1. Qubit rotations and the Hadamard gate

(a) $e^{-\frac{i\theta}{2}(n_xX+n_yY+n_zZ)} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}(n_xX+n_yY+n_zZ)$

Proof. $LHS = \sum_{k=0}^{\infty}\frac{1}{k!}\left[-\frac{i\theta}{2}(n_xX+n_yY+n_zZ)\right]^k$

而 $(n_xX+n_yY+n_zZ)^2 = (n_x^2+n_y^2+n_z^2)I_2 + n_xn_y(XY+YX) + n_yn_z(YZ+ZY) + n_zn_x(XZ+ZX) = I_2$

故 $LHS = \sum_{k=0}^{\infty}\frac{(-1)^k}{(2k)!}\frac{\theta^{2k}}{2^{2k}}I + \sum_{k=0}^{\infty}\frac{i(-1)^k}{(2k+1)!}\frac{\theta^{2k+1}}{2^{2k+1}}(n_xX+n_yY+n_zZ)$

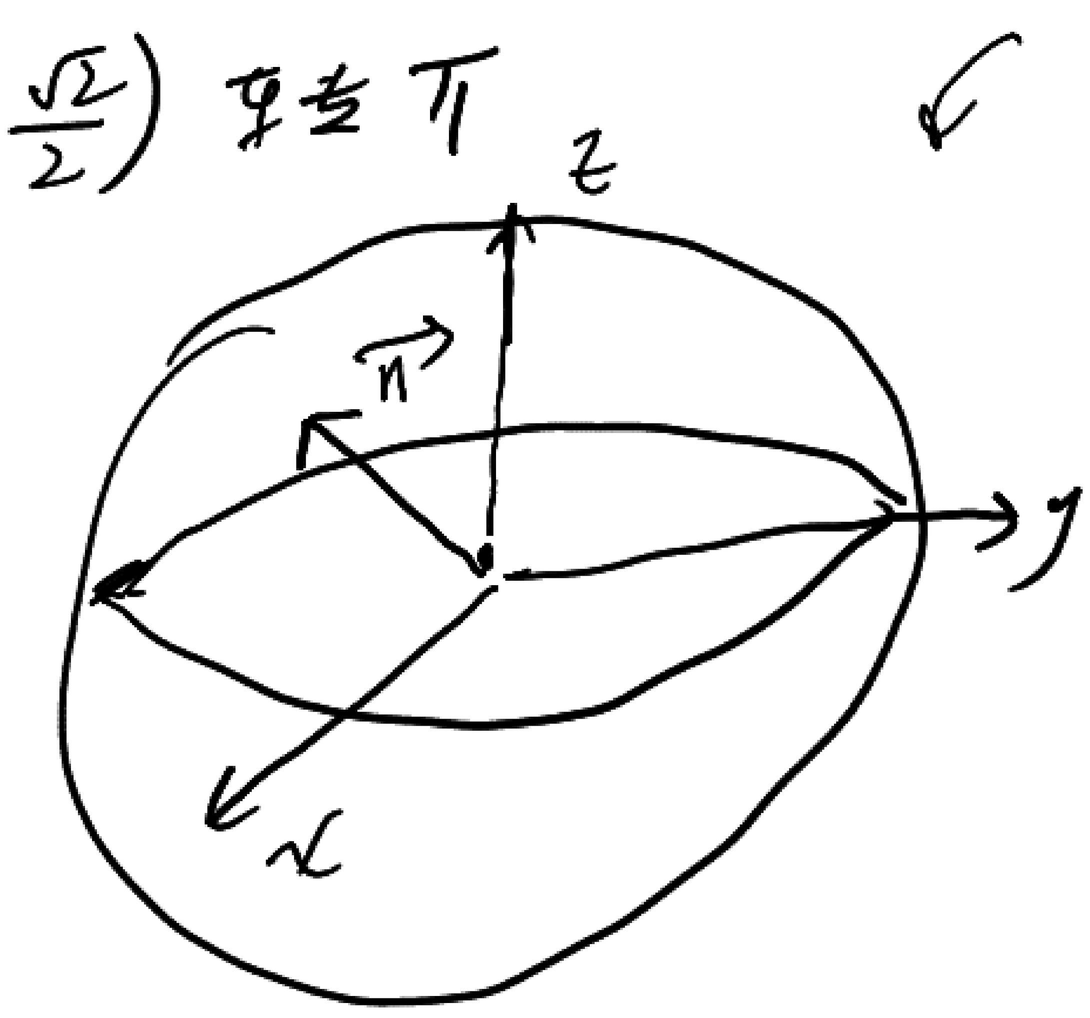
$= \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}(n_xX+n_yY+n_zZ)$, 根据 Taylor 展开 #

