Stabilizer Extent

Hiroki Hamaguchi

2024年4月13日

概要

This is just a memo for meeting. In order to practice, I wrote this memo in English.

1 Derivation of the Dual Problem by CVXPY formulation

In the cvxpy official userguide, the following problem is considered. We change the index from k to i for consistency with our notation.

$$
\begin{aligned}
\underset{\boldsymbol{x}}{\text{minimize}} \quad & \boldsymbol{c}^\top \boldsymbol{x} \\
\text{subject to} \quad & G_i \boldsymbol{x} + \boldsymbol{s}_i = \boldsymbol{h}_i, \qquad i = 0, \ldots, M, \\
& A\boldsymbol{x} = \boldsymbol{b}, \\
& \boldsymbol{s}_0 \succeq \boldsymbol{0}, \\
& s_{i0} \geq \|\boldsymbol{s}_{i1}\|_2, \quad i = 1, \ldots, M
\end{aligned}
$$

$$
\begin{aligned}
\underset{\boldsymbol{y}}{\text{maximize}} \quad & -\sum_{i=0}^{M} \boldsymbol{h}_i^\top \boldsymbol{z}_i - \boldsymbol{b}^\top \boldsymbol{y} \\
\text{subject to} \quad & \sum_{i=0}^{M} G_i^\top \boldsymbol{z}_i + A^\top \boldsymbol{y} + \boldsymbol{c} = \boldsymbol{0}, \\
& \boldsymbol{z}_0 \succeq \boldsymbol{0}, \\
& \boldsymbol{z}_{i0} \geq \|\boldsymbol{z}_{i1}\|_2, \quad i = 1, \ldots, M
\end{aligned}
$$

where $\succeq$ denotes element-wise inequality, and

$$
\begin{aligned}
\boldsymbol{s}_i &= (s_{i0}, \boldsymbol{s}_{i1}) \in \mathbb{R} \times \mathbb{R}^{r_i - 1}, \\
\boldsymbol{z}_i &= (z_{i0}, \boldsymbol{z}_{i1}) \in \mathbb{R} \times \mathbb{R}^{r_i - 1}.
\end{aligned}
$$

We adapt this problem to our problem, minimizing the complex L^1 norm.

$$\begin{aligned} \underset{\boldsymbol{x}\in\mathbb{C}^{|\mathcal{S}_n|}}{\text{minimize}} \quad & \|\boldsymbol{x}\|_1 \\ \text{subject to} \quad & A\boldsymbol{x} = \boldsymbol{b} \end{aligned}$$

Let e_i be a vector with the i-th component 1 and the others 0. Then, the problem can be written as follows.

$$\begin{aligned} \underset{\boldsymbol{t}\in\mathbb{R}^{|\mathcal{S}_n|},\, \boldsymbol{x}\in\mathbb{C}^{|\mathcal{S}_n|}}{\text{minimize}} \quad & \begin{bmatrix} \boldsymbol{1}^\top & \boldsymbol{0}^\top & \boldsymbol{0}^\top \end{bmatrix} \begin{bmatrix} \boldsymbol{t} \\ \mathrm{Re}(\boldsymbol{x}) \\ \mathrm{Im}(\boldsymbol{x}) \end{bmatrix} \\ \text{subject to} \quad & -\begin{bmatrix} e_i^\top & \boldsymbol{0}^\top & \boldsymbol{0}^\top \\ \boldsymbol{0}^\top & e_i^\top & \boldsymbol{0}^\top \\ \boldsymbol{0}^\top & \boldsymbol{0}^\top & e_i^\top \end{bmatrix} \begin{bmatrix} \boldsymbol{t} \\ \mathrm{Re}(\boldsymbol{x}) \\ \mathrm{Im}(\boldsymbol{x}) \end{bmatrix} + \boldsymbol{s}_i = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad i = 1, \dots, |\mathcal{S}_n|, \\ & \begin{bmatrix} 0_{2^n\times|\mathcal{S}_n|} & \mathrm{Re}(A) & -\mathrm{Im}(A) \\ 0_{2^n\times|\mathcal{S}_n|} & \mathrm{Im}(A) & \mathrm{Re}(A) \end{bmatrix} \begin{bmatrix} \boldsymbol{t} \\ \mathrm{Re}(\boldsymbol{x}) \\ \mathrm{Im}(\boldsymbol{x}) \end{bmatrix} = \begin{bmatrix} \mathrm{Re}(\boldsymbol{b}) \\ \mathrm{Im}(\boldsymbol{b}) \end{bmatrix}, \\ & s_{i0} \geq \|\boldsymbol{s}_{i1}\|_2, \quad i = 1, \dots, |\mathcal{S}_n| \end{aligned}$$

