Quantum worst-case to average-case reduction for lin prob

For a matrix $M \in \{0,1\}^{n \times n}$,

- take a vector $v \in \{0,1\}^n$,
- need to output $Mv \in \{0,1\}^n$. where addition is mod 2.

Naively, $O(n^2)$ time.

예시) $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Spse $\exists$ an average case alg ALG

- takes v u.a.r from $\{0,1\}^n$,
- outputs a correct answer wp $\geq \alpha$.

$$\Pr_{v, ALG}[ALG(v) = Mv] \geq \alpha.$$

Q. $\exists$ a sub-quadratic reduction ?

Bogolyubov's lemma

For any $X \subseteq \{0,1\}^n$ w/ $|X| \geq \rho \cdot 2^n$, let

$$4X := \{w+x+y+z \mid w, x, y, z \in X\}.$$

$\exists V \subseteq 4X$ of $\dim(V) \geq n - 1/\rho^2$.

Big picture

1. Let $X := \{x \in \{0,1\}^n \mid ALG(x)$ succeeds w/ good prob$\}$.
2. Decompose the given input $v \in \{0,1\}^n$ into
$$v = w + x + y + z, + s \quad \ldots (1)$$
where $w, x, y, z \in X$. s is sparse.
3. Run $ALG(w), \ldots, ALG(z)$ and obtain $b := ALG(w) + \cdots + ALG(z). + Ms$.
4. Verify if $Mv = b$

Q1. How to decompose in Step 2? (in sub-quad "time")?
Q2. How to verify in Step 4? (in sub-quad "time")?

~~Lem 6.1 Let $X \subseteq \{0,1\}^n$ w/ $|X| \geq \rho$ and R be a "good" set of entries w/ "heavy Fourier characters".~~

Lem Let $X \subseteq \{0,1\}^n$ w/ $|X| \geq \rho$,
R be a set of entries w/ "heavy Fourier characters" of $\mathbb{1}_X$,
V be the set orthogonal to R.
Then, $\dim(V) \geq n - O(1/\alpha^2)$ and for all $v \in \{0,1\}^n$,

$$\Pr_{x,y,z \in X}[v - x - y - z \in X] \geq \alpha^2,$$

where x, y, z are sampled u.a.r. from X.

- $\mathbb{1}_X$: indicator vector. If $n=3$, $X = \{0, 2, 7\}$, we have $\mathbb{1}_X = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$.
- Fourier characters. $v \underset{DFT^\dagger}{\overset{DFT}{\rightleftarrows}} \hat{v}$ ⇔ one-to-one correspondence.

Spse we have
Ⓐ a uniform sampler of X
Ⓑ a "good approximation" of $\mathbb{1}_X$,
we can decompose any $v \in \{0,1\}^n$ into (1) as follows:
1. Construct (a good approx of) R from Ⓑ
2. Let s be the restriction of v on basis(R).
3. Sample x, y, z from X using Ⓐ.
4. Obtain $w = v - x - y - z - s$.
5. Repeat sufficiently.

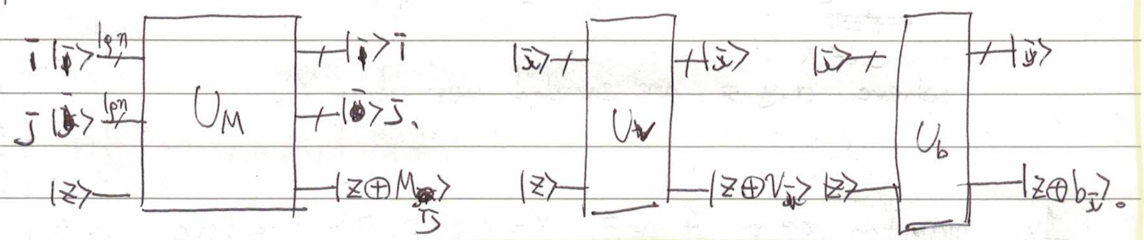
Q1-1. Uniform sampler of X
Q1-2. Good approx of $\mathbb{1}_X$. } just skim over.
Q2. How to verify? in detail

Quantum verification in subquad ~~time~~ query complexity.

