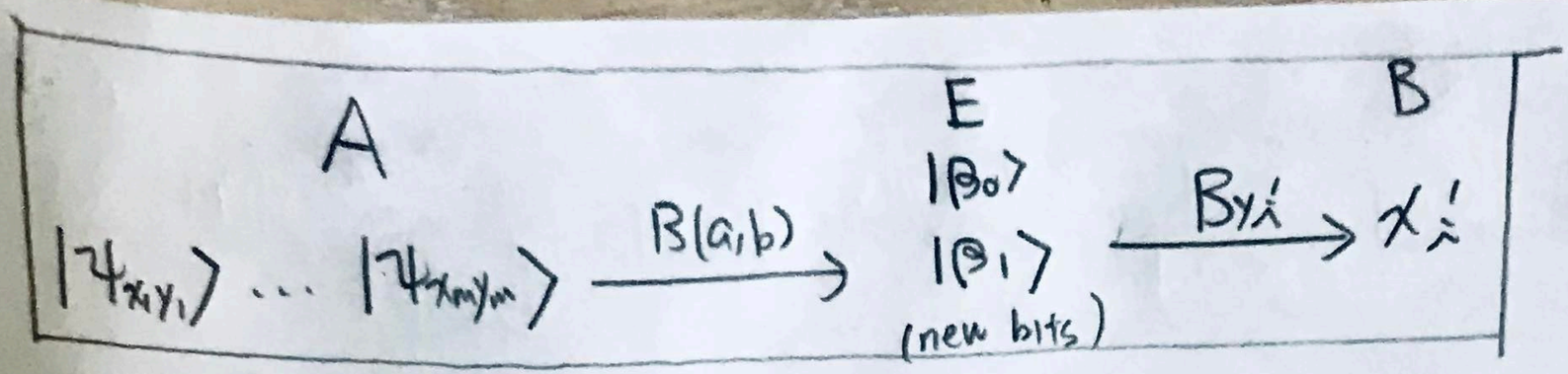
Problem 1



$\lvert\psi_{x_{\hat{x}}y_{\hat{x}}}\rangle$	$\begin{pmatrix}1\\0\end{pmatrix}$ $\lvert 0\rangle$	$\begin{pmatrix}0\\1\end{pmatrix}$ $\lvert 1\rangle$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ $\lvert +\rangle$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$ $\lvert -\rangle$
$P(E \text{ got } \beta_0)$	$\lvert a\rvert^2$ $\lvert\langle 0\lvert\beta_0\rangle\rvert^2$	$\lvert b\rvert^2$ $\lvert\langle 1\lvert\beta_0\rangle\rvert^2$	$\frac{\lvert a+b\rvert^2}{2}$ $\lvert\langle +\lvert\beta_0\rangle\rvert^2$	$\frac{\lvert a-b\rvert^2}{2}$ $\lvert\langle -\lvert\beta_0\rangle\rvert^2$
$P(E \text{ got } \beta_1)$	$\lvert b\rvert^2$	$\lvert a\rvert^2$	$\frac{\lvert a-b\rvert^2}{2}$	$\frac{\lvert a+b\rvert^2}{2}$
new bits of E	$\begin{cases}\beta_0, p=a^2\\ \beta_1, p=b^2\end{cases}$	$\begin{cases}\beta_0, p=b^2\\ \beta_1, p=a^2\end{cases}$	$\begin{cases}\beta_0, p=\frac{\lvert a+b\rvert^2}{2}\\ \beta_1, p=\frac{\lvert a-b\rvert^2}{2}\end{cases}$	$\begin{cases}\beta_0, p=\frac{\lvert a-b\rvert^2}{2}\\ \beta_1, p<\frac{\lvert a+b\rvert^2}{2}\end{cases}$
$P(B \text{ got error})$	$\lvert a\rvert^2\cdot(\lvert b\rvert^2)+$ $\lvert b\rvert^2\cdot(\lvert a\rvert^2)$	$\lvert b\rvert^2\cdot(\lvert a\rvert^2)$ $\lvert a\rvert^2\cdot(1-b^{*\lvert 2})$	$\frac{\lvert a+b\rvert^2}{2}\cdot\left(\frac{\lvert a-b\rvert^2}{2}\right)+$ $\frac{\lvert a-b\rvert^2}{2}\cdot\left(\frac{\lvert a+b\rvert^2}{2}\right)$	$\frac{\lvert a-b\rvert^2}{2}\cdot\left(\frac{\lvert a+b\rvert^2}{2}\right)+$ $\frac{\lvert a+b\rvert^2}{2}\cdot\left(\frac{\lvert a-b\rvert^2}{2}\right)$