(b) $H = e^{i\phi}e^{-i\frac{\theta}{2}(n_xX+n_yY+n_zZ)}$ Find $n_x\ n_y\ n_z\ \phi, \theta$

对比 $H = \begin{pmatrix}\frac{1}{\sqrt2} & \frac{1}{\sqrt2}\\ \frac{1}{\sqrt2} & -\frac{1}{\sqrt2}\end{pmatrix} = e^{i\phi}\begin{pmatrix}\cos\frac{\theta}{2}-i\sin\frac{\theta}{2}n_z & -i\sin\frac{\theta}{2}(n_x-in_y)\\ -i\sin\frac{\theta}{2}(n_x+in_y) & \cos\frac{\theta}{2}+i\sin\frac{\theta}{2}n_z\end{pmatrix}$

可以取 $\theta=\pi$, $n_x=\frac{1}{\sqrt2}$ $n_y=0$ $n_z=\frac{1}{\sqrt2}$, $\phi=\frac{\pi}{2}$ 可验证成立

在Bloch sphere 意义 H 可看作绕 $\vec{n}=(\frac{\sqrt2}{2}, 0, \frac{\sqrt2}{2})$ 转 π



(c) $H = e^{i\phi}R_y(\gamma)R_x(\beta)R_y(\alpha)$

取 $\gamma=0$, $\phi=\frac{\pi}{2}$ $=\pi$, $\alpha=\frac{\pi}{2}$

$e^{i\phi}R_y(\gamma)R_x(\beta)R_y(\alpha)$

$= i\begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt2} & -\frac{1}{\sqrt2}\\ \frac{1}{\sqrt2} & \frac{1}{\sqrt2}\end{pmatrix}$

$= H$ #

先绕 y 轴 $\frac{\pi}{2}$, 再绕 x 轴 π

2. One-out-of-four search

$(-1,1,1,-1,1,-1,1,-1)^T = v_1$
$(1,-1,-1,1,1,-1,1,-1)^T = v_2$
$(1,-1\ \ -1,-1,1,\ 1,-1\ )^T = v_3$
$(1,-1,1,\ ,1,-1,-1,1\ )^T = v_4$

(a) 3次，若有1，则已找到，否则是另一种

(b) $H|0\rangle = |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ $\quad H|1\rangle = |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

故 $H^{\otimes 3}|001\rangle = |++-\rangle = \frac{1}{2\sqrt{2}}(|0\rangle+|1\rangle)^2(|0\rangle-|1\rangle)$

$= \frac{1}{2\sqrt{2}}(|000\rangle+|100\rangle+|010\rangle+|110\rangle-|001\rangle-|101\rangle-|011\rangle-|111\rangle)$

$\xrightarrow{U_f} \frac{1}{2\sqrt{2}}(|00f(00)\rangle-|00\overline{f(00)}\rangle+|10f(10)\rangle-|10\overline{f(10)}\rangle+|01f(01)\rangle-|01\overline{f(01)}\rangle$
$+|11f(11)\rangle-|11\overline{f(11)}\rangle) = \frac{1}{2}\sum_{x\in\{0,1\}^2}(-1)^{f(x)}|x\rangle|-\rangle$

