Note for Quantum Information

吕铭 Lyu Ming

April 9, 2015

1 Basic definitions and tools

1. Mutually unbiased bases:

$$\{\psi_m\}_{m=0}^d, \{\phi_n\}_{n=0}^d, \langle\psi_m|\phi_n\rangle = 1/d \tag{1.1}$$

2. The Pavia notation (double ket notation):

$$|\Psi\rangle\!\rangle = \sum_{m,n} \langle m|\Psi|n\rangle\, |m\rangle\, |n\rangle \tag{1.2}$$
$$\langle\!\langle\Phi|\Psi\rangle\!\rangle = \mathrm{Tr}[\Phi^\dagger\Psi] \tag{1.3}$$
$$(A\otimes B)|\Psi\rangle\!\rangle = |A\Psi B^T\rangle\!\rangle \tag{1.4}$$
$$\big|\, |\alpha\rangle\langle\beta|\, \rangle\!\rangle = |\alpha\rangle\, |\beta^*\rangle \tag{1.5}$$
$$\langle\alpha|\, \langle\beta|\, \Psi\rangle\!\rangle = \langle\alpha|\Psi|\beta^*\rangle \tag{1.6}$$

Unlike the Dirac notation, he notation is basis dependent.

3. CHSH inequality (special case of Bell inequality)

$$\omega_C = \sum_\lambda p(\lambda)\left[\frac{1}{4}\sum_{a,b\in\{0,1\}}\sum_{x,y\in\{0,1\}}(-)^{x+y+ab}p_A(x|a,\lambda)p_B(y|b,\lambda)\right] \tag{1.7}$$
$$\leq \frac{1}{4}\sum_{a,b}(-)^{f_A(a)+f_B(b)+ab} \leq \frac{1}{2} \tag{1.8}$$
$$\omega_Q = \frac{1}{4}\sum_{a,b}\sum_{x,y}(-)^{x+y+ab}\left|\langle x,\theta_a|\langle y,\tau_b|\Psi^+\rangle\right|^2 \tag{1.9}$$
$$= \frac{1}{4}\sum_{a,b}(-)^{ab}\cos(\theta_a-\tau_b) \leq \frac{1}{\sqrt{2}} \tag{1.10}$$

4. Doing partial trace to get marginal states

5. Bell states for d dimensions:

$$|\Phi_{p,q}\rangle := (S^p M^q \otimes I)\,|\Phi\rangle \tag{1.11}$$

where $S = \sum |(n+1) \mod d\rangle\langle n|$, and $M = \sum \exp(2\pi i n/d)\,|n\rangle\langle n|$

6. Trace-norm: Let $\Psi : \mathcal{H}_B \to \mathcal{H}_A$ and its sigular balue decomposition (SVD): $\Psi = \sum_n \lambda_n |\alpha_n\rangle\langle\beta_n|$:

$$\|\Psi\|_1 := \sum_n |\lambda_n| \tag{1.12}$$

Alternative characterization of the trace norm:

$$\|\Psi\|_1 = \max_{V:\mathcal{H}_A\to\mathcal{H}_B, V^\dagger V = I_A} \mathrm{Tr}[\Psi V] \tag{1.13}$$

For pure states:

$$\|\pi_0 |\psi_0\rangle \langle\psi_0| - \pi_1 |\psi_1\rangle \langle\psi_1| \|_1 = \sqrt{1 - 4\pi_0\pi_1 |\langle\psi_0|\psi_1\rangle|^2} \tag{1.14}$$

p-norm:

$$\|\Psi\|_p := \left(\sum_n |\lambda_n|^p\right)^{1/p} \tag{1.15}$$

- $\forall c \in \mathbb{C}. \|\Psi\| = |c| \|\Psi\|$
- $\|\Psi\| = 0 \Leftrightarrow \Psi = 0$
- $\|\Psi + \Psi'\| \leq \|\Psi\| + \|\Psi'\|$
- $\|M \otimes N\| = \|M\| \|N\|$

2 General math model for Quantum computing

1. Quantum state as density matrix ρ:

$$\rho^\dagger = \rho, \quad \rho \geq 0, \quad \mathrm{Tr}[\rho] = 1 \tag{2.1}$$

The set of all density matrices is convex. The set of all pure states is the collection of all its extreme points.

2. Quantum evolution as Quantum channel $\mathscr{C}(\rho)$:

$$\begin{aligned} &\text{linear:} && \mathscr{C}(\alpha\rho_1 + \beta\rho_2) = \alpha\mathscr{C}(\rho_1) + \beta\mathscr{C}(\rho_2), && (2.2)\\ &\text{trace-preserving:} && \mathrm{Tr}[\mathscr{C}(\rho)] = \mathrm{Tr}[\rho], && (2.3)\\ &\text{completely positive:} && \forall \mathcal{H}_B, \rho \geq 0. \mathscr{C} \otimes \mathscr{I}_B(\rho) \geq 0 && (2.4) \end{aligned}$$

(a) Physical implementation:

$$\mathscr{C}(\rho) = \mathrm{Tr}_{B'}\left[U_{AB\to A'B'}(\rho_A \otimes \sigma_B) U^\dagger_{AB\to A'B'}\right] \tag{2.5}$$

(b) Mathematical description (Kraus theorem):

$$\mathscr{C}(\rho) = \sum_k C_k \rho C_k^\dagger, \quad \text{where } \sum_k C_k^\dagger C_k = I_A \tag{2.6}$$

(c) isometric encoding: To encode the information carried by a system A into a larger system A'.

$$\mathscr{V}(\rho) = V\rho V^\dagger \tag{2.7}$$

where $V^\dagger V = I_A$

3. Quantum measurement as POVM (*positive operator-valued measure*) $\{P_n\}$:

$$p(n) := \mathrm{Tr}[P_n\rho], \quad P_n \geq 0, \quad \sum_n P_n = I \tag{2.8}$$

(a) Physical implementation:

$$p(n) = \sum_k \langle n|\mathscr{C}(\rho)|n\rangle = \mathrm{Tr}\left[\sum_k C_k^\dagger |n\rangle \langle n| C_k \rho\right] \tag{2.9}$$

On the other hand:

$$\mathscr{C}(\rho) := \sum_n \mathrm{Tr}[P_n\rho] |n\rangle \langle n| \tag{2.10}$$