(a) average bit error rate $= \frac{1}{4}\left[2\lvert a\rvert^2\lvert b\rvert^2+2\lvert a\rvert^2\lvert b\rvert^2+\frac{\lvert a+b\rvert^2\lvert a-b\rvert^2}{2}+\frac{\lvert a+b\rvert^2\lvert a+b\rvert^2}{2}\right]$

$$= \frac{4\lvert a\rvert^2\lvert b\rvert^2+\lvert a+b\rvert^2\lvert a-b\rvert^2}{4} \quad \#$$

(b) $P(E \text{ learns correctly}) = \frac{1}{4}\left[\lvert a\rvert^2+\lvert a\rvert^2+\frac{\lvert a+b\rvert^2}{2}+\frac{\lvert a+b\rvert^2}{2}\right] = \frac{2\lvert a\rvert^2+\lvert a+b\rvert^2}{4}$ *

(c) Let $\lvert a\rvert=r$, $\lvert b\rvert=s$, $\langle a\lvert b\rangle = rs\cos\theta$, then $\lvert a+b\rvert^2 = r^2+s^2+2rs\cos\theta$, $r^2+s^2=\lvert a\rvert^2+\lvert b\rvert^2=1$.
$\lvert a-b\rvert^2 = r^2+s^2-2rs\cos\theta$

$$\frac{4\lvert a\rvert^2\lvert b\rvert^2+\lvert a+b\rvert^2\lvert a-b\rvert^2}{4} = r^2s^2+\frac{1}{4}\left[(1+2rs\cos\theta)(1-2rs\cos\theta)\right]$$

$$= r^2s^2+\frac{1}{4}-r^2s^2\cos^2\theta = \frac{1}{4}+r^2s^2\sin^2\theta \geq \frac{1}{4}.$$

. when a, b are reals, $\sin\theta=0$, its error rate is $\frac{1}{4}$, reaching the best!

(d) . ∵ a, b are reals ∴ at any θ, the bit error rate is minimal.

. $\frac{2\lvert a\rvert^2+\lvert a+b\rvert^2}{4} = \frac{2\cos^2\theta+(\cos\theta+\sin\theta)^2}{4} = \frac{2\cos^2\theta+2\sin\theta\cos\theta+1}{4} = \frac{2+\cos 2\theta+\sin 2\theta}{4} = \frac{2+\sqrt{2}\sin(\theta+45^\circ)}{4}$

, reaching max value $\frac{2+\sqrt{2}}{4}$ when $\theta = \frac{\pi}{8} = 22.5^\circ$.

#

Problem 2

(a) if $a \neq 0 \cdots 0$, let its $u_1, u_2, \ldots, u_m$-th bits are 1, others are 0.

$$P(f_a(x) = m \bmod 2) = P(m \text{ bits are } 1) + P(m-2 \text{ bits are } 1) + \ldots + P(\text{"}m \bmod 2\text{" bits are } 1)$$

$$= \frac{2^{n-m}}{2^n}\left(C_m^m + C_{m-2}^m + \ldots + C_{m \bmod 2}^m\right)$$

$$= \frac{1}{2^m}\left[C_{m-1}^{m-1} + \left(C_{m-1}^{m-1} + C_{m-2}^{m-1}\right) + \ldots + C_1^m + C_0^m\right]$$

$$= \frac{2^{m-1}}{2^m} = \underline{\frac{1}{2}}$$

$$P(f_a(x) = m-1 \bmod 2) = \frac{2^{n-m}}{2^n}\left(C_{m-1}^m + C_{m-3}^m + \ldots + C_{m-1 \bmod 2}^m\right)$$

$$= \frac{1}{2^m} \cdot 2^{m-1} = \underline{\frac{1}{2}} \quad \#$$

(b)

- obtain a_i by $f_a(e_i) = a_i$ for $i = 1, 2, \ldots, n$. # Query complexity n.
- if the query complexity $< n$, all input vectors can only form a subspace $\leq Z_2^n$.

