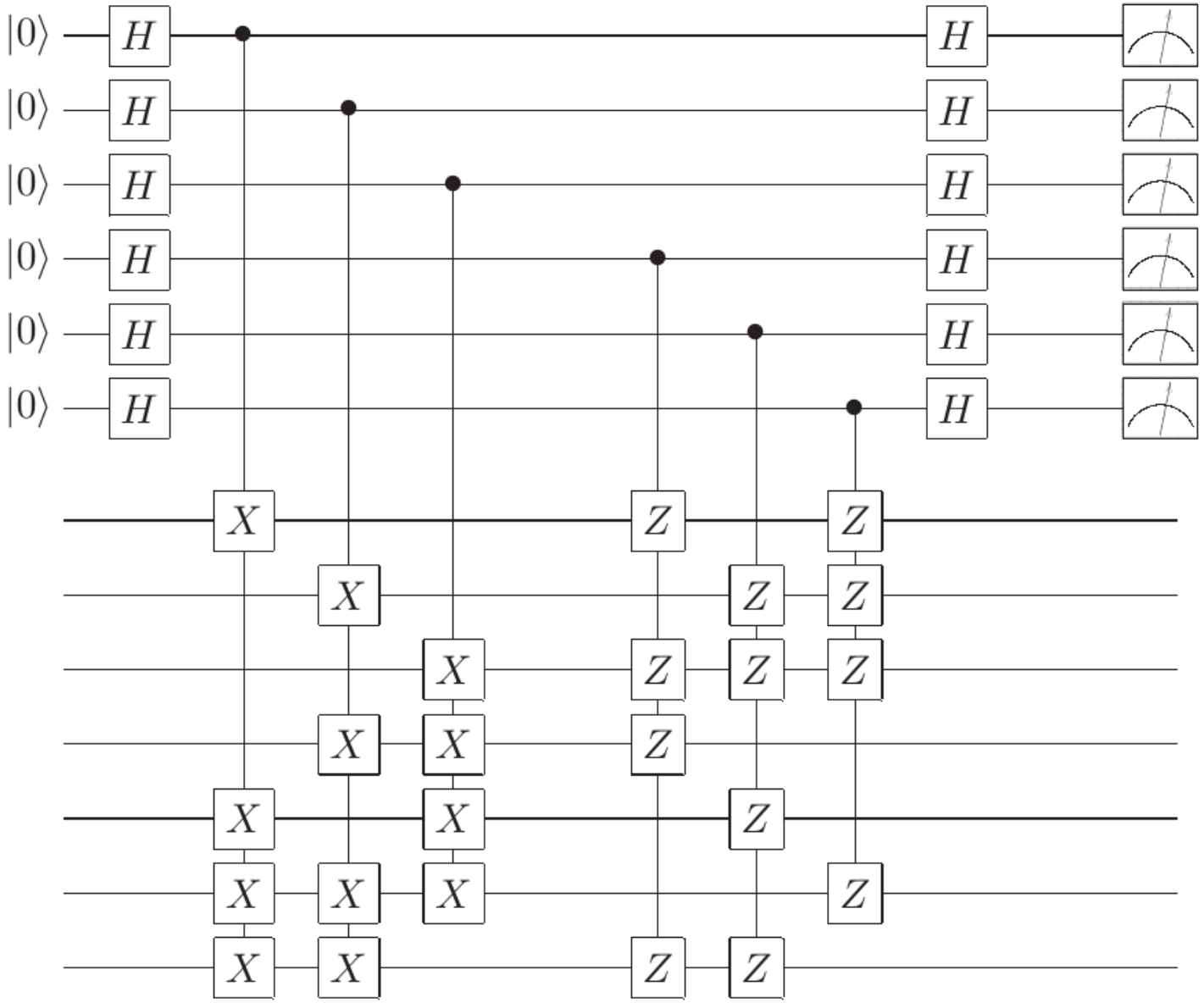
$$\begin{array}{r} \\ r\{ \\ n-k-r\{ \end{array} \left[\begin{array}{ccc|ccc} \overbrace{I}^{r} & \overbrace{A_1}^{n-k-r} & \overbrace{A_2}^{k} & \overbrace{B}^{r} & \overbrace{0}^{n-k-r} & \overbrace{C}^{k} \\ 0 & 0 & 0 & D & I & E \end{array}\right]$$