(b) Example: describing not-accurate ONB measurement

$$P_0 = \int p(\theta) |0,\theta\rangle \langle 0,\theta| \, \mathrm{d}\theta \tag{2.11}$$

$$P_1 = \int p(\theta) |1,\theta\rangle \langle 1,\theta| \, \mathrm{d}\theta \tag{2.12}$$

(c) Naimark's theorem:
For every POVM $\{P_n\}$ there exists a system B and a pure state $|\beta\rangle \in \mathcal{H}_B$ and a projective POVM $\{E_n\}$

$$\mathrm{Tr}[P_n \rho] = \mathrm{Tr}[E_n(\rho \otimes |\beta\rangle \langle\beta|)] \tag{2.13}$$

4. Indirect measurement as Quantum Instrument $\{\mathscr{Q}_n(\rho)\}$:

$$\mathscr{Q} = \sum_n \mathscr{Q}_n \text{ is a quantum channel} \tag{2.14}$$

$$p_n = \mathrm{Tr}[\mathscr{Q}_n(\rho)] \tag{2.15}$$

$$\rho_{|n} = \mathscr{Q}_n(\rho)/\,\mathrm{Tr}[\mathscr{Q}_n(\rho)] \text{ (Bayes rule for quantum states)} \tag{2.16}$$

where we also call $\mathscr{Q}_n$ quantum operation.

(a) Physical implementation:

$$\mathscr{Q}_n(\rho) := \mathrm{Tr}_B[(I_A \otimes Q_n)\mathscr{C}(\rho)] \tag{2.17}$$

where we can define:

$$\mathscr{C}(\rho) := \sum_n \mathscr{Q}_n(\rho) \otimes |n\rangle \langle n| \tag{2.18}$$

$$Q_n := |n\rangle \langle n| \tag{2.19}$$

3 Some mathematical operations

1. Purification:

(a) The Schmidt decomposition:

$$\rho_A = \sum_{m=1}^{r} p_m |\alpha_m\rangle \langle\alpha_m| = \mathrm{Tr}_B[\sum_{m=1}^{r} \sqrt{p_m} |\alpha_m\rangle |\beta_m\rangle] \tag{3.1}$$

where $\{|\alpha_m\rangle\}$ and $\{|\beta_m\rangle\}$ are ONBs. The proof is an immediate consequence of the singular value decomposition (SVD).

(b) The uniqueness:

$$\rho_A = \mathrm{Tr}_A[|\Psi\rangle \langle\Psi|] = \mathrm{Tr}_A[|\Psi'\rangle \langle\Psi'|] \tag{3.2}$$

$$\Rightarrow |\Psi'\rangle = (I_A \otimes S) |\Psi\rangle \tag{3.3}$$

where S is a partial isometry ($SS^\dagger$ and $S^\dagger S$ are projectors).

2. Universal steering:
Let $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a purification of ρ_A, then for every decomposition $\rho_A = \sum_m p_m \rho_m$, there exists a POVM on B: $\{Q_m\}$:

$$\mathrm{Tr}_B[I_A \otimes Q_m |\Psi\rangle \langle\Psi|] = p_m \rho_m \tag{3.4}$$

- From Bell state $|\Phi\rangle = \frac{1}{\sqrt{d}}|I\rangle\rangle$ to any state ρ with POVM $\{\rho^T, I - \rho^T\}$:

$$\mathrm{Tr}_B[(I_A \otimes \rho^T)\,|\Phi\rangle\,\langle\Phi|] = \frac{\rho}{d} \tag{3.5}$$

3. Encoding a quantum operation in a quantum state: Choi matrix

$$\Phi_{\mathscr{M}} := (\mathscr{M} \otimes \mathscr{I})(|\Phi\rangle\rangle\langle\langle\Phi|) \tag{3.6}$$

$$\mathscr{M}(\rho) = d\,\mathrm{Tr}_B[(I_A \otimes \rho^T)\Phi_{\mathscr{M}}] \tag{3.7}$$

- "Diagonalize" Kraus representation: $\mathscr{C}(\rho) = \sum_i C_i \rho C_i^\dagger$ with $\mathrm{Tr}[C_j^\dagger C_i] = \delta_{ij} p_i d_A$

4. No information without disturbance:
For the quantum instrument $\{\mathscr{Q}_n | \sum_n \mathscr{Q}_n = \mathscr{I}\}$ (that's the condition of non-disturbing), the outcome does not depend on measured system.

$$\sum_n \Phi_{\mathscr{Q}_n} = |\Phi\rangle\rangle\langle\langle\Phi| \Rightarrow \mathscr{Q}_n = p_n \mathscr{I}_n \tag{3.8}$$

5. The no-cloning theorem:
For two distinct non-orthogonal states $|\varphi_0\rangle$ and $|\varphi_1\rangle$, there is no quantum channel such that:

$$\forall i \in \{0,1\}. \mathscr{C}(|\varphi_i\rangle\,\langle\varphi_i|) = (|\varphi_i\rangle\,\langle\varphi_i|)^{\otimes 2} \tag{3.9}$$

What we still can do:

- Cloning orthogonal states
- The universal cloning machine

$$\mathscr{C}(\rho) = \frac{1}{2(d+1)}(I + \mathtt{SWAP})(\rho \otimes I_B)(I + \mathtt{SWAP}) \tag{3.10}$$

- Probabilistic cloning?..

Corollary:

- No-distinguishability theorem: It is impossible to construct a machine that distinguishes perfectly between two non-orthogonal states $|\psi_0\rangle$ and $|\psi_1\rangle$.
- Secure key distribution: the BB84 protocol (Bennett and Brassard, 1984).

