# Notes on Quantum Computing

Maris Ozols

May 20, 2012

## Contents

# 1 Mathematics of quantum information

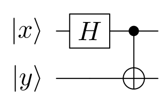
## 1.1 Basics

### 1.1.1 Bell basis, teleportatoin and superdense coding

Bell basis states:

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}} \tag{1}$$

Preparation of a Bell basis state ($H$ on the first qubit, followed by CNOT):




(2)

!!! p. 25 in NC !!!

### 1.1.2 Measurements

General measurement:

$$p_m = \mathrm{Tr}(M_m \rho M_m^\dagger) \quad \rho_m = \frac{M_m \rho M_m^\dagger}{p_m} \tag{3}$$

!!! POVM: !!!

**Fact** (Principle of deferred measurement)**.** *Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit. Any classically controlled operations that use the measurement results can be replaced by conditional quantum operations.*

### 1.1.3 Decompositions and normal forms

**Fact.** $(A \otimes I)|\phi\rangle = (I \otimes A^\mathsf{T})|\phi\rangle$ *where* $|\phi\rangle = \sum_i |i\rangle|i\rangle$ *is the maximally entangled state and* $A \in \mathrm{M}_n(\mathbb{C})$. *This follows by projecting both sides on* $\langle j|\langle k|$.

**Theorem** (Schmidt decomposition)**.** *If* $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$*, then there exist orthonormal bases* $\{|i_A\rangle\}_i$ *and* $\{|i_B\rangle\}_i$ *for* $\mathcal{H}_A$ *and* $\mathcal{H}_B$*, respectively, such that*

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle. \tag{4}$$

Note: one can take the first basis and the coefficients to be the eigenvectors and square roots of the eigenvalues of the reduced state $\mathrm{Tr}_B\big(|\psi\rangle\langle\psi|\big)$, respectively.

**Theorem** (Purification)**.** *If $\rho$ is a mixed state on system $A$, then there is a system $B$ and a pure state $|\psi\rangle$ on $AB$ such that*

$$\rho = \mathrm{Tr}_B\big(|\psi\rangle\langle\psi|\big). \tag{5}$$

**Lemma** (General purification)**.** *If $|\psi\rangle$ is a purification of $\rho$, then it can be written in the form*

$$|\psi\rangle = (\rho^{1/2} \otimes U)|\phi\rangle \tag{6}$$

*for some unitary $U$.*

**Theorem** (Polar decomposition)**.** *Any $A \in \mathrm{M}_n(\mathbb{C})$ can be written in the form*

$$A = UP = QU, \tag{7}$$

*where $P, Q \geq 0$, $U \in \mathrm{U}(n)$. In particular, $P = \sqrt{A^\dagger A}$ and $Q = \sqrt{AA^\dagger}$.*

### 1.1.4 Pauli matrices and Bloch sphere

Pauli matrices are:

$$X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \quad Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right) \quad Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \tag{8}$$

Any single qubit density matrix can be written as

$$\rho = \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma}) \tag{9}$$

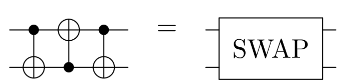
**Fact.** *If $A^2 = I$, then $e^{i\theta A} = \cos(\theta A) + i \sin(\theta A) = I \cos\theta + iA \sin\theta$.*

**Fact.** *$(\vec{r} \cdot \vec{\sigma})^2 = |\vec{r}|^2 I$ so $\vec{r} \cdot \vec{\sigma}$ has eigenvalues $\pm |\vec{r}|$.*

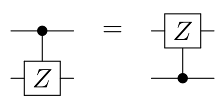
**Fact.** *Rotation around a unit vector $\vec{r}$ by angle $\alpha$ is given by*

$$e^{-i\frac{\alpha}{2}(\vec{r}\cdot\vec{\sigma})} = I \cos\tfrac{\alpha}{2} - i(\vec{r} \cdot \vec{\sigma}) \sin\tfrac{\alpha}{2}. \tag{10}$$

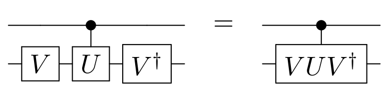
### 1.1.5 Elementary circuit identities



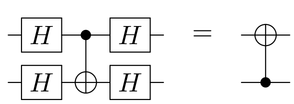

(11)




