1 Enumeration of the Stabilizer States

Proposition 1 ([1, Theorem 2], [2, Theorem 5.(ii)], [3])**.** *All stabilizer states can be written as follows:*

$$\begin{cases} |\phi\rangle := |t\rangle & \text{if } k = 0, \\ |\phi\rangle := \dfrac{1}{2^{k/2}} \displaystyle\sum_{x=0}^{2^k-1} (-1)^{x^\top Qx} i^{c^\top x} |Rx + t\rangle & \text{if } k > 0, \end{cases} \tag{1}$$

証明 By hamada? In particular, can we say that all states in this form are stabilizer states? □

A little modification of the above proposition gives us a efficient way to enumerate all the stabilizer states.

Theorem 1 In order to enumerate all stabilizer states, it is enough to consider the cases satisfying the following conditions:

- Q is a top-left $\mathbb{F}_2^{k\times k}$ matrix.
- R is a rank k $\mathbb{F}_2^{k\times(n-k)}$ rref(reduced row echelon form) matrix.
- t belongs to the complement of the row space of R.

証明 Main Ideas come from [1]. What we have to check is that this formulation can cover all the stabilizer states. It is easy to check that if $(Q_1, R_1, t_1) \neq (Q_2, R_2, t_2)$, then the corresponding states are also different, so we only have to check the number of stabilizer states. It is known that the number of rank k $\mathbb{F}_2^{k\times(n-k)}$ rref matrices is $\begin{bmatrix} n \\ k \end{bmatrix}_2$, which is a q-binomial coefficient with $q = 2$. Thus, The number of Q, c, R, t is $2^{k(k+1)/2}, 2^k, \begin{bmatrix} n \\ k \end{bmatrix}_2, 2^{n-k}$, respectively, and the total number of states is

$$2^n + \sum_{k=1}^{n} 2^{k(k+1)/2} 2^k \begin{bmatrix} n \\ k \end{bmatrix}_2 2^{n-k} = 2^n \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_2 2^{k(k+1)/2} = 2^n \prod_{k=1}^{n} (2^k + 1) = |\mathcal{S}_n|.$$

In the second last equation, we used the q-binomial theorem. Therefore, this formulation actually covers all the stabilizer states. □

In the above theorem, we used $\mathbb{F}_2$. By doing so, we can separate the coefficients of -1 and i since $i^0 = 1, i^1 = i$, without no appearance of -1. This is a nice property, but at the same time, the law of exponents does not hold due to $\mathbb{F}_2$, i.e., $1 + 1 = 0$ in $\mathbb{F}_2$ but $-1 = i^{1+1} \neq i^0 = 1$. This fact encourages us to allow $c^\top x$ to take non negative integer values, and here is another formulation with a slightly difference in order to solve this problem.

Corollary 1. *In the above theorem, We can change $\mathbb{F}_2$ to $\{0, 1\} \subset \mathbb{Z}$.*

証明 We only have to check the term $i^{c^\top x}$, since other terms are the same as the above theorem. By changing $\mathbb{F}_2$ to $\{0, 1\} \subset \mathbb{Z}$, the term $i^{c^\top x}$ change iff $p \equiv 2, 3 \pmod 4$, where p is the number of i such that $c_i = 1$ and $x_i = 1$. By flipping the value of Q_{ij} iff $c_i = c_j = 1 (i \neq j)$, we can flip this negative term, since

$$\binom{p}{2} \equiv \begin{cases} 0 \pmod 2 & \text{if } p \equiv 0, 1 \pmod 4, \\ 1 \pmod 2 & \text{if } p \equiv 2, 3 \pmod 4. \end{cases}$$

□

2 Calculating the Overlap

Thanks to the corollary 1, we can prove the following theorem.

Theorem 2 Fix k, R, t in the standard form (1). Then, we can compute the overlap $\langle\phi|\psi\rangle$ efficiently. (TODO: Write the exact computational cost.)

証明 (Following is rough and crude proof.)

We only consider the case $k > 0, R = 0, t = 0$ for the simplicity. Other cases are trivial or can be reduced to this case. Define $x := \begin{bmatrix} x_0 \\ \overline{x} \end{bmatrix}$, $c := \begin{bmatrix} c_0 \\ \overline{c} \end{bmatrix}$, and $Q := \begin{bmatrix} Q_{00} & Q_0^\top \\ 0 & \overline{Q} \end{bmatrix}$ (x_0, c_0 and Q_{00} are all in $\{0, 1\}$). Since $x^\top Q x = x_0(Q_{00} + Q_0^\top \overline{x}) + \overline{x}^\top \overline{Q}\overline{x}$ and $c^\top x = c_0 x_0 + \overline{c}^\top \overline{x}$, we can rewrite the state as

$$\begin{aligned} |\phi\rangle &= \sum_{x=0}^{2^k-1} (-1)^{x^\top Q x} i^{c^\top x} |x\rangle \\ &= \sum_{\overline{x}=0}^{2^{k-1}-1} (-1)^{\overline{x}^\top \overline{Q}\overline{x}} i^{\overline{c}^\top \overline{x}} \Big(|2\overline{x}\rangle + (-1)^{Q_{00} + Q_0^\top \overline{x}} i^{c_0} |2\overline{x} + 1\rangle \Big) \\ &= \sum_{\overline{x}=0}^{2^{k-1}-1} (-1)^{\overline{x}^\top \overline{Q}\overline{x}} i^{\overline{c}^\top \overline{x}} |\overline{x}'\rangle \end{aligned}$$

by defining $|\overline{x}'\rangle := |2\overline{x}\rangle + (-1)^{Q_{00} + Q_0^\top \overline{x}} i^{c_0} |2\overline{x} + 1\rangle$. (Question: Is it natural to equate integer $2\overline{x} + 1$ to the vector $\begin{bmatrix} 1 \\ \overline{x} \end{bmatrix}$?)

Thus, we can compute the overlap recursively with very small computational cost per each step. This leads to the efficient calculation of the overlaps, which concludes the proof. □

Proposition 2. *For the each steps, we can skip the calculation of the overlap if the following conditions are satisfied:*

$$\sum_{x=0}^{2^k-1} \langle Rx + t|\psi\rangle < \text{threshold}$$

証明 The overlap can be suppressed by L^1 norm of the state. (TODO: Write exact proof.) □

参考文献

[1] G.I. Struchalin, Ya. A. Zagorovskii, E.V. Kovlakov, S.S. Straupe, and S.P. Kulik. “Experimental Estimation of Quantum State Properties from Classical Shadows”. PRX Quantum **2**, 010307 (2021).

[2] Jeroen Dehaene and Bart De Moor. “Clifford group, stabilizer states, and linear and quadratic operations over GF(2)”. Physical Review A **68**, 042318 (2003).

[3] Maarten Van den Nest. “Classical simulation of quantum computation, the gottesman-Knill theorem, and slightly beyond”. Quantum Inf. Comput. **10**, 258–271 (2010).