Technion Israel Amit Levi

Algebric Background

The Inner Product

- Let $\mathcal{V}$ be an inner-product space over the field F. A set of vectors $\{u_i\} \subseteq \mathcal{V}$ is orthonormal if
$$\forall i,j : \langle u_i, u_j \rangle = \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$
The inner-product is a map $\langle \cdot, \cdot \rangle : V \times V \longrightarrow F$ that satisfies
  - Conjugate Symmetry
  $$\langle x, y \rangle = \langle y, x \rangle^*$$
  - Linearity in the second argument
  $$\langle x, \alpha y \rangle = \alpha \langle x, y \rangle$$
  $$\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$$
  - Positive-definiteness
  $$\langle x, x \rangle \geq 0$$
  $$\langle x, x \rangle = 0 \iff x = 0$$
- Cauchy–Schwarz inequality - For all vectors u, v of an inner-product space
$$|\langle u, v \rangle|^2 \leq \langle u, u \rangle \cdot \langle v, v \rangle$$
- In the $\mathbb{C}^n$ space, the inner product of $\vec{x}$ and $\vec{y}$ is defined as
$$\left\langle \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} \right\rangle = \vec{x}^\dagger \vec{y} = \sum_{i=1}^{n} x_i^* y_i$$

Vectors and Matrices

- The product of an $n \times n$ matrix A, whose columns are denoted by $\{A_k\}_{k=1}^n$, and a column vector $\vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ is
$$A\vec{x} = \sum_{k=1}^{n} x_k A_k$$
- The product of an $m \times n$ matrix A, whose rows are denoted by $\{A_i\}_{k=1}^m$, and an $n \times p$ matrix B, whose columns are denoted by $\{B^j\}_{j=1}^p$ is
$$AB = \begin{bmatrix} \langle A_1, B^1 \rangle & \langle A_1, B^2 \rangle & \cdots & \langle A_1, B^p \rangle \\ \langle A_2, B^1 \rangle & \langle A_2, B^2 \rangle & \cdots & \langle A_2, B^p \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle A_m, B^1 \rangle & \langle A_m, B^2 \rangle & \cdots & \langle A_m, B^p \rangle \end{bmatrix}$$
i.e. $(AB)_{i,j} = \langle A_i, B^j \rangle = \sum_{k=1}^n A_{i,k} B_{k,j}$
- Complex conjugation obeys
  - $A^\dagger = (A^*)^\top = (A^\top)^*$
  - $(\alpha A)^\dagger = \alpha^* A^\dagger$
  - $(A + B)^\dagger = (A^\dagger + B^\dagger)$
  - $(AB)^\dagger = B^\dagger A^\dagger$
- A matrix D is diagonal if $\forall i, j : i \neq j \Rightarrow D_{i,j} = 0$
- If D_1 and D_2 are diagonal matrices, then the sum $D_1 + D_2$ is diagonal, the product $D_1 D_2$ is diagonal, and $D_1 D_2 = D_2 D_1$
- A matrix $C_{n \times n}$ is circulant if exists $\{c_k\}_{k=0}^{n-1}$ such that $C_{i,j} = c_{(j-i) \mod n}$
- If C_1 and C_2 are circulant matrices, then the sum $C_1 + C_2$ is circulant, the product $C_1 C_2$ is circulant, and $C_1 C_2 = C_2 C_1$
- All circulant matrices have the same eigenvectors

Unitary Matrices

- If U is a square, complex matrix, then the following conditions are equivalent:
  - U is unitary
  - $U^\dagger$ is unitary
  - $UU^\dagger = U^\dagger U = I$
  - The columns of U are orthonormal
  - The rows of U are orthonormal
- If U is unitary, then for every u, v: $\langle Uu, Uv \rangle = \langle u, v \rangle$
- If U is unitary, then all of its eigenvalues lie on the unit circle
  - i.e. $\forall \lambda : |\lambda| = 1$

Hermitian Matrices

- A matrix A is hermitian if $A = A^\dagger$
- If A is Hermitian, then all of its eigenvalues are real.
- If A is Hermitian, then it is diagonalizable by a unitary matrix. $D = U^\dagger A U$

Kronecker Product

- If A is an $m \times n$ matrix and B is a $p \times q$ matrix, then the Kronecker product is the $mp \times nq$ matrix:
$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}$$
- Bilinearity and associativity:
  - $A \otimes (B + C) = A \otimes B + A \otimes C$
  - $(B + C) \otimes A = B \otimes A + C \otimes A$
  - $(kA) \otimes B = A \otimes (kB) = k(A \otimes B)$
  - $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
  - $A \otimes 0 = 0 \otimes A = 0$
- The mixed-product property:
$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$
$$A(B \otimes C) = (AB) \otimes C = B \otimes (AC)$$
$$(A \otimes B)C = (AC) \otimes B = A \otimes (CB)$$
$$A(B \otimes C) = (A \otimes C)B$$
- The inverse of a Kronecker product: It follows that $A \otimes B$ is invertible if and only if both A and B are invertible, in which case the inverse is given by
$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$$
- Transpose: Transposition and conjugate transposition are distributive over the Kronecker product:
$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$$
- Trace:
$$\mathrm{tr}(A \otimes B) = \mathrm{tr}(A) \cdot \mathrm{tr}(B)$$
- Inner Product:
$$\left\langle \vec{a} \otimes \vec{b}, \vec{c} \otimes \vec{d} \right\rangle = \langle \vec{a}, \vec{c} \rangle \cdot \left\langle \vec{b}, \vec{d} \right\rangle$$

Eigenvalues and Eigenvectors

- If $Av = \lambda v$ (for $v \neq 0$), then v is an eigenvector of A and the scale factor λ is the eigenvalue corresponding to that eigenvector
- Characteristic polynomial equation of matrix A
$$\det(\lambda I - A) = 0$$
The eigenvalues of A are the roots of its characteristic polynomial
- $\mathrm{tr}(A) = \sum_{k=1}^n \lambda_k$
- $\det(A) = \prod_{k=1}^n \lambda_k$
- If λ is a complex eigenvalue of A, then λ^* is also an eigenvalue of A
- If the sum of each row of A equals s, then s is an eigenvalue of A
- If the sum of each column of A equals s, then s is an eigenvalue of A

