Стабілізаторний формалізм

Лекція 10

11 квітня 2023

Стабілізаторний формалізм

Більшість винайдених кодів для корекції квантових похибок можна описати за допомогою мови, яку називають стабілізаторним формалізмом. В ній існують три основні поняття:

- Стабілізаторна група
- Стабілізаторні стани та підпростори станів
- Стабілізаторні гейти та схеми, що з них складаються

U-стабільний вектор та підпростір

Будемо казати, що унітарний оператор U є стабілізатором для $|\psi\rangle$, якщо $U|\psi\rangle = |\psi\rangle$. Іншими словами, $|\psi\rangle$ є власним вектором U із власним значенням 1.

При цьому кажуть, що $|\psi\rangle$ є стабільним відносно U, або ж U-стабільним. Зрозуміло, що будь-яка лінійна комбінація стабільних векторів є стабільним вектором відносно U.

Підпростір зі стабільних векторів U називають стабільним відносно U. Тобто це підпростір векторів, що відповідають власному значенню 1 оператора U.
Зрозуміло, що він буде також стабільним і для U^{-1}.

Стабілізаторна група

Для двох операторів U та V одночасно стабільним є підпростір, що є перетином стабільних підпросторів для U та для V. Цей перетин також є стабільним і для добутків UV, VU.

Загалом, якщо $|\psi\rangle$ стабільний відносно $U_1, U_2, \ldots, U_k$, то він стабільний і відносно групи $G = \langle U_1, U_2, \ldots, U_k \rangle$, що ними породжена. В такому випадку будемо казати, $|\psi\rangle$ є G-стабільним.

Зауважимо, що якщо U та V антикомутують, тобто $UV = -VU$, то така пара немає одночасно стабільних векторів.

Стабілізаторна група для стану Бела

Наприклад, розглянемо стан Бела

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Він стабілізується операторами $X \otimes X$, $Z \otimes Z$ (а значить і групою, що ними породжена).
З іншого боку, перетин стабільних підпросторів для цих двох операторів має розмірність 1. Тож стабільний стан для обох операторів єдиний з точністю до глобальної фази.

Загальна ідея стабілізаторного формалізму – кодувати (математично) стан за допомогою групи операторів, що його стабілізують. Але робиться це для операторів спеціального виду.

Група Паулі

Матриці Паулі

$$I = \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; X = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$Y = \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; Z = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

за операцією множення породжують підгрупу унітарних матриць, яку називають *групою Паулі*.

Вона складається з 16-ти елементів:

$$\Pi = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} =$$

$$\{e^{ik\pi/2}\sigma_l \mid k, l \in \{0, 1, 2, 3\}\}.$$

n-арна група Паулі

Для n кубітів *n-арною групою Паулі* називають підгрупу унітарних матриць, яка складається з усіх можливих n-арних тензорних добутків матриць Паулі. Вона складається з матриць

$$\Pi^n = \{e^{ik\pi/2} A_1 \otimes A_2 \otimes \cdots \otimes A_n \mid k \in \{0,1,2,3\}, A_j \in \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}\}$$

і має порядок 4^{n+1}.

Кожна матриця типу $A = A_1 \otimes A_2 \otimes \cdots \otimes A_n$ має рівно 2 власні значення ± 1, кратності 2^{n-1} кожне (окрім тривіального випадку $A = I$).

Будь-які дві матриці $M, N \in \Pi^n$ або комутують, або антикомутують, тобто $MN = NM$ або $MN = -NM$.

Стабілізаторні підгрупи n-арної групи Паулі

Нехай підгрупа $G \subset \Pi^n$ породжена k операторами, тобто

$$G = \langle g_1, g_2, \ldots, g_k \rangle.$$

Причому,

1. g_i попарно комутують
2. $-I \notin G$ (що еквівалентно тому, що $\forall i \;\; g_i^2 = I, g_i \neq -I$)
3. усі g_i незалежні, тобто підгрупа G не може бути породжена меншою підмножиною $\{g_i\}$

Тоді

1. G абелева (будь-які 2 елементи комутують)
2. G має порядок 2^k (загальний елемент має вигляд $g_1^{b_1} g_2^{b_2} \ldots g_k^{b_k}$, $b_i \in \mathbf{B}$)
3. G стабілізує підпростір розмірності 2^{n-k}, якому відповідає проектор

$$\frac{1}{2^k} \prod_{i=1}^{k} (I + g_i).$$

Стабілізаторний код та стани

Таку підгрупу з її стабілізаторним підпростором називають **стабілізаторним кодом** типу $[n, n-k]$.