如在 3个 qubit 的 computational basis 下

若 $f(00)=1$, output 为 $\frac{1}{2}(-|00\rangle+|01\rangle+|10\rangle+|11\rangle)|-\rangle = |\psi_1\rangle$
若 $f(01)=1$ output 为 $\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle+|11\rangle)|-\rangle = |\psi_2\rangle$
若 $f(10)=1$, output 为 $\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle+|11\rangle)|-\rangle = |\psi_3\rangle$
若 $f(11)=1$, output 为 $\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle-|11\rangle)|-\rangle = |\psi_4\rangle$

(c) 以 $\langle\psi_1|\psi_2\rangle$ 为例，$\langle\psi_1|\psi_2\rangle = \frac{1}{4}\langle -|(-\langle 00|+\langle 01|+\langle 10|+\langle 11|)(|00\rangle-|01\rangle+|10\rangle$
$+|11\rangle)|-\rangle = 0$ 　其余5组完全类似，故 $|\psi_i\rangle$ 两两垂直，因此

记 $B = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} = B^\dagger$，只需用 B 作用前2个qubit，再在 Computational basis 测量，

若 $f(x)=1$，则得出 $|x\rangle$

因此只需1次.

3 Swap tests

(a) 设 $|\psi\rangle = a|0\rangle + b|1\rangle$

$|\phi\rangle = c|0\rangle + d|1\rangle$

$|\psi\phi\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$

$SWAP|\psi\phi\rangle = ac|00\rangle + bc|01\rangle + ad|10\rangle + bd|11\rangle$

$= (c|0\rangle + d|1\rangle)(a|0\rangle + b|1\rangle) = |\phi\rangle|\psi\rangle$

$|0\rangle|\psi\rangle|\phi\rangle \xrightarrow{H\otimes I^{\otimes 2}} |+\rangle|\psi\rangle|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\psi\rangle|\phi\rangle)$

$\xrightarrow{C\text{-}SWAP} \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle|\phi\rangle + |1\rangle SWAP(|\psi\rangle|\phi\rangle))$

$= \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\psi\rangle)$

$\xrightarrow{H\otimes I^{\otimes 2}} \frac{1}{\sqrt{2}}(|+\rangle|\psi\rangle|\phi\rangle + |-\rangle|\phi\rangle|\psi\rangle)$

(b) output is $\frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|\psi\phi\rangle + \frac{|0\rangle-|1\rangle}{\sqrt{2}}|\phi\psi\rangle\right)$

$= \frac{\||\psi\phi\rangle+|\phi\psi\rangle\|}{2}|0\rangle\frac{|\psi\phi\rangle+|\phi\psi\rangle}{\||\psi\phi\rangle+|\phi\psi\rangle\|} + \frac{\||\psi\phi\rangle-|\phi\psi\rangle\|}{2}|1\rangle\frac{|\psi\phi\rangle-|\phi\psi\rangle}{\||\psi\phi\rangle-|\phi\psi\rangle\|}$

$= \frac{\sqrt{2+2|\langle\phi|\psi\rangle|^2}}{2}|0\rangle\frac{|\psi\phi\rangle+|\phi\psi\rangle}{\sqrt{2+2|\langle\phi|\psi\rangle|^2}} + \frac{\sqrt{2-2|\langle\phi|\psi\rangle|^2}}{2}|1\rangle\frac{|\psi\phi\rangle-|\phi\psi\rangle}{\sqrt{2-2|\langle\phi|\psi\rangle|^2}} \quad (\triangle)$

故 $Pr(|0\rangle) = \frac{1}{2} + \frac{1}{2}|\langle\phi|\psi\rangle|^2$

(其中$(\triangle)$是因为 $\||\psi\phi\rangle \pm |\phi\psi\rangle\| = \sqrt{2 \pm \langle\psi|\langle\phi||\psi\rangle|\phi\rangle \pm \langle\phi|\langle\psi||\phi\rangle|\psi\rangle}$

$= \sqrt{2\pm\langle\phi|\psi\rangle\langle\psi|\phi\rangle \pm \langle\psi|\langle\phi||\phi\rangle|\psi\rangle} = \sqrt{2\pm 2|\langle\phi|\psi\rangle|^2}$)