(12)




(13)




(14)

## 1.2 Trace distance

Trace distance:

$$D(p,q) := \frac{1}{2}\sum_{x\in X}|p_x - q_x| = \max_{S\subseteq X}(p(S)-q(S)). \tag{15}$$

$$D(\rho,\sigma) := \frac{1}{2}\operatorname{Tr}|\rho-\sigma| = \max_{I\geq P\geq 0}\operatorname{Tr}\big(P(\rho-\sigma)\big). \tag{16}$$

For qubits:

$$F(\mathbf{r}_1,\mathbf{r}_2) = \frac{1}{2}\left|\mathbf{r}_1 - \mathbf{r}_2\right|. \tag{17}$$

Tricks:

- If $P,Q\geq 0$, then $\operatorname{Tr}(PQ)\geq 0$,
- If $I\geq P\geq 0$ and $Q\geq 0$, then $\operatorname{Tr}(Q)\geq\operatorname{Tr}(PQ)$,
- $\rho-\sigma = Q-S$, where $Q,S\geq 0$ have orthogonal supports.

**Theorem.** *Let $\{E_m\}$ be a POVM. Then*

$$D(\rho,\sigma) = \max_{\{E_m\}} D(\{p_m\},\{q_m\}), \tag{18}$$

*where $p_m := \operatorname{Tr}(\rho E_m)$, and $q_m := \operatorname{Tr}(\rho E_m)$.*

## 1.3 Fidelity and Uhlmann's theorem

Fidelity:

$$F(p,q) := \sum_{x\in X}\sqrt{p_x q_x} = \sqrt{p}\cdot\sqrt{q} \tag{19}$$

$$F(\rho,\sigma) := \operatorname{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}} \tag{20}$$

$A$ and $A^\dagger$ have the same singular values, therefore $\operatorname{Tr}\left|A^\dagger\right| = \operatorname{Tr}|A|$. Fidelity is symmetric, since

$$\begin{aligned}
F(\rho,\sigma) &= \operatorname{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}} & (21)\\
&= \operatorname{Tr}\sqrt{(\sigma^{1/2}\rho^{1/2})^\dagger\sigma^{1/2}\rho^{1/2}} & (22)\\
&= \operatorname{Tr}\left|\sigma^{1/2}\rho^{1/2}\right| & (23)\\
&= \operatorname{Tr}\left|(\rho^{1/2}\sigma^{1/2})^\dagger\right| & (24)\\
&= \operatorname{Tr}\left|\rho^{1/2}\sigma^{1/2}\right| & (25)\\
&= F(\sigma,\rho). & (26)
\end{aligned}$$

For qubits:

$$F(\mathbf{r}_1,\mathbf{r}_2) := \frac{1}{2}\left(1+\mathbf{r}_1\cdot\mathbf{r}_2+\sqrt{(1-|\mathbf{r}_1|^2)(1-|\mathbf{r}_2|^2)}\right) \tag{27}$$

**Lemma.** *If $A$ is any operator and $U$ is unitary, then* $|\operatorname{Tr}(AU)| \leq \operatorname{Tr}|A|$.

**Theorem** (Uhlmann)**.**

$$F(\rho, \sigma) = \max_{|\psi\rangle, |\varphi\rangle} |\langle\psi|\varphi\rangle| \,. \tag{28}$$

## 1.4 Quantum operations

Different representations of a general quantum operation $\mathcal{E}$:

1. *Stinespring representation*: $\mathcal{E}(\rho) = \operatorname{Tr}_B\big(U(\rho \otimes |0\rangle\langle 0|)U^\dagger\big)$.
2. *Kraus representation*: $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$, where $\sum_k E_k^\dagger E_k = I$.
3. *Choi-Jamiołkowski representation*: $\mathcal{E}(\rho) = \operatorname{Tr}_B\big(J_{\mathcal{E}} \cdot (I \otimes \rho^{\mathsf{T}})\big)$, where $J_{\mathcal{E}} := (\mathcal{E} \otimes I)(|\phi\rangle\langle\phi|) = \sum_{ij} \mathcal{E}\big(|i\rangle\langle j|\big) \otimes |i\rangle\langle j|$.
4. *Completely positive and trace preserving*: $(\mathcal{E} \otimes I)(\rho) \geq 0$ and $\operatorname{Tr}\mathcal{E}(\rho) = \operatorname{Tr}\rho$ for all $\rho$.