6. Quantum teleportation (discribed as a quantum instrument)

$$\mathrm{Tr}_{A'A}[(I_B \otimes P_n)(|\Phi_0\rangle\,\langle\Phi_0|_{BA'} \otimes \rho_A)] = \frac{1}{4} U_n^\dagger \rho_A U_n \tag{3.11}$$

where $|\Phi_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, $|\Phi_i\rangle = |\sigma_i\rangle\rangle/\sqrt{2}$ are Bell states, $U_0 = I$, $U_i = \sigma_i$, $P_n = |\Phi_n\rangle\,\langle\Phi_n|$, means keep the state but transform it to another system. For higher dimension system:

$$\mathrm{Tr}_{AA'}[(|\Phi_{pq}\rangle\,\langle\Phi_{pq}|_{AA'} \otimes I_B)(\rho_A \otimes |\Phi_{00}\rangle\,\langle\Phi_{00}|_{A'B})] = \frac{1}{d^2} U_{pq}^\dagger \rho_B U_{pq} \tag{3.12}$$

4 Quantum discrimination

4.1 State discrimination

1. Helstrom's minimum error decoder:

$$\omega := p_{\text{succ}} - p_{\text{err}} = \sum_{x,y\in\{0,1\}} (-)^{x+y}\,\mathrm{Tr}[P_y \rho_x]\pi_x \leq \|\Delta\|_1 := \sum |\delta_n| \tag{4.1}$$

where δ_n is the eigenvalues of $\Delta = \pi_0\rho_0 - \pi_1\rho_1 = \sum_n \delta_n |\psi_n\rangle\langle\psi_n|$. We reach the upper bound by:

$$P_0 = \sum_{\delta_n > 0} |\psi_n\rangle\langle\psi_n|$$
$$P_1 = \sum_{\delta_n \le 0} |\psi_n\rangle\langle\psi_n|$$

- For pure state $\rho_0 = |\psi_0\rangle\langle\psi_0|$, $\rho_1 = |\psi_1\rangle\langle\psi_1|$,

$$\omega_{\max} = \sqrt{1 - 4\pi_0\pi_1 F}, \quad F := |\langle\psi_0|\psi_1\rangle|^2 \tag{4.2}$$

- Fidelity for mixed states:

$$1 - \sqrt{4\pi_0\pi_1 F(\rho_0,\rho_1)} \le \|\pi_0\rho_0 - \pi_1\rho_1\|_1 \le \sqrt{1 - 4\pi_0\pi_1 F(\rho_0,\rho_1)} \tag{4.3}$$

where:

$$F(\rho_0,\rho_1) := \sup_{\mathcal{H}_A} \max_{\mathrm{Tr}_A[|\Psi_0\rangle\langle\Psi_0|]=\rho_0} \max_{\mathrm{Tr}_A[|\Psi_1\rangle\langle\Psi_1|]=\rho_1} |\langle\Psi_0|\Psi_1\rangle|^2 \tag{4.4}$$

- Uhlmann's theorem

$$F(\rho_0,\rho_1) = \|\sqrt{\rho_0}\sqrt{\rho_1}\|_1^2 \tag{4.5}$$

- Minimum of the Bhattacharya coefficient:

$$F(\rho_0,\rho_1) = \min_N \min_{\forall \mathrm{POVM}\{P_n\}_{n=1}^N} \left(\sum_n \sqrt{\mathrm{Tr}[P_n\rho_0]\,\mathrm{Tr}[P_n\rho_1]}\right)^2 \tag{4.6}$$

- Quantum Chernoff bound: Error probability in distinguishing two states with N copies goes to zero at rate $O(C^N)$ where

$$C = \min_{p:0\le p\le 1} \mathrm{Tr}[\rho_0^p\rho_1^{1-p}](< \sqrt{F(\rho_0,\rho_1)}) \tag{4.7}$$

2. The unambiguous state discriminator: to distinguish $\{|\psi_i\rangle\}$, we use POVM $\{P_i, P_?\}$, where we get answer without error or we don't know about the answer:

$$\langle\psi_i|P_j|\psi_i\rangle = p_i\delta_{ij} \tag{4.8}$$
$$P_? = I - \sum_i P_i \tag{4.9}$$

It is possible if and only if $\{|\psi_n\rangle\}_{n=1}^N$ are linearly independent.

$$P_n = p\Phi^{-1}|\psi_n\rangle\langle\psi_n|\Phi^{-1} \tag{4.10}$$
$$\Phi := \sum_n |\psi_n\rangle\langle\psi_n| \tag{4.11}$$

For $N = 2$ system $p_? = \sqrt{F}$

4.2 Channel discrimination

1. Input any state:

$$\omega_{\max} = \max_{|\alpha\rangle\in\mathcal{H}_A} \|\pi_0\mathscr{C}_0(|\alpha\rangle\langle\alpha|) - \pi_1\mathscr{C}_1(|\alpha\rangle\langle\alpha|)\|_1 \tag{4.12}$$

2. Input an entangled state:

$$\omega_{\max}^{\mathrm{ent}} = \max_{\mathcal{H}_B} \max_{|\Psi\rangle\in\mathcal{H}_A\otimes\mathcal{H}_B} \|\pi_0(\mathscr{C}_0\otimes\mathscr{I}_B)(|\Psi\rangle\langle\Psi|) - \pi_1(\mathscr{C}_1\otimes\mathscr{I}_B)(|\Psi\rangle\langle\Psi|)\|_1 \tag{4.13}$$

3. diamond norm
$$\|\Delta\|_\diamond = \max_{|\Psi\rangle\in\mathcal{H}_A\otimes\mathcal{H}_A} \|\Delta\otimes\mathscr{I}_A(|\Psi\rangle\langle\Psi|)\|_1 \tag{4.14}$$

4. For unitary operator U_0, U_1. For eigenvalues $\mathrm{e}^{\mathrm{i}\theta_m}$ of $U_0^\dagger U_1$:
$$\omega = \sqrt{1-4\pi_0\pi_1 F} = \sqrt{1-4\pi_0\pi_1\left|\sum_m p_m \mathrm{e}^{\mathrm{i}\theta_m}\right|} \tag{4.15}$$
   - Entanglement does not help
   - Certainty answer can be get within finite number of times.
   - Extend to more gates

5 Quantum programming

1. programmable machine:
$$V|\alpha\rangle|n\rangle = U_n|\alpha\rangle|n\rangle \tag{5.1}$$
   Example: $V=\sum_n U_n\otimes|n\rangle\langle n|$

2. No-programming theorem (Nielsen-Chuang, PRL 1997): In order to program N distinct unitary gates, one needs N orthogonal program states.