Оскільки стабілізаторний підпростір має розмірність 2^{n-k}, то його можна ототожнити із простором станів квантової системи, що складається з $n-k$ кубітів.

У випадку, коли $k = n$, стабілізаторний підпростір буде мати розмірність 1, тож він породжений єдиним станом. Усі стани такого типу називають **стабілізаторними станами**.

Кодування стабілізаторного підпростору

Нехай $G \subset \Pi^n$ це стабілізаторна підгрупа. Тоді існують оператори $h_1, h_2, \ldots, h_{n-k} \in \Pi^n$ такі, що

$$\{g_1, g_2, \ldots, g_k, h_1, h_2, \ldots, h_{n-k}\}$$

– незалежні, комутують та не породжують $-I$.
Більше того, для будь-яких $b_i \in \mathbf{B}$ оператори

$$\{g_1, g_2, \ldots, g_k, (-1)^{b_1} h_1, (-1)^{b_2} h_2, \ldots, (-1)^{b_{n-k}} h_{n-k}\}$$

мають такі ж властивості. Стабілізаторний стан для підгрупи, що породжена таким набором, будемо позначати як

$$|b_1 b_2 \ldots b_{n-k}\rangle_L$$

Ці 2^{n-k} стабілізаторних станів є базисом стабілізаторного простору для G.

Приклад стабілізаторного кодування

Згадаємо, що у 3-х кубітному bit flip коді $|0\rangle \to |000\rangle$, $|1\rangle \to |111\rangle$. Позначимо

$$g_1 = Z_1 Z_2 = Z \otimes Z \otimes I, \qquad g_2 = Z_2 Z_3 = I \otimes Z \otimes Z.$$

Тоді для $G = \langle g_1, g_2 \rangle$ стабілізаторний підпростір як раз буде співпадати зі $\mathrm{span}\{|000\rangle, |111\rangle\}$. В якості h_1 можна взяти $Z_1 = Z \otimes I \otimes I$. Тоді $|000\rangle$ це стабілізаторний стан для

$$\langle Z_1 Z_2, Z_2 Z_3, Z_1 \rangle = \langle Z_1, Z_2, Z_3 \rangle,$$

а $|111\rangle$ це стабілізаторний стан для

$$\langle Z_1 Z_2, Z_2 Z_3, -Z_1 \rangle = \langle -Z_1, -Z_2, -Z_3 \rangle.$$

Також використовують наступний запис для цього коду:

$$ZZI$$
$$IZZ$$
$$\pm ZII$$

Дія гейтів

Нехай підгрупа $G \subset \Pi^n$ стабілізує підпростір V_G. Тобто для $\forall g \in G, \forall \left|\psi\right\rangle \in V_G : \; g\left|\psi\right\rangle = \left|\psi\right\rangle$. І нехай U це будь-який унітарний оператор. Тоді

$$UgU^\dagger U\left|\psi\right\rangle = U\left|\psi\right\rangle.$$

Це означає, що $U\left|\psi\right\rangle$ стабілізується $UgU^\dagger$. А значить і весь підпростір $U(V_G)$ стабілізується спряженою підгрупою $UGU^\dagger := \{UgU^\dagger \mid g \in G\}$. Зокрема, якщо $G = \langle g_1, \ldots, g_k \rangle$, то $UGU^\dagger = \langle Ug_1U^\dagger, \ldots, Ug_kU^\dagger \rangle$. Тобто підпростір $U(V_G)$ можна закодувати набором стабілізаторів $\{Ug_1U^\dagger, \ldots, Ug_kU^\dagger\}$.

Якщо $U \in \Pi^n$, то $UGU^\dagger \subset \Pi^n$, тобто підгрупа буде такого самого типу. Це, зокрема, означає, що стабілізаторний стан перейде у стабілізаторний стан під дією U.