It is not enough to solve the linear equation:

$$f_a(x_1 | x_2 | \ldots | x_m) \longleftrightarrow \begin{pmatrix} x_1 \\ \hline x_2 \\ \hline \vdots \\ \hline x_m \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \quad XA = B.$$

If $m < n$, $\operatorname{rank} X \leq m < n$, then it's impossible to solve A. #

(c)

- H: $|0\rangle \to |+\rangle = \frac{1}{\sqrt{2}}\left[(-1)^0|0\rangle + (-1)^0|1\rangle\right]$, $|1\rangle \to |-\rangle = \frac{1}{\sqrt{2}}\left[(-1)^0|0\rangle + (-1)^1|1\rangle\right]$, $\underline{H|x\rangle = \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle}$. #
- $H_n|a\rangle = \left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}(-1)^{a_1 y_1}|y_1\rangle\right) \cdots \left(\frac{1}{\sqrt{2}}\sum_{y_n=0}^{1}(-1)^{a_n y_n}|y_n\rangle\right)$

$$= \frac{1}{\sqrt{2^n}}\sum_{y_1, \ldots, y_n \in \{0,1\}}(-1)^{a_1 y_1 + \ldots + a_n y_n}|y_1\rangle|y_2\rangle\cdots|y_n\rangle = \underline{\frac{1}{\sqrt{2^n}}\sum_{y \in Z_2^n}(-1)^{a \cdot y}|y\rangle} \quad \#$$

d)

$$|0\rangle^{\otimes n}\otimes|1\rangle \xrightarrow{H^{\otimes(n+1)}} \frac{1}{\sqrt{2^n}}\Big(\sum_{x\in Z_2^n}|x\rangle\Big)\otimes|-\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}}\Big(\sum_{x\in Z_2^n}(-1)^{f(x)}|x\rangle\Big)|-\rangle$$

$$\xrightarrow{H_n\otimes I} |a\rangle|-\rangle.$$

$$\begin{cases} \text{if } a=00\cdots0, & f_a \text{ is constant} \\ \text{otherwise}, & f_a \text{ is balanced}. \ \# \end{cases}$$

Note: $U_f : |x\rangle|y\rangle \longrightarrow |x\rangle|y\oplus f(x)\rangle$

$$|x\rangle|-\rangle = \frac{1}{\sqrt{2}}(|x\rangle|0\rangle - |x\rangle|1\rangle) \longrightarrow \frac{1}{\sqrt{2}}|x\rangle(|f(x)\rangle - |f(x)\oplus 1\rangle)$$

$$= \frac{1}{\sqrt{2}}|x\rangle\left((-1)^{f(x)}|-\rangle\right) = \frac{1}{\sqrt{2}}(-1)^{f(x)}|x\rangle|-\rangle. \ \#$$

$$H_n\Big(\frac{1}{\sqrt{2^n}}\sum_{x\in Z_2^n}(-1)^{f(x)}|x\rangle\Big)$$

$$\leftrightarrow \frac{1}{\sqrt{2^n}}\sum_{x\in Z_2^n}(-1)^{a\cdot x}\left(\frac{1}{\sqrt{2^n}}\sum_{y\in Z_2^n}(-1)^{x\cdot y}|y\rangle\right)$$

$$\leftrightarrow \frac{1}{2^n}\sum_{\substack{x\in Z_2^n \\ y\in Z_2^n}}(-1)^{x\cdot(a\oplus y)}|y\rangle$$

$$\begin{cases} \text{if } a\oplus y=0, & H_n(\cdots) = \frac{1}{2^n}\sum_{\substack{x\in Z_2^n \\ y\in Z_2^n}}|y\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in Z_2^n}|y\rangle = H_n|0\rangle. \\ \text{if } a\oplus y\neq 0, & H_n(\cdots) \neq H_n|0\rangle. \quad \# \end{cases}$$

