1 Enumeration of the Stabilizer States

As a well-known fact, the stabilizer states have a simple form as shown in the following proposition.

Proposition 1 ([1, Theorem 2], [3, Section 5], [2, Theorem 5.(ii)]). *All stabilizer states can be written in the following form:*

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

where $Q \in \mathbb{F}_2^{k\times k}$, $c \in \mathbb{F}_2^k$, $R \in \mathbb{F}_2^{k\times(n-k)}$, $t \in \mathbb{F}_2^{n-k}$ *and* $\operatorname{rank}(R) = k$. *Also, any state that can be written in this form is a stabilizer state.*

A little modification of Proposition 1 gives us a efficient way to enumerate all the stabilizer states.

Theorem 1 The form (1) with the following conditions enumerates all the stabilizer states without any duplication or omission:

- Q is a upper triangular $\mathbb{F}_2^{k\times k}$ 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]. Firstly, we show that the mapping $\{(Q, c, R, t)\} \to \mathcal{S}_n$ is injective. We can say that

$$\begin{aligned} &\left\{R_1 x + t_1 \,\middle|\, x \in \mathbb{F}_2^{n-k}\right\} = \left\{R_2 x + t_2 \,\middle|\, x \in \mathbb{F}_2^{n-k}\right\} \\ \iff &\operatorname{Im}(R_1) = \operatorname{Im}(R_2) \wedge (t_2 - t_1) \in \operatorname{Im}(R_1) \\ \iff &R_1 = R_2 \wedge t_1 = t_2. \end{aligned}$$

The last equivalence is due to the property of the rref matrix and the complement condition. Since Q is a upper triangular matrix, we can uniquely determine Q and c for given state $|\phi\rangle$. Thus, if two states are the same, then the corresponding (Q, c, R, t) are also the same, which means that the mapping is injective.

Next, we show that the mapping is surjective. Since the mapping is injective, we only have to show that the cardinality of the domain is equal to that of the codomain, i.e., $|\mathcal{S}_n|$. It is known that the number of rank k $\mathbb{F}_2^{k\times(n-k)}$ rref matrices is $\left[{n \atop k}\right]_2$, which is a q-binomial coefficient with $q = 2$. Therefore, The number of Q, c, R, t is $2^{k(k+1)/2}, 2^k, \left[{n \atop k}\right]_2, 2^{n-k}$, 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, the mapping is surjective, which concludes the proof. $\square$

In theorem 1, we used $\mathbb{F}_2$. However, in the viewpoint of the dfs algorithm, it is more practical to use $\{0,1\} \subset \mathbb{Z}$ and allow the term $c^\top x$ to be any integer, since then the law of exponents holds true. Therefore, the following corollary is useful.

Corollary 1. *In theorem 1, We can substitute* $\mathbb{F}_2$ *with* $\{0,1\} \subset \mathbb{Z}$.

証明 By changing $\mathbb{F}_2$ to $\{0,1\} \subset \mathbb{Z}$, the term $(-1)^{x^\top Qx}$ is invariant, and the term $i^{c^\top x}$ is multiplied by -1 iff $p \equiv 2,3 \pmod 4$, where p is the number of i such that $c_i = 1$ and $x_i = 1$. Now, we consider the following form:

$$\begin{cases} |\phi\rangle := |t\rangle & \text{if } k = 0, \\ |\phi\rangle := \dfrac{1}{2^{k/2}} \displaystyle\sum_{x=0}^{2^k-1} (-1)^{x^\top (Q+Q')x} i^{c^\top x} |Rx + t\rangle & \text{if } k > 0, \end{cases} \tag{2}$$

where $Q \in \{0,1\}^{k\times k}, c \in \{0,1\}^k, R \in \{0,1\}^{k\times(n-k)}, t \in \{0,1\}^{n-k}, \mathrm{rank}(R) = k$ and $Q'_{ij} = 1$ iff $(i < j) \wedge (c_i = c_j = 1)$. Now, if the pair (Q,c,R,t) in (2) is the same as that of the original form (1), then the two states are representing the exactly same state since

$$(-1)^{x^\top Q' x} = (-1)^{\binom{p}{2}} = \begin{cases} 1 & \text{if } p \equiv 0,1 \pmod 4, \\ -1 & \text{if } p \equiv 2,3 \pmod 4. \end{cases}$$

Therefore, by identifying the $Q + Q'$ in $\mathbb{Z}$ with new Q'' in $\mathbb{F}_2$, we can conclude the proof. $\square$

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 $x^\top Qx = x_0(Q_{00} + Q_0^\top \overline{x}) + \overline{x}^\top \overline{Q}\overline{x}$ and $c^\top x = c_0 x_0 + \overline{c}^\top \overline{x}$, we can rewrite the state as

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

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).