Trace Identities

- $\mathrm{tr}(A_{N \times N}) = \sum_{i=1}^N a_{ii} = \sum_{i=1}^N \langle i | A | i \rangle$ (for any basis $\{|i\rangle\}$)
- Linearity:
$$\mathrm{tr}(\alpha A + \beta B) = \alpha\, \mathrm{tr}(A) + \beta\, \mathrm{tr}(B)$$
- For column vectors
$$\mathrm{tr}(xx^T) = x^T x$$
- $\mathrm{tr}(AB) = \mathrm{tr}(BA)$
  - $\mathrm{tr}(A_1 A_2 \ldots A_{n-1} A_n) = \mathrm{tr}(A_n A_1 A_2 \ldots A_{n-1})$
- Linearity of the expectation - $E(\mathrm{tr}(A)) = \mathrm{tr}(E(A))$

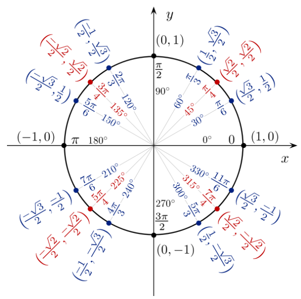
Basic Algebric Formulas

- $(a \pm b)^2 = a^2 \pm 2ab + b^2$
- $(a - b)(a + b) = a^2 - b^2$
- $(a \pm b)^3 = a^3 \pm 3a^2 b + 3ab^2 \pm b^3$
- $a^3 \pm b^3 = (a \pm b)(a^2 \mp ab + b^2)$

Trigonometric Identities

- $\sin^2\theta + \cos^2\theta = 1$
- $\sin\theta = \pm\sqrt{1 - \cos^2\theta}$
- $\cos\theta = \pm\sqrt{1 - \sin^2\theta}$
- $\sin(-\theta) = -\sin\theta$
- $\cos(-\theta) = \cos\theta$
- $\sin\left(\theta \pm \frac{\pi}{2}\right) = \pm\cos\theta$
- $\cos\left(\theta \pm \frac{\pi}{2}\right) = \mp\sin\theta$
- $\sin(\theta + \pi) = -\sin\theta$
- $\cos(\theta + \pi) = -\cos\theta$
- $\sin(\alpha \pm \beta) = \sin\alpha\cos\beta \pm \cos\alpha\sin\beta$
- $\cos(\alpha + \beta) = \cos\alpha\cos\beta \mp \sin\alpha\sin\beta$
- $\sin(2\theta) = 2\sin\theta\cos\theta$
- $\cos(2\theta) = \cos^2\theta - \sin^2\theta = 2\cos^2\theta - 1 = 1 - 2\sin^2\theta$
- $\sin^2\theta = \frac{1 - \cos(2\theta)}{2}$
- $\cos^2\theta = \frac{1 + \cos(2\theta)}{2}$
- $\sin\alpha \pm \sin\beta = 2\sin\left(\frac{\alpha \pm \beta}{2}\right)\cos\left(\frac{\alpha \mp \beta}{2}\right)$
- $\cos\alpha + \cos\beta = 2\cos\left(\frac{\alpha + \beta}{2}\right)\cos\left(\frac{\alpha - \beta}{2}\right)$
- $\cos\alpha - \cos\beta = -2\sin\left(\frac{\alpha + \beta}{2}\right)\sin\left(\frac{\alpha - \beta}{2}\right)$
- $2\cos\alpha\cos\beta = \cos(\alpha - \beta) + \cos(\alpha + \beta)$
- $2\sin\alpha\sin\beta = \cos(\alpha - \beta) - \cos(\alpha + \beta)$
- $2\sin\alpha\cos\beta = \sin(\alpha + \beta) + \sin(\alpha - \beta)$
- $2\cos\alpha\sin\beta = \sin(\alpha + \beta) - \sin(\alpha - \beta)$
- $e^{ix} = \cos x + i\sin x$
- $e^{-ix} = \cos x - i\sin x$
- $e^{ix} + e^{-ix} = 2\cos(x)$
- $e^{i\pi} = e^{-i\pi} = -1$
- $\forall k \in \mathbb{Z} : e^{i2\pi k} = 1$

$(\cos\theta, \sin\theta)$



Probability

- Joint probability:
$$p(x; y) = p(x)\, p(y \mid x) = p(y)\, P(x \mid y)$$
- Law of Total Probability
$$P(A) = \sum_i P(A \mid B_i)\, P(B_i)$$
where $\{B_i\}_i$ is a countable partition of the sample space
- Bayes' theorem
$$P(A \mid B) = \frac{P(B \mid A)\, P(A)}{P(B)}$$
- Law of Total Expectation
  - $E(X) = E(E(X \mid Y))$ for any random variables X, Y
  - $E(X) = \sum_i E(X \mid A_i)\, P(A_i)$ where $\{A_i\}_i$ is a countable partition of the sample space

Information Theory

- Self information:
$$I(x) = \log_2 \frac{1}{p(x)} = -\log_2 p(x)$$
  - $p(x) = P(X = x)$ is the a-priori probability of the occurence of x
- Entropy:
$$H(X) = \sum_x p(x)\, I(x) = -\sum_x p(x) \log_2 p(x)$$
  - $H(X) \geq 0$
- Conditional entropy:
$$H(X \mid Y) = \sum_y p(y)\, H(X \mid Y = y)$$
$$= -\sum_{x,y} p(x; y) \log_2 p(x \mid y)$$
  - $H(f(X) \mid X) = 0$
- Mutual entropy:
$$H(X; Y) = -\sum_{x,y} p(x; y) \log_2 p(x; y)$$
$$H(X; Y) = H(X) + H(Y \mid X)$$
$$H(X; Y) = H(Y) + H(X \mid Y)$$
  - $H(X; Y) \geq 0$
  - $\mathrm{H}(X; Y) = H(Y; X)$
- Mutual information:
$$I(X; Y) = H(X) - H(X \mid Y)$$
$$I(X; Y) = H(X) + H(Y) - H(X; Y)$$
$$I(X; Y) = H(X; Y) - H(X \mid Y) - H(Y \mid X)$$
  - $I(X; Y) \geq 0$
  - $I(X; Y) = I(Y; X)$
- If X and Y are two independent random variables:
$$H(X \mid Y) = H(X)$$
$$I(X; Y) = 0$$
- Binary entropy function:
$$h_2(p) = -p\log_2(p) - (1 - p)\log_2(1 - p)$$

