# Linear algebra

2021年9月7日 7:40

Examples of two-level systems

- Spin of a single electron
- Conformation of molecules

Vector spaces

- Complex vector space($C^n$): the space of n-tuples of complex numbers $z_1, z_2, \dots, z_n$.
- The vector elements of the space are column matrices $\begin{pmatrix} z_1 \\ z_2 \\ \dots \\ z_n \end{pmatrix}$.
- Closure under addition
  - Adding two vectors in $C^n$ produces another vector in $C^n$.
- Closure under scalar multiplication
  - Multiplication of a vector in $C^n$ by a complex scalar gives another vector in $C^n$.
- A vector space contains a zero vector denoted by $0$.
  - Note: $|0\rangle$ has a different meaning.
  - $|v\rangle + 0 = |v\rangle$.
  - $z0 = 0$ for any $z \in C$.

Ket vector $|\psi\rangle$:

- Standard shorthand in quantum mechanics for a vector in the vector space (Dirac's notation).

Basis vectors

- Definition: let $|v_i\rangle, i = 1, \dots, n$ be the set spanning the vector space
- Any vector $|v\rangle$ can be written as a linear combination of $|v_i\rangle$.
  - $|v\rangle = \sum_i a_i |v_i\rangle, a_i \in \mathbb{C}$.
- Spanning set for $\mathbb{C}^2$: $|v_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |v_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
  - In ket form: $|v\rangle = a_1 |v_1\rangle + a_2 |v_2\rangle$ where $a_i \in z$.
  - In column vector form: $|v\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ in the $|v_1\rangle, |v_2\rangle$ basis.
  - Phase bases $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
- Second spanning set: $|w_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, |w_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.
  - Consider $|v\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ in the $|v_1\rangle, |v_2\rangle$ basis, write the vector in $|w_i\rangle$ basis.
  - $|v\rangle = \frac{a_1 + a_2}{\sqrt{2}} |w_1\rangle + \frac{a_1 - a_2}{\sqrt{2}} |w_2\rangle$.

Linear independence

- A set of non-zero vectors $|v_i\rangle$ are linearly dependent if there exists a set of complex coefficients $a_i$ with $a_1 \neq 0$ for at least one value of $i$, such that $\sum_i a_i |v_i\rangle = 0$.
- A set of vectors is linearly independent if and only if it is not linearly dependent
- Any two sets of linearly independent vectors which span a vector space $V$ contain the same number of elements and such a set is a basis for $V$.
  - $\mathbb{C}^2$ always have two elements in the basis.
- E.g. $\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ are linearly dependent.

Dimension of vector space

- Definition: The number of elements in the basis for $V$ is called the dimension of $V$.
  - The use of the space $\mathbb{C}^n$ with $n$ finite restricts us to finite dimensional vector spaces.
- For $N$ qubits, $n = 2^N$.

- Quantum physics has infinite dimension

Linear operators

- Definition: A linear operator between vector spaces $V$ (dimension $n$) and $W$ (dimension $m$) is defined to be a map $A: V \rightarrow W$ which is linear in its input.
  - Linearity means: $A\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i A|v_i\rangle$.
    - E.g. $A\left(|v_1\rangle + |v_2\rangle\right) = A|v_1\rangle + A|v_2\rangle$.
  - Usually write $A\left(|v_i\rangle\right) = A|v_i\rangle$.
- A linear operator $A$ on a vector space $V$ is a linear operator from $V$ to $V$
- Definition: There exists two operators, the identity $I$, and the zero operator 0
  - Identity: $I|v\rangle = |v\rangle$
  - Zero: $0|v\rangle = 0$.
- Definition: The composition of two linear operations $A$ and $B$ is written as $BA$.
  - Suppose $V, W, X$ are vector spaces and we have $A: V \rightarrow W$ and $B: W \rightarrow X$.
  - $(BA)|v\rangle = B(A|v\rangle) = BA|v\rangle$.
  - Note: $BA \neq AB$.
- Equivalence of linear operators to matrices
  - Application of a linear operator $A: V \rightarrow W$ to a vector $|v\rangle$ is equivalent to multiplication of a $m \times n$ complex matrix $A$ with the column vector $a_i$ representing the coefficients of the vector $|v\rangle$ in the basis $|v_i\rangle$.
  - The matrix representation of $A$ is specific to both the basis $|v_i\rangle$ and $|w_i\rangle$ and is governed by $A|v_j\rangle = \sum_i A_{ij}|w_i\rangle$.
- E.g. $V$ is a vector space with basis $|0\rangle$ and $|1\rangle$ and $A$ is a linear operator such that $A|0\rangle = |1\rangle$ and $A|1\rangle = |0\rangle$.
  - $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
- $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Pauli matrices

- $\sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- $\sigma_X = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
- $\sigma_Y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$.
- $\sigma_Z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
- $XY = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.
- $YX = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$.
- $XY - YX = 2iZ$.

Inner product

- Definition: A inner product takes two vectors $|v\rangle$ and $|w\rangle$, each of which belongs to the same vector space $V$, to a complex scalar.
  - Notation $\langle v|w\rangle$.
  - $|v\rangle^\dagger$ denotes the adjoint of the vector where $\dagger$ is the adjoint operator.
    - $|v\rangle^\dagger = \langle v|$.
- A finite dimensional vector space is called a Hilbert space if it has an inner product
- Properties
  - Linearity: $\langle v| \sum_i \lambda_i |w_i\rangle\rangle = \sum_i \lambda_i \langle v|w_i\rangle$ .
  - Complex conjugate: $\langle v|w\rangle^* = \langle w|v\rangle$.
- The inner product of $|v\rangle$ with $|w\rangle$ is a measure of the projection of $|v\rangle$ on $|w\rangle$ in the vector space.
  - The measure is in an abstract space

    - $\langle v|w\rangle = |v\rangle^{\dagger}|w\rangle = (a_1^* \, a_2^* \ldots, a_n^*)\begin{pmatrix} b_1 \\ b_2 \\ \ldots \\ b_n \end{pmatrix} = \sum_i a_i^* b_i$ .

Norm

- Definition: the norm $\left||v\rangle\right|$ is an inner product of the vector with itself $\left||v\rangle\right| = \sqrt{\langle v|v\rangle}$.
- The norm $\left||v\rangle\right| = \sqrt{\sum_i |a_i|^2}$ is a measure of the square length of the vector in the abstract space
- $\langle v|v\rangle \geq 0$ and $\langle v|v\rangle = 0$ if any only if $|v\rangle = 0$.
- Unit vector $\left||v\rangle\right| = 1$.

Orthogonality

- Definition: two vectors $|v\rangle$, $|w\rangle$ are orthogonal if their inner product is $\langle v|w\rangle = 0$.
- Orthonormality: a basis is said to be orthonormal if and only if $\langle v_i|v_j\rangle = 0$ .
- Gram-Schmidt procedure: generate an orthonormal basis $|v_i\rangle$ in which $\langle v_i|v_j\rangle = \delta_{ij}$ from a basis $|w_i\rangle$.
    - Define (normalize vector) $|v_1\rangle = \frac{|w_1\rangle}{\left||w_1\rangle\right|}$.
    - For $k = 1$ to $d-1$, define $|v_{k+1}\rangle = \frac{|w_{k+1}\rangle - \sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle}{\left||w_{k+1}\rangle - \sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle\right|}$.
        - $proj_v(w) = \frac{\langle v|w\rangle}{\langle v|v\rangle} v,\ v_k = w_k - \sum_{i=1}^{k-1} proj_{v_j}(w)$
    - This is subtracting off the projection of vectors 1 to k onto vector k+1 from vector k+1, then it is orthonormal to vectors 1 to k

Completeness

- Definition: let $|i\rangle$ be any orthonormal basis for a vector space $V$. Then an arbitrary vector $|v\rangle$ can be written as $|v\rangle = \sum_i v_i|i\rangle$ where $v_i = \langle i|v\rangle$. This is the completeness relation
- Proof: $\sum_i |i\rangle\langle i| = I$.
    - $\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i |i\rangle\langle i|v\rangle = \sum_i v_i|i\rangle = |v\rangle$ .
- Representation of linear operator: a linear operator can be written in a basis $|v_i\rangle$ as $\sum_{i,j}|v_i\rangle A_{ij}\langle v_j|$ with $A_{ij} = \langle v_i|A|v_j\rangle$.
    - $A = IAI$, so $\sum_{i,j}|v_i\rangle A_{ij}\langle v_j| = \sum_i |v_i\rangle\langle v_i|\, A_{ij} \sum_j |v_j\rangle\langle v_j| = \sum_{i,j}|v_i\rangle\langle v_i|A|v_j\rangle\langle v_j|$.
- Dirac (bra-ket) notation
    - $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|$.
    - $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$.
    - $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$.

Eigenvectors and eigenvalues

- Eigenvectors $|v\rangle \neq 0$ and complex eigenvalues $v$ of a linear operator $A$ satisfy the relation $A|v\rangle = v|v\rangle$.
    - Applying the operator $A$ to an eigenvector returns the same eigenvector
- Eigenvalues $v$ are the roots $\lambda_i$ of the characteristic polynomial $c(\lambda) = \det|A - \lambda I|$.
- Eigenvectors $v_i$ of eigenvalue $v = \lambda_i$ are found by solving for $v_i$ in $A|v_i\rangle = \lambda_i|v_i\rangle$.
- An operator of dimension $n$ has $n$ eigenvectors and eigenvalues and some eigenvalues can be repeated
    - Fundamental theorem of algebra: a polynomial of degree $n$ has $n$ complex roots, some of which can have the same value.
- Eigenspace corresponding to the eigenvalue $v$ is the set of vectors $|v\rangle$ that have the same eigenvalue $v$
- Spectral decomposition: Operator $A$ can be expressed in terms of its eigenvalues and

eigenvetors $A = \sum \lambda_i |i\rangle\langle i|$.

- Matrix $A$ in the basis of the eigenvectors is $A_{ij} = \delta_{ij}\lambda_i$.
- If eigenspace is more than 1-dimensional, it is called degenerate with a degeneracy of the size of the subspace
- E.g. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in the basis $|0\rangle, |1\rangle$, $X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in eigenbases.

Adjoint

- Definition: Suppose $A$ is a linear operator on a Hilbert space $V$. There exists a unique linear operator $A^\dagger$ on $V$ such that for any $|v\rangle, |w\rangle$ in $V$, $|v\rangle^\dagger A|w\rangle = \left(A^\dagger|v\rangle\right)^\dagger |w\rangle$
  - Equivalently, $\left(|v\rangle, A|w\rangle\right) = \left(A^\dagger|v\rangle, |w\rangle\right)$.
  - $A^\dagger$ is the adjoint or Hermitian conjugate of $A$
  - $|v\rangle^\dagger = \langle v|$
  - $\left(A|v\rangle\right)^\dagger = \langle v|A^\dagger$
- $(AB)^\dagger = B^\dagger A^\dagger$
- $\left(|v\rangle\langle w|\right)^\dagger = |w\rangle\langle v|$.
- Adjoint is given by complex conjugate followed by a transpose ($A^\dagger = (A^*)^T$)

Hermitian

- An operator $A$ that is the same as its adjoint $A^\dagger$ (Hermitian conjugate) is called Hermitian
- Hermitian operators $M$ can be written as $M = \sum_i \lambda_i |i\rangle\langle i|$ in a well-defined basis.
  - $\lambda_i$ are real numbers.
  - $|i\rangle$ is the eigenvectors of $M$ with eigenvalue $\lambda_i$.
  - It is called the spectral decomposition of $M$.

Unitary

- An operator $U$ is Unitary if $UU^\dagger = U^\dagger U = I$.
- Inner products are invariant to transformation by the Unitary matrix $U$.
  - $(U|v\rangle)^\dagger (U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|w\rangle$.

# Quantum mechanics

2021年9月10日 20:35

State space

- State needs to be described in a way that allows for fundamental uncertainty present in quantum mechanical systems
- Postulate 1: associated to any physical system is a complex vector space with an inner product (Hilbert space) known as the state space of the system. The system state is specified by its state vector ($|\psi\rangle$), a unit vector in the system's state space
    - Do not assign definite values to properties like position, momenta, angular momenta
- The simplest quantum mechanical system is described by a state vector with dimension 2 ($|0\rangle, |1\rangle$).
    - They can represent any aspect of the system we wish and they span the vector space
        - A particle being at two positions
        - A particle having two energies
        - A particle having an intrinsic angular momentum $\pm\frac{\hbar}{2}$.
- State of two-level systems can be written as quantum superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ of the two states $|0\rangle, |1\rangle$ .
    - Equivalently, $|\psi\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$.
    - It is a special aspect of quantum mechanics
    - This axiom permits the system to simultaneously be in the state $|0\rangle$ and $|1\rangle$.
- The state is a unit vector $\||\psi\rangle\| = \sqrt{|\alpha|^2 + |\beta|^2} = 1$.
    - $\||\psi\rangle\| = \langle\psi|\psi\rangle^{\frac{1}{2}}$.

