Реалізації логічних гейтів. Відмовостійкі квантові обчислення.

Лекція 13

16 травня 2023

Реалізація логічних гейтів для коду Стіні

Нагадаємо, що код Стіні задається як

$$g_1 = \mathtt{IIIXXXX} \qquad g_4 = \mathtt{IIIZZZZ}$$
$$g_2 = \mathtt{IXXIIXX} \qquad g_5 = \mathtt{IZZIIZZ}$$
$$g_3 = \mathtt{XIXIXIX} \qquad g_6 = \mathtt{ZIZIZIZ}$$
$$\bar{Z} = \mathtt{ZZZZZZZ} \qquad \bar{X} = \mathtt{XXXXXXX}$$

В цьому коді логічні $\bar{X}$ та $\bar{Z}$ мають дуже просту форму, кожне складається з 7ми однокубітних операції.
А як реалізувати усі інші логічні операції, зокрема мільтикубітні, до того ж такі, які діють на блоках із кубітів (в кожному блоці по 7 кубітів)?
Як відомо, будь-яку квантову операцію можна реалізувати як комбінацію CNOT та однокубітних гейтів. В свою чергу, однокубітни гейти можна апроксимувати комбінацією H та $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$. Якщо ж нас цікавить лише група Кліфорда, то достатньо вміти реалізовувати CNOT, H та $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

Реалізація логічних гейтів для коду Стіні

В якості логічного H можна взяти $\bar{H} = H_1 H_2 H_3 H_4 H_5 H_6 H_7$.
Не важко бачити, що

$$\bar{H}\bar{Z}\bar{H}^\dagger = \bar{X}, \quad \bar{H}\bar{X}\bar{H}^\dagger = \bar{Z},$$

тобто виконуються співвідношення як і для звичайних H, X, Z.

Цієї властивості достатньо для того, щоб з точністю до глобальної фази $\bar{H}$ діяв як логічний H, тобто виконувалося

$$\bar{H}(a\,|0\rangle_L + b\,|1\rangle_L) = e^{i\theta}\left(\frac{a+b}{\sqrt{2}}\,|0\rangle_L + \frac{a-b}{\sqrt{2}}\,|1\rangle_L\right).$$

(Існують різні реалізації логічних гейтів, наприклад, $g_5 H_1 H_2 H_3 H_4 H_5 H_6 H_7$ теж реалізує логічний H.)

Реалізація логічних гейтів для коду Стіні

Дійсно, нехай операція U діє на 7ми кубітах коду, не змінює його стабілізаторний підпростір $C(S) = \mathrm{span}\{|0\rangle_L, |1\rangle_L\}$, тобто

$$U(\mathrm{span}\{|0\rangle_L, |1\rangle_L\}) = \mathrm{span}\{|0\rangle_L, |1\rangle_L\},$$

(що те саме, що U комутує з проектором $\prod_i (I + g_i)/2$), і при цьому виконується

$$U\bar{Z}U^\dagger = \bar{X}, \quad U\bar{X}U^\dagger = \bar{Z}.$$

Оскільки $|0_L\rangle\langle 0_L| = (I + \bar{Z})/2 \prod_{i=1}^{6} (I + g_i)/2$, то виходить

$$U|0_L\rangle\langle 0_L|U^\dagger = U(I + \bar{Z})/2U^\dagger \prod_{i=1}^{6} (I + g_i)/2 =$$

$$= (I + \bar{X})/2 \prod_{i=1}^{6} (I + g_i)/2 = |+_L\rangle\langle +_L|.$$

Реалізація логічних гейтів для коду Стіні

Використовуючи аналогічний прийом загалом отримуємо

$$U|0_L\rangle\langle 0_L|U^\dagger = |+_L\rangle\langle +_L|, \quad U|1_L\rangle\langle 1_L|U^\dagger = |-_L\rangle\langle -_L|,$$
$$U|+_L\rangle\langle +_L|U^\dagger = |0_L\rangle\langle 0_L|, \quad U|-_L\rangle\langle -_L|U^\dagger = |1_L\rangle\langle 1_L|.$$

Цих рівностей достатньо для того, щоб однозначно визначити дію U на підпросторі $C(S)$ з точністю до глобальної фази, адже матриці $|0_L\rangle\langle 0_L|$, $|1_L\rangle\langle 1_L|$, $|+_L\rangle\langle +_L|$, $|-_L\rangle\langle -_L|$ утворюють лінійний базис для усіх матриць на $C(S)$.
Нарешті, зрозуміло, що дія

$$|0_L\rangle \longrightarrow |+_L\rangle, \quad |1_L\rangle \longrightarrow |-_L\rangle$$
$$|+_L\rangle \longrightarrow |0_L\rangle, \quad |-_L\rangle \longrightarrow |1_L\rangle$$

підходить як розв'язок для U. Значить така дія на підпросторі $C(S)$ існує єдина з точністю до глобальної фази.
Альтернативно це можна довести використовуючи те, що операція спряження є лінійним відображенням на просторі матриць.