Discrete Fourier Transform

- The DFT matrix of size $M \times M$ is defined as
$$[DFT] = \frac{1}{\sqrt{M}} \begin{bmatrix} (W^*)^{0 \cdot 0} & \cdots & (W^*)^{0 \cdot (M-1)} \\ \vdots & \ddots & \vdots \\ (W^*)^{(M-1) \cdot 0} & \cdots & (W^*)^{(M-1) \cdot (M-1)} \end{bmatrix}$$
where $W = e^{i\frac{2\pi}{M}}$, $W^* = e^{-i\frac{2\pi}{M}}$
- The DFT matrix is symmetric and unitary

- $[DFT]^{\dagger}=\frac{1}{\sqrt{M}}\begin{bmatrix} W^{0\cdot 0} & \cdots & W^{0\cdot(M-1)} \\ \vdots & \ddots & \vdots \\ W^{(M-1)\cdot 0} & \cdots & W^{(M-1)\cdot(M-1)} \end{bmatrix}$
- The $[DFT]^{\dagger}$ matrix digonalizes any circulant matrix
- The eigenvalues of a circulant matrix can be calculated using its first row and the $[DFT]^{\dagger}$ matrix
$$\begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \vdots \\ \lambda_N \end{bmatrix} = [DFT]^{\dagger} \begin{bmatrix} c_0 \\ c_{N-1} \\ c_{N-2} \\ \vdots \\ c_1 \end{bmatrix}$$

Quantum Theory

The Postulates of Quantum Mechanics

- At each instant the state of a physical system is represented by a ket $|\psi\rangle$ in the space of states
- Every observable attribute of a physical system is described by an operator that acts on the kets that describe the system
- The only possible result of the measurement of an observable A is one of the eigenvalues of the corresponding operator A
- When a measurement of an observable A is made on a generic state $|\psi\rangle$, the probability of obtaining an eigenvalue λ_i is given by the square of the inner product of $|\psi\rangle$ with the eigenstate $|\psi_i\rangle$, $|\langle\psi_i|\psi\rangle|^2$
- Immediately after the measurement of an observable A has yielded a value λ_i, the state of the system is the normalized eigenstate $|\psi_i\rangle$

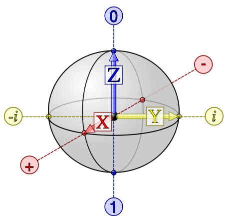
Pure States

- Any state which can be described by a ket $|\psi\rangle$ is a pure state
- Normalization of $|\psi\rangle=\sum_j \alpha_j|\psi_j\rangle$, where $\{|\psi_j\rangle\}$ is an orthonormal basis: $\sum_j|\alpha_j|^2$
- Probability of measuring v_i: $\Pr(v_i)=|\langle v_i|\psi\rangle|^2=\langle v_i|\psi\rangle\langle\psi|v_i\rangle$

Mixed States

- Any state which can be described by an ensemble - $\{p_i,|\psi_i\rangle\}$ of at least size 2
  - $\{|\psi_i\rangle\}$ are not necessarily orthonormal
  - Meaning that with probability p_i, the state is $|\psi_i\rangle$
- Normalization: $\sum_i p_i=1$
- Probability of measuring v_j: $\Pr(v_j)=\sum_i p_i|\langle v_j|\psi\rangle|^2=\sum_i p_i\langle v_j|\psi\rangle\langle\psi|v_j\rangle$
- The completely mixed state: $\{\frac{1}{n},|i\rangle\}_{i=0}^{n-1}$

Bloch Sphere



- The Bloch sphere is a geometrical representation of the pure state space of a two-level quantum mechanical system (qubit)
- The surface of the Bloch sphere represents all the pure states of a two-dimensional quantum system, whereas the interior corresponds to all the mixed states
- Antipodal points on the sphere correspond to a pair of mutually orthogonal state vectors
- Every state ρ can be represented as $\frac{I+r_x\sigma_x+r_y\sigma_y+r_z\sigma_z}{2}$
  - $\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix}$
  - $\sigma_y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$
  - $\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$
  - $\vec{r}=(\sin\theta\cos\phi,\sin\theta\sin\phi,\cos\theta)$
- Pauli matrices are anti-commutative
  $\sigma_x\sigma_y=-\sigma_y\sigma_x \quad \sigma_x\sigma_z=-\sigma_z\sigma_x \quad \sigma_z\sigma_y=-\sigma_y\sigma_z$
- If the state ρ is a mix of states $\{\rho_i\}$ with probabilities p_i and vectors $\vec{r_i}$:
$$\vec{r}=\sum_i p_i\vec{r_i}$$
- The completely mixed state: $\rho=\frac{I_n}{n}$

Density Matrix

- The density matrix of a pure state $|\psi\rangle$ is $\rho_\psi=|\psi\rangle\langle\psi|$
- The density matrix of a mixed state is $\rho_{\text{mixed}}=\sum_j p_j|\psi_j\rangle\langle\psi_j|$
- $\Pr(v_i)=\langle v_i|\rho|v_i\rangle$
- $\rho^2=\rho \iff$ the state is pure
- $\mathrm{tr}(A\rho)=\sum_i p_i\langle\psi_i|A|\psi_i\rangle$
- Two states are the same $\iff$ their density matrices are equal