Unitary evolution

- Time evolution of a state $|\psi(t)\rangle$ is described by a unitary linear operator $U$. The state $|\psi(t_2)\rangle$ at time $t_2$ is related to the state $|\psi(t_1)\rangle$ by $U(t_2 - t_1)$.
    - $|\psi(t_2)\rangle = U(t_2 - t_1)|\psi(t_1)\rangle$.
    - If we know the initial state and the unitary matrix, we can predict the final state.
- The operations that manipulate information in quantum computers are all unitary operators
    - Pauli matrices $\sigma_X = X$(bit flip), $\sigma_Y = Y$ and $\sigma_Z = Z$ (phase flip), $I$ (identity).
        - Phase flip: changes the relative phase of $|0\rangle$ and $|1\rangle$ by 180.
    - Hadamard gate $H = 2^{-\frac{1}{2}}\begin{pmatrix}1 & 1 \\ 1 & -1\end{pmatrix}$.
        - $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
        - $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
        - Tells the relative phase
    - Phase gate $S = \begin{pmatrix}1 & 0 \\ 0 & i\end{pmatrix}$.
        - $Z = S^2$
        - Advances state of $|1\rangle$.
    - T gate $T = \begin{pmatrix}1 & 0 \\ 0 & e^{i\pi/4}\end{pmatrix}$.
        - $S = T^2$.
        - Any quantum algorithm that only works with the previous three gates can be efficiently implemented on classical computers
- Information encoded in quantum mechanical degrees of freedom is manipulated using unitary operators

Schrodinger equation

- Evolution of the state $|\psi(t)\rangle$ of an isolated quantum system obeys the Schrodinger equation

$i\hbar\frac{d|\psi(t)\rangle}{dt} = H(t)|\psi\rangle$

- $\hbar = 1.055 \times 10^{-34} Js$ is the reduced Planck's constant, $E = \hbar\omega$
- $H(t)$ is the Hamiltonian of the system, a Hermitian operator whose classical equivalent is the total energy of the system

- E.g. $H = \frac{\hbar\gamma B}{2}\sigma_Z, \left|\psi(t)\right\rangle = \begin{pmatrix} c_1(t) \\ c_2(t) \end{pmatrix}$ gives $c_p(t) = c_p(0)\exp\left(i(-1)^p \frac{\gamma B}{2} t\right)$.
- The dynamics of the state of a classical system specified by $x_i$ and $p_i$ can be solved using the classical Hamiltonian $H(t)$.
  - $\frac{dp_i}{dt} = -\frac{\partial H(t)}{\partial x_i}, \frac{dx_i}{dt} = \frac{\partial H(t)}{\partial p_i}$.
  - $H = \frac{p^2}{2m} + U(r)$, $p$ and $r$ do not commute.
    - $x_i p_j - p_j x_i = i\hbar\delta_{ij} I$ (Heisenberg Uncertainty principal).
- There exists a basis $|E\rangle$ where $H = \sum_E E|E\rangle\langle E|$.
  - $E$ are real-valued energies of the isolated system
  - The corresponding eigenvectors $|E\rangle$ are the energy eigen states
  - Time-dependence of an energy eigenstate $|E\rangle$ is $\left|E(t_2)\right\rangle = \exp\left(-\frac{iE(t_2-t_1)}{\hbar}\right)\left|E(t_1)\right\rangle$.
- If $\left|\psi(0)\right\rangle = \sum_E c_E|E\rangle$, then the time evolution of the state is $\left|\psi(t)\right\rangle = \sum_E c_E \exp(-\frac{iEt}{\hbar})\,|E\rangle$.
- More generally, $U\left(t_2 - t_1\right) = \exp\left(-\frac{iH(t_2-t_1)}{\hbar}\right) = \sum\exp\left(-\frac{i\lambda t}{\hbar}\right)\left(|\lambda\rangle\langle\lambda|\right)$.

Measurement postulate

- The action of measurement of a quantum state $|\psi\rangle$ is described by a collection $\{M_m\}$ of measurement operators
  - A measurement performed on a system in a state $|\psi\rangle$ will yield the result $m$ with probability $p(m) = \left\langle\psi\left|M_m^\dagger M_m\right|\psi\right\rangle$.
    - Inner product of $M_m|\psi\rangle$ with itself.
  - If the measurement outcome is $m$, then the state of the system after the measurement is $\left|\psi'\right\rangle = \frac{M_m|\psi\rangle}{\left\|M_m|\psi\rangle\right\|}$.
  - Measurement operators satisfy an operator completeness relation $\sum_m M_m^\dagger M_m = I$.
- Finding measurement operators
  - For two-level systems, every operators can be made from four basis operators $\sigma_0, \sigma_X, \sigma_Y, \sigma_Z$.
  - Projection onto Bloch sphere
  - Outer product of the basis
- $\sum_m p(m) = 1$ The sum of the probabilities of each possible measurement outcome $m$ is unity.
- For a state $\left|\psi\right\rangle = \alpha|0\rangle + \beta|1\rangle, p(0) = |\alpha|^2, p(1) = \left|\beta\right|^2$.

Distinguishing quantum states

- Case 1: the states are orthonormal $\left\langle\psi_i\middle|\psi_j\right\rangle = \delta_{ij}$.
  - Define measurement operators $M_i = |\psi_i\rangle\langle\psi_i|$, one for each sate $i$ and an additional measurement operator $M_0 = I - \sum_{i\neq 0}|\psi_i\rangle\langle\psi_i|$.
  - Then $p(j) = \left\langle\psi_i\middle|M_j\middle|\psi_i\right\rangle = \delta_{ij}$.
  - Note that $M_i^\dagger M_i = I$, for all $i$.
  - It is possible to distinguish orthonormal states $|\psi_i\rangle$.
- Case 2: the states are non-orthonormal
  - $\left|\psi_2\right\rangle = \alpha\left|\psi_1\right\rangle + \beta|\phi\rangle$ contains a non-zero component parallel to $\left|\psi_1\right\rangle$ and a component orthogonal to $\left|\psi_1\right\rangle$.
  - When applying the measurement operators, we get $p(1) = |\alpha|^2$, so the state $|\psi_1\rangle$ is detected sometimes.
  - The non-orthogonal states cannot be distinguished

Projective measurement (special case of measurement)

- The most common types of measurements in quantum physics

- Projector: suppose $V$ is a d-dimensional vector subspace spanned by an orthonormal basis $|i\rangle$ with $i = 1, \dots, d$, and $W$ is a k-dimensional subspace spanned by an orthonormal basis $|i\rangle$ with $i = 1, \dots, k$, where $k < d$. The projector onto the subspace W is $P = \sum_{i=1}^{k} |i\rangle\langle i|$.
    - $P$ takes a vector $V$ in and brings it into the subspace $W$.
    - $Q = I - P$ is a projector onto the space spanned by $|k+1\rangle \dots |d\rangle$.
- E.g. project from $|v\rangle = \sum_{i=1}^{5} a_i |v_i\rangle$ to $|w\rangle = \sum_{i=1}^{3} a_i |v_i\rangle$.
    - $P_{V \to W} = \sum_{i=1}^{3} |i\rangle\langle i| = |v_1\rangle\langle v_1| + |v_2\rangle\langle v_2| + |v_3\rangle\langle v_3|$ .
- A projective measurement is described by an observable $M$, a Hermitian operator. The observable $M$ has a spectral decomposition $M = \sum_m m P_m$ where $P_m$ is the projector onto the eigenstates of $M$ with eigenvalue $m$
    - $p(m) = \langle\psi|P_m|\psi\rangle$.
    - Given $m$ occured, the state of the quantum system immediately after the measurement is $\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$.
    - The possible outcomes $m$ are the eigen values of the observable $M = \sum_m \sum_{i=1}^{n_m} m|m_i\rangle\langle m_i|$.
        - Recall that $P_m = \sum_{i=1}^{n_m} |m_i\rangle\langle m_i|$ where $|m_i\rangle$ are the eigenvectors with the same eigenvalue $m$.
- Measurement is fundamentally probabilistic
- The only thing that evolves with certainty is the state
- Measurement changes the state of the system in general.
- If an eigenvalue is repeated, we can have the state after measurement as superposition of the eigenstates

Measurement statistics and examples

- Average value of projective measurement: $E(M) = \sum_m m p(m) = \langle\psi|M|\psi\rangle = \langle M\rangle$.
- Standard deviation: $\sqrt{\langle \delta M^2\rangle} = \sqrt{\langle (M - \langle M\rangle)^2\rangle} = \sqrt{\langle M^2\rangle - \langle M\rangle^2}$, $\langle \delta M^2\rangle = \langle\psi|(M - \langle M\rangle)^2|\psi\rangle$.
    - If $|\psi\rangle$ is an eigenvector of $M$, then $\langle \delta M^2\rangle = 0$ for $|\psi\rangle$.
- Observable $\sigma_X = |\psi_+\rangle\langle\psi_+| - |\psi_-\rangle\langle\psi_-|$ where $|\psi_\pm\rangle = 2^{-\frac{1}{2}}(|0\rangle \pm |1\rangle)$.
    - Projectors $P_{+1} = |\psi_+\rangle\langle\psi_+|$.
- Operator $v \cdot \sigma = v_x\sigma_x + v_y\sigma_y + v_z\sigma_z$.

# Quantum information

2021年9月10日 20:35

Quantum bits

- Bit is the fundamental concept in classical information
- Quantum bit/qubit: analogous in quantum information
- Qubit state can be in a linear superposition of $|0\rangle$ and $|1\rangle$, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ .
- Since $|\alpha|^2 + |\beta|^2 = 1$, $|\psi\rangle = e^{i\gamma}\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right)$ for real $\theta, \phi, \gamma$.
    - Phase pre-factor $e^{i\gamma}$: does not influence the measurement statistics.
    - $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$. (if consider only one qubit)
- Bloch sphere
    - Geometric representation of the state $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$ to spherical coordinates.
        - North pole $|0\rangle$: $\theta = 0$.
        - South pole $|1\rangle$: $\theta = \pi$.
        - $2^{-\frac{1}{2}}(|0\rangle + |1\rangle)$: $\theta = \frac{\pi}{2}, \phi = 0$. (positive $x$ axis)
        - $2^{-\frac{1}{2}}(|0\rangle + i|1\rangle)$: $\theta = \frac{\pi}{2}, \phi = \frac{\pi}{2}$. (positive $y$ axis)
    - It transforms the concept of quantum superposition into a point on spherical coordinates
- Information encoded
    - Information can only be obtained by measurement
    - From one measurement, we obtain one bit of information
    - If we do not measure the qubit
        - The state of the qubit contains a considerable amount of information
        - Amount of information and the rate of growth are high

State of two quantum bits

- $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.
- Equivalently $|\psi\rangle = \sum_{i,j\in\{0,1\}} \alpha_{ij}|ij\rangle$.
- We form the state of multiple qubits by concatenating the vector spaces of individual qubits together to form larger vector spaces

Tensor product $\otimes$

- If $V$ and $W$ are vector spaces of $m$ and $n$ respectively, then $V \otimes W$ is an $mn$ dimensional vector space
- The elements of $V \otimes W$ are tensor products of the elements $|v\rangle$ and $|w\rangle$ of spaces $V$ and $W$ respectively
- If $|i\rangle$ and $|j\rangle$ are orthonormal bases for $V$ and $W$, then $|i\rangle \otimes |j\rangle$ is a basis for $V \otimes W$
- $|v\rangle \otimes |w\rangle = |v\rangle|w\rangle = |vw\rangle$.
- Properties
    - $z \in \mathbb{C}, |w\rangle \in W, |v\rangle \in V, z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$.
    - $|v_1\rangle, |v_2\rangle \in V, |w\rangle \in W, (|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$.
    - $|v\rangle \in V, |w_1\rangle, |w_2\rangle \in W, |v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$.
- If $A$ operates on $V$ and $B$ operates on $W$, then the tensor product allows for $A \otimes B$ operates on $V \otimes W$.
    - $(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$.
    - $(A \otimes B)\left(\sum_{i,j} a_{ij}|v_i\rangle \otimes |w_j\rangle\right) = \sum_{i,j} a_{ij}A|v_i\rangle \otimes B|w_j\rangle$. (linearity)
- Inner product on $V \otimes W$: $\left(\sum_{i,j} a_{ij}|v_i\rangle \otimes |w_j\rangle\right)^\dagger \left(\sum_{i,j} b_{ij}|v_i'\rangle \otimes |w_j'\rangle\right) = \sum_{i,j} a_i^* b_j \langle v_i|v_j{}'\rangle\langle w_i|w_j{}'\rangle$ .
- Operators property
    - $(A \otimes B)^* = (A^* \otimes B^*)$.
    - $(A \otimes B)^T = (A^T \otimes B^T)$.
    - $(A \otimes B)^\dagger = (A^\dagger \otimes B^\dagger)$.