How to convert between these representations:

- Stinespring $\Rightarrow$ Kraus: $E_k := (I \otimes \langle k|)U(I \otimes |0\rangle)$
- Kraus $\Rightarrow$ Stinespring: $U(I \otimes |0\rangle) := \sum_k E_k |k\rangle$

Physical interpretation of Kraus representation: $\mathcal{E}(\rho) = \sum_k p_k \rho_k$, where

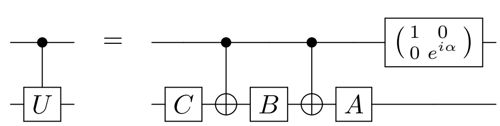
$$p_k := \operatorname{Tr}(E_k \rho E_k^\dagger) \quad \text{and} \quad \rho_k := \frac{E_k \rho E_k^\dagger}{\operatorname{Tr}(E_k \rho E_k^\dagger)}. \tag{29}$$

## 1.5 Quantum gates, circuit model, and universality

**Theorem** (Z-Y decomposition)**.** *For any $U \in \mathrm{U}(2)$ there exist $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$, where $R_k(\theta) = e^{-i\frac{\theta}{2}\sigma_k}$.*

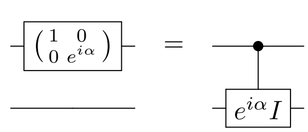
**Theorem.** *For any $U \in \mathrm{U}(2)$ there exist $A, B, C \in \mathrm{U}(2)$ such that $ABC = I$ and $U = e^{i\alpha} AXBXC$ for some $\alpha \in \mathbb{R}$.*

Given such decomposition for $U$, we can implement c-$U$ as follows:



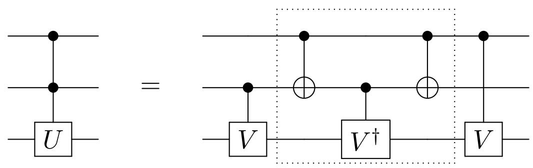

(30)

Note that




(31)

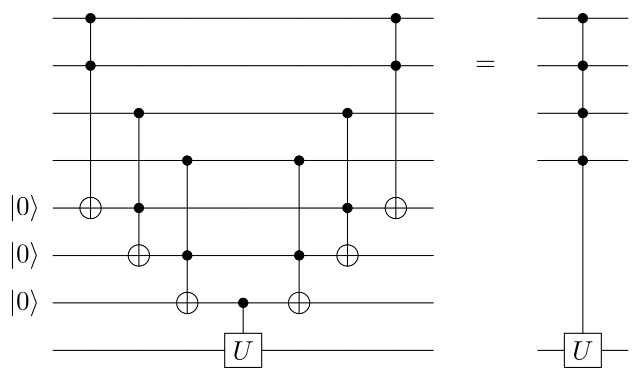
If $V^2 = U$ then we can implement cc-$U$ as follows:




(32)

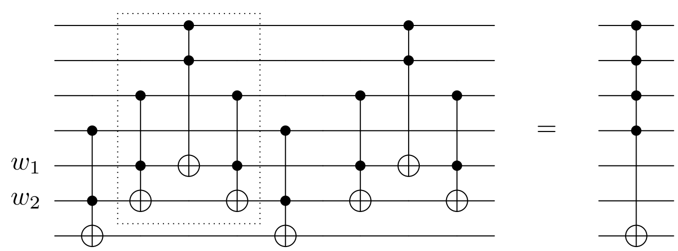
Note: the marked region performs $V^\dagger$ controlled on XOR of the first two bits.

More controls can be added using workspace qubits initialized in $|0\rangle$:




(33)

We can add more controls to Toffoli gate without imposing any restrictions on the initial state of the workspace:




(34)

Note: the marked gates act as follows:

- invert $w_1$ if and only if the first 2 bits are set to 1,
- invert $w_2$ if and only if the first 3 bits are set to 1.