Реалізація логічних гейтів

Попереднє твердження можна узагальнити. Нехай є стабілізаторний код $S = \langle g_1, \ldots, g_{n-k} \rangle$ типу $[n, k]$.
Нехай ми маємо операцію U, що діє на k кубітах.
Для $l = 1, \ldots, k$ позначимо

$$UX_lU^\dagger = U_{X_l}, \quad UZ_lU^\dagger = U_{Z_l}.$$

Припустимо ми знайшли логічні версії $\bar{X}_l$, $\bar{Z}_l$, $\bar{U}_{X_l}$, $\bar{U}_{Z_l}$, що діють на n кубітах, для всіх l.

Тоді, якщо для операції $\bar{U}$, яка діє на n кубітах і не змінює підпротір $C(S)$ коду, по всім l виконується

$$\bar{U}\bar{X}_l\bar{U}^\dagger = \bar{U}_{X_l}, \quad \bar{U}\bar{Z}_l\bar{U}^\dagger = \bar{U}_{Z_l},$$

то $\bar{U}$ є логічною версією U (з точністю до глобальної фази), тобто дія $\bar{U}$ на $C(S) = \mathrm{span}\{|0_L\rangle, \ldots, |k_L\rangle\}$ відповідає дії U на $\mathrm{span}\{|0\rangle, \ldots, |k\rangle\}$.

Реалізація логічних гейтів для коду Стіні

Наприклад, розглянемо гейт $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. Маємо що

$$SZS^\dagger = Z, \quad SXS^\dagger = Y = iXZ.$$

В кодуванні Стіні розглянемо $\bar{U} = S_1 S_2 S_3 S_4 S_5 S_6 S_7$. Будемо мати

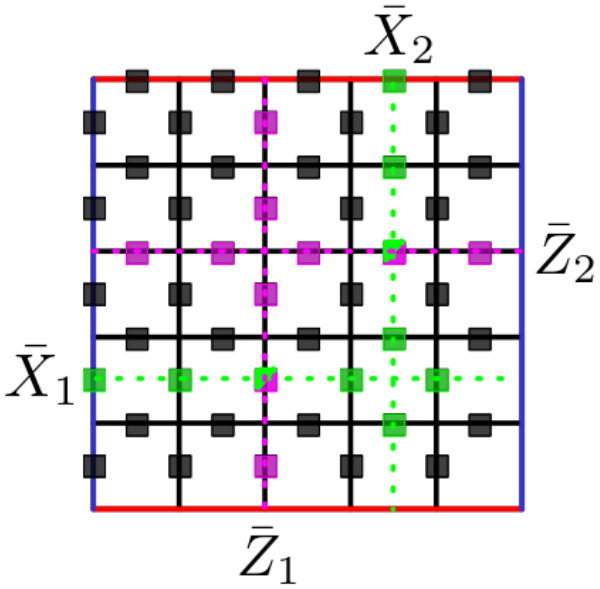
$$\bar{U}\bar{Z}\bar{U}^\dagger = \bar{Z}, \quad \bar{U}\bar{X}\bar{U}^\dagger = Y_1 Y_2 Y_3 Y_4 Y_5 Y_6 Y_7 = i^7 \bar{X}\bar{Z} = -i\bar{X}\bar{Z}.$$

Видно, що таке $\bar{U}$ не зовсім підходить на роль логічного S. Але це не складно виправити. Достатньо взяти

$$\bar{S} = \bar{Z}\bar{U} = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7 S_1 S_2 S_3 S_4 S_5 S_6 S_7.$$

CNOT для одного блоку торичного коду

Нагадаємо, що кодування логічних X, Z та кубітів в торичному коді відбувається за правилом



$$|00\rangle_L \leftrightarrow \langle \{A_s\}', \{B_t\}', \bar{Z}_1, \bar{Z}_2 \rangle,$$

$$|01\rangle_L \leftrightarrow \langle \{A_s\}', \{B_t\}', \bar{Z}_1, -\bar{Z}_2 \rangle,$$

$$|10\rangle_L \leftrightarrow \langle \{A_s\}', \{B_t\}', -\bar{Z}_1, \bar{Z}_2 \rangle,$$

$$|11\rangle_L \leftrightarrow \langle \{A_s\}', \{B_t\}', -\bar{Z}_1, -\bar{Z}_2 \rangle.$$