$$\begin{aligned} \underset{\boldsymbol{y}\in\mathbb{C}^{2^n}}{\text{maximize}} \quad & -\begin{bmatrix} \mathrm{Re}(\boldsymbol{b})^\top & \mathrm{Im}(\boldsymbol{b})^\top \end{bmatrix} \begin{bmatrix} \mathrm{Re}(\boldsymbol{y}) \\ \mathrm{Im}(\boldsymbol{y}) \end{bmatrix} \\ \text{subject to} \quad & -\sum_{i=1}^{M} \begin{bmatrix} e_i & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & e_i & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & e_i \end{bmatrix} \begin{bmatrix} z_{i0} \\ \mathrm{Re}(z_{i1}) \\ \mathrm{Im}(z_{i1}) \end{bmatrix} + \begin{bmatrix} 0_{|\mathcal{S}_n|\times 2^n} & 0_{|\mathcal{S}_n|\times 2^n} \\ \mathrm{Re}(A)^\top & \mathrm{Im}(A)^\top \\ -\mathrm{Im}(A)^\top & \mathrm{Re}(A)^\top \end{bmatrix} \begin{bmatrix} \mathrm{Re}(\boldsymbol{y}) \\ \mathrm{Im}(\boldsymbol{y}) \end{bmatrix} + \begin{bmatrix} \boldsymbol{1} \\ \boldsymbol{0} \\ \boldsymbol{0} \end{bmatrix} = \boldsymbol{0}, \\ & z_{i0} \geq |z_{i1}|, \quad i = 1, \dots, |\mathcal{S}_n| \end{aligned}$$

Furthermore, let the i-th column of the matrix A be $\boldsymbol{a}_i$. Then, the problem can be written as follows.

$$\begin{aligned} \underset{\boldsymbol{y}\in\mathbb{C}^{2^n}}{\text{maximize}} \quad & -\mathrm{Re}(\boldsymbol{b}^\dagger \boldsymbol{y}) \\ \text{subject to} \quad & z_{i0} = 1, \quad i = 1, \dots, |\mathcal{S}_n|, \\ & z_{i1} = \boldsymbol{a}_i^\dagger \boldsymbol{y}, \quad i = 1, \dots, |\mathcal{S}_n|, \\ & z_{i0} \geq |z_{i1}|, \quad i = 1, \dots, |\mathcal{S}_n| \end{aligned}$$

$$
\begin{aligned}
\underset{\boldsymbol{y} \in \mathbb{C}^{2^n}}{\text{maximize}} \quad & -\operatorname{Re}(\boldsymbol{b}^\dagger \boldsymbol{y}) \\
\text{subject to} \quad & \left| \boldsymbol{a}_i^\dagger \boldsymbol{y} \right| \leq 1, \quad i = 1, \ldots, |\mathcal{S}_n|
\end{aligned}
$$

Even if we flip the sign of the objective function, the optimal solution does not change thanks to the absolute value in the constraints. Thus, the dual problem of the original problem is

$$
\begin{aligned}
\underset{\boldsymbol{y} \in \mathbb{C}^{2^n}}{\text{maximize}} \quad & \operatorname{Re}(\boldsymbol{b}^\dagger \boldsymbol{y}) \\
\text{subject to} \quad & \left| \boldsymbol{a}_i^\dagger \boldsymbol{y} \right| \leq 1, \quad i = 1, \ldots, |\mathcal{S}_n|.
\end{aligned} \tag{1}
$$

2 Derivation of the Dual Problem by Lagrangian

We can derive the dual problem more directly using the Lagrangian. The original problem was formulated as follows.

$$
\begin{aligned}
\underset{\boldsymbol{x} \in \mathbb{C}^{|\mathcal{S}_n|}, \boldsymbol{t} \in \mathbb{R}^{|\mathcal{S}_n|}}{\text{minimize}} \quad & \sum_{i=1}^{|\mathcal{S}_n|} t_i \\
\text{subject to} \quad & \begin{bmatrix} \operatorname{Re}(A) & -\operatorname{Im}(A) \\ \operatorname{Im}(A) & \operatorname{Re}(A) \end{bmatrix} \begin{bmatrix} \operatorname{Re}(\boldsymbol{x}) \\ \operatorname{Im}(\boldsymbol{x}) \end{bmatrix} = \begin{bmatrix} \operatorname{Re}(\boldsymbol{b}) \\ \operatorname{Im}(\boldsymbol{b}) \end{bmatrix}, \\
& |x_i| \leq t_i, \quad i = 1, \ldots, |\mathcal{S}_n|
\end{aligned} \tag{2}
$$