Група Кліфорда

Але існують й інші оператори U, які зберігають групу Паулі при дії спряженням. Нагадаємо, що

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \; S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

Виконуються наступні рівності:

$$HXH = Z, \; HYH = -Y, \; HZH = X,$$

$$SXS^\dagger = Y, \; SYS^\dagger = -X, \; SZS^\dagger = Z.$$

До того ж, операція CX (CNOT) також зберігає групу Паулі:

$$CX \cdot (X \otimes I) \cdot CX = X \otimes X, \quad CX \cdot (I \otimes X) \cdot CX = I \otimes X,$$

$$CX \cdot (Z \otimes I) \cdot CX = Z \otimes I, \quad CX \cdot (I \otimes Z) \cdot CX = Z \otimes Z.$$

Група Кліфорда

Унітарні операції, які зберігають n-арну групу Паулі при дії спряженням, утворюють групу, яку називають **групою Кліфорда**.

Групу Кліфорда можна породити лише операціями $H, S, CNOT$. Елементи групи Кліфорда називають **стабілізаторними гейтами**, а схеми з них – **стабілізаторними схемами**.

Теорема
Будь-який стабілізаторний стан можна отримати з $|00\ldots0\rangle$ дією якогось стабілізаторного гейту.

Дія вимірювань

Нехай $|\psi\rangle$ це стабілізаторний стан, що має код $\langle g_1, \ldots, g_n \rangle$. Нехай $g \in \Pi^n$, $g^2 = I$, яке ми будемо розуміти як таке, що задає вимірювання (воно розбиває простір в пряму суму двох власних просторів з власними значеннями $+1, -1$).

Який буде результат вимірювання та новий стан після нього?

Можливі два випадки

1. g комутує з усіма g_i
2. g антикомутує з деякими g_i

Розберемо їх.

Дія вимірювань

В першому випадку виходить, що або g або $-g$ стабілізують $|\psi\rangle$. Дійсно, маємо $g_i g\,|\psi\rangle = g g_i\,|\psi\rangle = g\,|\psi\rangle$. Тож $g\,|\psi\rangle$ належить до стабілізаційного підпростору коду $\langle g_1, \ldots, g_n\rangle$, тобто до $\mathrm{span}\{|\psi\rangle\}$. А значить $g\,|\psi\rangle = \lambda\,|\psi\rangle = \pm\,|\psi\rangle$.

Це означає, що при $g\,|\psi\rangle = |\psi\rangle$ результатом вимірювання буде мітка $+1$ з ймовірністю 1, а при $g\,|\psi\rangle = -\,|\psi\rangle$ буде мітка -1 з ймовірністю 1. При цьому новий стан залишиться таким самим.

Дія вимірювань, випадок 2

Другий випадок можна звести до такого, в якому g антикомутує з g_1 та комутує з усіма іншими, за допомогою зміни генераторів коду. Наприклад, якщо g також антикомутує з g_2, то g буде комутувати з $g_1 g_2$. Ми тоді просто замінюємо генератор g_2 на $g_1 g_2$ у коді.

Дія вимірювань, випадок 2

Проектори, що відповідають вимірюванню g, можна записати як $P_+ = (I + g)/2$, $P_- = (I - g)/2$. Для ймовірностей будемо мати

$$p_+ = \langle\psi| \left(I + g\right)/2) \left|\psi\right\rangle, \quad p_- = \langle\psi| \left(I - g\right)/2) \left|\psi\right\rangle.$$

Оскільки $g_1 \left|\psi\right\rangle = \left|\psi\right\rangle$ та $g_1 g = -g g_1$, то

$$\langle\psi| g_1 (I - g)/2) g_1 \left|\psi\right\rangle = \langle\psi| \left(I + g\right)/2) \left|\psi\right\rangle.$$

Тобто $p_- = p_+$, а значить вони дорівнюють по $1/2$.
Новим станом після вимірювання буде $\left|\psi_\pm\right\rangle = \frac{1}{\sqrt{2}}(I \pm g) \left|\psi\right\rangle$.
Не важко бачити, що стабілізаційним кодом для $\left|\psi_+\right\rangle$ буде $\langle +g, g_2, \ldots, g_n\rangle$, а для $\left|\psi_-\right\rangle$ буде $\langle -g, g_2, \ldots, g_n\rangle$.

Відстеження та виправлення похибок

Нехай $G = \langle g_1, \ldots, g_k \rangle \subset \Pi^n$ це якійсь стабілізаційний код типу $[n, n-k]$. Він задає підпростір V_G розмірності 2^{n-k}.