(c) 为 $\frac{|\psi\phi\rangle+|\phi\psi\rangle}{\sqrt{2}\sqrt{1+|\langle\phi|\psi\rangle|^2}}$

(d) 记 $|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x|x\rangle \quad |\phi\rangle = \sum_{y\in\{0,1\}^n} b_y|y\rangle$

$SWAP\,|\psi\phi\rangle = swap\sum_{x,y\in\{0,1\}^n} a_x b_y|x\rangle|y\rangle = \sum_{x,y\in\{0,1\}^n} a_x b_y|y\rangle|x\rangle$

$= |\phi\rangle|\psi\rangle$ 仔细检查，发现(a)(b)(c)推导依然成立，故结果不变.

4 The Bernstein-Vazirani Problem

(a) 需要 n 次.

一方面, 取 $x^1 = (1,0,\cdots 0)$ $\quad x^1 \cdot s = s_1 \pmod 2$ 知 s_1

$x^2 = (0,1,\cdots 0)$ $\quad x^2 \cdot s = s_2 \pmod 2$ 知 s_2 $\quad$ 可知 s

$\vdots$

$x^n = (0,\cdots 1)$ $\quad x^n \cdot s = s_n \pmod 2$ 知 s_n

另方面, 若只取 $n-1$ 次, s 真实值为 0

得到 $b_1 = x_1 \cdot s = 0 \pmod 2 \cdots$ $\quad b_{n-1} = x_{n-1} \cdot s = 0 \pmod 2$

设 $V_s = \mathrm{span}\langle x_1 \cdots x_{n-1}\rangle$ 为 $V = (\mathbb{F}_2)^n = (\mathbb{Z}/2\mathbb{Z})^n$ 的 $\le n-1$ 维子空间,

$V = V_s \oplus V_s^\perp$, $\dim(V^\perp) \geq 1$, $V_s^\perp$ 为 V_s 在 V 正交补 取 $s^* \in V^\perp \setminus \{0\}$,

则 $s^* \cdot x_j = 0 \pmod 2$, $\forall j = 1, \cdots n-1$ 因此无法排除 $s = s^*$ 情况. $n-1$ 不够.

(b) 若 $u = 00\cdots 0$ $\quad \sum_{v\in\{0,1\}^n} (-1)^{u\cdot v} = \sum_{v\in\{0,1\}^n} 1 = 2^n$

否则, 设 i_0 为 u 第一个为 1 的位 $(1 \le i_0 \le n)$ 记 $A = \{v \in \{0,1\}^n \mid u\cdot v = 0 \bmod 2\}$

$B = \{v \in \{0,1\}^n \mid u \cdot v = 1 \bmod 2\}$

考虑映射 $T: A \to B$

$(s_1, \cdots s_n) \mapsto (s_1, \cdots \overline{s_{i_0}}, \cdots s_n)$

$R: B \to A$

$(s_1, \cdots s_n) \mapsto (s_1, \cdots \overline{s_{i_0}}, \cdots s_n)$

由于 $T \circ R = id_B$, $R \circ T = id_A$, T 为双射 故 $|A| = |B|$

故 $\sum_{v\in\{0,1\}^n} (-1)^{u\cdot v} = \sum_{v\in A} (-1)^0 + \sum_{v \in B} (-1)^1 = |A| - |B| = 0$ #

(c) $(H^{\otimes n} \otimes I)\, |0\rangle^{\otimes n} |-\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle |-\rangle = \frac{1}{\sqrt{2^{n+1}}} \Big(\sum_{x\in\{0,1\}^n} |x\rangle|0\rangle$

$- \sum_{x\in\{0,1\}^n} |x\rangle|1\rangle \Big) \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}} \right)$