#### 1.5.1 Givens rotations

If $\alpha \neq 0$ and $\beta \neq 0$ then

$$\overbrace{\frac{1}{\sqrt{|\alpha|^2 + |\beta|^2}} \begin{pmatrix} \alpha^* & \beta^* \\ -\beta & \alpha \end{pmatrix}}^{G(\alpha,\beta)} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \sqrt{|\alpha|^2 + |\beta|^2} \\ 0 \end{pmatrix} \tag{35}$$

Note that $G(\alpha, \beta) \in \mathrm{SU}(2)$. In general a two-level unitary

$$G_{ij}(\alpha, \beta) = \frac{1}{\sqrt{|\alpha|^2 + |\beta|^2}} \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & \alpha^* & & \beta^* & & \\ & & & \ddots & & & \\ & & -\beta & & \alpha & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \tag{36}$$

is called *Givens rotation*. If $U \in \mathrm{U}(n)$ then for appropriately chosen parameters $\alpha$ and $\beta$ we have

$$G_{1n} \dots G_{13} G_{12} U = \begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix} \tag{37}$$

where $U' \in \mathrm{U}(n-1)$. By recursively applying this procedure we obtain a diagonal matrix of the form $\mathrm{diag}(1, \dots, 1, \det U)$.

!!! implementing a 2-level unitary (Gray code) !!!

# 2 Elementary quantum algorithms

## 2.1 Phase kickback

If $a \in \{0, 1\}$ then

$$X^a |-\rangle = (-1)^a |-\rangle. \tag{38}$$

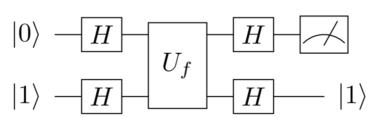
If $f : \{0,1\}^n \to \{0,1\}$ and $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ then

$$U_f |x\rangle|-\rangle = (-1)^{f(x)} |x\rangle|-\rangle. \tag{39}$$

## 2.2 Deutsch's algorithm

**Problem.** *Determine whether* $f : \{0,1\} \to \{0,1\}$ *is constant or balanced. Equivalently, compute* $f(0) \oplus f(1)$.

**Circuit.**




(40)

**Analysis.**

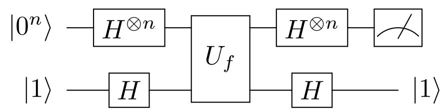
$$|+\rangle|-\rangle \xmapsto{U_f} \frac{1}{\sqrt{2}} \Big( (-1)^{f(0)} |0\rangle|-\rangle + (-1)^{f(1)} |1\rangle|-\rangle \Big) \tag{41}$$

$$= (-1)^{f(0)} \underbrace{\frac{1}{\sqrt{2}} \Big( |0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle \Big)}_{|+\rangle \text{ or } |-\rangle \text{ depending on } f(0) \oplus f(1)} |-\rangle \tag{42}$$

### 2.3 Deutsch–Jozsa algorithm

**Problem.** *Determine whether* $f : \{0,1\}^n \to \{0,1\}$ *is constant or balanced.*

**Circuit.**




(43)

**Analysis.** Recall the formula:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{\vec{x}\cdot\vec{y}} |y\rangle \tag{44}$$

We have

$$|+\rangle^{\otimes n}|-\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|-\rangle \tag{45}$$

$$\xmapsto{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle|-\rangle \tag{46}$$

$$\xmapsto{H^{\otimes(n+1)}} \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{\vec{x}\cdot\vec{y}+f(x)}|y\rangle|1\rangle \tag{47}$$

The amplitude for $\vec{y} = \vec{0}$ is given by

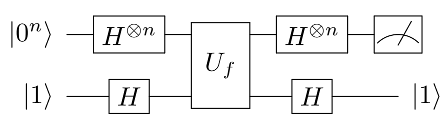
$$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} = \begin{cases} \pm 1 & \text{if } f \text{ is constant} \\ 0 & \text{if } f \text{ is balanced} \end{cases} \tag{48}$$