Quantum registers

- Described by states in a vector space that is the tensor product of the vector spaces of many individual qubits
- Linear operators on the space are defined as operators that are the tensor product of operators on the individual

qubits

- Inner product is defined on the tensor product space so it is also a Hilbert space

Matrix representation of tensor product

- Let $|a\rangle = \sum_i a_i |v_i\rangle \in V$ with dimension $m$, $|b\rangle = \sum_j b_j |w_j\rangle \in W$ with dimension $p$. Then $|a\rangle \otimes |b\rangle = \begin{pmatrix} a_1 b \\ a_2 b \\ \dots \\ a_m b \end{pmatrix}$ with dimenstion $mn$.
- Let $A: V \to V'$ with representation $A_{ij}$ and dimensions $m \times n$, $B: W \to W'$ with $B_{ij}$ and dimensions $p \times q$. Then the tensor product: $A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \dots & \dots & \dots & \dots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{pmatrix}$.
- $|\psi\rangle^{\otimes k}$ denotes the state $|\psi\rangle$ tensor with itself $k$ times.
    - E.g. $|\psi\rangle = 2^{-1/2}(|0\rangle + |1\rangle)$, $|\psi\rangle^{\otimes 2} = \begin{pmatrix} 2^{-\frac{1}{2}} \begin{pmatrix} 2^{-\frac{1}{2}} \\ 2^{-\frac{1}{2}} \end{pmatrix} \\ 2^{-\frac{1}{2}} \begin{pmatrix} 2^{-\frac{1}{2}} \\ 2^{-\frac{1}{2}} \end{pmatrix} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.
- Apply the Hadamard operator to each bit in an $n$ qubit register, denoted as $H^{\otimes n}$.
    - $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \sum_{x_j=0}^{1} \sum_{y_j=0}^{1} (-1)^{x_j y_j} |x_j\rangle\langle y_j|$.
    - $H^{\otimes n} = 2^{-n/2} \sum_{x,y} (-1)^{x \cdot y} |x\rangle\langle y|$ where $x \cdot y = \sum_{i=1}^{n} x_i y_i$, $|x\rangle = |x_1 x_2 \dots x_n\rangle$, $|y\rangle = |y_1 y_2 \dots y_n\rangle$.

Commutators

- The commutator of two operators $A$ and $B$ is defined to be $[A, B] = AB - BA$
    - If $[A, B] = 0$, we say $A$ commutes with $B$
- The anti-commutator of two operators $A$ and $B$ is defined to be $\{A, B\} = [A, B]_{+} = AB + BA$
    - If $\{A, B\} = 0$, we say $A$ anti-commutes with $B$
- Simultaneous eigenvectors
    - Suppose $A$ and $B$ are Hermitian operators. Then $[A, B] = 0$ if and only if there exists an orthonormal basis such that both $A$ and $B$ are diagonal with respect to that basis. We say that $A$ and $B$ are simultaneously diagonalizable
    - Then there is a basis of eigenvectors $|i\rangle$ such that $A = \sum_i a_i |i\rangle\langle i|$ and $B = \sum_i b_i |i\rangle\langle i|$.
- $[X, Y] = 2iZ$, $[Y, Z] = 2iX$, $[Z, X] = 2iY$.
    - When we have multiple different qubits $[X_i, Y_j] = 2iZ\delta_{ij}$ (if they are applying on different qubits, they commute).

Uncertainty relations

- Suppose $A$ and $B$ are two Hermitian operators with corresponding physical observables and $|\psi\rangle$ is a quantum state, then $\langle \delta A^2 \rangle \langle \delta B^2 \rangle \geq \left| \frac{1}{2i} \langle \psi | [A, B] | \psi \rangle \right|^2$.
- Uncertainty principal for $\delta A = \sqrt{\langle \delta A^2 \rangle}$, $\delta B = \sqrt{\langle \delta B^2 \rangle}$, $\delta A \delta B \geq \left| \frac{1}{2i} \langle \psi | [A, B] | \psi \rangle \right|$.
- If we prepare many quantum systems in identical states, then performing measurements of an observable $A$ on some states and of $B$ on the other states, the statistics of $\delta A \delta B$ will satisfy the inequality
- If $[A, B] = 0$, and it is possible that measurements of $A$ and $B$ can be obtained on the same state, we call $A$ and $B$ compatible or simultaneous observables.
    - Same state means they should have the same eigenstates (same eigenvalues and eigenvectors)
    - Usually, Heisenberg uncertainty works for the sequence: prepare-measure-prepare-..., but for compatible observables, we can do prepare-measure-measure-....
- If $|\psi\rangle = |0\rangle$ then $\langle \delta Z^2 \rangle = 0$.

Entanglement

- Entanglement is a property of quantum states that is connected to what gives quantum computers enhanced computational power
- If a state cannot be written as a tensor product of states, then it is entangled.
    - An $n$ particle state is unentangled if it can be written as a tensor product of states $|\psi\rangle = |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$.
- Bell states

- $|\Psi_+\rangle = 2^{-\frac{1}{2}}(|01\rangle + |10\rangle), |\Psi_-\rangle = 2^{-\frac{1}{2}}(|01\rangle - |10\rangle)$.
  - $|\Phi_+\rangle = 2^{-\frac{1}{2}}(|00\rangle + |11\rangle), |\Phi_-\rangle = 2^{-\frac{1}{2}}(|00\rangle - |11\rangle)$.
  - None of these states can be written as a single tensor product
  - All of the states are entangled.
- If a state $|\psi\rangle = 2^{-\frac{1}{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$ is prepared, $A$ measures $\pm 1$, then $B$ measures $\mp 1$.

Bell inequalities

- Provide a means to distinguish a quantum mechanical version of reality from any version of reality where there is no fundamental uncertainty, only hidden variables
- Classical: $E(QS) + E(RS) + E(RT) - E(QT) \leq 2$.
  - With $Q = \pm 1, R = \pm 1, S = \pm 1, T = \pm 1$.
- Quantum: $\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2}$
  - Quantum state: $|\psi\rangle = 2^{-\frac{1}{2}}(|01\rangle - |10\rangle)$.
  - Measurements: $Q = Z_1, R = X_1, S = 2^{-\frac{1}{2}}(-Z_2 - X_2), T = 2^{-\frac{1}{2}}(Z_2 - X_2)$ .
    - Note that $Q$ and $R$ are orthogonal (along x and z axis), $T$ and $S$ are orthogonal (but along 135 and -135 degree lines).
    - If we change the relative angle of the axis $QR$ and $ST$, the output is different. This set provides the largest violation (largest sum of expected values)
    - We can also have a probabilistic state preparation
  - If properties $P_Q, P_R, P_S, P_T$ have definite values $Q, R, S, T$ independent of observation, then our theory has realism.
  - If A performing measurement does not influence the result of B's measurement, our theory has locality
- Nature is neither local or real

# Quantum circuits

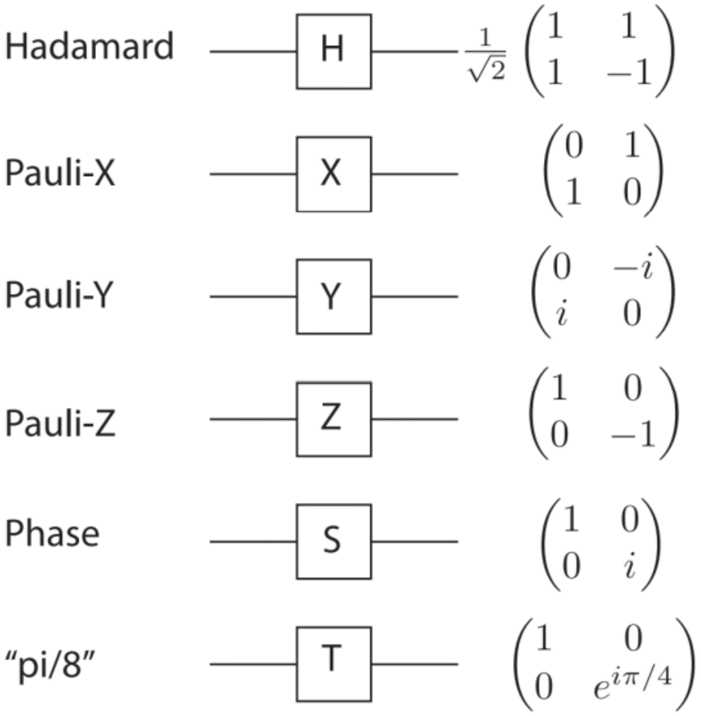
2021年9月10日 20:35

Reversible single classical bit operations

- Identity: $x \rightarrow x$.
- NOT (inverter): $x \rightarrow \bar{x}$.

Single qubit operations:

- Operation must preserve the norm of the vector (unitary matrix)
- Pauli matrices (rotation by $\pi$)
  - Rotation around $X$: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
  - Rotation around $Y$: $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$.
  - Rotation around $Z$: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
- Hadamard: $H = 2^{-\frac{1}{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.
- Phase: $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
  - $S^{\dagger} = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$.
- T-gate ($\frac{\pi}{8}$ gate): $T = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{i\pi}{4}\right) \end{pmatrix} = e^{\frac{i\pi}{8}} \begin{pmatrix} e^{-\frac{i\pi}{8}} & 0 \\ 0 & e^{\frac{i\pi}{8}} \end{pmatrix}$
- $H = 2^{-\frac{1}{2}}(X + Z)$.
- $S = T^2$.


Hadamard
H
$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli-X
X
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-Y
Y
$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z
Z
$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Phase
S
$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
"pi/8"
T
$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Rotation matrices

- $\exp(iAx) = \cos x \, I + i \sin x \, A$, $A^2 = I$.
- $R_X(\theta) = \exp\left(-\frac{i\theta X}{2}\right) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) X$.
- $R_Y(\theta) = \exp\left(-\frac{i\theta Y}{2}\right) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Y$.
- $R_Z(\theta) = \exp\left(-\frac{i\theta Z}{2}\right) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Z$.

- Rotation operator: $R_{\hat{n}}(\theta) = \exp\left(-i\,\theta\,\frac{\hat{n}\cdot\vec{\sigma}}{2}\right)$.
    - Rotates a qubit state represented by a vector $\vec{\lambda}$ on the Bloch sphere by an angle $\theta$ about the axis $\hat{n}$.
- Arbitrary rotation:
    - Suppose $U$ is a unitary operation on a single qubit. Then there exist real numbers $\alpha, \beta, \gamma, \delta$ such that $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.
    - Any single qubit gate can be written as $U = e^{i\alpha} R_n(\beta) R_m(\gamma) R_n(\delta)$ where $m$ and $n$ are non-parallel unit vectors
    - We only need to be able to rotate a qubit along two non-parallel axes to be able to implement any single qubit gate
- Suppose $U$ is a unitary gate on a single qubit. Then there exist unitary operators $A, B, C$ on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$
    - $A = R_z(\beta) R_y\left(\frac{\gamma}{2}\right)$, $B = R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta+\beta}{2}\right)$, $C = R_z\left(\frac{\delta-\beta}{2}\right)$.
    - Note $XYX = -Y$, $X, Y$ are Pauli $X, Y$ matrices.
    - $XR_y(\theta)X = R_y(-\theta)$.
    - $HXH = Z$.
    - $HYH = -Y$.
    - $HZH = X$.

Multi-bit classical gates

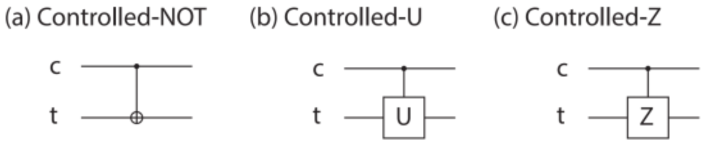
- AND
- OR
- XOR
- NAND
- NOR

Multi-qubit gates

- When the gate has two or more inputs, they are called multi-qubit gates
- CNOT: controlled-NOT gate
    - Inputs:
        - Control qubit: $|c\rangle$.
        - Target qubit: $|t\rangle$.
    - If control bit is 0, target bit is unchanged
    - If control bit is 1, apply $X$ gate to the target qubit
    - $|c\rangle|t\rangle \to |c\rangle|t \oplus c\rangle$.
        - i.e. It is similar to an XOR gate
    - $CNOT(2,1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$.
        - Qubit 2 is the control qubit and qubit 1 is the target qubit
        - In Dirac notation (with basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$), $CNOT(2,1) = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$.
- Controlled $U$ gate:
    - Inputs:
        - 1 control qubit
        - $n$ target qubits.
    - If the control bit is 0, the target qubits are unchanged
    - If the control bit is 1, the unitary $U$ is applied to the target qubit
    - $|c\rangle|t\rangle \to |c\rangle U^c|t\rangle$.
- CZ gate: controlled-Z gate
    - If the control bit is 0, the target qubit is unchanged
    - If the control bit is 1, we apply a $Z$ gate to the target qubit
    - $CZ(2,1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & Z \end{pmatrix}$.
        - Qubit 2 is the control qubit and qubit 1 is the target qubit
        - In Dirac notation (with basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$), $CZ(2,1) = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$.

- Swap gate: $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
    - $|10\rangle \rightarrow |01\rangle, |01\rangle \rightarrow |10\rangle$.

Quantum circuit diagrams

- The horizontal axis refers to time
- 

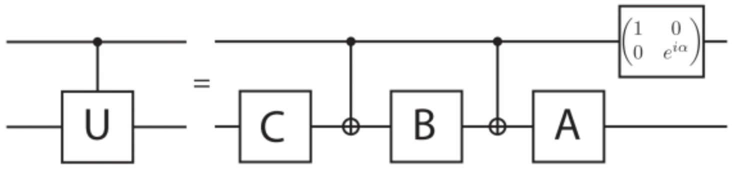
Controlled-X can be implemented by $H^{(1)}CNOT(2,1)H^{(1)}$ since $X = HZH$

- $H^{(1)}$ means hadamard applied on qubit 1.