The Lagrangian of the problem (2) can be defined by

$$
\begin{aligned}
L(\boldsymbol{x}, \boldsymbol{t}, \boldsymbol{y}, \boldsymbol{s}) = & \sum_{i=1}^{|\mathcal{S}_n|} t_i \\
& + \operatorname{Re}(\boldsymbol{y}^\top)(\operatorname{Re}(A)\operatorname{Re}(\boldsymbol{x}) - \operatorname{Im}(A)\operatorname{Im}(\boldsymbol{x}) - \operatorname{Re}(\boldsymbol{b})) \\
& + \operatorname{Im}(\boldsymbol{y}^\top)(\operatorname{Im}(A)\operatorname{Re}(\boldsymbol{x}) + \operatorname{Re}(A)\operatorname{Im}(\boldsymbol{x}) - \operatorname{Im}(\boldsymbol{b})) \\
& + \sum_{i=1}^{|\mathcal{S}_n|} s_i(|x_i| - t_i) \\
= & -\operatorname{Re}(\boldsymbol{y}^\dagger \boldsymbol{b}) \\
& + \sum_{i=1}^{|\mathcal{S}_n|} (1 - s_i) t_i + \sum_{i=1}^{|\mathcal{S}_n|} \left(s_i |x_i| + \begin{bmatrix} \operatorname{Re}(\boldsymbol{a}_i^\dagger \boldsymbol{y}) \\ \operatorname{Im}(\boldsymbol{a}_i^\dagger \boldsymbol{y}) \end{bmatrix}^\top \begin{bmatrix} \operatorname{Re}(\boldsymbol{x}) \\ \operatorname{Im}(\boldsymbol{x}) \end{bmatrix} \right).
\end{aligned}
$$

By using this relation, we can obtain the Lagrange dual function as follows.

$$
g(\boldsymbol{y}, \boldsymbol{s}) = \inf_{\boldsymbol{x}, \boldsymbol{t}} L(\boldsymbol{x}, \boldsymbol{t}, \boldsymbol{y}, \boldsymbol{s})
$$

$$
\begin{aligned}
&= -\operatorname{Re}(\boldsymbol{b}^\dagger \boldsymbol{y}) \\
&\quad + \begin{cases} 0 & \text{if } s_i \neq 1 \\ -\infty & \text{otherwise} \end{cases} \\
&\quad + \begin{cases} 0 & \text{if } \left|\boldsymbol{a}_i^\dagger \boldsymbol{y}\right| \leq 1 \\ -\infty & \text{otherwise} \end{cases}
\end{aligned}
$$

Thus, the dual problem of the original problem is

$$
\begin{aligned}
\underset{\boldsymbol{y} \in \mathbb{C}^{2^n}}{\text{maximize}} \quad & -\operatorname{Re}(\boldsymbol{b}^\dagger \boldsymbol{y}) \\
\text{subject to} \quad & \left|\boldsymbol{a}_i^\dagger \boldsymbol{y}\right| \leq 1, \quad i = 1, \ldots, |\mathcal{S}_n|,
\end{aligned}
$$

and even if we flip the sign of the objective function, the optimal solution does not change thanks to the absolute value in the constraints. Thus, the dual problem of the original problem is

$$
\begin{aligned}
\underset{\boldsymbol{y} \in \mathbb{C}^{2^n}}{\text{maximize}} \quad & \operatorname{Re}(\boldsymbol{b}^\dagger \boldsymbol{y}) \\
\text{subject to} \quad & \left|\boldsymbol{a}_i^\dagger \boldsymbol{y}\right| \leq 1, \quad i = 1, \ldots, |\mathcal{S}_n|,
\end{aligned}
\tag{3}
$$

which is consistent with the dual problem (1).