$= \frac{1}{\sqrt{2^n}} \Bigg(\sum_{\substack{x\in\{0,1\}^n \\ f(x)=0}} |x\rangle|-\rangle - \sum_{\substack{x\in\{0,1\}^n \\ f(x)=1}} |x\rangle|-\rangle \Bigg) = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle|-\rangle$

$$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s} |x\rangle|-\rangle \xrightarrow{H^{\otimes n} \otimes I} \frac{1}{\sqrt{2^n}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot (y \oplus s)} |y\rangle|-\rangle$$

$$= \sum_{y \in \{0,1\}^n} \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot (y \oplus s)} \right) |y\rangle|-\rangle$$

$= |s\rangle|-\rangle$ （根据(b)，当且仅当 $y=s$，$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot (y \oplus s)} = 1$

其它情况 $\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot (y \oplus s)} = 0$ ） #

(d) 对前 n 个 qubit 作 computational basis 的 measurement 即可得到 s

（因为 s 是其中一个基）

故只需1次

5 A fast approximate QFT

(a) CR_k 矩阵表示为 $\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$, $B := CR_k + (CR_k)^\dagger = \begin{pmatrix} 2 & & & \\ & 2 & & \\ & & 2 & \\ & & & 2\cos\frac{2\pi}{2^k} \end{pmatrix}$

$\frac{1}{\sqrt{2^n}} \sum_{y\in \mathbb{Z}_2^n} e^{\frac{2\pi i x y}{2^n}} |y\rangle$

$y = 2^{i_1} + \cdots + 2^{i_k} = (0\cdots1 0\cdots1\cdots1\cdots)$

$\frac{x}{2^{n-i_k}}$

$$E(CR_k, I) = \max_{|\psi\rangle} \| CR_k|\psi\rangle - |\psi\rangle \|$$

$$= \max_{|\psi\rangle} \sqrt{(\langle\psi|(CR_k)^\dagger - \langle\psi|)(CR_k|\psi\rangle - |\psi\rangle)}$$

$$= \max_{|\psi\rangle} \sqrt{2\langle\psi|\psi\rangle - \langle\psi|CR_k|\psi\rangle - \langle\psi|(CR_k)^\dagger|\psi\rangle}$$

$$= \max_{|\psi\rangle} \sqrt{2 - \langle\psi|B|\psi\rangle}$$

设 $|\psi\rangle = a_1|00\rangle + a_2|01\rangle + a_3|10\rangle + a_4|11\rangle$, $\sum |a_i|^2 = 1$, $a_i \in \mathbb{C}$

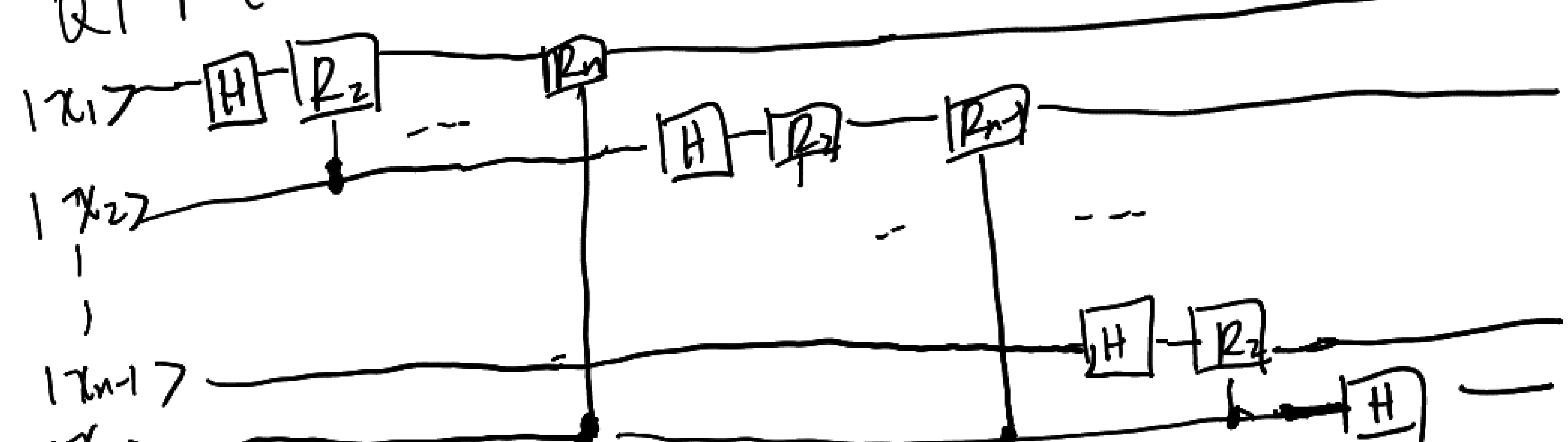
$\langle\psi|B|\psi\rangle = 2(|a_1|^2 + |a_2|^2 + |a_3|^2) + 2\cos\frac{2\pi}{2^k}|a_4|^2 = 2\left(1 - (1-\cos\frac{2\pi}{2^k})|a_4|^2\right)$