3. Universal set of quantum gates: Every qubit gate can be approximated with arbitrary precision with a circuit consisting only of 2 elementary gates. And for a system in dimension $d\geq 2$, it is enough to use $O(\log^2 d)$ gates.
   - For N qubits system (dimension 2^N), It is enough to have a universal set for every qubit and a entangling gate W_{ij} on every two qubits.
   - Usually we use $\{H, T, \texttt{CNOT}\}$:
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{5.2}$$
$$= \mathrm{i}\exp\left[\frac{-\mathrm{i}\pi\boldsymbol{n}\cdot\boldsymbol{\sigma}}{2}\right] \qquad \boldsymbol{n}=\frac{1}{\sqrt{2}}(1,0,1)^T \tag{5.3}$$
$$T = \exp\left[\frac{-\mathrm{i}\pi\sigma_z}{8}\right] \tag{5.4}$$
$$\texttt{CNOT} = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes\sigma_x \tag{5.5}$$
   - Solovay-Kitaev's Theorem: Let $\texttt{U}$ be a universal set of unitary gates in dimension d with the property that $\forall U\in\texttt{U}.\ \ U^\dagger\in\texttt{U}$. Then, every unitary gate in dimension d can be approximated within an error ϵ as a product of N gates in $\texttt{U}$, where $N\sim O(-\log^c\epsilon)$, where $0<c<2$ is a suitable constant.
   - No theory about $O(\log^\alpha d)$..

6 Quantum Error Correction

1. Basic steps:
   (a) Encoding : $\mathscr{V}(\rho) = V\rho V^\dagger$ (with isometry $V:\mathcal{H}_A\mapsto\mathcal{H}_{A'}, V^\dagger V = I$)
   (b) Error: a quantum channel $\mathscr{E}:\mathcal{H}_{A'}\mapsto\mathcal{H}_{A'}$
   (c) Measurement: a quantum instrument $\{\mathscr{Q}_i\}$
   (d) Recovery: a unitary gate U_i according to the outcome

(e) Decoding: $\mathscr{D}$

The recovery channel $\mathscr{R}$: the last three steps together, $\mathscr{R}(\rho) := \sum_i \mathscr{D}\left(U_i \mathscr{Q}_i(\rho) U_i^\dagger\right)$
Therefore here we require:

$$\mathscr{R}\mathscr{E}\mathscr{V} = \mathscr{I}_A \tag{6.1}$$

2. Definitions:

   - A quantum channel $\mathscr{C} : \mathcal{H}_A \mapsto \mathcal{H}_{A'}$ is correctable iff $\exists \mathscr{R}.\quad \mathscr{R}\mathscr{C} = \mathscr{I}$

3. Knill-Laflamme (KL) condition: A channel $\mathscr{C}(\rho) = \sum_i C_i \rho C_i^\dagger$ is correctable iff:

$$C_j^\dagger C_i = \sigma_{ij} I_a \tag{6.2}$$

   where $\sigma \in \mathsf{St}(\mathcal{H})$.

   (a) if $A = A'$, $\mathscr{C}$ is unitary, i.e. $\mathscr{C}(\rho) = U\rho U^\dagger$

   (b) KL condition is equivalent to $\mathscr{C}(\rho) = \sum_m p_m V_m \rho V_m$ where $V_m^\dagger V_n = \delta_{mn} I_A$. That means the correctable channels are those that encode randomly the state into different **orthogonal subspaces**.

   (c) Correction: measurement with $\{\mathscr{Q}_m\}$ and corresponding recovery $\mathscr{R}_m$:

$$\mathscr{Q}_m(\rho) = P_m \rho P_m, \qquad (P_m = V_m V_m^\dagger, P_0 = I_{A'} - \sum P_m) \tag{6.3}$$

$$\mathscr{R}_m(\rho) = V_m^\dagger \rho V_m + \mathrm{Tr}[(I_{A'} - V_m V_m^\dagger)\rho] \left|0\right\rangle \left\langle 0\right| \tag{6.4}$$

   (d) physical meaning of σ: If we generally define the channel $\mathscr{C}(\rho) = \mathrm{Tr}_B[W\rho W^\dagger]$ and its *complementary channel* $\tilde{\mathscr{C}}(\rho) = \mathrm{Tr}_{A'}[W\rho W^\dagger]$, we have

$$\forall \rho \in \mathsf{St}(\mathcal{H}_A). \qquad \tilde{\mathscr{C}}(\rho) = \sigma \tag{6.5}$$

   which means that a channel is correctable iff its complementary channel is an erasure channel.

   (e) KL condition for good codes: Let error $\mathscr{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ ans the subspace $\mathcal{S}$ is a good code for $\mathscr{E}$ iff

$$PE_j^\dagger E_i P = \sigma_i j P \tag{6.6}$$

   where $\sigma \in \mathsf{St}(\mathcal{H})$ ans P is a projector on $\mathcal{S}$

4. Quantum packing bound: $d_{A'} \geq d_A \mathsf{rank}(\sigma) = d_A \mathsf{rank}(\Phi_{\mathscr{C}})$

5. Quantum packing bound non-degenerate codes: if given an orthogonal Kraus representation for $\mathscr{E}(\rho = \sum_i^k E_i \rho E_i^\dagger$, than $d_{A'} \geq d_A k$. In principle degenerate code could probably do better.

6. the quantum Hamming bound for arbitrary Pauli errors:

$$\mathscr{E}(\rho) = (1-p)\rho + \frac{p}{t} \sum_{m=1}^{t} \frac{m!(N-m)!}{N!3^m} \sum_{\boldsymbol{n}} \sum_{\boldsymbol{k}} \mathscr{U}_{\boldsymbol{n},\boldsymbol{k}}(\rho) \tag{6.7}$$

   where $\boldsymbol{n} = (n_1, \cdots, n_m)$ labels m qubits affected and $\boldsymbol{k} = (k_1, \cdots, k_m)$ the Pauli matrix acted. To encode K qubits into N qubits, the quantum packing bound for non-degenerate codes gives

$$2^{N-K} \geq \sum_{m=0}^{t} \frac{N!3^m}{(N-m)!m!} \tag{6.8}$$

   Whether there is better code is an open question.

7. Correct one to correct them all: Let two channel $\mathscr{C}(\rho) = \sum C_i \rho C_i^\dagger$ and $\mathscr{D}(\rho) = \sum D_j \rho D_j^\dagger$ with $D_j \in \mathsf{Span}\{C_i\}$, and if $\mathscr{C}$ is correctable, $\mathscr{D}$ is also correctable with same recovery channel and good code subspaces.