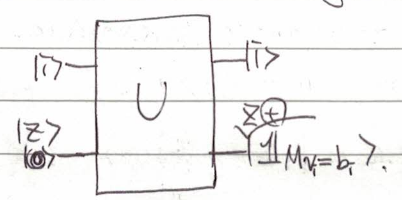
For a matrix M,
- take $v, b \in \{0,1\}^n$,
- output whether $Mv = b$.

Oracle for M, ~~v~~, b

Spse

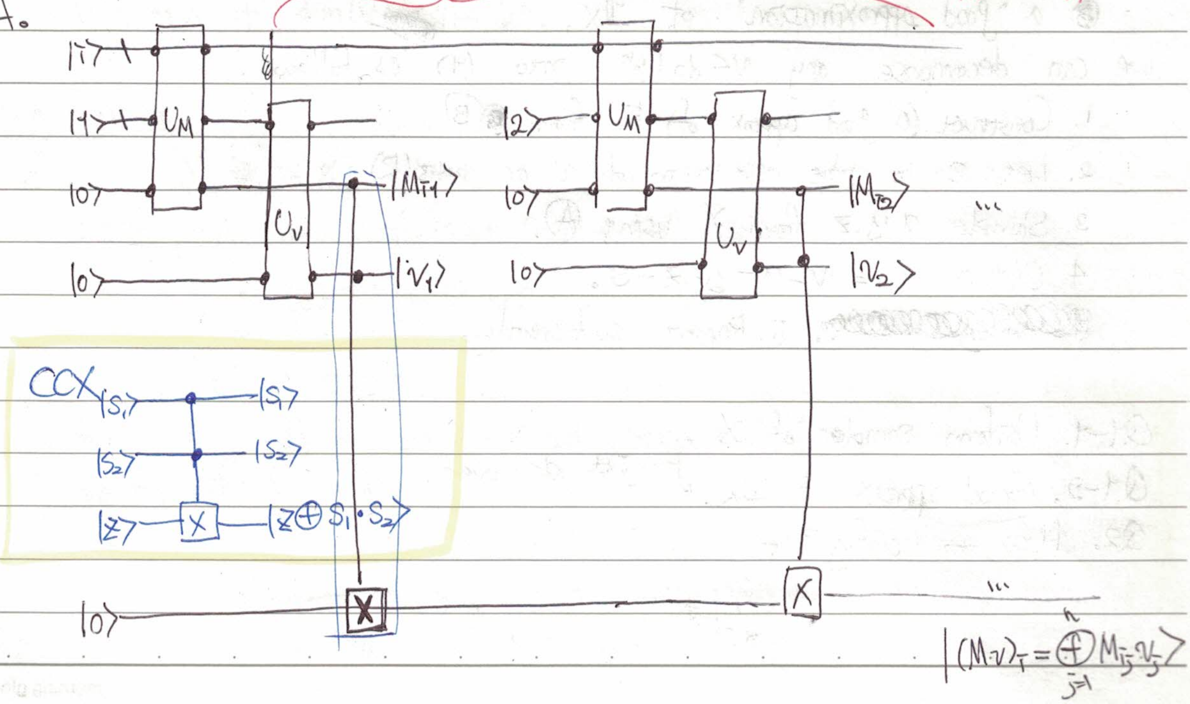


- Want to construct U s.t. given an index i, returns $(Mv)_i = b_i$, i.e.,

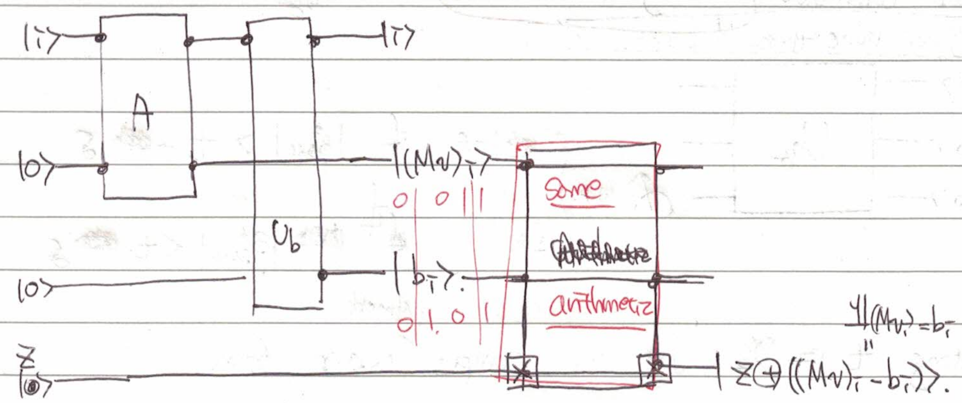


$O(n)$ queries to U_M & U_v

A.

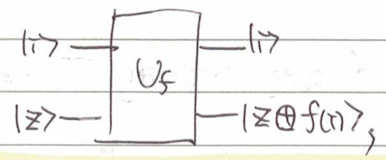


B.



Recall, Grover's search

Given $f: \{1, \cdots, n\} \to \{0,1\}$ w/ oracle.



one can find i s.t. $f(i) = 1$ w/ $O(\sqrt{n})$ queries)

If $Mv \neq b$, $\exists i$ s.t. $(Mv-b)_i = 1$. If $Mv = b$, all ~~values~~ 0.

→ Extending the Grover's search, we can verify if $Mv=b$ w/ $O(\sqrt{n})$ queries to U (and hence $O(n^{3/2})$ queries to U_M, U_v, U_b in total).

Uniform sampling from ΦX & Good approx of $\mathbb{1}X$.

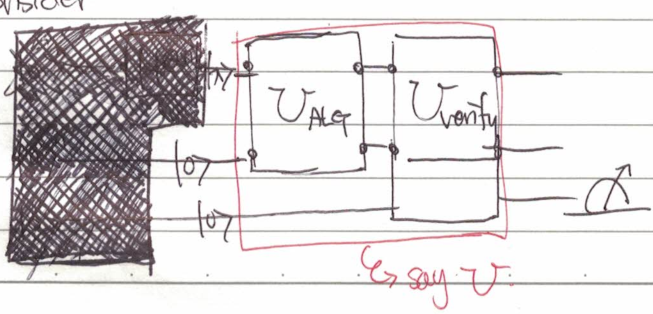
Model the average-case alg ALG as follows

$$U_{ALG}|\lambda\rangle|z\rangle = \beta^{\lambda}_{succ}|\lambda\rangle|z \oplus M\lambda\rangle + \beta^{\lambda}_{fail}|\lambda\rangle|\psi\rangle$$