Combining Two Systems

- Given a subsystem A in the state $|\psi_A\rangle$ and a subsystem B in the state $|\psi_B\rangle$, their joint state in the combined system is given by $|\psi_A\rangle\otimes|\psi_B\rangle=|\psi_A\psi_B\rangle$
- If a state in a combined system cannot be expressed as a tensor product, it is called an entangled state
  - Given a joint state $\sum_{i,j}b_{ij}|ij\rangle$, if $b_{00}b_{11}\neq b_{01}b_{10}$ then it is entangled
- Given a joint state $|\psi\rangle_{AB}=\sum_{i,j}\alpha_{ij}|i\rangle_A|j\rangle_B$: measuring in the $\{|j\rangle_B\}$ basis yields $|j\rangle_B$ with probability $p(j)=\sum_i|\alpha_{ij}|^2$, and the state in system A will be $|\phi^j\rangle_A=\frac{1}{\sqrt{p(j)}}\sum_i\alpha_{ij}|i\rangle_A$
  - $|\psi_{AB}\rangle$ can be expressed as $\sum_j\sqrt{p(j)}|\phi^j\rangle_A|j\rangle_B$ or $\sum_i\sqrt{p(i)}|i\rangle_A|\phi^i\rangle_B$

Partial Inner Product

Assume $|\psi\rangle_{AB}=\sum_{i,j}\alpha_{ij}|i\rangle_A|j\rangle_B$

- $\langle\phi_B|\psi_{AB}\rangle=\sum_i\left(\sum_j\beta_j^*\alpha_{ij}\right)|i\rangle_A$
- $\langle\phi_B|\psi_{AB}\rangle=\sum_{i,j}\alpha_{ij}|i\rangle_A\langle\phi_B|j\rangle_B$
- $\langle\phi_A|\psi_{AB}\rangle=\sum_{i,j}\alpha_{ij}\langle\phi_A|i\rangle_A|j\rangle_B$
- Meaning: The state of subsystem A after a measurement in subsystem B
  - $|\psi_{AB}\rangle$ is the initial joint state
  - $|\phi\rangle_B$ is the result of the measurement in subsystem B

Partial Measurement (Trace-Out)

- Given a joint state represented by the denstiry matrix ρ_{AB}, the state of system A is given by $\rho_A=\mathrm{tr}_B(\rho_{AB})=\sum_j\langle j|_B\,\rho_{AB}\,|j\rangle_B$
- For a pure state $|\psi\rangle_{AB}=\sum_j\sqrt{p(j)}|\phi^j\rangle_A|j\rangle_B$, then $\rho_A=\sum_k p(k)|\phi^k\rangle\langle\phi^k|$
- $\mathrm{tr}_A(|\psi\rangle_A\otimes|\psi_B\rangle)=|\psi_B\rangle$
- $\mathrm{tr}_B(|\psi\rangle_A\otimes|\psi_B\rangle)=|\psi_A\rangle$
- Generally, $\mathrm{tr}_B(\rho)\otimes\mathrm{tr}_A(\rho)\neq\rho$
- A quantum state is entangled $\iff$ ρ_A (or ρ_B) is a mixed state
- Purification: Given a mixed state ρ_A in subsystem A, its purification is a pure state $|\psi\rangle_{AB}$ in a combined system such that $\mathrm{tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|)=\rho_A$
- For the completely mixed state, $\rho=\frac{I_n}{n}$, $\rho_A=\frac{I_{n/2}}{n/2}$

For 2-qubit systems, the partial trace is explicitly

$$\mathrm{Tr}_2\begin{bmatrix}\rho_{00,00}&\rho_{00,01}&\rho_{00,10}&\rho_{00,11}\\\rho_{01,00}&\rho_{01,01}&\rho_{01,10}&\rho_{01,11}\\\rho_{10,00}&\rho_{10,01}&\rho_{10,10}&\rho_{10,11}\\\rho_{11,00}&\rho_{11,01}&\rho_{11,10}&\rho_{11,11}\end{bmatrix}=\begin{bmatrix}\rho_{00,00}+\rho_{01,01}&\rho_{00,10}+\rho_{01,11}\\\rho_{10,00}+\rho_{11,01}&\rho_{10,10}+\rho_{11,11}\end{bmatrix}$$

and

$$\mathrm{Tr}_1\begin{bmatrix}\rho_{00,00}&\rho_{00,01}&\rho_{00,10}&\rho_{00,11}\\\rho_{01,00}&\rho_{01,01}&\rho_{01,10}&\rho_{01,11}\\\rho_{10,00}&\rho_{10,01}&\rho_{10,10}&\rho_{10,11}\\\rho_{11,00}&\rho_{11,01}&\rho_{11,10}&\rho_{11,11}\end{bmatrix}=\begin{bmatrix}\rho_{00,00}+\rho_{10,10}&\rho_{00,01}+\rho_{10,11}\\\rho_{01,00}+\rho_{11,10}&\rho_{01,01}+\rho_{11,11}\end{bmatrix}$$

Schmidt Decomposition

- A state $|\psi\rangle_{AB}=\sum_{i,j}\alpha_{ij}|i\rangle_A|j\rangle_B$ can be expressed uniquely as
$$|\psi\rangle_{AB}=\sum_k^N\lambda_k|u_k\rangle_A|v_k\rangle_B$$
  - $N=\min(\dim(A),\dim(B))$
  - λ_i are real, non-negative
  - The sets $\{u_k\}_1^N,\{v_k\}_1^N$ are orthonormal
  - $\rho_A=\mathrm{tr}_B(|\psi\rangle_{AB}\langle\psi|_{AB})=\sum_k^N\lambda_k^2|u_k\rangle_A\langle u_k|_A$
  - $\rho_B=\mathrm{tr}_A(|\psi\rangle_{AB}\langle\psi|_{AB})=\sum_k^N\lambda_k^2|v_k\rangle_B\langle v_k|_B$
- Schmidt Number: $|\{\lambda_i\mid\lambda_i\neq 0\}|$ (i.e., the number of non-zero λ_i's)
- A quantum state is entangled $\iff$ its Schmidt number is greater than 1