А операцію $\mathrm{CNOT} = \mathrm{CX}$ можна визначити з рівнянь

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

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

CNOT для одного блоку торичного коду

Тож для знаходження логічного CNOT, що діє на логічних кубітах з одного блоку, потрібно знайти $\bar{U}$, що зберігає стабілізаторний підпростір коду та виконується

$$\bar{U}\bar{X}_1\bar{U}^\dagger = \bar{X}_1\bar{X}_2, \quad \bar{U}\bar{X}_2\bar{U}^\dagger = \bar{X}_2,$$
$$\bar{U}\bar{Z}_1\bar{U}^\dagger = \bar{Z}_1, \quad \bar{U}\bar{Z}_2\bar{U}^\dagger = \bar{Z}_1\bar{Z}_2.$$

Еквівалентно, має виконуватися

$$\bar{U}\,|00\rangle_L = |00\rangle_L\,, \quad \bar{U}\,|01\rangle_L = |01\rangle_L\,,$$
$$\bar{U}\,|10\rangle_L = |11\rangle_L\,, \quad \bar{U}\,|11\rangle_L = |10\rangle_L\,.$$

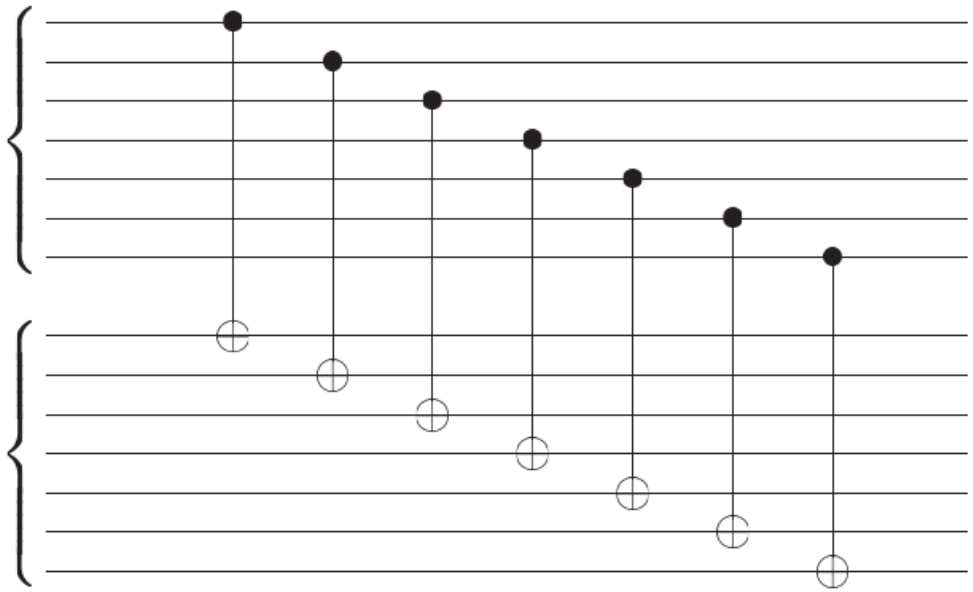
(Тут таке $\bar{U}$ будується нетривіально за допомогою так званих lattice surgery і наведено лише для прикладу.)

CNOT між блоками коду Стіні

В багатьох випадках реалізувати CNOT, що діє між логічним кубітом з одного закодованого блоку, і кубітом з іншого блоку набагато простіше.

Наприклад, нехай є блок A з семи кубітів, що кодують один логічний кубіт $|\phi_L\rangle_1$ кодом Стіні, і блок B з інших семи кубітів, що кодують інший логічний кубіт $|\psi_L\rangle_2$.

Для реалізації логічного $\overline{CNOT}_{A,B}$ достатньо застосувати $CNOT_{A_i,B_i}$ для кожної пари кубітів де A_i це i-й кубіт з першого блоку, а B_i це i-й кубіт з другого.