Після приведення до стандартної форми провірочна матриця коду Стейна буде, наприклад, така

$$\left[\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right]$$

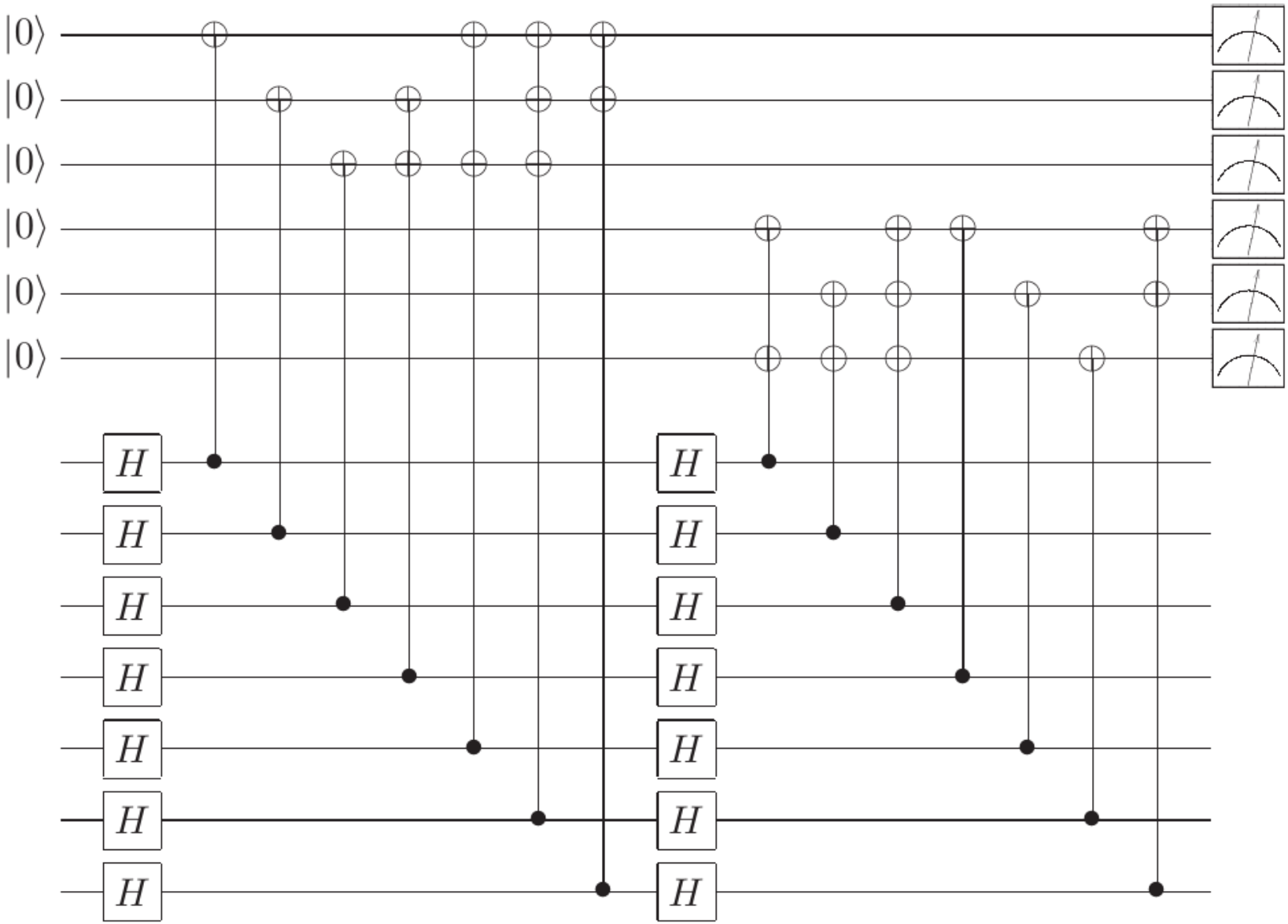
Реалізація вимірювань коду Стейна

Наступна схема реалізує синдромні вимірювання коду Стейна



Реалізація вимірювань коду Стейна

Схема, еквівалентна до попередньої:



Реалізація кодування

Нехай ми маємо стабілізаторний код $\langle g_1, \ldots, g_{n-k} \rangle \subset \Pi^n$, а також логічні $\bar{Z}_1, \ldots, \bar{Z}_k$ та $\bar{X}_1, \ldots, \bar{X}_k$. Нагадаємо, що для коду у стандартній формі їх можна взяти із матриць H та F:

$$H = \left[\begin{array}{ccc|ccc} 0 & 0 & 0 & A_2^T & 0 & I \end{array}\right],$$

$$F = \left[\begin{array}{ccc|ccc} 0 & E^T & I & C^T & 0 & 0 \end{array}\right].$$

Маємо, що

$$|b_1 \ldots b_k\rangle_L \leftrightarrow \langle g_1, \ldots, g_{n-k}, (-1)^{b_1}\bar{Z}_1, \ldots, (-1)^{b_k}\bar{Z}_k \rangle,$$

або ж

$$|b_1 \ldots b_k\rangle_L = \bar{X}_1^{b_1} \ldots \bar{X}_k^{b_k} |0 \ldots 0\rangle_L,$$

де

$$|0 \ldots 0\rangle_L \leftrightarrow \langle g_1, \ldots, g_{n-k}, \bar{Z}_1, \ldots, \bar{Z}_k \rangle.$$

Як реалізувати це кодування?