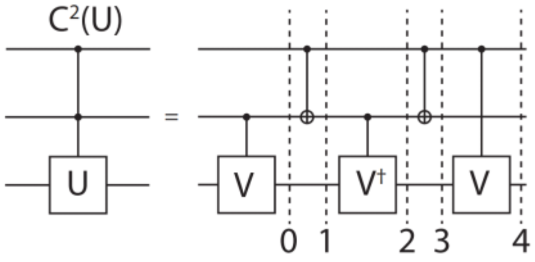
Identities

- Let $C = CNOT(1,2)$
- $CX_1C = X_1X_2$
- $CY_1C = Y_1Y_2$
- $CZ_1C = Z_1$
- $CX_2C = X_2$
- $CY_2C = Z_1Y_2$
- $CZ_2C = Z_1Z_2$
- $R_{z,1}(\theta)C = CR_{z,1}(\theta)$
- $R_{x,2}(\theta)C = CR_{x,2}(\theta)$

Controlled-Unitary implementation

- Step 1: controlled application of $AXBXC$ to the target qubit
    - Achieved by $A^{(1)}CNOT(2,1)B^{(1)}CNOT(2,1)C^{(1)}$.
- Step 2: controlled application of $I \exp(i\alpha)$ to the target qubit
    - Can be achieved by applying $\begin{pmatrix} 1 & 0 \\ 0 & \exp(i\alpha) \end{pmatrix}$ to the control qubit.
    - Note: when control bit is 0, we are not adding phase to the target; when control bit is 1, we add a phase to the target. That's why we apply the gate to the control qubit
- 

Conditioning on multiple qubits

- Define operation $C^n(U)$ that performs a controlled $U$ operation if all n control qubits are 1 in the following way: $C^n(U)|x_1x_2 \dots x_n\rangle|\psi\rangle = |x_1x_2 \dots x_n\rangle U^{x_1x_2 \dots x_n}|\psi\rangle$.
    - Where $x_1x_2 \dots x_n$ in the exponent of $U$ is the product of the bits $x_1, x_2, \dots, x_n$.
- 

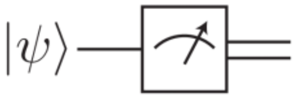
    - From top to bottom $c_2, c_1, t$
    - $V^\dagger V = I, U = V^2$.

| $i$ ($\|c_1c_2\rangle\|\psi\rangle$) | 0 (apply V if $c_1 = 1$) | 1 (flip $c_1$ if $c_2 = 1$) | 2 (apply $V^\dagger$ if $c_1 = 1$) | 3 (flip $c_1$ if $c_2 = 1$) | 4 (apply $V$ if $c_2 = 1$) |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| $\|00\rangle\|\psi\rangle$ | $\|00\rangle\|\psi\rangle$ | $\|00\rangle\|\psi\rangle$ | $\|00\rangle\|\psi\rangle$ | $\|00\rangle\|\psi\rangle$ | $\|00\rangle\|\psi\rangle$ |
| $\|01\rangle\|\psi\rangle$ | $\|01\rangle V\|\psi\rangle$ | $\|01\rangle V\|\psi\rangle$ | $\|01\rangle V^\dagger V\|\psi\rangle$ | $\|01\rangle\|\psi\rangle$ | $\|01\rangle\|\psi\rangle$ |
| $\|10\rangle\|\psi\rangle$ | $\|10\rangle\|\psi\rangle$ | $\|11\rangle\|\psi\rangle$ | $\|11\rangle V^\dagger\|\psi\rangle$ | $\|10\rangle V^\dagger\|\psi\rangle$ | $\|10\rangle\|\psi\rangle$ |
| $\|11\rangle\|\psi\rangle$ | $\|11\rangle V\|\psi\rangle$ | $\|10\rangle V\|\psi\rangle$ | $\|10\rangle V\|\psi\rangle$ | $\|11\rangle V\|\psi\rangle$ | $\|11\rangle V^2\|\psi\rangle$ |

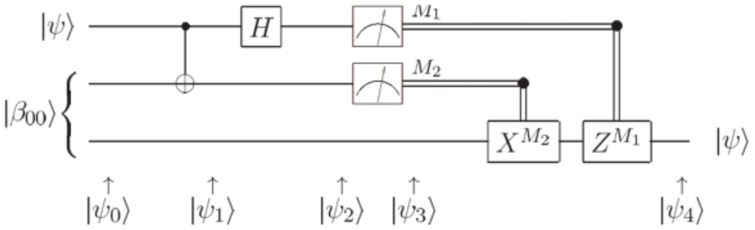
- E.g. Toffoli gate ($C^2(X)$).
  - It is a controlled NOT with 2 inputs
  - $V = (1-i)(I+iX)/2, V^2 = X.$
- Logic can be conditioned from multiple qubits
  - To define new basic gates that might hep in compilation of a quantum algorithm into gates

Measurement

- The circuit symbol for measurement in the computational basis $|0\rangle$ and $|1\rangle$ is a meter
  - 

- Measurement is irreversible because information contained in the measured bit is lost. The output of measurement is always classical
- Single/multi qubit operations are unitary operations that are reversible
- Principle of deferred measurement
  - Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit.
  - If the measurement results are used at any stage of the circuit, then classically controlled operations can be replaced by conditional quantum operations
  - Important: often measurements are made at an intermediate stage
  - State changes, but the possible outcomes don't
- Principle of implicit measurement
  - Any qubits that remain unmeasured at the end of an algorithm can be considered to be measured
  - If a measurement is performed on qubit 2, this does not influence the un-conditioned statistics of the measurement of qubit 1
- In certain situations, measurement of a qubit need not throw information away information in the other qubits
  - Quantum teleportation
  - Quantum error correction

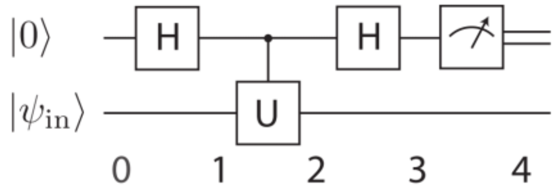
Quantum teleportation

- The procedure that allows quantum information to be moved from A to B, even when a quantum channel for transmitting information is absent
  - A and B share a Bell State: $|\beta_{00}\rangle = 2^{\frac{1}{2}}(|00\rangle + |11\rangle)$
  - A has an unknown qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
  - A can only send classical information to B
- The shared Bell state is what allows B to obtain $|\psi\rangle$ through only transmission of a small amount of classical information
  - 

    - $|\psi_0\rangle = |\psi\rangle \otimes |\beta_{00}\rangle = 2^{-\frac{1}{2}}\big(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\big)$
    - $|\psi_3\rangle = 2^{-\frac{1}{2}}\big(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)\big) + 2^{-\frac{1}{2}}\big(|10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\big).$
      - □ If measurement outcome is $|00\rangle$, $M_{00} = |00\rangle\langle 00|$, we directly get $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
      - □ If measurement outcome is $|01\rangle$, $M_{01} = |01\rangle\langle 01|$, we apply $X$ (flip the bit) to get $|\psi\rangle$.
      - □ If measurement outcome is $|10\rangle$, $M_{10} = |10\rangle\langle 10|$, we apply $Z$ (flip the phase) to get $|\psi\rangle$.
      - □ If measurement outcome is $|11\rangle$, $M_{11} = |11\rangle\langle 11|$, we apply both $X$ and $Z$ to get $|\psi\rangle$.

    - Interacting the qubit with A's half of the Bell state
    - Applying a Hadamard on the qubit
    - Measuring A's qubits in the computational basis
    - Sending that results to B
    - Conditional operations on B's half of the EPR state
- Observations
    - Without classical information transmission, no information is transmitted
    - No clone of the state has been created. The state $|\psi\rangle$ disappeared from A side when A measured the state
    - Quantum teleportation is intimately related to the properties of quantum error correction codes

Measuring a Hermitian Unitary

- Suppose we have a single qubit operator $U$ with eigenvalues $\pm 1$ so that $U$ is both Hermitian (observable) and unitary (a quantum gate)
- The circuit $H^{(2)} cU(2,1) H^{(2)}$ applied to $|0\rangle_2 |\psi\rangle_1$ followed by measurement of qubit 2 in the computational basis implements measurement of the observable $U$ on the state $|\psi\rangle$.
    - 

    - $|0\rangle$ is the ancilla qubit.
    - $U$ allows qubit 1 and 2 to be entangled, then we can measure qubit 2 to get info about qubit 1.
    - $H^{(2)} cU(2,1) H^{(2)} = 2^{-\frac{1}{2}} H^{(2)} cU(2,1)\big(|0\rangle + |1\rangle\big)|\psi\rangle = 2^{-\frac{1}{2}} H^{(2)}\big(|0\rangle|\psi\rangle + |1\rangle U|\psi\rangle\big) = \frac{1}{2}\Big(|0\rangle\big(|\psi\rangle + U|\psi\rangle\big) + |1\rangle\big(|\psi\rangle - U|\psi\rangle\big)\Big)$.
    - Calculate probability of outcomes $+1$ and $-1$ for observable $U = P_+ - P_-$ on qubit 2.
    - Calculate probability of outcomes 0 and 1 for qubit 1.

Universal quantum gates

- Classical: A set of gates is called universal for classical computation if we can implement an arbitrary logic operation exactly using that set
    - NAND is universal: it can be used to obtain AND, XOR, and NOT
- Quantum: a set of gates is called universal for quantum computation if we can implement an unitary operation to arbitrary accuracy using that set
    - Hadamard, Phase, CNOT and T is such a set

Approximating a unitary operator

- Using a discrete set of gates, we can only approximate the continuous space of possible unitary operators
- Error when a unitary operator $U$ is approximated by a different unitary operator $V$ as $E(U,V) = \max\big\|(U-V)|\psi\rangle\big\|$.
    - Maximum is over all normalized quantum states in the state space (worst case error)
    - When the error is small, any measurement performed on the state $V|\psi\rangle$ gives approximately the same measurement statistics as $U|\psi\rangle$
- Solovay-Kitaev Theorem (efficiency): Convergence to the desired gate can be guaranteed rather quickly. An arbitrary single-qubit gate can be approximated to an accuracy of order $\epsilon$ using of order $\log^{c} \epsilon^{-1}$ gates from the universal set with $c \approx 2$.
    - The overhead of increasing accuracy is low.
- A circuit with $m$ CNOTs and single qubit unitary can be approximated to accuracy $\epsilon$ with $\sim m \log^{c}(m/\epsilon)$ gates

# Quantum computation

2021年9月10日 20:35

Computational process in the gate model

- Start with a set of quantum states. Define:
    - An input state $x$ in an $n$-qubit register $|x\rangle_n$.
    - An output state $f(x)$ in an $m$-qubit register $|y\rangle_m$.
    - This gives $n+m$ qubits ignoring intermediate steps (ancilla)
- Computation is performed by performing a reversible transformation $U_f$ on the combination of the input and output states
    - $U_f\left(|x\rangle_n|y\rangle_m\right) = |x\rangle_n|y \oplus f(x)\rangle_m$.
    - $\oplus$ is the exclusive-OR that is obtained using the CNOT gate.
    - If output is initialized to $|0\rangle_m$, then $U_f\left(|x\rangle_n|0\rangle_m\right) = |x\rangle_n|f(x)\rangle_m$.
        - The answer is contained in the output register
- Can initialize all input qubits to $|0\rangle$, and apply a Hadamard gate to each of the output qubits.
    - $H^{\otimes n} = H \otimes H \otimes \cdots \otimes H$.
    - This produces an input state that is a super position over all of the possible input states
    - $H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n$.
        - e.g. $n=3, x=000, x=001, \ldots, x=111$
    - Then the input state to the computational process is: $\left(H^{\otimes n} \otimes I_m\right)\left(|0\rangle_n \otimes |0\rangle_m\right)$.
- Apply $U_f$ once to the superposition, we get $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n|f(x)\rangle_m$.
    - Result of the computation is described by a state whose structure cannot be explicitly specified without knowing the result of all $2^n$ evaluations of the function $f$.
    - This is quantum parallelism

Quantum parallelism

- $U_f\left(\left(H^{\otimes n} \otimes I_m\right)\left(|0\rangle_n \otimes |0\rangle_m\right)\right) = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n|f(x)\rangle_m$
- Describing the final state requires an exponentially growing number of function evaluations as the number of bits in the input register grows linearly
- However, the result of calculation might not be $2^n$ evaluations of $f$.
- The outcome of a projective measurement of the registers in the computational basis will be
    - Input: a random value of $x$ equally distributed between 0 and $2^n - 1$.
    - Output: the function $f(x)$ for the value $x$ in the input register
- The random selection of $x$, for which $f(x)$ can be learned is made after the calculation is carried out
- However, cannot get values of $f(x)$ for several different random $x$ due to no-cloning
- To exploit quantum parallelism
    - Apply additional unitary gates to one or both of the input and output registers before and/or applying $U_f$.
    - We can learn the relationships between different values of $f(x)$ for several different values of $x$ all at once, but not the values for any particular value of $x$ due to uncertainty principle

No cloning theorem

- Copying a quantum state is prohibited in quantum mechanics
- Assume we have an operator $U$ that clones quantum states $|\psi\rangle$ and $|\phi\rangle$ by transforming the output state to the input state, leaving the input state unaffected
    - $U\left(|\psi\rangle|0\rangle\right) = |\psi\rangle|\psi\rangle$ (cloning $|\psi\rangle$ to output register)
    - $U\left(|\phi\rangle|0\rangle\right) = |\phi\rangle|\phi\rangle$ (cloning $|\phi\rangle$ to output register)
- Then $U\left(a|\psi\rangle + b|\phi\rangle\right)|0\rangle = \left(a|\psi\rangle + b|\phi\rangle\right) \otimes \left(a|\psi\rangle + b|\phi\rangle\right) = a^2|\psi\rangle|\psi\rangle + b^2|\phi\rangle|\phi\rangle + ab|\psi\rangle|\phi\rangle + ab|\phi\rangle|\psi\rangle$.