   - Specially for arbitrary Pauli errors

   $$\mathscr{E}(\rho) = (1-p)\rho + \frac{p}{3N}\sum_{n=1}^{N}\sum_{k=1}^{3} \mathscr{U}_{n,k}(\rho) \tag{6.9}$$

   where $\mathscr{U}_{n,k}$ is σ_k applied on n-th qubit. A good code for $\mathscr{E}$ is a good code for any quantum channel acting on a single qubit, even erasure channel.

7 Quantum entropy

1. LOCC protocol and one-way LOCC protocol
2. Lo-Popescu theorem: LOCC protocol and one-way LOCC protocol are equivalent.
3. $|\Psi\rangle$ is more entangled than $|\Psi'\rangle$ iff there exists a LOCC channel that transforms $|\Psi\rangle$ into $|\Psi'\rangle$
   - A product state is less entangled than any other bipartite state.
   - Bell states is more entangled than any other bipartite state.
4. $\rho \in \mathsf{St}(\mathcal{H})$ is more mixed than $\rho' \in \mathsf{St}(\mathcal{H})$ iff ρ can be obtained by applying a *random-unitary (RU) channel*:
   $$\rho = \sum_i p_i U_i \rho' U_i^\dagger \tag{7.1}$$
   - Every state ρ is more mixed than a **pure state** $\rho' = |\psi\rangle\langle\psi|$
   - No state ρ is more mixed than the state $\rho' = I/d$ (**maximally mixed state**), ρ' is more mixed than any other state
5. Let $|\Psi\rangle, |\Psi'\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be two *pure* bipartite states, the following are equivalent
   - $|\Psi\rangle$ is more entangled
   - the marginal of $|\Psi\rangle$ is more mixed
6. Generalization: Let $\rho \in \mathsf{St}(\mathcal{H}_A)$ and $\rho' \in \mathsf{St}(\mathcal{H}_{A'})$, ρ is more mixed than ρ' iff $\rho \otimes |\alpha'\rangle_{A'}\langle\alpha'|_{A'}$ is more mixed than $|\alpha\rangle_A\langle\alpha|_A \otimes \rho'$
7. The majorization criterion: Let $\rho = \sum_i p_i |\alpha_i\rangle\langle\alpha_i|$ with $p_1 \geq p_2 \geq \cdots \geq p_d \geq 0$, than ρ is more mixed than ρ' iff $\boldsymbol{p}$ is majorized by $\boldsymbol{p}'$ ($\boldsymbol{p} \preceq \boldsymbol{p}'$)
   $$\forall k \in \{1, \cdots, d-1\}, \qquad \sum_{i=1}^{k} p_i \geq \sum_{i=1}^{k} p_i' \tag{7.2}$$
8. Measurement of mixedness: Schur-concave function
9. Rényi entropies: a group of Schur-concave functions
   $$H_\alpha = \frac{1}{1-\alpha}\log\left[\sum_{i=1}^{d} p_i^\alpha\right] \qquad \alpha \geq 0 \tag{7.3}$$
   And quantum Rényi entropies[1]
   $$S_\alpha = \frac{\alpha}{1-\alpha}\log\|\rho\|_\alpha \tag{7.4}$$

[1] Here for convenience to discuss bits and qubits, the $\log\ \cdot$ means $\log_2\ \cdot$.

- $\forall \alpha. \quad S_\alpha(\rho) = 0 \Leftrightarrow \mathsf{rank}\rho = 1$
- $\forall \alpha > 0. \quad S_\alpha = \log d \Leftrightarrow \rho = I/d$
- $\forall \alpha. \quad 0 \leq S_\alpha(\rho) \leq \log d$
- Additivity property: $S_\alpha(\rho \otimes \sigma) = S_\alpha(\rho) + S_\alpha(\sigma)$

Special values of α:

(a) $\alpha = 0$, max-entropy

$$S_0(\rho) = \log[\mathsf{rank}(\rho)] \tag{7.5}$$

(b) $\alpha \to \infty$, min-entropy

$$S_\infty(\rho) = -\log p_1 \tag{7.6}$$

(c) $\alpha \to 1$ classically Shannon entropy, and quantumly von-Neumann entropy

$$S(\rho) := \lim_{\alpha \to 1} S_\alpha(\rho) = -\operatorname{Tr}[\rho \log \rho] \tag{7.7}$$

10. Asymptotic transformations

(a) A rate R is achievable if for every N there exists a LOCC channel $\{\mathscr{L}_N\}_{N \in \mathbb{N}}$

$$\lim_{N \to \infty} \|\mathscr{L}_N((|\Psi\rangle\langle\Psi|)^{\otimes N}) - (|\Psi'\rangle\langle\Psi'|)^{\otimes RN}\|_1 = 0 \tag{7.8}$$

(b) Achievable rates and von-Neumann entropy

$$\sup\{R | R \text{ is achievable}\} = \frac{S(\rho)}{S(\rho')} \tag{7.9}$$

11. *Concurrence: measurement of entanglement, PhysRevLett.78.5022
For two qubit system with states$|\psi\rangle = \sum_i \alpha_i |\Phi_i\rangle$ with Bell bases defined as

$$|\Phi_1\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \tag{7.10}$$
$$|\Phi_2\rangle = \mathrm{i}(|00\rangle - |11\rangle)/\sqrt{2} \tag{7.11}$$
$$|\Phi_3\rangle = \mathrm{i}(|01\rangle + |10\rangle)/\sqrt{2} \tag{7.12}$$
$$|\Phi_4\rangle = (|01\rangle - |10\rangle)/\sqrt{2} \tag{7.13}$$

Calculate the von-Neumann entropy of the marginal we get the measurement of its entanglement

$$E(\psi) = \mathcal{E}(C(\psi)) \tag{7.14}$$

with $\mathcal{E}(x) := H(\frac{1}{2} + \frac{1}{2}\sqrt{1 - x^2})$, $H(x) := x \log x + (1 - x)\log(1 - x)$, and the concurrence $C(\psi)$

$$C(\phi) = \left| \sum_i \alpha_i^2 \right| \tag{7.15}$$

7.1 Quantum data compression

1. Encoding channel $\mathscr{E} : \mathcal{H}_A \mapsto \mathcal{H}_B$ with $d_B < d_A$ and decoding channel $\mathscr{D} : \mathcal{H}_B \mapsto \mathcal{H}_A$ so that the average fidelity

$$F = \sum_x p_x \langle\psi_x|\mathscr{D}\mathscr{E}(|\psi_x\rangle\langle\psi_x|)|\psi_x\rangle \tag{7.16}$$

is close to 1.