(a) $\mathcal{P}(\chi_0)$ is a plane, 2-dim orthonormal linear independent set is enough for a basis!

$$\Theta \triangleq \left\{ |\gamma_0\rangle, |\gamma_0^\perp\rangle \triangleq \frac{|\chi_1\rangle - \langle\gamma_0|\chi_0\rangle|\gamma_0\rangle}{\| |\chi_0\rangle - \langle\gamma_0|\chi_0\rangle|\gamma_0\rangle \|} \right\}. \quad \#$$

(b) let α be the angle s.t. $\langle\gamma_0|\chi_0\rangle = \cos(90^\circ - \alpha) = \sin\alpha$, $\alpha \in [0, \frac{\pi}{2}]$ → $\cos\alpha, \sin\alpha \in [0,1]$.

Then • $\| |\chi_0\rangle - \langle\gamma_0|\chi_0\rangle|\gamma_0\rangle \|^2$

$= \langle\chi_0|\chi_0\rangle - 2\langle\gamma_0|\chi_0\rangle^2 + \langle\gamma_0|\chi_0\rangle^2\langle\gamma_0|\gamma_0\rangle$

$= 1 - 2\sin^2\alpha + \sin^2\alpha \cdot 1 = \underline{\cos^2\alpha}.$

• $\langle\gamma_0^\perp|\chi_0\rangle = \frac{1}{\cos\alpha}\left[\langle\chi_0|\chi_0\rangle - \langle\gamma_0|\chi_0\rangle^2\right] = \frac{1}{\cos\alpha}[1-\sin^2\alpha] = \underline{\cos\alpha}.$

• $|\gamma_0^\perp\rangle = \frac{|\chi_0\rangle - \sin\alpha|\gamma_0\rangle}{\cos\alpha}$

• $I_{|\chi_0\rangle}|\gamma_0\rangle = |\gamma_0\rangle - 2\sin\alpha|\chi_0\rangle$

• $g|\gamma_0\rangle = I_{|\gamma_0^\perp\rangle} I_{|\chi_0\rangle}|\gamma_0\rangle = I_{|\gamma_0^\perp\rangle}|\gamma_0\rangle - 2\sin\alpha\, I_{|\gamma_0^\perp\rangle}|\chi_0\rangle$

$= |\gamma_0\rangle - 2\sin\alpha(|\chi_0\rangle - 2\cos\alpha|\gamma_0^\perp\rangle)$

$= |\gamma_0\rangle - 2\sin\alpha(\sin\alpha|\gamma_0\rangle - \cos\alpha|\gamma_0^\perp\rangle)$

$= \cos 2\alpha|\gamma_0\rangle + \sin 2\alpha|\gamma_0^\perp\rangle$

• $I_{|\chi_0\rangle}|\gamma_0^\perp\rangle = |\gamma_0^\perp\rangle - 2\cos\alpha|\chi_0\rangle$

• $g|\gamma_0^\perp\rangle = I_{|\gamma_0^\perp\rangle}|\gamma_0^\perp\rangle - 2\cos\alpha\, I_{|\gamma_0^\perp\rangle}|\chi_0\rangle$

$= -|\gamma_0^\perp\rangle - 2\cos\alpha(\sin\alpha|\gamma_0\rangle - \cos\alpha|\gamma_0^\perp\rangle)$

$= \cos 2\alpha|\gamma_0^\perp\rangle - \sin 2\alpha|\gamma_0\rangle.$

$$\Rightarrow \begin{pmatrix} g|\gamma_0^\perp\rangle \\ g|\gamma_0\rangle \end{pmatrix} = \begin{pmatrix} \cos 2\alpha & -\sin 2\alpha \\ \sin 2\alpha & \cos 2\alpha \end{pmatrix} \begin{pmatrix} |\gamma_0^\perp\rangle \\ |\gamma_0\rangle \end{pmatrix} \quad \#$$

↓ rotate 2α angle !!