Bell States

- $|\psi_-\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}$ $\quad|\phi_-\rangle=\frac{|00\rangle-|11\rangle}{\sqrt{2}}$
  $|\psi_+\rangle=\frac{|01\rangle+|10\rangle}{\sqrt{2}}$ $\quad|\phi_+\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- $|\psi_-\rangle=\frac{|-+\rangle-|+-\rangle}{\sqrt{2}}$
- $|\psi_+\rangle=\frac{|++\rangle-|--\rangle}{\sqrt{2}}$
- Measuring $|\psi_-\rangle$ in any basis yields opposing results (i.e. $|0\rangle,|1\rangle$ or $|+\rangle,|-\rangle$)

Werner State

- $\chi=\lambda|\psi_-\rangle\langle\psi_-|+\frac{1-\lambda}{3}[|\psi_+\rangle\langle\psi_+|+|\phi_-\rangle\langle\phi_-|+|\phi_+\rangle\langle\phi_+|]$
- Werner state is pure for $\lambda=1$
- Werner state is completely mixed for $\lambda=\frac{1}{4}$
- Werner state is entangled $\iff$ $\lambda>\frac{1}{2}$

Fidelity

- Fidelity: a measure of the "closeness" of two quantum states
  - $F(\psi,\psi')=\langle\psi|\rho_{\psi'}|\psi\rangle=\mathrm{tr}\left(\rho_\psi\rho_{\psi'}\right)$
  - $\mathrm{F}(\rho,\psi)=\langle\psi|\rho|\psi\rangle=\mathrm{tr}(\rho\rho_\psi)$
  - $F(\rho,\sigma)=\mathrm{tr}(\rho\sigma)$
  - Fidelity is the probability of measuring $|\psi\rangle$ in the orthonormal basis $\{|\psi\rangle,|\bar{\psi}\rangle\}$

Quantum Information

- Von Neumann entropy:
$$S(\rho)=-\sum_{i=0}^{n-1}\lambda_i\cdot\log_2\lambda_i$$
  Where $\{\lambda_i\}_{i=0}^{n-1}$ are the eigenvalues of ρ
  - For a pure state ρ, $S(\rho)=0$
- Holevo bound:
$$I(X;Y)\leq S(\rho)-\sum_i p_iS(\rho_i)$$

Teleportation

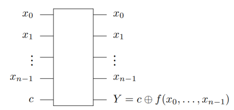
- Assume Alice has a qubit in the state $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$, which she wants to send to Bob. To do so:
  - Alice and Bob share an EPR pair: $|\psi_-\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}$
  - Alice performs a Bell measurement of her qubits (her half of the EPR pair, and the original qubit in state $|\psi\rangle$)
    - This measurement has 4 possible results, and therefore can be encoded using 2 classical bits
  - Alice tells Bob the result of her measurements
  - Bob performs an inverse transformation corresnpoding to the measurement, to change his half of the EPR pair into $|\psi\rangle$.

Alice's Measurement	Bob's Result	Inverse Transformation
$\lvert\phi_+\rangle$	$-\beta\lvert 0\rangle+\alpha\lvert 1\rangle$	$\begin{pmatrix}0&1\\-1&0\end{pmatrix}$
$\lvert\phi_-\rangle$	$\beta\lvert 0\rangle+\alpha\lvert 1\rangle$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$
$\lvert\psi_+\rangle$	$\alpha\lvert 0\rangle-\beta\lvert 1\rangle$	$\begin{pmatrix}1&0\\0&-1\end{pmatrix}$
$\lvert\psi_-\rangle$	$\alpha\lvert 0\rangle+\beta\lvert 1\rangle$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$

Quantum Computing

Quantum Gates

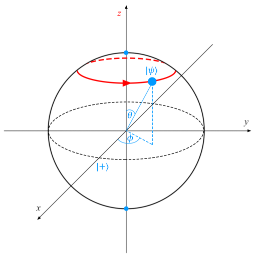
- Reversible gate: A gate which implements a Boolean function which is a permutation.
  - Every gate can be expressed as a reversible gate, as demostrated in the following figure:



Technion Israel Amit Levi

Operator	Gate(s)	Matrix
Pauli-X (X)	X	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$
Pauli-Y (Y)	Y	$\begin{bmatrix}0 & -i\\i & 0\end{bmatrix}$
Pauli-Z (Z)	Z	$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$
Hadamard (H)	H	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$
Controlled Z (CZ)	Z	$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$
Fredkin (CSWAP)		$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\end{bmatrix}$

- Phase: $R_\phi = \begin{pmatrix} 1 & 1 \\ 0 & e^{i\phi} \end{pmatrix}$

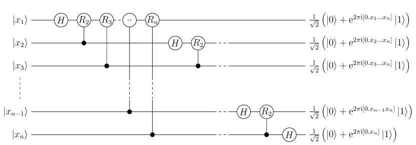


- General control gate:
$$\begin{pmatrix} U_0 & 0 \\ 0 & U_1 \end{pmatrix}$$
  - $U_0, U_1, 0$ are all 2×2 matrices
  - If control bit is 0, applies U_0 on target bit
  - If control bit is 1, applies U_1 on target bit
  - Usually, $U_0 = I$
- Gate with n control bits: $c^n\text{-}V = \begin{pmatrix} I_{2^n} & 0 \\ 0 & V \end{pmatrix}$
- Functional completeness: a functionally complete set of Boolean operators is one which can be used to express all possible truth tables by combining members of the set into a Boolean expression.
  - $\{CNOT\} \cup \{A \mid A \text{ is a 1-bit operator}\}$ is universal
  - Any 1-bit operator can be approximated using $\left\{H, R_{\frac{\pi}{4}}\right\}$ up to an error of $R(\varepsilon)$
  - $\left\{CNOT, H, R_{\frac{\pi}{4}}\right\}$ is universal