    - By linearity, $U\left(a|\psi\rangle + b|\phi\rangle\right)|0\rangle = aU\left(|\psi\rangle|0\rangle\right) + bU\left(|\phi\rangle|0\rangle\right) = a|\psi\rangle|\psi\rangle + b|\phi\rangle|\phi\rangle$
    - They are equal if one of $a$ or $b$ is zero or if $|\psi\rangle = |\phi\rangle$.
- A given cloning procedure will only be effective at cloning a single state $|\psi_0\rangle$, not a general state
    - A unitary transformation can approximately clone two states only if they are nearly the same ($\langle\psi|\phi\rangle \approx 1$)

Deutsch's problem

- How a trade-off can be made that sacrifices particular information about a function $f(x)$ for relational information
- Let both input and output registers contain only a single qubit and $U_f\left(|x\rangle|y\rangle\right) = |x\rangle|y \oplus f(x)\rangle$ .
    - $f_0(0) = 0, f_0(1) = 0.$
    - $f_1(0) = 0, f_1(1) = 1.$
    - $f_2(0) = 1, f_2(1) = 0.$
    - $f_3(0) = 1, f_3(1) = 1.$
- Problem: Suppose we are given a black box that executes the function $U_f$ for one of the four functions $f_i(x)$, but are not told which value of $i$. Objective is to learn if $f$ is constant ($f(0) = f(1)$)
    - It shows how a quantum computer can do this in one run of the unitary $U_f$.
    - However, we will learn nothing about the individual values of $f(0)$ and $f(1)$.
- Function evaluation quantum circuit
    - For the following, assume qubit numbering $|x\rangle_1|y\rangle_2$.
    - For $f_0(x) = 0$, $|0 \oplus f\rangle = |f\rangle$, $|1 \oplus f\rangle = |\tilde{f}\rangle$ ($\tilde{f} = \text{not f}$), $U_{f0} = I$.
    - For $f_1(x) = x$, $U_{f1} = CNOT(1,2)$.
    - $U_{f2} = X(2)CNOT(1,2)$.
    - $U_{f3} = X(2)$.
- Overall circuit
    - To learn if $f$ is constant ($f(0) = f(1)$) using a Unitary such that $U_f\left(|x\rangle|y\rangle\right) = |x\rangle|y \oplus f(x)\rangle$.
    - $U_f(H \otimes I)\left(|0\rangle|0\rangle\right) = 2^{-\frac{1}{2}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\right)$.
        - The outcome will be randomly 1 or 0 in the input bit and $f(1)$ or $f(0)$ in the output bit
        - Need to run this at least twice to determine if $f(0) = f(1)$.
    - Inverting both the input and output and applying Hadamard gave more useful result
        - $(H \otimes H)\left(|1\rangle|1\rangle\right) = \frac{1}{2}\left(|0\rangle|0\rangle - |1\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|1\rangle\right)$.
    - Applying $U_f$, we get $|\psi\rangle = \frac{1}{2}\left(|0\rangle|f(0)\rangle - |1\rangle|f(1)\rangle - |0\rangle|\tilde{f}(0)\rangle + |1\rangle|\tilde{f}(1)\rangle\right)$ .
    - If $f(0) = f(1)$, then $|\psi\rangle = \frac{1}{2}(|0\rangle - |1\rangle)\left(|f(0)\rangle - |\tilde{f}(0)\rangle\right)$, Hadamard gives $|1\rangle$.
    - If $\tilde{f}(0) = f(1)$, then $|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle)\left(|f(0)\rangle - |\tilde{f}(0)\rangle\right)$, Hadamard gives $|0\rangle$.
    - Append $H \otimes 1$ to the end.
        - If $f(0) = f(1)$, we get $|1\rangle 2^{-1/2}\left(|f(0)\rangle - |\tilde{f}(0)\rangle\right)$.
        - If $f(0) \neq f(1)$, we get $|0\rangle 2^{-1/2}\left(|f(0)\rangle - |\tilde{f}(0)\rangle\right)$.

# Quantum Fourier transform

2021年9月10日 20:35

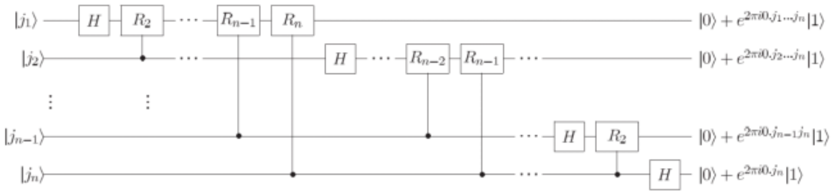
Discrete Fourier transform

- Converts a function in a spatial or temporal coordinates to frequency or spatial frequency coordinates
- $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi ijk}{N}}$.

Quantum Fourier Transform

- An operator $U_{FT}$ that acts on a particular basis state $|j\rangle$ in a basis $|k\rangle = |0\rangle \dots |N-1\rangle$ yielding a state summed over all states in the basis with certain complex amplitudes
  - $|k\rangle = |0\rangle, |1\rangle, |2\rangle, |3\rangle = |00\rangle, |01\rangle, |10\rangle, |11\rangle$.
  - $U_{FT}|j\rangle = N^{-1/2} \sum_{k=0}^{N-1} e^{\frac{2\pi ijk}{N}} |k\rangle$.
  - Equivalently, $U_{FT} \sum_{j=0}^{N-1} x_j |j\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$ where $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi ijk}{N}}$ is the discrete Fourier transform.
    - This is an extension to vectors
- Bit strings: we are working in the computational basis $|k\rangle$ of a quantum computer with $N$ qubits so the quantities $k$ and $j$ are integers that can be represented as strings of bits $k_0, \dots k_{N-1}$ and $j_0, \dots, j_{N-1}$
  - $k = \sum_{i=0}^{N-1} k_i 2^i$.
  - $j = \sum_{i=0}^{N-1} j_i 2^i$.
- QFT applied to the basis $|0 \dots 0\rangle$ state produces the same as the $H^{\otimes n}$ on $|0 \dots 0\rangle$.
  - $U_{FT}|0 \dots 0\rangle = N^{-\frac{1}{2}} \sum_{k=0}^{N-1} |k\rangle$.
  - This is only true for the $|0 \dots 0\rangle$ state and not general input states $|j\rangle$.
- Tensor product representation ($N = 2^n$)
  - $U_{FT}\left|j\right\rangle = 2^{-n/2} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \otimes_{l=1}^{n} \exp\left(2\pi ijk_l 2^{-l}\right) \left|k_l\right\rangle = 2^{-\frac{n}{2}} \otimes_{l=1}^{n} \left(|0\rangle + e^{2\pi ij2^{-l}}|1\rangle\right)$.
    - Binary representation of $k$
  - Define $j$ as a reversed bit-string, $j = \sum_{k=1}^{n} j_k 2^{n-k}$.
    - $U_{FT}\left|j\right\rangle = 2^{-\frac{n}{2}} \otimes_{l=1}^{n} \left(|0\rangle + \exp\left(2\pi i \sum_{k=n-l+1}^{n} j_k \, 2^{n-k-l}\right) |1\rangle\right)$.
  - Equivalently, $U_{FT}\left|j\right\rangle = 2^{-\frac{n}{2}}\left(|0\rangle + e^{2\pi i0.j_n}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i0.j_{n-1}j_n}|1\rangle\right) \otimes \dots \otimes \left(|0\rangle + e^{2\pi i0.j_1 \dots j_{n-1}j_n}|1\rangle\right)$.

Quantum circuit for QFT

- The controlled phase $\frac{2\pi}{2^k}$ is the key controlled-unitary for implementing the QFT together with single-qubit Hadamard gates, so we can use $R_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{pmatrix}$.
  - $R_k$ is a controlled rotation gate.
- 
$|j_1\rangle$
$|j_2\rangle$
$|j_{n-1}\rangle$
$|j_n\rangle$
$H$
$R_2$
$R_{n-1}$
$R_n$
$H$
$R_{n-2}$
$R_{n-1}$
$H$
$R_2$
$H$
$|0\rangle + e^{2\pi i0.j_1 \dots j_n}|1\rangle$
$|0\rangle + e^{2\pi i0.j_2 \dots j_n}|1\rangle$
$|0\rangle + e^{2\pi i0.j_{n-1}j_n}|1\rangle$
$|0\rangle + e^{2\pi i0.j_n}|1\rangle$
  - Qubit 1 has a single 1-qubit gate and $n-1$ 2-qubit controlled $R_k$ gates.
  - Qubit 2 has a single 1-quibit gate and $n-2$ 2-qubit controlled $R_k$ gates.
  - Qubit n has a single 1-quibit gate and 0 2-qubit controlled $R_k$ gates.
  - A total of $n$ H gates, $\frac{n(n-1)}{2}$ controlled phase gates, compared to $n \exp n$ gates in classical computing

Phase estimation algorithm

- The eigen vectors $|u\rangle$ of a unitary operator $U$ have eigenvalues with norm 1, so $U|u\rangle = e^{2\pi i\phi}|u\rangle$.
- Algorithm: the phase estimation algorithm is an algorithm to determine the phase of an eigenvector
  - Approximate the eigenvalues of a unitary operator
- Ingredients
  - Assume we have a quantum circuit that can prepare a state $|u\rangle$ or at least similar to $|u\rangle$
  - Assume we have a quantum circuit that can efficiently evaluate controlled- $U^{2^j}$ operators
  - An inverse QFT circuit
- Plausibility argument

    - A system represented by $n$ qubits has a unitary matrix dimension $N \times N$ where $N = 2^n$
    - Calculating the eigenvalue for an operator $U$ and eigenvector $|u\rangle$ requires $N = 2^n$ operations
    - The unitary matrix and circuit for estimating the phase can be efficiently represented by a polynomial number qubit manipulations
- Qubit required
    - Input register initialized to zero with t qubits
    - Output register with as many qubits as needed to store the vector
- Stages
    - Controlled $U^{2^j}$ operators for $j = 0, \dots, t-1$
        - Apply H gates to all inputs
        - Controlled $U^{2^j}$ on the second register where $U$ acts on the entire state
        - State at the end: $|\psi\rangle = 2^{-\frac{t}{2}}\left(|0\rangle + e^{2\pi i(2^{t-1}\phi)}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i\phi 2^0}|1\rangle\right) \otimes |u\rangle$.
        - Can express $\phi$ in base 2 using $t$ bits $\phi_j$ (either 0 or 1), $\phi = \frac{\phi_2}{2} + \frac{\phi_3}{4} + \cdots + \frac{\phi_t}{2^{t-1}}$.
            - □ Then $|\psi\rangle = 2^{-\frac{t}{2}}(|0\rangle + e^{2\pi i 0.\phi_t}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi i 0.\phi_1 \dots \phi_t}|1\rangle) \otimes |u\rangle$
    - Implements the inverse of QFT (Hermitian conjugate $U_{FT}^\dagger$).
        - $x_k = N^{-\frac{1}{2}} \sum_{j=0}^{N-1} y_j e^{-\frac{2\pi ijk}{N}}$.
        - End result: The inverse quantum Fourier transform to the stage 1 output is the state $U_{FT}^\dagger\left(2^{-\frac{t}{2}} \sum_{j=0}^{2^t-1} e^{2\pi i\phi j}|j\rangle|u\rangle\right) = |\tilde{\phi}\rangle|u\rangle$.
        - By measuring the input state, we obtain a binary representation $\tilde{\phi}$ for the phase of the eigenvalue
- Errors
    - The fraction representation $\phi = 0.\phi_1\phi_2 \dots \phi_t$ is not exact because of the finite representation in $t$ bits.
        - Integer representation $\phi_1 \dots \phi_t$ (remove the highest zero).
    - To bound the error $e$ on the measured value $m$ of the phase at the end of the phase estimation algorithm, let $b$ be a $t$-bit integer in the range 0 to $2^t - 1$, error is given by $\delta = \phi - \frac{b}{2^t}$
    - $p(|m - b| > e) < \frac{1}{2(e-1)}$.
    - If we need to approximate $\phi$ to an accuracy $2^{-n}$, choose $e = 2^{t-n} - 1$ and $t = n + p$ qubits, then the probability that the accuracy is worse than $2^{-n}$ is $p\left(|m - b| > 2^{t-n} - 1\right) < \frac{1}{2(2^p - 1)}$.
    - The error is exponentially suppressed by adding more bits to the phase register
- How to get the eigenvectors of $U$? Suppose we prepare an input state that is a superposition over all eigen states $|0\rangle_t \otimes |\psi\rangle = |0\rangle_t \otimes \sum_u c_u|u\rangle$ where $U|u\rangle = e^{2\pi i\phi_u}|u\rangle$
    - Output state: $\sum_u c_u|\phi_u\rangle|u\rangle$ where $|\phi_u\rangle = \sum_j a_j|j\rangle$.
        - $|\phi_u\rangle$ may be a superposition of all the eigenstates
    - The probability to get an eigen value is $p(\phi_i) = \sum_{\phi_k = \phi_i}|c_k|^2$
- Phase estimation is exact when the $t$-bit representation is exact