↳ element-wise add.

where ψ is an arbitrary superposition other than $z \oplus M\lambda$.

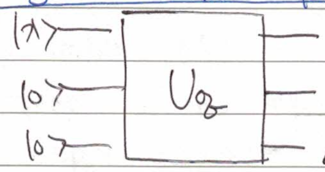
Consider



→ w/ prob $|\beta^{\lambda}_{succ}|^2$, we can verify ALG succeeds w/ input λ.

One can construct for any threshold t w/ $O_{\varepsilon,\delta}(1)$ queries to U.

[singular value threshold projection?]



$$\hat{x} \text{ w.p. } \begin{cases} \geq 1-\varepsilon & \text{if } |\beta^*_{succ}| > t+\delta \\ \leq \varepsilon & \text{if } |\beta^*_{succ}| < t-\delta \end{cases}$$

- By setting $t := \alpha/2$ we can sample almost u.a.r from

$$X_t := \{x \in \{0,1\}^n \mid \Pr[ALG(x) = Mx] > \alpha/2\}.$$

- Using this as quantum oracle for $\mathbb{1}_X$.

Thm Let ALG be an average-case quantum alg of query complexity T that satisfies

$$\Pr_{v, ALG}[ALG(v) = Mv] \geq \alpha.$$

For every const $\delta > 0$, $\exists$ a worst-case quantum alg ALG' of query complexity $O_{\alpha,\delta}(T + n^{3/2})$ that, for any $v \in \{0,1\}^n$,

$$\Pr_{ALG'}[ALG'(v) = Mv] \geq 1-\delta.$$