$\geq 2\cos\frac{2\pi}{2^k}$，且当 $|\psi\rangle = |11\rangle$ 取等

故 $E(CR_k, I) = \max_{|\psi\rangle} \sqrt{2 - \langle\psi|B|\psi\rangle} = \sqrt{2 - 2\cos\frac{2\pi}{2^k}} = 2\sin\frac{\pi}{2^k} \leq \frac{2\pi}{2^k}$ #

(b) 记 $K = K(c) = \lfloor \log_2 n + c \rfloor$

QFT 电路图 (F)



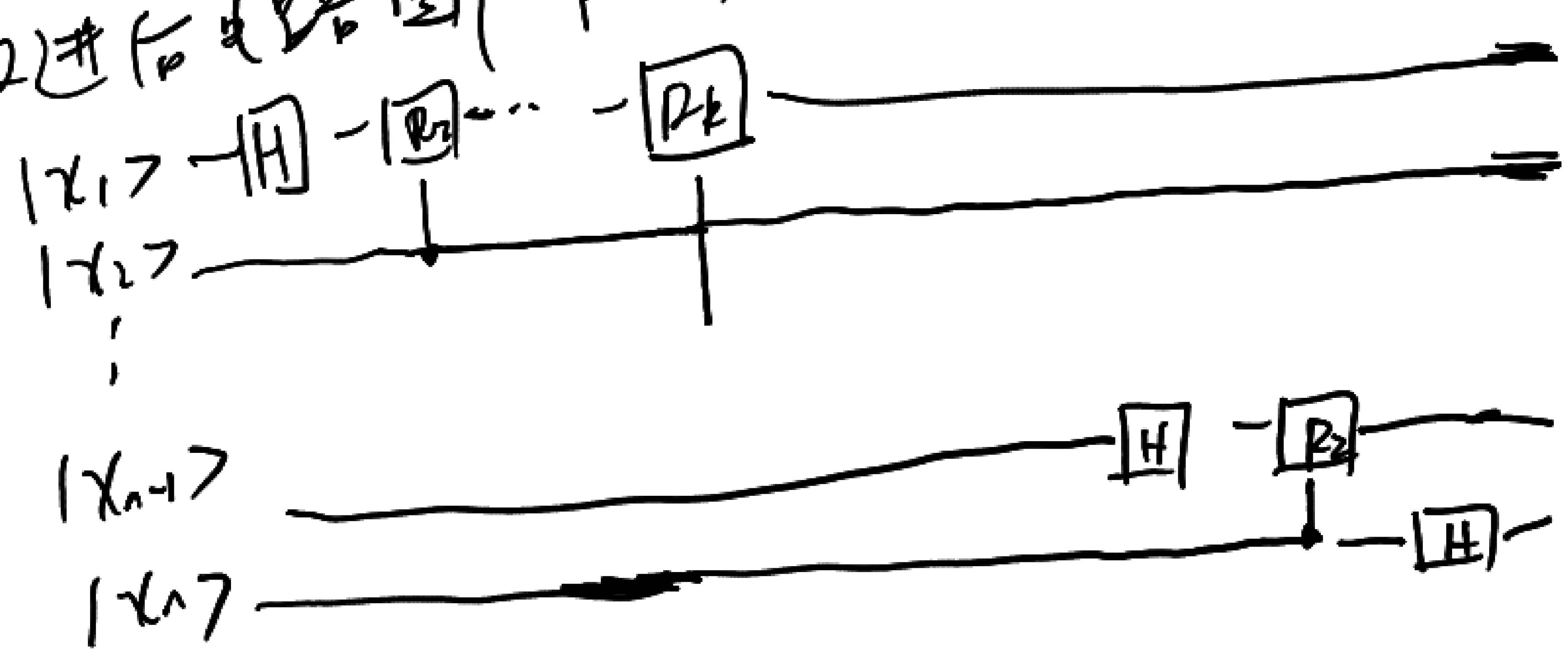
$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\, 0.x_1\cdots x_n}|1\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \times 0.x_2\cdots x_n}|1\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \times 0.x_{n-1}x_n}|1\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \times 0.x_n}|1\rangle)$