### 2.4 Bernstein–Vazirani problem

**Problem.** *Determine* $\vec{s} \in \{0,1\}^n$ *by querying* $f : \{0,1\}^n \to \{0,1\}$ *given by*

$$f(\vec{x}) = \vec{s}\cdot\vec{x} = s_1x_1 \oplus s_2x_2 \oplus \cdots \oplus s_nx_n \tag{49}$$

**Circuit.**




(50)

**Analysis.** Apply the Hadamard transform formula in the backward direction:

$$|+\rangle^{\otimes n}|-\rangle \xmapsto{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{\vec{x}\cdot\vec{s}}|x\rangle|-\rangle \tag{51}$$

$$\xmapsto{H^{\otimes(n+1)}} \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{\vec{x}\cdot(\vec{y}+\vec{s})}|y\rangle|1\rangle \tag{52}$$

The amplitude for $\vec{y} = \vec{s}$ is clearly 1, so the other amplitudes must be 0.

### 2.5 Simon's algorithm

# 3 Quantum Fourier transform and phase estimation

Let $y/2^n = \sum_{l=1}^n y_l 2^{-l} = 0.y_1y_2\dots y_n$. Then

$$\mathrm{QFT}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i x y/2^n} |y\rangle \tag{53}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} e^{2\pi i x \sum_{l=1}^n y_l 2^{-l}} |y\rangle \tag{54}$$

$$= \bigotimes_{l=1}^{n} \Big( |0\rangle + e^{2\pi i x 2^{-l}} |1\rangle \Big) \tag{55}$$

# 4 Shor's algorithm for factoring

## 4.1 Period finding

$f : \{0, 1, \dots, 2^n - 1\} \to \{0, 1\}^m$. Promise: $f(x) = f(y) \Leftrightarrow x \equiv y \pmod b$.

$$|0\rangle^{\otimes n}|0\rangle^{\otimes m} \xmapsto{\mathrm{QFT}} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle \tag{56}$$

$$\xmapsto{U_f} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle \tag{57}$$

If we get outcome $f(x_0)$ after measuring the 2nd register we get, the state that is left over is

$$\frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} |x_0 + jr\rangle, \tag{58}$$

where $k \in \{\lceil \frac{2^n}{r} \rceil, \lfloor \frac{2^n}{r} \rfloor\}$. Applying $\mathrm{QFT}^{-1}$ we get

$$\frac{1}{\sqrt{2^n k}} \sum_{y=0}^{2^n-1} \sum_{j=0}^{k-1} e^{-\frac{2\pi i}{2^n}(x_0+jr)} |y\rangle. \tag{59}$$

If $r \nmid 2^n$, then

$$\Pr(y) = \frac{1}{2^n k} \frac{\sin^2 \frac{\pi y r k}{2^n}}{\sin^2 \frac{\pi y r}{2^n}} \tag{60}$$

# 5 Grover's quantum search algorithm

# 6 Computational complexity

In what follows DTM stands for a Deterministic Turing Machine.

**Definition.** A *promise problem* is a pair $A = (A_{\text{yes}}, A_{\text{no}})$, where $A_{\text{yes}}, A_{\text{no}} \subseteq \{0,1\}^*$ and $A_{\text{yes}} \cap A_{\text{no}} = \emptyset$.

| | Compute | Verify |
|---|---|---|
| Deterministic | P, PSPACE | NP |
| Probabilistic | BPP, PP | MA |
| Quantum | BQP, BPP | QMA |

Table 1: The success probabilities of numerical QRACs.

!!! PICTURE !!!

Most of the following definitions start with "A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in [*complexity class*] if and only if…".

**Definition** (P)**.** …there exists a DTM $\mathscr{M}$ that runs in polynomial time such that

- $\forall x \in A_{\text{yes}} : \mathscr{M}(x) = 1$,
- $\forall x \in A_{\text{no}} : \mathscr{M}(x) = 0$.

**Definition** (PSPACE)**.** Similar to P, except $\mathscr{M}$ runs in polynomial space.

**Definition** (NP)**.** …there exists a DTM $\mathscr{M}$ that runs in polynomial time and a polynomial $p$ such that

- $\forall x \in A_{\text{yes}} \; \exists y \in \{0,1\}^{p(|x|)} : \mathscr{M}(x,y) = 1$ (*completeness*),
- $\forall x \in A_{\text{no}} \; \forall y \in \{0,1\}^{p(|x|)} : \mathscr{M}(x,y) = 0$ (*soundness*).