2. Compressing entanglement:

$$F_{\text{ent}} = \langle\Psi|(\mathscr{D}\mathscr{E} \otimes \mathscr{I}_R)(|\Psi\rangle\langle\Psi|)|\Psi\rangle \leq F \tag{7.17}$$

3. Subspace encodings:
$$\mathscr{E}(\rho) = P\rho P + \mathrm{Tr}[(I-P)\rho] \left|\psi_0\right\rangle \left\langle\psi_0\right| \tag{7.18}$$
where P is the projector on subspace $\mathcal{S}$ and $|\psi_0\rangle$ is in the orthogonal complement of $\mathcal{S}$
$$F_{\mathrm{ent}} \geq \left| \sum_x p_x \langle\psi_x|P|\psi_x\rangle \right|^2 := p_{\mathrm{yes}}^2 \tag{7.19}$$

4. asymptotic scenario: compression $\rho^{\otimes N}$ into $\mathcal{S}_N$ with dimension d_N, define the compression rate
$$R := \limsup_{N\to\infty} \frac{\log d_N}{N} \tag{7.20}$$
And achievable rate requires a sequence of coding so that
$$\limsup_{N\to\infty} F_N = 1 \tag{7.21}$$
   (a) Define the description of $\rho^{\otimes N}$:
   $$\rho^{\otimes N} = \sum_{\boldsymbol{m}} q_N(\boldsymbol{m}) \left|\psi_{\boldsymbol{m}}\right\rangle \left\langle\psi_{\boldsymbol{m}}\right| \tag{7.22}$$
   where
      - $\boldsymbol{m} = (m_1, \cdots, m_N) \in \{1, \cdots, d_A\}^{\times N}$
      - $q_N(\boldsymbol{m})$ is the probability $q_N(\boldsymbol{m}) = \prod_i q_{m_i}$
      - $|\psi_{\boldsymbol{m}}\rangle$ is the product vector $|\psi_{\boldsymbol{m}}\rangle := |\psi_{m_1}\rangle |\psi_{m_2}\rangle \cdots |\psi_{m_N}\rangle$
   (b) the type of a sequence $\boldsymbol{m}$ defined by $t_{\boldsymbol{m}} := (N_1/N, \cdots, N_d/N)$
      i. total number of types: $T_N \sim 1$
      ii. the number of sequences of type t:
      $$S_{N,t} \sim \exp[NH(t)] \tag{7.23}$$
      where $H(t_{\boldsymbol{m}}) := -\sum_{i=1}^d t_i \ln t_i$ is the Shannon entropy
      iii. the probability that a sequence is of type t:
      $$Q_{N,t} \sim \exp[-ND(t\|q)] \tag{7.24}$$
      where $D(t\|q) := \sum_{i=1}^d t_i \ln \frac{t_i}{q_i}$ is the Kullback-Leibler divergence

   Kullback-Leibler divergence satisfies the following properties
      - $D(t\|q) \geq 0$ and the equality holds iff $t = q$
      - if $\lim_{N\to\infty} D(t_N\|q) = 0$, than $\lim_{N\to\infty} H(t_N) = H(q)$

   From which we can see
   $$\sum_{t:D(t\|q)\leq\epsilon_N} Q_{N,t} \sim 1 - \exp[-N\epsilon] \tag{7.25}$$
   $$\sum_{t:D(t\|q)\leq\epsilon_N} \frac{\log S_{N,t}}{N} = H(q) \tag{7.26}$$
   (c) Schumacher's theorem, direct part: Let $\rho \in \mathsf{St}(\mathcal{H})$, then every compression rate $R \geq S(\rho)$ is achievable
   (d) Schumacher's theorem, strong converse: Let $\rho = \sum_i q_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$ be a diagonalization of ρ and let F_N be the fidelity of data compression for the states $\{|\psi\rangle_i\}$ with probabilities $\{q_i\}$, then for every $R < S(\rho)$, $\lim_{N\to\infty} F_N = 0$

(e) Entanglement dilution: Using LOCC to produce M_N pairs of $|\Psi\rangle$ from N pairs of Bell state $|\Phi^+\rangle$, the achievable rate

$$R_{\text{dil}} = \liminf_{N\to\infty} \frac{M_N}{N} < 1/S(\text{Tr}_A[|\Psi\rangle\langle\Psi|]) \tag{7.27}$$

(f) Entanglement distillation: Using LOCC to produce M_N pairs of Bell state $|\Phi^+\rangle$ from N pairs of $|\Psi\rangle$, the achievable rate

$$R_{\text{dist}} = \liminf_{N\to\infty} \frac{M_N}{N} < S(\text{Tr}_A[|\Psi\rangle\langle\Psi|]) \tag{7.28}$$

(g) Asymptotic transformations of pure entangled states:$R = S(\text{Tr}_A[|\Psi\rangle\langle\Psi|])/S(\text{Tr}_A[|\Psi'\rangle\langle\Psi'|])$

8 Quantum algorithm

8.1 Grover's quantum search algorithm

1. Classic model: from a function

$$f : \{1, \cdots, N\} \mapsto \{0, 1\} \tag{8.1}$$

find n so that $f(n) = 1$. Usually we assume that $S = |\{n|f(n) = 1\}| \ll N$. Time complexity $O(N) \times O(f)$

2. Two quantum version:

- we have the system

$$|\alpha\rangle = |f(1)\rangle |f(2)\rangle \cdots |f(N)\rangle \tag{8.2}$$

And define the control unitary gate

$$U = \sum_{n=1}^{N} Z_n \otimes |n\rangle\langle n| \tag{8.3}$$

with Pauli gate defined by $Z_n |\alpha\rangle = (-)^{f(n)} |\alpha\rangle$.
For simplicity we define the *Grover's gate* V_f on the control system as

$$V_f = \sum_{n=1}^{N} (-)^{f(n)} |n\rangle\langle n| \tag{8.4}$$

which comes from $U|\alpha\rangle|\beta\rangle = |\alpha\rangle(V_f|\beta\rangle)$[2]

- We may describe the classic search as:

$$(\rho) = \sum_n \langle n|\rho|n\rangle |f(n)\rangle\langle f(n)| \left(\text{Tr}_A \left[U_f(\rho \otimes |0\rangle\langle 0|)U_f^\dagger\right]\right) \tag{8.5}$$

And quantum version by the gate $U_f = \sum_n |n\rangle\langle n| \otimes X^{f(n)}$, which also leads to Grover's gate V_f by

$$U_f |\beta\rangle |-\rangle = (V_f|\beta\rangle)|-\rangle \tag{8.6}$$

This version seems to show how quantum version of U_f is more powerful than $\mathscr{C}_f$ and show that preparing a huge system of $|\alpha\rangle$ is not necessary.