## Order finding problem

- For positive integers $x$ and $N$, $x < N$, with no common factors, the order of $x$ modulo $N$ is the least positive integer $r$ such that $x^r \equiv 1 \; mod \; N$
    - $L = \lceil \log_2 N \rceil$.
- Quantum algorithm: phase estimation algorithm applied to the unitary transformation $U$ that implements
    - $U|y\rangle = |xy \; mod \; N\rangle$.
    - $y$ is an $L$ −bit number
    - For an input state $|y\rangle$ where $y < N$, the transformation maps the input state $|y\rangle$ to $|xy \; mod \; N\rangle$
    - For $|y\rangle$ where $N \le y \le 2^{L-1}$, the transformation returns $|y\rangle$.
    - The eigenvectors of $U$ satisfies $|u_s\rangle = r^{-1/2} \sum_{k=0}^{r-1} e^{2\pi isk/r}|x^k \; mod \; N\rangle$.
        - $U|u_s\rangle = e^{-2\pi is/r} r^{-1/2} \left(\sum_{k=1}^{r-1} e^{2\pi isk/r}|x^k \; mod \; N\rangle + e^{2\pi is}|x^r \; mod \; N\rangle\right) = e^{-2\pi is/r}|u_s\rangle$.
            - □ Note: $e^{2\pi is}|x^r \; mod \; N\rangle = e^{2\pi is\frac{0}{r}}|x^0 \; mod \; N\rangle$
    - $|u_s\rangle$ is an eigenvector of $U$ with eigenvalue $\exp\left(-\frac{2\pi ir}{s}\right)$, the phase estimation will enable us to obtain $r$.
    - To prepare $|u_s\rangle$, $r^{-\frac{1}{2}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$.
        - Use $t = 2L + 1 + \left\lceil \log_2\left(2 + \frac{1}{2\epsilon}\right) \right\rceil$ for the number of qubits in the phase to obtain an answer accurate to $2L + 1$ bits with a probability of success of at least $1 - \epsilon$.
        - Can initialize the vector to $|1\rangle$.
- Errors
    - Continued fractions algorithm

        - We know $\phi \approx \frac{s}{r}$ up to $2L + 1$ bits.
        - We know a priori that $\phi$ is a rational number.
        - If we can compute the nearest fraction to $\phi$, we can get $r$.
    - Suppose $\frac{s}{r}$ is a rational number such that $\left|\frac{s}{r} - \phi\right| \leq \frac{1}{2r^2}$. Then $\frac{s}{r}$ is convergent of the continued fraction for $\phi$ and thus $s'$ and $r'$ with no common factor such that $\frac{s}{r} = \frac{s'}{r'}$ can be computed in $\sim cL^3$ operations using the continued fractions algorithm for large $L$
    - Failing conditions
        - The phase estimation procedure might produce a bad estimation to $\frac{s}{r'}$, but this occurs with probability at most $e$ that can be improved exponentially by adding a few qubits
        - Because the values of $r$ and $s$ obtained are probabilistic, the values $s$ and $r$ might have a common factor, so $s'$ and $r'$ from the continued fractions algorithm might not be equal to $r$ and $s$. Thre are many ways to correct this, with the most expensive being $\sim L^3$ overhead, and the least being $\sim L^0$.

Factoring

- Suppose $N$ is an $L$ bit composite number, and $x$ is a non-trivial solution to the equation $x^2 \equiv 1 \; mod \; N$ in the range $1 < x \leq N$, and neither $x \equiv 1 \; mod \; N$ or $x \equiv (N-1) \; mod \; N$. Then at least one of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a non-trivial factor of $N$ that can be computed using $O\left(L^3\right)$ operations
- Suppose $N = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ is the prime factorization of an odd composite positive integer. Let $x$ be an integer chosen uniformly at random, subject to $1 < x \leq N-1$ and $x$ is co-prime to $N$. Let $r$ be the order of $x$ mod $N$.
    - Then $p\left(r \; is \; even \; and \; x^{r/2} \neq (N-1) mod \; N\right) \geq 1 - 2^{-m}$.
    - All of the steps of the algorithms can be performed efficiently on a classical computer except the order finding
    - A quantum computer provides an efficient subroutine for order finding

# Quantum search

2021年9月10日 20:35

Problem: find the index of the record in the database

- Assume index: $[0, N-1]$.
- Assume $N = 2^n$ so the index can be stored in $n$ bits
- Assume that there are $M$ solutions where $1 \leq M \leq N$

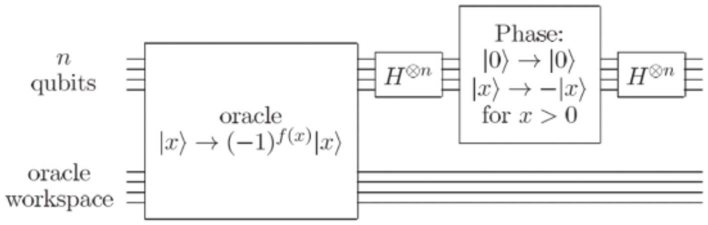
Suppose we have a function $f(x)$ that takes the index $x \in [0, N-1]$

- If $x$ is a solution, then $f(x) = 1$, $f(x) = 0$ otherwise

Quantum oracle

- Assume we have a circuit for the function that can recognize solutions to the problem by implementing a quantum oracle circuit $U_O$ which accomplishes: $U_O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$.
    - The oracle can be implemented efficiently in a quantum circuit if it can be implemented in a classical circuit because a quantum circuit can be implemented using reversible logic in a number of operations that is within a factor of 2 of a classical irreversible logic
    - The register $|q\rangle$ is a single qubit. If it is initialized to $|0\rangle$, the oracle is flipped when $f(x) - 0$, and not flipped when $f(x) = 1$.
        - If $f(x) = 0$, then $U_O|x\rangle|b\rangle = |x\rangle|b\rangle$.
        - If $f(x) = 1$, then $U_O|x\rangle|b\rangle = |x\rangle|\tilde{b}\rangle$.
    - If $|q\rangle = 2^{-\frac{1}{2}}(|0\rangle - |1\rangle)$, then $U_O|x\rangle 2^{-\frac{1}{2}}(|0\rangle - |1\rangle) = (-1)^{f(x)}|x\rangle 2^{-\frac{1}{2}}(|0\rangle - |1\rangle)$.
- If there are $N$ entries and $M$ solutions, Grover will do the search in $\alpha\sqrt{N/M}$ oracle evaluations.

Grover search algorithm

- Initialization
    - Establishes an equal superposition of all input states using $H^{\otimes n}$ for the input register $|x\rangle$ for the oracle $|\psi\rangle = H^{\otimes n}|0\rangle = N^{-1/2}\sum_{x=0}^{N-1}|x\rangle$ where $N = 2^n$.
- Grover Iteration $G$
    - Apply the oracle to the register $|x\rangle$, $U_O|x\rangle = (-1)^{f(x)}|x\rangle$ .
    - Apply the Hadamard transformation $H^{\otimes n}$ to the register.
    - Perform a conditional phase shift $U_P|x\rangle = -(-1)^{\delta_{x0}}|x\rangle$.
    - Apply the Hadamard transform $H^{\otimes n}$ to $|x\rangle$.
    - 
n
qubits
oracle
workspace
oracle
$|x\rangle \to (-1)^{f(x)}|x\rangle$
$H^{\otimes n}$
Phase:
$|0\rangle \to |0\rangle$
$|x\rangle \to -|x\rangle$
for $x > 0$
$H^{\otimes n}$
    - It can be written as $\left(H^{\otimes n}(2|0\rangle_n\langle 0|_n - 1)H^{\otimes n}\right)U_O = \left(2|\psi\rangle\langle\psi| - I\right)U_O$ .
    - It is described by the unitary transformation consisting of the composition of the oracle $U_O$ and a second unitary
        - The oracle $U_O$ implements $U_O|x\rangle = (-1)^{f(x)}|x\rangle$ where $f(x) = 1$ if $x$ is a solution to the problem
        - Second unitary: $2|\psi\rangle\langle\psi| - I$ where $|\psi\rangle = \sum_{x=0}^{N-1}|x\rangle$.

Geometric interpretation

- Let $|\alpha\rangle = (N-M)^{-1/2}\sum_x''|x\rangle$ where are not in the solution space, $|\beta\rangle = M^{-\frac{1}{2}}\sum_x'|x\rangle$ where $|x\rangle$ are in the solution space.
- $|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$.

- Grove algorithm is broken into two reflections
  - The oracle performs a reflection about the vector $|\alpha\rangle$ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$.
  - The operator $2|\psi\rangle\langle\psi| - I$ performs a reflection about the vector $|\psi\rangle$ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$.
  - Let $\cos\left(\frac{\theta}{2}\right) = \sqrt{\frac{N-M}{N}}$, $\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}}$ so that $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle$, then $G$ is a rotation $G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.
    - $2|\psi\rangle\langle\psi| - I = \cos(\theta)\,|\alpha\rangle\langle\alpha| - \cos(\theta)\,|\beta\rangle\langle\beta| + \sin(\theta)\,\big(|\alpha\rangle\langle\beta| + |\beta\rangle\langle\alpha|\big)$.
- Applying Grover iteration $k$ times swings towards the $\beta$ axis where the solutions to the problem lie
  - $G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$.
  - If the final state is equal or close to $|\beta\rangle$, measurement will reveal a solution with a high probability. (equivalently, $\frac{2k+1}{2}\theta = \frac{\pi}{2}$)
  - Asymptotic: using $\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}}$, we get $k = \frac{\pi}{2}\sqrt{N/M}$.

# Decoherence, implementation

2021年9月10日 20:35

Physical implementation of a quantum computer

- A system of quantum bits
- A physical apparatus that we use to manipulate and measure the system of quantum bits
- Invariably, aspects of the apparatus that we don't have direct control
  - Introduces difficulty because of decoherence from environment

Decoherence

- Def: A physical process that interferes with our manipulation of quantum systems
  - Quantum computers rely on logic operations that generate quantum superpositions
  - Decoherence interferes with out quantum superpositions, and quantum algorithms
  - It is a process that turns quantum uncertainty into classical uncertainty
- Decoherence comes from unwanted interactions of quantum systems with elements in the environment that we have little knowledge of or control over
- Qubits that tend to have long coherence times tend to be hidden from the environment hence hard to manipulate with single-qubit and two-qubit logic gates

Density matrix

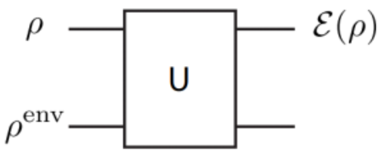
- A tool in statistical quantum physics to study decoherence
- It is useful to describe a quantum system in terms of a subsystem
  - We can control and measure
  - The environment that we do not control or measure but interacts with a controllable or measurable subsystem
- It describes quantum mechanical and classical uncertainty
- Suppose a quantum system is in a state $|i\rangle$ with classical probability $W_i$, where $\sum_i W_i = 1$. The density matrix $\rho = \sum_i |i\rangle W_i \langle i|$.
- For a pure state $|\psi\rangle$, $\rho = |\psi\rangle\langle\psi|$.
- If the state $|\psi\rangle$ evolves with time as $|\psi(t)\rangle = U(t)|\psi(0)\rangle$, then the density matrix of the system evolves as $\rho(t) = U(t)\rho(0)U^\dagger(t)$.
- For density matrix $\rho$, the mean value of the measurement of an observable $A$ is $\langle A\rangle = Tr(\rho A)$ where $Tr(M) = \sum_k \langle k|M|k\rangle$ is the trace (the sum of the diagonal elements) and the sum is over all basis elements $|k\rangle$.
  - So $\langle A\rangle = \sum_i W_i \langle i|A|i\rangle = \sum_i Tr\left(W_i |i\rangle\langle i|A\right)$.
- If a density matrix can be written in the form $\rho = |\psi\rangle\langle\psi|$, then it is a pure state. If not, it is a mixed state
  - A system in a pure state is in a quantum state $|\psi\rangle$ with a certainty 100%
  - A system in a mixed state is not in a well defined quantum state

Reduced density matrix

- The reduced density matrix $\rho^A$ of a subsystem in a subspace $A$ within a larger system defined by the space $A$ and $B$, $A \otimes B$ is given by $\rho^A = Tr_B(\rho) = \sum_{b_1=0}^{1} \dots \sum_{b_m=0}^{1} \langle b_1 \dots b_m|\rho|b_1 \dots b_m\rangle$.
  - $|b_1 \dots b_m\rangle$ is an element in space $B$.
  - $Tr_B(\rho_A \otimes \rho_B) = \rho_A Tr(\rho_B) = \rho_A$.
- Turns quantum uncertainty (superposition) into classical uncertainty (ignorance)
  - Decoherence: the process that turns quantum uncertainty into classical uncertainty

Quantum operations

- Quantum operations formalism is a tool for describing the dynamics of quantum systems in a wide variety of circumstances.
- The density evolution under a quantum operation is given by $\rho' = \mathcal{E}(\rho)$.
  - $\mathcal{E}$ is the quantum operation
  - $\rho$ is initial density operator (qubit status) of subsystem
  - $\rho'$ is the qubits after the operation
  - Useful because the environment density matrix is not in it.
- Simple examples with no environment
  - Unitary evolution: $\mathcal{E}_U(\rho) = U\rho U^\dagger$

    - Measurement: $\mathcal{E}_M(\rho) = \left(M_m \rho M_m^\dagger\right)/p(m)$ .
- The quantum operator for a subsystem $\rho$ that interacts with its environment $\rho^{env}$ via a unitary operator $U$ obeys the following circuit
    - 

    - $\mathcal{E}(\rho) = Tr_{env}\left(U\left(\rho \otimes \rho^{env}\right)U^\dagger\right)$.
    - One way that the subsystem and environment can be prepared into a tensor product initial state is by measuring the subsystem
- $CNOT\left(\rho, \rho_{env}\right)$ use subsystem to impact the environment, so that the environment learns about the subsystem qubit
    - $\rho_f = U\rho_i U^\dagger = (P_0 \otimes I + P_1 \otimes X)\rho \otimes P_0\left(P_0 \otimes I + P_1 \otimes X\right)^\dagger$.
    - $= P_0\rho P_0 \otimes P_0 + P_1\rho P_0 \otimes XP_0 + P_0\rho P_1 \otimes P_0 X + P_1\rho P_1 \otimes XP_0X$.