CNOT між блоками коду Стіні

Дійсно, виходить що

$$\overline{CNOT}_{A,B} \cdot \bar{X}_A \otimes I_B \cdot \overline{CNOT}_{A,B} =$$

$$= \prod_{i=1}^{7} CNOT_{A_i,B_i} \cdot \Big(\prod_{i=1}^{7} (X_{A_i} \otimes I_{B_i}) \Big) \cdot \prod_{i=1}^{7} CNOT_{A_i,B_i}$$

$$= \prod_{i=1}^{7} (X_{A_i} \otimes X_{B_i}) = \bar{X}_A \otimes \bar{X}_B.$$

Аналогічно, матимемо

$$\overline{CNOT}_{A,B} \cdot I_A \otimes \bar{X}_B \cdot \overline{CNOT}_{A,B} = I_A \otimes \bar{X}_B,$$

$$\overline{CNOT}_{A,B} \cdot \bar{Z}_A \otimes I_B \cdot \overline{CNOT}_{A,B} = \bar{Z}_A \otimes I_B,$$

$$\overline{CNOT}_{A,B} \cdot I_A \otimes \bar{Z}_B \cdot \overline{CNOT}_{A,B} = \bar{Z}_A \otimes \bar{Z}_B.$$

CNOT між блоками коду Стіні

Поглянемо на 14 кубітів, що розділені на 2 блоки по 7. Тоді код

$$S \otimes S = \langle \{g_i \otimes I_B\}_{i=1}^{6} \cup \{I_A \otimes g_j\}_{j=1}^{6} \rangle \subset \Pi^{14}$$

буде стабілізаторним кодом типу $[14, 2]$, тобто буде кодувати 2 логічні кубіти. Логічні $\bar{Z}_1, \bar{Z}_2, \bar{X}_1, \bar{X}_2$ відповідно будуть

$$\bar{Z}_1 = \bar{Z}_A \otimes I_B, \quad \bar{Z}_2 = I_A \otimes \bar{Z}_B,$$

$$\bar{X}_1 = \bar{X}_A \otimes I_B, \quad \bar{X}_2 = I_A \otimes \bar{X}_B.$$

Не важко перевірити, що $\overline{CNOT}_{A,B}$ зберігає стабілізаторний підпростір $C(S \otimes S)$ (еквівалентно, спряження за допомогою $\overline{CNOT}_{A,B}$ зберігає підгрупу $S \otimes S$). Тож $\overline{CNOT}_{A,B}$ дійсно відповідає логічному CNOT між блоками коду Стіні

CNOT між блоками CSS кодів

Попередня конструкція узагальнюється і на інші CSS коди.

Нехай є CSS код типу $[n, 1]$, тобто частина генераторів складається лише з Z множників, а частина з X. До того ж, логічні $\bar{Z}$ та $\bar{X}$ побудовані стандартним чином, тобто також складаються з Z та X множників відповідно.

Тоді логічний $\overline{CNOT}$ між логічним кубітом з блоку A і логічним кубітом з блоку B реалізується як добуток $CNOT$, що діють між відповідними куітами з блоків A та B.

Трансверсальні та відмовостійкі операції

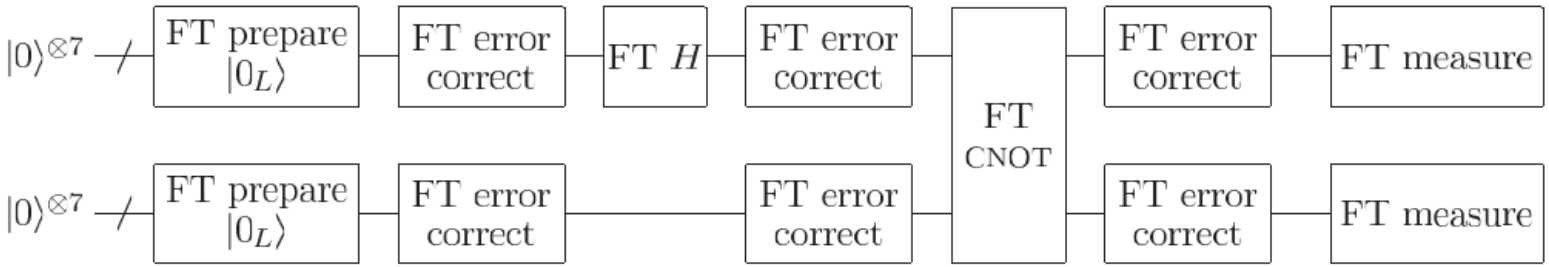
Попередні приклади реалізацій квантових операцій називають *трансверсальними*.
Їх поєднує те, що фізичний кубіт з одного блоку коду при операції не взаємодіє з іншими кубітами з того самого блоку. (хоча в літературі існують різні варіації поняття трансверсальності.)