3. The algorithm ($O(\sqrt{N})$):

[2] In the following we discuss the *query complexity* defined by the number of uses of gate V_f, and ignore the elementary gates needed to perform V_f (which leads to *gate complexity*).

(a) prepare system in Fourier basis state

$$|e_N\rangle = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} |n\rangle \tag{8.7}$$

(b) Apply Grover's gate V_f

(c) Apply the gate

$$W = 2\,|e_N\rangle\,\langle e_N| - I \tag{8.8}$$

(d) Repeat steps 3b and 3c for k times, where

$$k = \frac{\pi}{4}\sqrt{\frac{N}{S}} \tag{8.9}$$

(e) Measure the system on computational basis, with probability of success

$$p_{\text{succ}} \geq 1 - \frac{S}{N} \tag{8.10}$$

Proof of the algorithm:
The input state can be expressed as:

$$|e_N\rangle = \sqrt{1 - \frac{S}{N}}\,|\psi_+\rangle + \sqrt{\frac{S}{N}}\,|\psi_-\rangle := \cos\theta\,|\psi_+\rangle + \sin\theta\,|\psi_-\rangle \tag{8.11}$$

where $|\psi^+\rangle$ and $|\psi_-\rangle$ are eigenstates of V_f with eigenvalue ± 1:

$$|\psi_+\rangle := \frac{1}{\sqrt{N-S}} \sum_{n:f(n)=0} |n\rangle \tag{8.12}$$

$$|\psi_-\rangle := \frac{1}{\sqrt{S}} \sum_{n:f(n)=1} |n\rangle \tag{8.13}$$

And $|e_N\rangle$ and $|e_N^{\perp}\rangle := -\sin\theta\,|\psi_+\rangle + \cos\theta\,|\psi_-\rangle$ are eigenstates of W with eigenvalue ± 1. So

$$WV_f(\cos\alpha\,|\psi_+\rangle + \sin\alpha\,|\psi_-\rangle) = \cos(\alpha + 2\theta)\,|\psi_+\rangle + \sin(\alpha + 2\theta)\,|\psi_-\rangle \tag{8.14}$$

therefore

$$(WV_f)^k\,|e_N\rangle = \cos[(2k+1)\theta]\,|\psi_+\rangle + \sin[(2k+1)\theta]\,|\psi_-\rangle \tag{8.15}$$

with $(2k+1)\theta \approx \pi/2$, we have the conclusion above.

4. Dependence of the algorithm on the number of solutions. Quantum phase estimation algorithm allows us to find out the angle $\tau = 2\arcsin\sqrt{S/N}$ within an interval of size $1/M$ with the control-unitary gate

$$T = \sum_{m=1}^{M} V_f^m \otimes |m\rangle\,\langle m| \tag{8.16}$$

5. $O(\sqrt{N})$ is the best scaling allowed by quantum mechanics
Proof: For simplicity here we only discuss the case $S = 1$, with

$$V_f = -\,|x\rangle\,\langle x| + \sum_{n \neq x} |n\rangle\,\langle n| =: V_x \tag{8.17}$$

Generally the algorithm could be

$$|\Psi_{k,x}\rangle = U_k(V_x \otimes I_B)U_{k-1} \cdots U)1(V_x \otimes I_B)\,|\Psi_0\rangle \tag{8.18}$$

with $|\Psi_0\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be the input system combined with a auxiliary system B. And we hope to get the result $|\Phi_{k,x}\rangle = |x\rangle |\beta_{k,x}\rangle$, which leads to the quality of the algorithm (average on x)

$$
\begin{aligned}
\eta_k &:= \frac{1}{N} \sum_{x=1}^{N} \| |\Psi_{k,x}\rangle - |\Phi_{k,x}\rangle \|^2 && (8.19)\\
&\geq \frac{1}{N} \sum_x \Big(\| |\Psi_{k,x}\rangle - |\Psi_k\rangle \| - \| |\Psi_k\rangle - |\Phi_{k,x}\rangle \| \Big)^2 && (8.20)\\
&\geq \frac{1}{N} \left(\sqrt{\sum_x \| |\Psi_{k,x}\rangle - |\Psi_k\rangle \|^2} - \sqrt{\sum_x \| |\Psi_k\rangle - |\Phi_{k,x}\rangle \|^2} \right)^2 && (8.21)\\
&:= \left(\frac{\|\boldsymbol{a}_k\| - \|\boldsymbol{b}_k\|}{\sqrt{N}} \right)^2 && (8.22)
\end{aligned}
$$

where $|\Psi_k\rangle := U_k U_{k-1} \cdots U_1 |\Psi\rangle$ and the items

$$
\begin{aligned}
\|\boldsymbol{a}_k\| &= \sqrt{\sum_x \| |\Psi_{k,x}\rangle - |\Psi_k\rangle \|^2} \leq 2k && (8.23)\\
\|\boldsymbol{b}_k\| &= \sqrt{\sum_x \| |\Psi_k\rangle - |\Phi_{k,x}\rangle \|^2} && (8.24)\\
&\geq \sqrt{2\left(N - \sqrt{N}\right)} && (8.25)
\end{aligned}
$$

So to promise $\eta_k \to 0$, it have to be $k = \Theta(\sqrt{N})$

- It makes no difference to use $U_x = \sum_n |n\rangle \langle n| \otimes X^{f(n)}$ because

$$U_x = I_A \otimes |+\rangle \langle +| + V_x \otimes |-\rangle \langle -| \tag{8.26}$$