Припустимо, що на елемент $|\psi\rangle \in V_G$ подіяла якась похибка $e \in \Pi^n$, тобто $|\psi\rangle$ перейшов у стан $e|\psi\rangle$.

Коли і яким чином її можна відстежити і виправити?

Ясно, що якщо $e \in G$, то виправляти нічого не доведеться.

Відстеження та виправлення похибок

Якщо e антикомутує з деякими g_i (тобто $eg_ie^\dagger = -g_i$), то $e\,|\psi\rangle$ потрапить до підпростору $e(V_G)$, код якого буде мати тип $\langle \pm g_1, \pm g_2, \ldots, \pm g_k \rangle$.

Щоб визначити таку помилку проведемо k вимірювань, що відповідають $g_1, g_2, \ldots, g_k$. Вони дадуть нам k значень ± 1 (і при цьому не змінять стан $e\,|\psi\rangle$). По цим значенням ми знаходимо помилку і робимо відновлення.

Множина похибок, що виправляються

Проблемними є похибки $e \in \Pi^n$ такі, що e комутує з усіма g_i (тобто e належить нормалізатору $N(G)$), але $e \notin G$. Таку множину позначають як $N(G)\backslash G$. Вважатимемо, що такі похибки ми виправляти не можемо для коду G.
Загалом, маємо наступну основну теорему

Теорема
Нехай ми маємо код $G = \langle g_1, \ldots, g_k \rangle \subset \Pi^n$. Припустимо, що $e_1, \ldots, e_m \in \Pi^n$ такі, що $e_k^\dagger e_j \notin N(G)\backslash G$ для будь-яких k, j. Тоді множина $\{e_1, \ldots, e_m\}$ є множиною похибок, що виправляються кодом G.

Приклад

Повернемося до прикладу bit flip коду, що заданий $G = \langle g_1, g_2 \rangle = \langle Z_1 Z_2, Z_2 Z_3 \rangle$. Для цього коду множина помилок $\{I, X_1, X_2, X_3\}$ є множиною похибок, що ним виправляються. Адже їх попарні добутки антикомутують або з $g_1 = Z_1 Z_2$ або з $g_2 = Z_2 Z_3$.

Наприклад, для X_1 маємо $X_1 g_1 X_1 = -g_1$, $X_1 g_2 X_1 = g_2$. Тож при такій похибці стабілізатор перейде у $\langle -Z_1 Z_2, Z_2 Z_3 \rangle$.

Синдромні вимірювання, що відповідають g_1, g_2, при цьому дадуть $-1, +1$. Для X_2 синдром буде $-1, -1$, а для X_3 буде $+1, -1$.

По синдрому застосовуємо обернену операцію похибки для виправлення. Якщо синдром для двох похибок однаковий, то можна використати будь-яку з них для випаравлення.

5-кубітний оптимальний код виправлення однокубітної помилки

Оптимальний код для виправлення будь-якої однокубітної помилки виглядає як

$$
\begin{aligned}
&XZZXI\\
&IXZZX\\
&XIXZZ\\
&ZXIXZ\\
\pm&ZZZZZ
\end{aligned}
$$

де $\bar{X} = XXXXX$, $\bar{Z} = ZZZZZ$ – це логічні X та Z.

5-кубітний оптимальний код виправлення однокубітної помилки

Таблиця синдромів для нього це

X_1	0001	Z_1	1010	Y_1	1011
X_2	1000	Z_2	0101	Y_2	1101
X_3	1100	Z_3	0010	Y_3	1110
X_4	0110	Z_4	1001	Y_4	1111
X_5	0011	Z_5	0100	Y_5	0111

Більш детально див. `https://en.wikipedia.org/wiki/Five-qubit_error_correcting_code`

Завдання

1. Визначити стабілізаторний стан $|\psi\rangle$ на трьох кубітах, що відповідає

$$G = \langle g_1, g_2, g_3 \rangle = \langle Y_1, X_2X_3, Z_2Z_3 \rangle;$$

2. для $H_1H_2 |\psi\rangle = (H \otimes H \otimes I) |\psi\rangle$ навести його код G';
3. по коду G' визначити результат вимірювання, що відповідає $g = Y_1$.