Іншим важливим поняттям є так звані *відмовостійкі* операції. Формально це такі операції, при яких похибка на одному з фізичних кубітів не може призвести до поширення похибки на кілька (більше одного) кубітів в одному блоці (але поширення похибки на кілька різних блоків дозволяється).

Відмовостійкі квантові обчислення

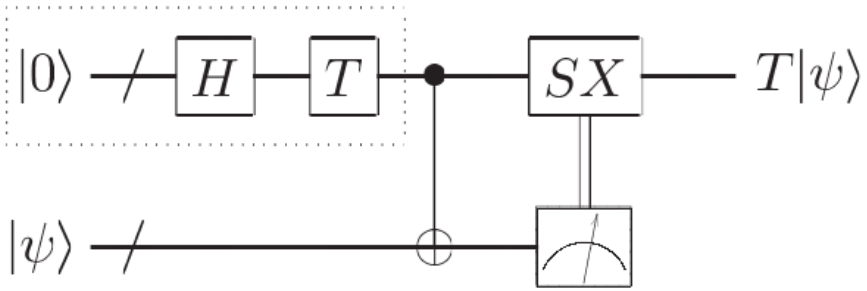
Відмовостійкими квантовими обчисленнями називають такі, що складаються лише з відмовостійких операцій і використовують алгоритм виправлення похибок після кожної з операцій.

Загальну ідею можна пояснити на прикладі наступної схеми



Відмовостійка реалізація гейту T

Для реалізації логічного $T|\psi\rangle$ для $|\psi\rangle = a|0\rangle + b|1\rangle$ використовують наступну схему



Ідея полягає в застосуванні додаткового логічного кубіту, що знаходиться у стані

$$|\Theta\rangle = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$$

(на схемі пунктиром позначена його можлива генерація).

Відмовостійка реалізація гейту T

Після операції CNOT зі схеми загальний стан вийде

$$CNOT\,|\Theta\rangle \otimes |\psi\rangle =$$

$$= \frac{1}{\sqrt{2}}\left[(a\,|0\rangle + be^{i\pi/4}\,|1\rangle)\,|0\rangle + (b\,|0\rangle + ae^{i\pi/4}\,|1\rangle)\,|1\rangle\right]$$

Тож якщо вимірювання другого кубіту (там де був ψ) показало 0, то стан першого кубіту сколапсує до $a\,|0\rangle + be^{i\pi/4}\,|1\rangle$, тобто до в точності до $T\,|\psi\rangle$. В іншому випадку стан сколапсує до $b\,|0\rangle + ae^{i\pi/4}\,|1\rangle$, яке можна привести до $T\,|\psi\rangle$ (з точністю до фази) застосуванням SX.

Залишається зрозуміти як реалізувати стан $|\Theta\rangle$ (ясно, що ми не можемо використати T адже ми намагаємо його побудувати).

Реалізація $|\Theta\rangle$

Не складно перевірити, що $|\Theta\rangle$ це власний вектор зі значенням $+1$ для оператору

$$THZHT^\dagger = TXT^\dagger = e^{-i\pi/4}SX.$$

Тож можна виміряти $|0\rangle$ у $e^{-i\pi/4}SX$. Результат $+1$ буде означати, що стан перейде як раз у $|\Theta\rangle$. Якщо ні, тобто ми отримаємо стан для власного вектору -1, то або можна спробувати повторити процедуру вимірювання, або ж застосувати $ZSXZ = -SX$, що переведе власний вектор для -1 як раз до $|\Theta\rangle$.

Для реалізації вимірювання, що відповідає $e^{-i\pi/4}SX$, існують алгоритми, які є відмовостійкі.

Завдання

Нехай ми маємо 5ти кубітний код типу $[5, 1]$ заданий через

$$g_1 = \mathtt{XZZXI}$$
$$g_2 = \mathtt{IXZZX}$$
$$g_3 = \mathtt{XIXZZ}$$
$$g_4 = \mathtt{ZXIXZ}$$
$$\bar{Z} = \mathtt{ZZZZZ}$$
$$\bar{X} = \mathtt{XXXXX}$$

Чи буде $\bar{U} = H_1 H_2 H_3 H_4 H_5$ відповідати логічному H?
(подивитися чи зберігається група

$$\mathcal{S} = \langle g_1, g_2, g_3, g_4 \rangle = \{ g_1^{b_1} g_2^{b_2} g_3^{b_3} g_4^{b_4} \}_{b_i \in \{0,1\}}$$

при спряженні $\bar{U}$, тобто чи $\bar{U} \mathcal{S} \bar{U}^\dagger = \mathcal{S}$)