而 改进后电路图 ($\hat{F}$)



$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \times 0.x_1\cdots x_k}|1\rangle)$

⋮

$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \times 0.x_{n-1}x_n}|1\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \times 0.x_n}|1\rangle)$

$F = H_1 V_2 \cdots V_n H_2 V_2 \cdots V_{n-1} \cdots H_{n-1} V_2 H_n$，其中 V_i, H_i 为 $\mathbb{C}^{\otimes n}$ 上正交变换（每个门）

$\tilde{F} = H_1 V_2 \cdots V_k I \cdots I H_2 V_2 \cdots V_k I \cdots I \cdots H_{n-1} V_2 H_n$

由 $E(\cdot,\cdot)$ 的次可加性，$E(F, \tilde{F}) \le E(V_{k+1}, I) + \cdots + E(V_n, I)$

$+ E(V_{k+1}, I) + \cdots + E(V_{n-1}, I) + \cdots + E(V_{k+1}, I)$

$$= \sum_{s=k+1}^{n} (n+1-s) E(V_s, I)$$

不妨设 $V_s = CR_s \otimes I^{n-2}$

$$V_s = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & e^{\frac{2\pi i}{2^s}} & & \\ & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix} \quad B := V_s + V_s^\dagger = \begin{pmatrix} 2 & & & \\ & \ddots & & \\ & & 2\cos\frac{2\pi}{2^s} & \\ & & & \ddots \\ & & & & 2 \end{pmatrix}$$

类似于 (a)，$E(V_s, I) = \max\limits_{\substack{|\psi\rangle \in \mathbb{C}^{\otimes n} \\ \langle\psi|\psi\rangle = 1}} \sqrt{2 - \langle\psi|B|\psi\rangle} \le \frac{2\pi}{2^s}$

故 $E(F, \tilde{F}) \le \left[\sum_{s=k+1}^{n} \frac{(n+1-s)}{2^s}\right] 2\pi = 2\pi\left[\frac{n-k-1}{2^k} + \frac{1}{2^n}\right]$

注意到 $k = \lfloor \log_2 n + C \rfloor$

则有 $E(F, \tilde{F}) \le 2\pi\left[\frac{1}{2^n} + \frac{n - \log_2 n - C}{n 2^{C-1}}\right]$

但注意到有隐含约束 $n \ge \log_2 n + C$（否则 $F = \tilde{F}$，$E(F, \tilde{F}) = 0$）

故 $E(F, \tilde{F}) \le 2\pi\left(\frac{1 + 2(n - \log_2 n - C)}{n 2^C}\right) \le 2\pi \cdot \frac{4n}{n 2^C} = \frac{8\pi}{2^C} < \varepsilon$

当 $C > \log_2\left(\frac{8\pi}{\varepsilon}\right)$ #

(c) 记 $k = \lceil \log_2 n + C \rceil$

从电路图可以看出，共用了 $n + k(n-k) + k-1 + \cdots + 1$

$= O(n \log n)$ 个门.