Hadamard

- $H|0\rangle = |+\rangle \quad H|+\rangle = |0\rangle$
  $H|1\rangle = |-\rangle \quad H|-\rangle = |1\rangle$
- $H\sigma_x H^\dagger = \sigma_z$
- $H\sigma_z H^\dagger = \sigma_x$
- $H\sigma_y H^\dagger = -\sigma_y$
- $H^{-1} = H^\dagger = H$
- $H_n = H^{\otimes n} = \frac{1}{\sqrt{2^n}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n}$
  - $H_2 = H^{\otimes 2} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$
- $H_n|y\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{y\cdot x}|x\rangle$
  - $y\cdot x$ is the dot-product of y, x, i.e. $\sum_i y_i x_i$

Quantum Fourier Transform



- phase gate: $R_m = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^m}} \end{pmatrix}$
- fractional binary notation: $[0.x_1\ldots x_m] = \sum_{k=1}^m x_k 2^{-k}$
- The quantum Fourier transform acts on a quantum state $|x\rangle = \sum_{i=0}^{N-1} x_i|i\rangle$ and maps it to a quantum state $\sum_{i=0}^{N-1} y_i|i\rangle$ according to the formula:
$$y_k = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} x_n\omega_N^{kn}$$
  - $\omega_N = e^{\frac{2\pi i}{N}}$
- Implementation requires n H gates, and $\frac{(n-1)n}{2}$ R_m gates
  - Total of $\frac{n(n+1)}{2}$ gates

Oracles

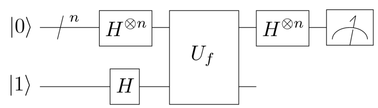
- An oracle V_f of a function $f:\{0,1\}^n : \{0,1\}^m$ is a gate which performs the operation:
$$V_f|x\rangle|b\rangle = |x\rangle|b\oplus f(x)\rangle$$
  where $|b\rangle$ are ancilla bits
- In the case of $f:\{0,1\}^n : \{0,1\}$, we can choose $|b\rangle = H|1\rangle = |-\rangle$ and get:
$$V_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$
  Thus, we can denote $U_f|x\rangle = (-1)^{f(x)}|x\rangle$

Complexity

- Complexity:
$$P \subseteq BPP \subseteq BQP \subseteq PSPACE$$

Quantum Algorithms

Deutsch Jozsa Algorithm



Problem: Given an oracle that implements a function $f:\{0,1\}^n \to \{0,1\}$ that is either constant or balanced, determine if f is constant or balanced

- Constant: returns 0 on all outputs or 1 on all outputs
- Balanced: returns 1 for half of the input domain and 0 for the other half

Algorithm:

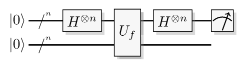
1. Initialize a register of length n to $\left|\vec{0}\right\rangle$, and another register of length 1 to $|1\rangle$
2. Apply H on both registers
3. Apply f on second register
4. Apply Hon first register
5. Measure the first register
   (a) If measurement yielded $|0\rangle$ - f is constant
   (b) Otherwise - f is balanced

Analysis: The states during the first 3 steps of the algorithm:
$$\left|\vec{0}\right\rangle|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2^n}}\sum_x|\vec{x}\rangle|-\rangle \xrightarrow{f} \frac{1}{\sqrt{2^n}}\sum_x(-1)^{f(\vec{x})}|\vec{x}\rangle|-\rangle$$

- If f is constant: The state after applying f is
$$\frac{1}{\sqrt{2^n}}\sum_x(-1)^c|\vec{x}\rangle|-\rangle = \pm\frac{1}{\sqrt{2^n}}\sum_x|\vec{x}\rangle|-\rangle$$
  Therefore, the final state is $\pm\left|\vec{0}\right\rangle|-\rangle$ and measurement yields $\left|\vec{0}\right\rangle$ with probability 1
- If f is balanced: The final state is
$$\frac{1}{\sqrt{2^n}}\sum_x(-1)^{f(\vec{x})}[H|\vec{x}\rangle]|-\rangle$$
$$= \frac{1}{2^n}\sum_y\sum_x(-1)^{f(\vec{x})}(-1)^{\vec{x}\cdot\vec{y}}|\vec{y}\rangle|-\rangle$$
  Therefore, since f is balanced, the probability of measuring $\left|\vec{0}\right\rangle$ is
$$\sum_x(-1)^{f(\vec{x})}(-1)^{\vec{x}\cdot\vec{0}} = \frac{2^n}{2}\cdot(-1) + \frac{2^n}{2}\cdot 1 = 0$$

In conclusion, we measure $\left|\vec{0}\right\rangle \iff f$ is constant

Simon's Algorithm



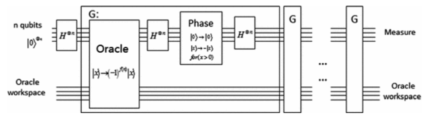
Problem: Given an oracle that implements a $2\to 1$ function $f:\{0,1\}^n \to \{0,1\}^n$ that is s-periodic (i.e. $\forall x\neq y: f(x) = f(y) \iff y = x\oplus s$), find s

Algorithm:

1. Repeat until there are $n-1$ different measurement results:
   (a) Initialize 2 registers of length n to $\left|\vec{0}\right\rangle$
   (b) Apply H on first register
   (c) Apply f on second register
   (d) Apply Hon first register
   (e) Measure first register
2. Solve for s

Analysis: The states during each iteration of the algorithm:
$$\left|\vec{0}\right\rangle\left|\vec{0}\right\rangle \xrightarrow{H} \frac{1}{\sqrt{2^n}}\sum_x|x\rangle\left|\vec{0}\right\rangle \xrightarrow{f} \frac{1}{\sqrt{2^n}}\sum_x|x\rangle|f(x)\rangle$$
$$\xrightarrow{H} \frac{1}{\sqrt{2^n}}\sum_x\sum_y(-1)^{x\cdot y}|y\rangle|f(x)\rangle$$
Let S be the maximal group such that $\forall x, y\in S: f(x)\neq f(y)$ (Notice that $|S| = \frac{|S|}{2}$). The final state can be written as
$$\frac{1}{\sqrt{2^n}}\sum_y|y\rangle\left[\sum_{z\in S}(-1)^{z\cdot y}|f(z)\rangle + (-1)^{(z\otimes s)\cdot y}|f(z)\rangle\right]$$
$$= \frac{1}{\sqrt{2^n}}\sum_y|y\rangle\left[\sum_{z\in S}(-1)^{z\cdot y}\left(1+(-1)^{s\cdot y}\right)|f(z)\rangle\right]$$
Measuring this state will yield some y' with the following probability:
$$\Pr\left(y'\right) = \begin{cases}\frac{1}{2^{n-1}} & y'\cdot s\equiv 0 \mod 2\\ 0 & y'\cdot s\equiv 1 \mod 2\end{cases}$$
Repeating the algorithm $n-1$ times has a probability greater than $\frac{1}{4}$ of yielding linearly independent y's such that $y\cdot s\equiv 0 \mod 2$, which can then be used to solve for s.