**Definition** (PP)**.** …there exists a DTM $\mathscr{M}$ that runs in polynomial time and a polynomial $p$ such that

- $\forall x \in A_{\text{yes}} : \left|\{r \in \{0,1\}^{p(|x|)} : \mathscr{M}(x,r) = 1\}\right| / 2^{p(|x|)} > \frac{1}{2}$,
- $\forall x \in A_{\text{no}} : \left|\{r \in \{0,1\}^{p(|x|)} : \mathscr{M}(x,r) = 1\}\right| / 2^{p(|x|)} \leq \frac{1}{2}$.

**Definition** (BPP)**.** Similar to PP, except the probabilities are "$\ldots \geq \frac{2}{3}$" and "$\cdots \leq \frac{1}{3}$", respectively.

**Definition** (MA)**.** …there exists a DTM $\mathscr{M}$ that runs in polynomial time and polynomials $p$ and $q$ such that

- $\forall x \in A_{\text{yes}} \; \exists y \in \{0,1\}^{p(|x|)} : \left|\{r \in \{0,1\}^{q(|x|)} : \mathscr{M}(x,y,r) = 1\}\right| \geq \frac{2}{3}$ (*completeness*),

- $\forall x \in A_{\text{no}}\ \forall y \in \{0,1\}^{p(|x|)} : \left|\{r \in \{0,1\}^{q(|x|)} : \mathscr{M}(x,y,r) = 1\}\right| \leq \frac{1}{3}$ (*soundness*).

**Definition** (BQP)**.** ...there exists a polynomial-time generated family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$, where each circuit $Q_n$ takes $n$ input qubits and produces one output qubit, such that

- $\forall x \in A_{\text{yes}} : \Pr[Q_{|x|} \text{ accepts } x] \geq \frac{2}{3}$,
- $\forall x \in A_{\text{no}} : \Pr[Q_{|x|} \text{ accepts } x] \leq \frac{1}{3}$.

**Definition** (QMA)**.** ...there exists a polynomial-time generated family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$, where each circuit $Q_n$ takes $n + p(n)$ input qubits and produces one output qubit, such that

- $\forall x \in A_{\text{yes}}\ \exists \rho \in D(2^{p(|x|)}) : \Pr[Q_{|x|} \text{ accepts } (x,\rho)] \geq \frac{2}{3}$ (*completeness*),
- $\forall x \in A_{\text{no}}\ \forall \rho \in D(2^{p(|x|)}) : \Pr[Q_{|x|} \text{ accepts } (x,\rho)] \leq \frac{1}{3}$ (*soundness*),

where $D(d)$ stands for the set of all $d \times d$ density matrices.

# 7 Quantum error correction and fault tolerance

Action via conjugation:

$$H : X \mapsto Z \qquad H : Z \mapsto X \qquad H : Y \mapsto -Y \tag{61}$$

$$S : X \mapsto Y \qquad S : Y \mapsto -X \qquad S : Z \mapsto Z \tag{62}$$

$$\text{CNOT} : X \otimes I \mapsto X \otimes X \tag{63}$$
$$\text{CNOT} : I \otimes X \mapsto I \otimes X \tag{64}$$
$$\text{CNOT} : Z \otimes I \mapsto Z \otimes I \tag{65}$$
$$\text{CNOT} : I \otimes Z \mapsto Z \otimes Z \tag{66}$$

## 7.1 Quantum error correction

**Theorem** (Quantum error-correction condition)**.** *Let $C$ be a quantum code and $\Pi_C$ the projector onto the code subspace, and $\mathcal{E} = \{E_i\}$ a quantum operation. An operation for correcting $\mathcal{E}$ on $C$ exists if and only if*

$$\Pi_C E_i^\dagger E_j \Pi_C = \alpha_{ij} \Pi_C \tag{67}$$

*for some Hermitian matrix $\alpha$.*

**Theorem** (Discretization of errors)**.** *Let $C$ be a quantum code and $\mathcal{R}$ be the error-correction operation to recover from $\mathcal{E} = \{E_i\}$ constructed in the proof of the previous theorem. If $\mathcal{F} = \{F_j\}$ where $F_j = \sum_i m_{ji} E_i$ for some complex matrix $m$, then $\mathcal{R}$ also corrects for $\mathcal{F}$ on the code $C$.*