Problem 4.

A	B
$\|\psi_1\rangle\|\psi_2\rangle\cdots\|\psi_n\rangle$	$\longrightarrow x' = x_1' x_2' \cdots x_n'$.

(a)

$\|\psi_i\rangle$	$\begin{pmatrix}1\\0\end{pmatrix}$ $\|0\rangle$ (Z basis)	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ $\|+\rangle$ (Z basis)	$\begin{pmatrix}1\\0\end{pmatrix}$ $\|0\rangle$ (X basis)	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ $\|+\rangle$ (X basis)
P(Bob get 0)	1	$\frac{1}{2}$	$\frac{1}{2}$	1
P(Bob get 1)	0	$\frac{1}{2}$ sure	$\frac{1}{2}$ sure	0
P(Bob sure)	$\frac{1}{4}$		$\frac{1}{4}$	

$\mu = \frac{1}{4}$ #

(b) Suppose Eve use basis $\left\{\begin{pmatrix}a\\b\end{pmatrix}, \begin{pmatrix}-b^*\\a^*\end{pmatrix}\right\}$.

$\|\psi_i\rangle$	$\begin{pmatrix}1\\0\end{pmatrix}$ $\|0\rangle$ "Z basis"		$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ $\|+\rangle$ "Z basis"		$\begin{pmatrix}1\\0\end{pmatrix}$ $\|0\rangle$ "X basis"		$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ $\|+\rangle$ "X basis"	
Eve get bit	0 ($p=\|a\|^2$)	1 ($p=\|b\|^2$)	0 ($p=\frac{\|a+b\|^2}{2}$)	1 ($p=\frac{\|a-b\|^2}{2}$)	0 ($p=\|a\|^2$)	1 ($p=\|b\|^2$)	0 ($p=\frac{\|a+b\|^2}{2}$)	1 ($p=\frac{\|a-b\|^2}{2}$)
Eve send State	$\begin{pmatrix}1\\0\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$
P(Bob get 0)	1	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$	1
P(Bob get 1)	0	$\frac{1}{2}$ sure 0	0	$\frac{1}{2}$ sure 0	$\frac{1}{2}$ sure 1	0	$\frac{1}{2}$ sure 1	0
P(Bob sure)	$\frac{\|b\|^2}{2}$		$\frac{\frac{\|a-b\|^2}{2}}{2}$		$\frac{\|a\|^2}{2}$		$\frac{\frac{\|a+b\|^2}{2}}{2}$	

$$\mu' = \frac{1}{4}\left[\frac{|b|^2}{2} + \frac{\frac{|a-b|^2}{2}}{2} + \frac{|a|^2}{2} + \frac{\frac{|a+b|^2}{2}}{2}\right] = \frac{1}{4}\cdot 1 = \frac{1}{4} \#$$

(c) B sure but wrong: "$|+\rangle$ & Z basis", "$|0\rangle$ & X basis"

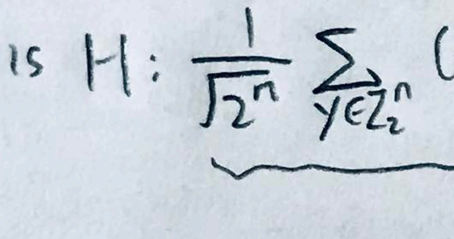
B sure and right: "$|0\rangle$ & Z basis", "$|+\rangle$ & X basis"