- The proof holds even if we use the gate $V_x^t \otimes I_B$ as one step, which means the optimal of $\Theta(\sqrt{N})$ is not only the times needed to use V_x but also the steps needed

8.2 Shor's algorithm

1. From period finding to factoring:
   (a) Take a random integer $a < N$ and check if a divides N
   (b) If a divides N, you are done: this means that either $a = p$ or $a = q$. If not, then proceed to the next step
   (c) Find the period of the function $f(x) = ax \mod N$. Call the period r
   (d) If r is odd, then go back to first step. If r is even, then proceed to the next step
   (e) Compute $x_+ = a^{r/2} + 1$ and $x = a^{r/2} - 1$.
   (f) If $x_+ = 0 \mod N$, then go back to first step. Otherwise, proceed to the next step
   (g) Output the solution $\{p, q\} = \{\gcd(N, x_+), \gcd(N, x_-)\}$.
2. Quantum period-finding algorithm (Shor's algorithm) with the gate U_f

$$U_f := \sum_{x=1}^{d} |x\rangle \langle x| \otimes S^{f(x)} \tag{8.27}$$

with $f(x)$ a "strong periodic" function

$$f(x) = f(y) \Longleftrightarrow x = y + kr, k \in \mathbb{Z} \tag{8.28}$$

(for example what we need in factorization $f(x) = a^x \mod N$) and shift gate $S = \sum |i \oplus 1\rangle \langle i|$

(a) Prepare system A in Fourier state $|e_0\rangle = \frac{1}{\sqrt{d_A}} \sum_x |x\rangle$ and system B in $|0\rangle$

(b) Apply U_f

(c) Measure B in the computational basis

(d) Measure A in the Fourier basis with result $|e_n\rangle$

(e) In the easy case where d is a multiple of the period, it is enough to compute the fraction n/d and reduce it to minimal terms $n/d = k_0/r_0$, in this case, r_0 is a divisor of the period.

Proof

$$U_f |e_0\rangle |0\rangle = \frac{1}{\sqrt{d}} \sum_{x=1}^{d} |x\rangle |f(x)\rangle \tag{8.29}$$

$$= \frac{1}{\sqrt{d}} \sum_{x=1}^{r} \left(\sum_{m=0}^{M_x-1} |x+mr\rangle \right) |f(x)\rangle \tag{8.30}$$

After the measurement of system B, the state of system A becomes

$$|\psi_x\rangle = \frac{1}{\sqrt{M_x}} \sum_{m=0}^{M_x-1} |x+mr\rangle \tag{8.31}$$

and the result of measurement of system A is

$$p(n|x) = |\langle e_x|\psi_x\rangle|^2 \tag{8.32}$$

$$= \frac{1}{M_x} \left| \sum_{m=0}^{M_x-1} \langle e_n|x+mr\rangle \right|^2 \tag{8.33}$$

$$= \frac{1}{M_x d} \left| \sum_{m=0}^{M_x-1} \exp\left[-\frac{2\pi i n m r}{d} \right] \right|^2 \tag{8.34}$$

If $d = rM$ (means d is a multiple of the period), then the probability is independent on x

$$p_n = \frac{1}{r} \left| \frac{1}{M} \sum_{m=0}^{M-1} \exp\left[-\frac{2\pi i n m}{M} \right] \right|^2 = \frac{1}{r} \sum_{k=1}^{r} \delta_{n,kM} \tag{8.35}$$

Therefore the outcome $n = kM$, and $n/d = k/r$, so r_0 should be a divisor of r
If d is not a multiple of the period, it is easy to see that with large M_x (or large d, for example $d \sim N^2$), the probability is peaked around $n = kd/r$

- The complexity:
  - the gate U_f with $f = a^x \mod N$: $O(L^3)$
  - prepare the Fourier basis: the "multiply operator" $|e_k\rangle = M^k |e_0\rangle$

$$M = \sum_{n=1}^{N} \exp\left[\frac{2\pi i n}{N} \right] |n\rangle \langle n| \tag{8.36}$$

And to express in binary qubit:

$$|x\rangle = |x_1\rangle |x_2\rangle \cdots |x_L\rangle \tag{8.37}$$

with $x_i \in \{0,1\}$ and $x = \sum_i 2^{L-i} x_i$, than we have:

$$|e_0\rangle = |+\rangle^{\otimes L} = (H|0\rangle)^{\otimes L} \tag{8.38}$$

And "multiply operator"

$$M|n\rangle = \bigotimes_{i=1}^{L}\left[\exp\left(\frac{2\pi \mathrm{i} n_i}{2^i}\right)|n_i\rangle\right] \tag{8.39}$$

$$= R_1|n_1\rangle \otimes R_2|n_2\rangle \otimes \cdots \otimes R_L|n_L\rangle \tag{8.40}$$

where the single-qubit gate

$$R_i := \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi \mathrm{i}}{2^i}\right) \end{pmatrix} \tag{8.41}$$

which can be realized with $O(-\log^c \epsilon) \sim O(1)$, and so is M^k (leads to multiple of L). And all these sums up to the complexity $O(L)$

– measurement on the Fourier basis: The key is to realize the Fourier gate:

$$F = \sum_{n=1}^{N} |e_n\rangle\langle n| \tag{8.42}$$

Define the control-unitary gate on the control n and target m

$$C_i^{(mn)} := I^{(m)} \otimes |0\rangle_n \langle 0|_n + R_i^{(m)} \otimes |1\rangle_n \langle 1|_n \tag{8.43}$$

and gates (the Hadamard gate H defined above)

$$U_1 := C_L^{(1L)} \cdots C_3^{(13)} C_2^{(12)} H^{(1)} \tag{8.44}$$

$$U_2 := C_{L-1}^{(2L)} \cdots C_3^{(24)} C_2^{(23)} H^{(2)} \tag{8.45}$$

$$\vdots \tag{8.46}$$

$$U_L := H^{(L)} \tag{8.47}$$

And the Fourier gate

$$F = U_L U_{L-1} \cdots U_2 U_1 \tag{8.48}$$

with complexity $O(L^2)$ to realizing a physical Fourier transform[3]

All above sums up to $O(L^3)$

[3]Classically we need $\Theta(N \log N)$ to perform *fast Fourier transform*. It does not mean we could do better in quantum computation because we cannot get all factors in $F|k\rangle$.