Реалізація кодування

Один із способів - це взяти довільний стан $|\psi\rangle$ (можна просто $|0^n\rangle$) і послідовно провести вимірювання $g_1, \ldots, g_{n-k}$ та $\bar{Z}_1, \ldots, \bar{Z}_k$.
Результатом буде послідовність з n значень ± 1, а $|\psi\rangle$ перейде у стабілізаторний стан із відповідним кодом

$$\langle \pm g_1, \ldots, \pm g_{n-k}, \pm \bar{Z}_1, \ldots, \pm \bar{Z}_k \rangle.$$

Якщо усі g_i зі знаками $+$, то отриманий стан буде відповідати якомусь

$$|b_1 \ldots b_k\rangle_L ,$$

який можна перевести у потрібний застосуваннями $\bar{X}_i$.

Реалізація кодування

Якщо деякі g_i зі знаками $-$, то отриманий стан буде відповідати якомусь

$$E\,|b_1 \dots b_k\rangle_L$$

де $E \in \Pi^n$ це похибка, що антикомутує з g_i де був $-$, та комутує з іншими g_i, де вимірювання показали $+$.

Тож щоб отримати $|b_1 \dots b_k\rangle_L$ достатньо зробити виправлення R для похибки E.

Для множини можливих похибок $\{E_j\} \subset \Pi^n$ ми можемо наперед порахувати синдроми, тобто для кожного E_j визначити для яких i є антикомутація $E_j g_i E_j^\dagger = -g_i$. Але це не може бути не достатньо ефективно.

По синдромам ± 1 існує ефективний спосіб визначення усіх $R \in \Pi^n$, таких що R антикомутує з відповідними g_i.

Ефективне знаходження виправлень по синдромам

Антикомутація між R та g_i еквівалентна тому, що

$$b(g_i)\begin{bmatrix}0 & I_n\\ I_n & 0\end{bmatrix}b(R)^T = 1 \mod 2,$$

а значить

$$G\begin{bmatrix}0 & I_n\\ I_n & 0\end{bmatrix}b(R)^T = (l_1,\ldots,l_{n-k})^T$$

де G це провірочна матриця для $\{g_1,\ldots,g_{n-k}\}$, а l_i дорівнює 1 якщо є антикомутація R з g_i, та 0 інакше.

Оскільки g_i незалежні, то $G\begin{bmatrix}0 & I_n\\ I_n & 0\end{bmatrix}$ має ранг $n-k$. А значить для будь-якого вектору $(l_1,\ldots,l_{n-k})^T$ можна знайти прообраз v, тобто

$$G\begin{bmatrix}0 & I_n\\ I_n & 0\end{bmatrix}v = (l_1,\ldots,l_{n-k})^T.$$

Тож в якості R можна взяти таке, що $b(R) = v^T$. Загалом, цей спосіб дає всі шукані R при переборі прообразів v.

Знаходження нормалізатору $\mathcal{N}(S)$

Точно такий же прийом працює і для знаходження $\mathcal{N}(S) = \mathcal{Z}(S)$ стабілізаторного коду $S = \langle g_1, \ldots, g_{n-k} \rangle$.

Усі оператори $M \in \mathcal{N}(S)$ знаходяться із

$$G \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} v = (0, \ldots, 0)^T,$$

$$b(M) = v^T.$$

Насправді, не важко показати, що якщо відомі $\bar{Z}_1, \ldots, \bar{Z}_k$, $\bar{X}_1, \ldots, \bar{X}_k$ для коду S, то разом з g_i вони в точності породжують $\mathcal{N}(S)$:

$$\mathcal{N}(S) = \langle g_1, \ldots, g_{n-k}, \bar{Z}_1, \ldots, \bar{Z}_k, \bar{X}_1, \ldots, \bar{X}_k \rangle.$$

Завдання

1. Для коду Стейна записаного у вигляді

$$g_1 = \mathtt{IIIXXXX} \qquad g_4 = \mathtt{IIIZZZZ}$$
$$g_2 = \mathtt{IXXIIXX} \qquad g_5 = \mathtt{IZZIIZZ}$$
$$g_3 = \mathtt{XIXIXIX} \qquad g_6 = \mathtt{ZIZIZIZ}$$

$$\bar{Z} = \mathtt{ZZZZZZZ} \qquad \bar{X} = \mathtt{XXXXXXX}$$

перевірити, що у загальному елементі $g = g_1^{b_1} \dots g_6^{b_6}$ групи $S = \langle g_1, \dots, g_6 \rangle$ будуть присутні або 4 X та 3 I, або 4 Z та 3 I, або 4 Y та 3 I, або 2 X та 2 Z та 2 Y та 1 I (без урахування фаз). На основі цього знайти відстань цього коду.
2. Пояснити, чому відстань торичного коду на $2n^2$ кубітах буде не більша за n (насправді ж вона дорівнює n).