Grover's Search Algorithm



Problem: Given an oracle of a function $f:\{0,1\}^n \to \{0,1\}$ such that $f(x) = \begin{cases}1 & x=\beta\\ 0 & x\neq\beta\end{cases}$, find β

Algorithm:

1. Initialize a register of length n to $\left|\vec{0}\right\rangle$
2. Apply H
3. Repeat the following "Grover Iteration" $M = \frac{\pi\sqrt{N}}{4}$ times:
   (a) Apply U_f
   (b) Apply H
   (c) Apply $I_0 = 2|0\rangle\langle 0| - I$ (Phase shift of all states $|x\rangle\neq|0\rangle$)
   (d) Apply H
4. Measure

The algorithm can be written as $G^M H|0\rangle$, where $G = (HI_0HU_f)$

Analysis: Define $\alpha = \frac{1}{\sqrt{N-1}}\sum_{i\neq\beta}|i\rangle$ (super-position of all other states), and denote the state before the first iteration as
$$|\psi_0\rangle = H|0\rangle \triangleq \cos\phi|\alpha\rangle + \sin\phi|\beta\rangle$$
where:

- $\cos\phi = \frac{\sqrt{N-1}}{N}$

- $\sin\theta = \frac{1}{\sqrt{N}}$

Grover's Iteration can be written in the $(|\alpha\rangle, |\beta\rangle)$ plane as

$$G_{|\alpha\rangle,|\beta\rangle} = \begin{pmatrix} \cos\omega & -\sin\omega \\ \sin\omega & \cos\omega \end{pmatrix}$$

where:

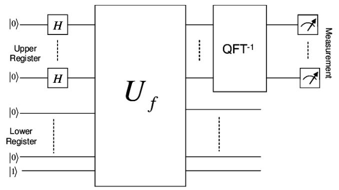
- $\cos\omega = 1 - \frac{2}{N}$
- $\sin\omega = \frac{2\sqrt{N-1}}{N}$

Therefore, Grover's Iteration rotates the state by ω on the $(|\alpha\rangle, |\beta\rangle)$ plane. The state after m iterations is $|\psi_m\rangle = G^m H |0\rangle = \cos(\omega m + \phi)|\alpha\rangle + \sin(\omega m + \phi)|\beta\rangle$ and the probability of measuring $|\beta\rangle$ is

$$\Pr_m(\beta) = |\langle\beta|\psi_m\rangle|^2 = \sin^2(\omega m + \phi) = \frac{1}{2} - \frac{1}{2}\cos(2\omega m + 2\phi)$$

For $m = M = \frac{\pi\sqrt{N}}{4}$, this probability is approximately 1

Quantum Period-Finding Algorithm



Problem: Given an oracle that implements a $A \to 1$ function $f : \{0,1\}^n \to \{0,1\}^n$ that is r-periodic (i.e. $\forall x \neq y : f(x) = f(y) \iff \exists j : y = x + j \cdot r$), find r

Algorithm:

1. Initialize 2 registers of length n to $\left|\vec{0}\right\rangle$
2. Apply H on first register
3. Apply f on second register
4. Apply QFTon first register
5. Measure first register
6. Use the Continued Fraction Method to round the measurement result and find r
7. if $f(0) \neq f(r)$, then go back to step 1

Analysis: The states during each iteration of the algorithm

$$\left|\vec{0}\right\rangle\left|\vec{0}\right\rangle \xrightarrow{H} \frac{1}{\sqrt{2}^n}\sum_x |x\rangle\left|\vec{0}\right\rangle \xrightarrow{f} \frac{1}{\sqrt{2}^n}\sum_x |x\rangle|f(x)\rangle$$

Assume we measure the second register (this is not required for the algorithm). Measuring yields some value $f(x_0)$, and the state of the first register is

$$\frac{1}{\sqrt{A}}\sum_{j=0}^{A-1}|x_0 + j\cdot r\rangle$$
$$\xrightarrow{QFT} \frac{1}{\sqrt{A\cdot 2^n}}\sum_{y=0}^{2^n-1}\sum_{j=0}^{A-1} e^{\frac{2\pi i}{2^n}(x_0+j\cdot r)y}|y\rangle$$
$$= \frac{1}{\sqrt{A\cdot 2^n}}\sum_{y=0}^{2^n-1} e^{\frac{2\pi i}{2^n}x_0\cdot y}\sum_{j=0}^{A-1} e^{\frac{2\pi i}{2^n}j\cdot r\cdot y}|y\rangle$$

Measuring this state will yield some y' such that $-\frac{r}{2} \leq r\cdot y \mod 2^n \leq \frac{r}{2}$ with probability $r\cdot\frac{4}{\pi^2 r} \approx 0.41$

We know that there is some d such that $-\frac{r}{2} \leq r\cdot y - d\cdot 2^n \leq \frac{r}{2}$. This inequality is equivalent to

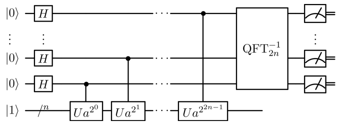
$$-\frac{1}{2\cdot 2^n} \leq \frac{y}{2^n} - \frac{d}{r} \leq \frac{1}{2\cdot 2^n}$$

There is only one fraction $\frac{d}{r}$ such that $1 \leq r < N$, which can be found using CFM.