Operator sum representation

- Assuming the environment is in a pure state $\rho^{env} = |e_0\rangle\langle e_0|$, we can cast the quantum operator $\mathcal{E}(\rho)$ into the operator sum on the density matrix
    - $\mathcal{E}(\rho) = \sum_k \langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle = \sum_k E_k \rho E_k^\dagger$, where $E_k = \langle e_k|U|e_0\rangle$.
- The action is equivalent to
    - Randomly placing $\rho$ by $\frac{E_k \rho E_k^\dagger}{Tr(E_k \rho E_k^\dagger)}$
    - The replacement occurs with probability $Tr(E_k \rho E_k^\dagger)$

Bit flip and phase flip channel errors

- Operator sum of $E_0$ and $E_1$: $\rho' = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger$.
- Bit flip channels: assume a bit flip occurs with a probability $1 - p$ over an interval of time
    - $E_0 = \sqrt{p}I$ (does not flip), $E_1 = \sqrt{1-p}X$ (flip), $\rho' = p\rho + (1-p)X\rho X$.
- Phase flip channels: assume a phase flip on 1 occurs with a probability 1 – p over an interval of time
    - $E_0 = \sqrt{p}I$, $E_1 = \sqrt{1-p}Z$, $\rho' = p\rho + (1-p)Z\rho Z$.

Depolarizing channel

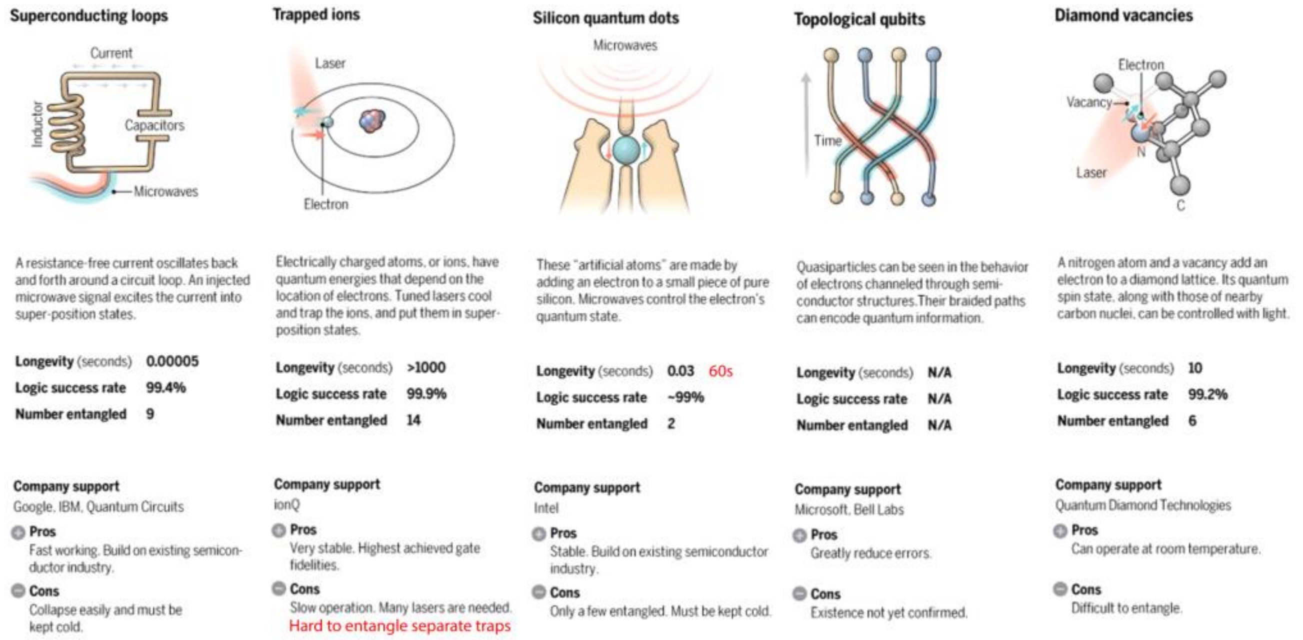
- It takes qubits and maps them into completely mixed states $U\rho U^\dagger = \frac{I}{2}$.
- Assume the depolarization occurs with a probability $1 - p$ over an interval of time
- The state of principal quantum system after the noise is $\mathcal{E}(\rho) = p\rho + (1-p)\frac{I}{2}$.

Fidelity: the similarity of a density matrix and a quantum state.

- Bit flip error may or may not affect a state
- Two kinds of flip (bit, phase) have different impact on a single state

Di Vincenzo Criteria

- A set of criteria for physical realization of quantum computers:
    - A scalable physical system with well defined quantum bits
    - The ability to measure qubits
    - A universal set of quantum gates
        - To approximate any unitary gates
    - The ability to initialize the qubits to a well-defined state
    - Long coherence times of qubit superposition states compared to gate and measurement times



| Superconducting loops | Trapped ions | Silicon quantum dots | Topological qubits | Diamond vacancies |
|---|---|---|---|---|
| A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into super-position states. | Electrically charged atoms, or ions, have quantum energies that depend on the location of electrons. Tuned lasers cool and trap the ions, and put them in super-position states. | These "artificial atoms" are made by adding an electron to a small piece of pure silicon. Microwaves control the electron's quantum state. | Quasiparticles can be seen in the behavior of electrons channeled through semi-conductor structures.Their braided paths can encode quantum information. | A nitrogen atom and a vacancy add an electron to a diamond lattice. Its quantum spin state, along with those of nearby carbon nuclei, can be controlled with light. |
| **Longevity** (seconds) 0.00005 | **Longevity** (seconds) >1000 | **Longevity** (seconds) 0.03 60s | **Longevity** (seconds) N/A | **Longevity** (seconds) 10 |
| **Logic success rate** 99.4% | **Logic success rate** 99.9% | **Logic success rate** ~99% | **Logic success rate** N/A | **Logic success rate** 99.2% |
| **Number entangled** 9 | **Number entangled** 14 | **Number entangled** 2 | **Number entangled** N/A | **Number entangled** 6 |
| **Company support**<br>Google, IBM, Quantum Circuits | **Company support**<br>ionQ | **Company support**<br>Intel | **Company support**<br>Microsoft, Bell Labs | **Company support**<br>Quantum Diamond Technologies |
| ⊕ **Pros**<br>Fast working. Build on existing semiconductor industry. | ⊕ **Pros**<br>Very stable. Highest achieved gate fidelities. | ⊕ **Pros**<br>Stable. Build on existing semiconductor industry. | ⊕ **Pros**<br>Greatly reduce errors. | ⊕ **Pros**<br>Can operate at room temperature. |
| ⊖ **Cons**<br>Collapse easily and must be kept cold. | ⊖ **Cons**<br>Slow operation. Many lasers are needed.<br>Hard to entangle separate traps | ⊖ **Cons**<br>Only a few entangled. Must be kept cold. | ⊖ **Cons**<br>Existence not yet confirmed. | ⊖ **Cons**<br>Difficult to entangle. |

- Current number of qubits
  - Superconducting loop: 53
  - Trapped ion: 20
  - Silicon (spin): 4
    - Industrially easy to build

Spin-based qubits

- Angular momentum ($L = r \times p$): a particle in motion can have an angular momentum dependent on position ($r$) and momentum ($p$)
- Elementary particles posses an intrinsic angular momentum
  - It is the angular momentum possessed by an elementary particle even when it is not spinning in space
  - Stern-Gerlach experiment is the first to show that an electron possesses an intrinsic angular momentum
  - The intrinsic angular momentum of an electron can take one of two values when measured ($\pm\frac{\hbar}{2}$)
- Particles can be categorized based on the magnitude of their intrinsic angular momentum (in units $\hbar$)
  - Fermions: particles with $\frac{2n+1}{2}$ spin ($\pm\frac{\hbar}{2}, \pm\frac{3\hbar}{2}, \ldots$)
  - Bosons: particles with integer spin ($\pm\hbar, \pm 2\hbar, \ldots$)
- In addition to spin, elementary particles possess an orbital degree of freedom due to their motion and the quantum analog of $L$ is the orbital angular momentum
- Spin-based quantum bits are quantum bits where the two levels that form the computational subspace derive from the spin degree of freedom of an elementary particle
- They are distinguished by a few different properties
  - Method of confinement for particles: electrostatic, impurity, impurity complex
  - Type of particles involved: conduction band (electron, $S = \frac{1}{2}$), valence band (hole, $L = 1, J = 3/2$ dut to $L \cdot S$ coupling)
  - Number of particles to make a single qubit
    - 1 electron: $S = \frac{1}{2}$.
  - Material host of particle: silicon, germanium, gallium arsenide
    - Different environment, vastly different coherence properties
    - Silicon: low error, long coherence time
    - Germanium: easy to scale
    - Gallium arsenide: no stable nuclei, short coherence time

Spin-based qubits in solids

- Qubits composed of a single charged particle with a spin $S = \frac{1}{2}$ are very promising
- Model for an isolated single particle in a magnetic field $\vec{B}$ is the Zeeman Hamiltonian: $H = \frac{1}{2} g \mu_B \vec{B} \cdot \vec{\sigma}$.
  - $g$: Lande g-factor (material dependent).
  - $\mu_B$: Bohr magneton.

- In static magnetic field, the eigenvalues of the Hamiltonian give the energies of the spin up and down states
  - $E = \pm \frac{g\mu_b B}{2}$.

Measurement of spin qubits in solids

- Detecting the intrinsic angular momentum is hard
- Spin to charge conversion: the process by which the spin of a particle is measured by detecting a change in the charge configuration of a system
  - The motion of a charge can depend on the value of the spin
  - It is relatively easy to measure a small fraction of the charge of an electron quickly
  - Fast charge measurement: single electron transistor, quantum point contact, nanowire
- Energy selective tunneling (spin to charge conversion)
  - Suppose we have a reservoir into which electron tunneling is possible that is filled up to the Fermi energy $E_F$
    - Spin up is unable to tunnel to the reservoir (detectable by a charge measurement)
  - The energy of the qubit levels must be tuned using an electrical voltage applied to a gate electrode so that they straddle the Fermi energy
- Spin selective tunneling
  - Suppose we have an isolated electron whose spin is known and a spin qubit whose state is not known
  - It requires more energy to tunnel from right to left when the spins are parallel
    - Pauli exclusion principal: at most one electron can occupy any given energy level
    - If the electrons have the same spin on the same site, one electron must be in an excited orbital

Rabi model

- The simplest methods available to control qubits
  - Two level system driven by a time-varying electromagnetic field that causes a transition between two states
- Application of a time-varying magnetic field $\overrightarrow{B_1}(t) = B_1 \hat{n} \cos \omega t$ allows to manipulate a spin-1/2 system and ultimately to perform quantum logic gates
  - With a static magnetic field $\hat{z}B_0$, we can have rotations, $H = g\mu_b B \cdot \sigma = \frac{\epsilon_z}{2\sigma_z}$ if $B = B_0$.
- Adding the time-varying magnetic field $\overrightarrow{B_1}(t)$ to the static magnetic field: $H = \frac{1}{2} g\mu_B \left(\hat{z}B_0 + \hat{x}B_1 \cos \omega t\right) \cdot \vec{\sigma}$.
  - $H = \left(\frac{\epsilon_Z}{2}\right) \sigma_Z + \left(\frac{\epsilon_{01}}{2}\right) \cos \omega t \, \sigma_X$, $\epsilon_{01} = g\mu_B B_1$, $\epsilon_Z = g\mu_B B_0$.
    - $\frac{\epsilon_Z}{2}$ is the Zeeman energy.
    - $\frac{\epsilon_{01}}{2} \cos \omega t$ is the term that flips 0 to 1
  - We want $B_1 \ll B_0$, then the equations can be solved by representing the state as a time-dependent sum in the computational basis.
- This gives $|\psi(t)\rangle = c_0(t) e^{-\frac{i\epsilon_Z t}{2\hbar}} |0\rangle + c_1(t) e^{\frac{i\epsilon_Z t}{2\hbar}} |1\rangle$ .
  - If there is no driving force, $c_0(t)$, $c_1(t)$ will be constant.
- Let $\omega_{01} = \frac{\epsilon_Z}{\hbar}$ and $\Omega_{01} = \frac{\epsilon_{01}}{\hbar}$. (driving frequency)
- Ignoring the dynamics at a frequency $\omega_{01} + \omega \approx 2\omega_{01}$ is called the rotating wave approximation (RWA).
- Define Rabi frequency $\Omega_R = \sqrt{\left(\omega_{01} - \omega\right)^2 + \Omega_{01}^2}$, we get $c_1(t) = i \left(\frac{\Omega_{01}}{\Omega_R}\right) e^{\frac{i(\omega_{01} - \omega)t}{2} - i\phi} \sin\left(\frac{\Omega_R t}{2}\right)$ .
  - Probability: $p_1(t) = \left(\frac{\Omega_{01}}{\Omega_R}\right)^2 \sin^2\left(\frac{\Omega_R t}{2}\right)$.
- When $\omega = \omega_{01}$, it is called being on resonance, because the energy of the radiation matches the energy of the transition.
  - On resonance, the system oscillates from 0 to 1 and back to 0 with a frequency $\Omega_R = \Omega_{01} = \frac{g\mu_B B_1}{\hbar}$.
  - Off resonance, the system oscillates with a reduced amplitude, but at a higher frequency $\Omega_R > \Omega_{01}$ for the same value of $B_1$.