→ bit error rate = $\frac{1}{2}$ #

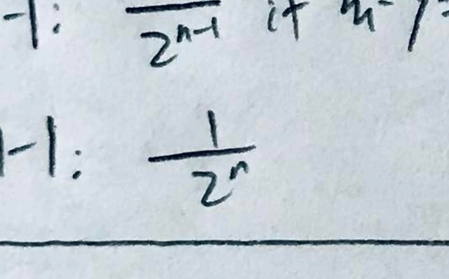
(a)

$$|0\rangle^{\otimes 2n} \xrightarrow{H^{\otimes n}\otimes I^{\otimes n}} \frac{1}{\sqrt{2^n}}\sum_{x\in Z_2^n}|x\rangle|0\rangle^{\otimes n} \xrightarrow{U_f} \frac{1}{\sqrt{2^n}}\sum_{x\in Z_2^n}|x\rangle|f(x)\rangle \xrightarrow{\text{measurement}} \begin{cases} f \text{ is } 2\text{-}1: \frac{1}{\sqrt{2}}(|x\rangle+|x\oplus 4\rangle) \\ f \text{ is } 1\text{-}1: |x\rangle \end{cases} \overset{\triangleq}{=} |\alpha\rangle.$$

measure $|\alpha\rangle$: f is 2-1:



f is 1-1:



Problem 5

(b)

$$|\alpha\rangle \xrightarrow{H^{\otimes n}} |\Theta\rangle = \begin{cases} f \text{ is } 2\text{-}1: \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in Z_2^n}(-1)^{x\cdot y}+(-1)^{(x\oplus 4)\cdot y}|y\rangle = \frac{2}{\sqrt{2^{n+1}}}\sum_{4\cdot y=0}(-1)^{x\cdot y}|y\rangle + \frac{1}{\sqrt{2^{n+1}}}\sum_{4\cdot y\neq 0}(-1)^{x\cdot y}|y\rangle + (-1)^{x\cdot y}|y\rangle \\ f \text{ is } 1\text{-}1: \frac{1}{\sqrt{2^n}}\sum_{y\in Z_2^n}(-1)^{x\cdot y}|y\rangle \end{cases}$$

measure $|\Theta\rangle$: f is 2-1: $\frac{1}{2^{n-1}}$ if $4\cdot y=0$ / $\frac{1}{2^{n-1}}$ if $4\cdot y\neq 0$

f is 1-1: $\frac{1}{2^n}$

(c)

P(add y_i s.t. $y_1, y_2, \dots, y_i$ linear independent):

$P(y_1)=1$

$P(y_2)=1-\frac{1}{2^{n-1}}$

$P(y_3)=1-\frac{2}{2^{n-1}}$

$P(y_4)=1-\frac{2^2}{2^{n-1}}$

$\vdots$

$\Big\} \prod_{k=1}^{n-1}\left(1-\frac{2^{k-1}}{2^{n-1}}\right) \triangleq P.$

$\because (1-a)(1-b)=1-a-b+ab \geq 1-a-b$ if $a,b>0$

$$\therefore P=\frac{1}{2}\prod_{k=1}^{n-2}\left(1-\frac{2^{k-1}}{2^{n-1}}\right) \geq \frac{1}{2}\left(1-\sum_{k=1}^{n-2}\frac{2^{k-1}}{2^{n-1}}\right)=\frac{1}{2}\left(1-\frac{1}{2^{n-1}}\left(1\cdot\frac{2^{n-2}-1}{2-1}\right)\right)=\frac{1}{2}\left(1-\frac{2^{n-2}-1}{2^{n-1}}\right)$$

$$> \frac{1}{4} \quad \#$$

(d) n times $\overset{Q}{\leftrightarrow}$ $P \geq \frac{1}{4}$

$\forall t\in N$, $n\cdot t$ times $\overset{Q}{\leftrightarrow}$ $P \geq 1-(\frac{3}{4})^t \geq 1-\varepsilon$

That is, $(\frac{4}{3})^t \geq \frac{1}{\varepsilon}$, $t \geq \log_{\frac{4}{3}}(\frac{1}{\varepsilon})$.

Given $\varepsilon>0$, When $t=\lceil \log_{\frac{4}{3}}(\frac{1}{\varepsilon})\rceil$, which is a constant, $n\cdot t$ times Query has probability $\geq 1-\varepsilon$. #

$n\cdot t \to O(n)$