3 Enumeration of the Stabilizer States

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

$$
\begin{cases}
|\phi\rangle := |t\rangle & \text{if } k = 0, \\
|\phi\rangle := \dfrac{1}{2^{k/2}} \displaystyle\sum_{x=0}^{2^k-1} (-1)^{x^\top Q x} i^{c^\top x} |Rx + t\rangle & \text{if } k > 0,
\end{cases}
\tag{4}
$$

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

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

□

4 Calculating the Overlap

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

Theorem 2 Fix k, R, t in the standard form (4). 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.) □

5 For the Case $|\psi\rangle$ is Real

Assume that the state $|\psi\rangle$ is real. Now, we consider the following optimization problem:

$$
\begin{aligned}
\underset{x \in \mathbb{C}^{|\mathcal{S}_n|}}{\text{minimize}} \quad & \|x\|_1 \\
\text{subject to} \quad & \sum_{\phi_i \in \mathcal{S}_n} x_i |\phi_i\rangle = |\psi\rangle
\end{aligned}
$$

$$
\begin{aligned}
\underset{|y\rangle \in \mathbb{C}^{2^n}}{\text{maximize}} \quad & \mathrm{Re}(\langle \psi | y \rangle) \\
\text{subject to} \quad & |\langle \phi_i | y \rangle| \leq 1, \quad \forall \phi_i \in \mathcal{S}_n
\end{aligned}
$$

Let $\mathcal{T}_n$ be the collection of the states in $\mathcal{S}_n$ with real coefficients. This means $\mathcal{T}_n$ is the collection of the states with $\boldsymbol{c} = 0$ and $|\mathcal{T}_n| = |\mathcal{S}_n|/(2^n)$. Now, we consider the following restricted optimization problem:

$$
\underset{x \in \mathbb{R}^{|\mathcal{T}_n|}}{\text{minimize}} \quad \|x\|_1
$$

$$\text{subject to} \quad \sum_{\phi_j \in \mathcal{T}_n} x_j \left|\phi_j\right\rangle = \left|\psi\right\rangle$$

$$\begin{aligned} &\underset{|y\rangle \in \mathbb{R}^{2^n}}{\text{maximize}} && \langle\psi|y\rangle \\ &\text{subject to} && |\langle\phi_j|y\rangle| \leq 1, \quad \forall \phi_j \in \mathcal{T}_n \end{aligned}$$

Let x^* and y^* be the optimal solutions of the restricted primal and dual problems, respectively. These vectors always exist since $\mathcal{T}_n$ forms a over complete basis. We now show that the x^*, y^* are optimal not only for the restricted problems but also for the original problems.

Lemma 1. *Suppose $|y\rangle$ is real and satisfies $|\langle\phi_j|y\rangle| \leq 1$ for all $\phi_j \in \mathcal{T}_n$. Then, $|y\rangle$ satisfies $|\langle\phi_i|y\rangle| \leq 1$ for all $\phi_i \in \mathcal{S}_n$.*

証明 We check the all states $|\phi_i\rangle \in \mathcal{S}_n$ respectively. It is trivial for the case $k = 0$ since the corresponding columns both exist in $\mathcal{S}_n$ and $\mathcal{T}_n$. We set $|\phi_i\rangle = \frac{1}{2^{k/2}} \sum_{x=0}^{2^k-1} (-1)^{x^\top Qx} i^{c^\top x} |Rx + t\rangle$ with $k > 0$ and $\langle\phi_i|y\rangle = \alpha + i\beta (\alpha, \beta \in \mathbb{R})$. The following two states

$$|\phi_+\rangle \coloneqq \frac{1}{2^{k/2}} \sum_{x=0}^{2^k-1} (-1)^{x^\top Qx} |Rx + t\rangle, \quad |\phi_-\rangle \coloneqq \frac{1}{2^{k/2}} \sum_{x=0}^{2^k-1} (-1)^{x^\top Qx + c^\top x} |Rx + t\rangle$$

are in $\mathcal{T}_n$, and satisfy $\langle\phi_+|y\rangle = \alpha + \beta, \langle\phi_-|y\rangle = \alpha - \beta$. From the assumption, we have

$$|\langle\phi_i|y\rangle| = \sqrt{\alpha^2 + \beta^2} \leq |\alpha| + |\beta| = \max\{|\alpha + \beta|, |\alpha - \beta|\} \leq 1,$$

which completes the proof. □

Theorem 3 The optimal solutions for the restricted problems x^* and y^* are also optimal for the original problems.

証明 Let OPT be the optimal value for the original primal problem. Since x^* can be a feasible solution for the original primal problem, it is clear that OPT $\leq \|x^*\|_1$. By the strong duality theorem, OPT is also the optimal value for the original dual problem. From the lemma 1, we can see that y^* is a feasible solution for the original dual problem and OPT $\geq \langle\psi|y^*\rangle$. Again, by applying the strong duality theorem to the restricted problems, we have $\|x^*\|_1 = \langle\psi|y^*\rangle$, which means that OPT $= \|x^*\|_1 = \langle\psi|y^*\rangle$. Therefore, x^* and y^* are also optimal for the original problems. □

Acknowledgements.—

acknowledgements acknowledgements acknowledgements

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).