CFM:

1. Start with $\frac{a}{b}$
2. Calculate $\frac{1}{b/a} = \frac{1}{k + c/a}$
3. if $c = 1$, return $\frac{1}{k}$
4. Otherwise, perform CFM on $\frac{c}{a}$ and return $\frac{1}{k + CFM(c/a)}$

Shor's Factorization Algorithm



Problem: Given a number N such that $N = PQ$, where P, Q are primes, find P, Q

Algorithm:

1. Pick a random integer $a < N$
2. Compute $z = \gcd(a, N)$
3. if $z \neq 1$, it a nontrivial factor of N, so we are done
4. Otherwise, use the quantum period-finding algorithm to find the period r of $f(x) = a^x \mod N$
5. if r is odd or $a^{r/2} \equiv -1 \mod N$, then go back to step 1
6. Otherwise, at least one of $\gcd\left(a^{r/2}+1, N\right)$, $\gcd\left(a^{r/2}-1, N\right)$ is a nontrivial factor of N, so we are done

Analysis: By definition, r is the smallest integer such that

$$a^r \equiv 1 \mod N$$

Therefore, if r is even, then

$$a^r - 1 = \left(a^{r/2}+1\right)\left(a^{r/2}-1\right) \equiv 0 \mod N$$

We can tell that $a^{r/2} - 1 \not\equiv 0 \mod N$ (otherwise $\frac{r}{2}$ would have been the period). Since $a^{r/2} \not\equiv -1 \mod N$, then also $a^{r/2} + 1 \not\equiv 0 \mod N$. In conclusion:

- $PQ \mid \left(a^{r/2}+1\right)\left(a^{r/2}-1\right)$
- $PQ \nmid \left(a^{r/2}+1\right)$
- $PQ \nmid \left(a^{r/2}-1\right)$

Therefore, $P \mid \left(a^{r/2}+1\right)$ and $Q \mid \left(a^{r/2}-1\right)$ (or vice versa).

$$\gcd\left(a^{r/2}+1, N\right) = \gcd(kP, PQ) = P$$
$$\gcd\left(a^{r/2}-1, N\right) = \gcd(kQ, PQ) = Q$$

Remarks:

1. It is possible to construct an oracle of $f(x) = a^x \mod N$, because it can be calculated efficiently, even classically.
   - A commonly used method is to express $x = \sum_{i=0}^{n-1} x_i 2^i$
   - Then, $a^x \mod N = \prod_{i=0}^{n-1}\left[a^{2^i}\right]^{x_i} \mod N$
   - $\left\{a^{2^i}\right\}$ are calculated classically, and are used to construct control-$U_{a^{2^i}}$ gates that multiply by a^{2^i} if the control bit x_i is 1
2. The algorithm has a high chance of succeeding, because the probability that r is odd and that $a^{r/2} \equiv -1 \mod N$ is less than $\frac{1}{2}$
3. Required number of bits: $\lceil\log_2(N^2)\rceil + \lceil\log_2(N)\rceil$
   - $n = \lceil\log_2(N^2)\rceil$ is due to the requirement $N^2 < 2^n < 2N^2$
   - $m = \lceil\log_2(N)\rceil$ is for storing the result $a^x \mod N$

Error Correction

- Repetition code: Repeat each bit n times (e.g. $0 \mapsto 000$)
- Hamming Distance: number of different characters between two words
- A code C is k-error-detecting $\iff$ the minimum Hamming distance in C is at least $k+1$
- A code C is k-error-correcting $\iff$ the minimum Hamming distance in C is at least $2k+1$
- Parity check: Matrix H such that $Hy = 0 \iff y \in C$
- Given an error $y' = y \oplus e$: $Hy' = Hy \oplus He = He$
  - He is caled the syndrome
  - Each error e has a unique syndrome
- Linear code: $\forall c_i, c_j \in C : c_i \oplus c_j \in C$
  - A matrix G is called a generator if for all x of length k, $Gx = y$ is a code word of length n
  - $\forall x : HGx = 0$
- Given the parity check matrix of a code C, $[H_C]$, $[H_C]^T$ is a generator of $C^\perp$. i.e. $[H_C]^T = G_{C^\perp}$
  - $\forall y \in C, z \in C^\perp : z \cdot y = 0$

Qubit Error Types

- No error: I
- Bit change: $\sigma_x = X$
- Phase change: $\sigma_z = Z$
- Bit and phase change: $\sigma_y = Y$
- Minimum number of bits of encoding for correcting an error in 1 qubit: 5
  - $6n + 2$ different states, depending on the error and the qubit (1: no error. $3n$: error in one bit. multiply by 2: $|\psi_0\rangle, |\psi_1\rangle$)
  - Need to be orthonormal, orthonormal basis is of size 2^n
  - $2^n \geq 6n + 2 \Rightarrow n \geq 5$

Qunatum Key Distribution

BB84

1. A chooses bits and basis randomly $(|0_x\rangle, |1_x\rangle, |0_z\rangle, |1_z\rangle)$
2. A sends qubits to B
3. A announces the basis she chose
4. B measures in A's basis
   - Sometimes B measures in a random basis, then A and B compare their basis choices. If they chose the same basis - they keep their bits, otherwise they throw them away

- To deal with errors/attacks:
  - TEST: A chooses randomly subgroup as test group. A and B calculate error rate of this group
  - EC: if error rate is less than some threshold, the check passes. A announces an error correcting code for B
  - PA: A and B have the same string, and use Privacy Amplification to reduce the string size, and the information E has.

Common Results

- $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$
- $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$
- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- $|00\rangle = \frac{1}{2}(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle)$
- $|01\rangle = \frac{1}{2}(|++\rangle - |+-\rangle + |-+\rangle - |--\rangle)$
- $|10\rangle = \frac{1}{2}(|++\rangle + |+-\rangle - |-+\rangle - |--\rangle)$
- $|11\rangle = \frac{1}{2}(|++\rangle - |+-\rangle - |-+\rangle + |--\rangle)$
- $|++\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
- $|+-\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
- $|-+\rangle = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle)$
- $|--\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$