#### 7.1.1 The Shor code

$$|0\rangle \mapsto |+\rangle^{\otimes 3} \mapsto \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3} = |0_L\rangle \tag{68}$$

$$|1\rangle \mapsto |-\rangle^{\otimes 3} \mapsto \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3} = |1_L\rangle \tag{69}$$

# 8 Quantum information theory and basic communication protocols

## 8.1 Resource tradeoffs

Let $x \in \{0,1\}$. The ability to perform the corresponding transformation for any basis vector is a resource:

- qubit: $|x\rangle_A \mapsto |x\rangle_B$,
- cbit: $|x\rangle_A \mapsto |x\rangle_B |x\rangle_E$,
- cobit: $|x\rangle_A \mapsto |x\rangle_A |x\rangle_B$.

Trivial inequalities:

$$1 \text{ qubit} \geq 1 \text{ cobit} \geq 1 \text{ cbit}. \tag{70}$$

(Alice can perform a CNOT to create a coherent copy of the state in standard basis, and send one half to Bob. Alice can discard her half of the coherent bit to get a classical bit.) Ability to transmit coherent bits can be used to generate entanglement by using $|+\rangle$ as input:

$$1 \text{ cobit} \geq 1 \text{ ebit}. \tag{71}$$

Irreversible transformations:

- $1 \text{ qubit} + 1 \text{ ebit} \geq 2 \text{ cbits}$ (superdense coding),
- $2 \text{ cbits} + 1 \text{ ebit} \geq 1 \text{ qubit}$ (teleportation).

Reversible transformations given a catalyst ebit:

- $(1 \text{ qubit} + 1 \text{ ebit}) \geq (2 \text{ cobits})$,
- $(2 \text{ cobits}) + 1 \text{ ebit} \geq (1 \text{ qubit} + 1 \text{ ebit}) + 1 \text{ ebit}$ (send over a coherent copy without measuring it).

(Before running the superdense coding protocol, Alice makes local copies of her two classical bits; this does not require the catalyst ebit. Alice performs a unitary that maps Bell basis to standard basis (see circuit in Eq. (2)) on the qubit in an unknown state and her half of the ebit; instead of measuring and transmitting two classical bits, she uses coherent communication; conditional on the two received coherent bits, Bob corrects his half of the ebit; they end up generating two ebits from the coherent communication, and Bob also ends up having the unknown state.) Conclusion:

$$(2 \text{ cobits}) + 1 \text{ ebit} = (1 \text{ qubit} + 1 \text{ ebit}) + 1 \text{ ebit} \tag{72}$$

where the ebit is used as a catalyst.

## 8.2 Nayak's bound

**Theorem.** *If $X \in \{0,1\}^m$ is drawn uniformly at random, encoded in $n$ qubits, and recovered to $Y$, the probability that $X = Y$ is at most $2^n/2^m$.*

*Proof.* Let $\{\Pi_x : x \in \{0,1\}^m\}$ be an orthonormal measurement in $(\mathbb{C}^2)^{\otimes n}$, i.e., a set of projectors that sum to identity, and $|\phi_x\rangle \in (\mathbb{C}^2)^{\otimes n}$ the encoding of $x$. Then

$$\begin{aligned}
\Pr[X = Y] &= \frac{1}{2^m} \sum_{x \in \{0,1\}^m} \left\| \Pi_x |\phi_x\rangle \right\|^2 &(73)\\
&= \frac{1}{2^m} \sum_{x \in \{0,1\}^m} \operatorname{Tr}\bigl(\Pi_x |\phi_x\rangle\langle\phi_x|\bigr) &(74)\\
&\leq \frac{1}{2^m} \sum_{x \in \{0,1\}^m} \operatorname{Tr}(\Pi_x \Pi_C) &(75)\\
&= \frac{1}{2^m} \operatorname{Tr} \Pi_C &(76)\\
&= \frac{2^n}{2^m}. &(77)
\end{aligned}$$

□