Single qubit logic

- For a single $S = \frac{1}{2}$ qubit
  - $\sigma_Z$ field comes from a static magnetic field oriented along the $z$ direction. The static field causes the spin to rotate around the $z$ axis.
  - Rotation about the $x$ axis on the Bloch sphere is implemented by an oscillating magnetic field along the $x$ directions in space.
  - Rotation about the $y$ axis on the Bloch sphere can also be implemented by an oscillating magnetic field along the $x$ direction in space (change the phase)

        - Can also point the magnetic field along $y$ direction, but not necessary.
- Implement $S$ and $T$.
    - Change reference frame.
    - Adjust phase by the third method
- The amount of rotation is set by the time spent with the oscillating magnetic field on
    - High-precision microwave

Two qubit logic

- Two-qubit entangling gates are possible via spin-dependent interactions between qubits
- The wave-like behavior of an electron means that its spatial position is blurred out into a cloud-like orbital
- When the orbitals overlap in space, we get exchange interaction: $H = J\,\overrightarrow{\sigma^1}\cdot\overrightarrow{\sigma^2} = J\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 2 & 0\\ 0 & 2 & -1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$.
- Exchange on its own can be used to yield a SWAP-like interaction for $U$
- A CNOT gate can be obtained by combining the SWAP interaction with single qubit rotations

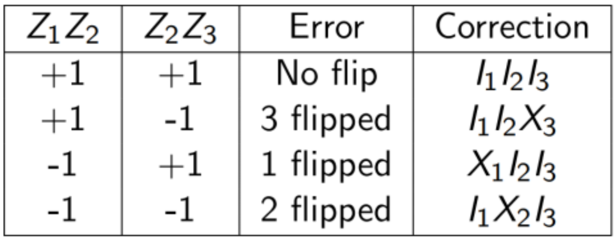
# Error correction

2021年9月10日 20:35

Error correcting codes

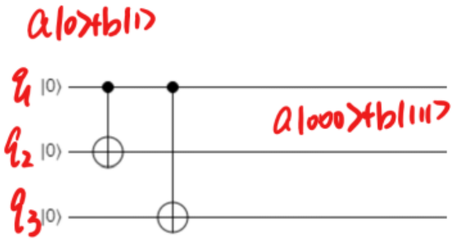
- Error correction works by adding redundant information such that if the amount of corruption is small, we can still process the information
  - 000 is logical 0, 111 is logical 1.
- Suppose 001 is received, each bit flips with an error $p$.
  - $p(001|000) = p(1-p)^2, p(001|111) = p^2(1-p)$.
- Majority vote:
  - Where the decoded output is the value 0 or 1 that occurs more in the value
- Probability of incorrect vote:
  - The probability that two or more bit are flipped is $p(e) = 3p^2(1-p) + p^3$.
  - Without encoding, the probability of error is $p$.
- Break even:
  - Encoding is better when $3p^2(1-p) + p^3 < p$ $(p < \frac{1}{2})$
- Quantum error correcting codes
  - Three fundamental differences between classical and quantum error correction
    - No cloning: creating redundancy by copying the qubit state is forbidden
    - Measurement destroys quantum information: observation generally destroys the quantum state
    - Continuous errors: an error can manifest as an arbitrarily small perturbation in the coefficients $\alpha, \beta$ of a single qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

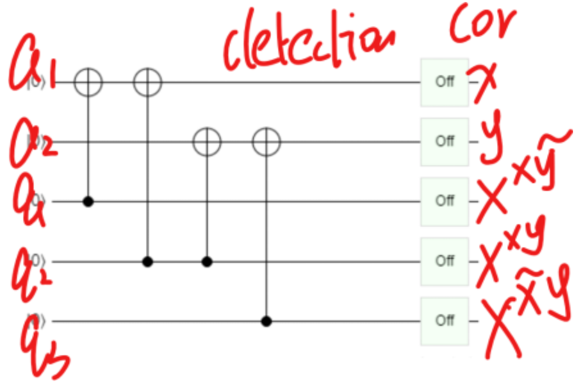
3-qubit Bit flip code

- Suppose a qubit in a state $|\psi\rangle$ can be corrupted by bit flips with probability $p$ to $X|\psi\rangle$ and is untouched with probability $1-p$, where $X = \sigma_X$.
  - A valid qubit state: $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$.
- Syndromes $P_i$: projective measurement operators
  - $P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|, P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$.
  - $P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|, P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$
  - The measurement does not change the state of the system that has been acted on by a single bit flip error
  - The four possible syndromes tell us how to correct the state.
    - If $i = 0$, do nothing.
    - If $i > 0$, flip bit $i$.
- Syndrome operators $Z_1Z_2$ and $Z_2Z_3$ where the subscripts refer to the qubit measured.
  - Rules: $Z|0\rangle = |0\rangle$ $Z|1\rangle = -|1\rangle$.
  - Assume 1 error only
  - 

| $Z_1Z_2$ | $Z_2Z_3$ | Error | Correction |
|---|---|---|---|
| +1 | +1 | No flip | $I_1I_2I_3$ |
| +1 | -1 | 3 flipped | $I_1I_2X_3$ |
| -1 | +1 | 1 flipped | $X_1I_2I_3$ |
| -1 | -1 | 2 flipped | $I_1X_2I_3$ |

- It cannot protest against phase flip errors
- Circuits

- 

- Ancilla qubits are needed in circuits that calculate syndromes, since measurement of the qubits that encode information themselves causes information to be lost irreversibly
- 

    - If $x = 0$ and $y = 0$, no flip.
    - If $x = 0$ and $y = 1$, $q_3$ flip, we flip $q_3$ again.
    - If $x = 1$ and $y = 0$, $q_1$ flip.
    - If $x = 1$ and $y = 1$, $q_2$ flip.
- Only $\alpha|000\rangle + \beta|111\rangle$ works, $\alpha|001\rangle + \beta|110\rangle$ is not allowed.

- e.g. start with $|\psi\rangle = a|0\rangle_L + b|1\rangle_L = a|000\rangle + b|111\rangle$, $\rho = |\psi\rangle\langle\psi|$.
    - If bit 2 is flipped, $|\psi'\rangle = a|010\rangle + b|101\rangle$, $\rho' = X_2|\psi\rangle\langle\psi|$.
- e.g. bit flip: $\rho = (1-p)|\psi\rangle\langle\psi| + pX|\psi\rangle\langle\psi|X$ applied to $|\psi\rangle = a|000\rangle + b|111\rangle$.
    - $\rho$

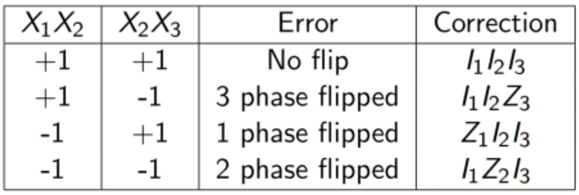
$$= p^0(1-p)^3|\psi\rangle\langle\psi| + p(1-p)^2\sum_{i=1}^{3} X_i|\psi\rangle\langle\psi|X_i$$

$$+ p^2(1-p)\sum_{i=1}^{3}(X_3X_2X_1)X_i|\psi\rangle\langle\psi|X_i(X_1X_2X_3)$$

$$+p^3(1-p)^0 X_3X_2X_1|\psi\rangle\langle\psi|X_1X_2X_3.$$

- No threshold

3-qubit phase flip code

- Suppose a qubit $|\psi\rangle$ can be corrupted by phase flips with probability $p$ to $Z|\psi\rangle$ and is untouched with probability $1-p$.
    - $|0\rangle_L = |+++\rangle$, $|1\rangle_L = |---\rangle$. (Use subscript $L$ to denote logic state)
    - $|\pm\rangle = 2^{-\frac{1}{2}}(|0\rangle \pm |1\rangle)$ and $Z|\pm\rangle = |\mp\rangle$.
- Syndromes: $X_1X_2$ and $X_2X_3$.
    - Rules: $X|+\rangle = |+\rangle$, $X|-\rangle = -|-\rangle$.
    - 

| $X_1X_2$ | $X_2X_3$ | Error | Correction |
|---|---|---|---|
| +1 | +1 | No flip | $I_1I_2I_3$ |
| +1 | -1 | 3 phase flipped | $I_1I_2Z_3$ |
| -1 | +1 | 1 phase flipped | $Z_1I_2I_3$ |
| -1 | -1 | 2 phase flipped | $I_1Z_2I_3$ |

- This cannot correct bit flip errors
- No threshold

Steane code

- 7-qubit code that has simple and appealing properties
  - Can correct phase flip and bit flip errors
    - Up to 1 phase flip + up to 1 bit flip at 6 ancilla qubits
    - Option 1: no error, 1 way
    - Option 2: 1 phase flip, 0 bit flip, 7 ways
    - Option 3: 1 bit flip, 0 phase flip, 7 ways
    - Option 4: 1 bit flip, 1 phase flip, 49 ways
    - 4 options give a total of 64 ways of errors, can be fixed by 6 qubits ($2^6$).
  - Operations on the coded states are simple
  - Can be described using stabilizers
- Stabilizers:
  - A state that is an eigenvector of an operator $O$ with eigenvalue 1 is said to be stabilized by the operator $O$.
    - For $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $Z_1 Z_2 |\psi\rangle = X_1 X_2 |\psi\rangle = |\psi\rangle$, $|\psi\rangle$ is stablized by these two operators.
  - Many quantum states can be more easily described by working with the operators that stabilize them rather than the states themselves
    - We measure the operator by measuring ancilla
    - e.g. measurement of a Hermitian unitary operator $A$ can be achieved by $(H \otimes I)cA(H \otimes I)|0\rangle|\psi\rangle$.
      Then, we measure the ancilla qubit $|0\rangle$.
- Steane code stabilizers
  - It uses six mutually commuting operators to diagnose the error syndrome
    - $M_0 = X_0 X_4 X_5 X_6$, $M_1 = X_1 X_3 X_5 X_6$, $M_2 = X_2 X_3 X_4 X_6$.
    - $N_0 = Z_0 Z_4 Z_5 Z_6$, $N_1 = Z_1 Z_3 Z_5 Z_6$, $N_2 = Z_2 Z_3 Z_4 Z_6$.
    - All 6 operators square to the identity
    - $M_i$ trivially commute with each other
    - $N_i$ traivially commute with each other
    - $M_i$ commute with $N_j$
  - Valid an invalid codewords of Steana code qubits are distinguished by the combinations of eigenvalues of these operators
- Steane code syndrome
  - A Hermitian unitary operator can be obtained from a circuit $(H \otimes I)cA(H \otimes I)|0\rangle|\psi\rangle$ with a controlled-A operation and Hadamard gates
    - If $A^2 = I$, then it becomes $|0\rangle P_0^A|\psi\rangle + |1\rangle P_1^A|\psi\rangle$.
  - A measurement outcome of the first qubit results in the state of the other qubit becoming the projection of $|\psi\rangle$ onto the subspace of eigenvalue $\pm 1$ of the operator $A$.
  - 6 ancilla qubits implement:
    - $(H \otimes I)cM_i(H \otimes I)|0\rangle|\psi\rangle$ .
    - $(H \otimes I)cN_i(H \otimes I)|0\rangle|\psi\rangle$ .
  - The 7-qubit code-words are defined by
    - $|0\rangle_L = 2^{-\frac{3}{2}}(1 + M_0)(1 + M_1)(1 + M_2)|0\rangle_7$.
    - $|1\rangle_L = 2^{-\frac{3}{2}}(1 + M_0)(1 + M_1)(1 + M_2)X^{\otimes 7}|0\rangle_7$.
- Small rotation with error correction
  - If there is a small angle error $R_x(\epsilon)|\psi\rangle$.
  - We apply the error correction circuit.
  - If ancilla is 1, we get $|\psi'\rangle = R_x(\pi)|\psi\rangle$. (We can detect and correct the error)
  - If ancilla is 0, we get $|\psi'\rangle = |\psi\rangle$. (There is no error)
- There is an $O(10^{-5})$ threshold

Fault-tolerance

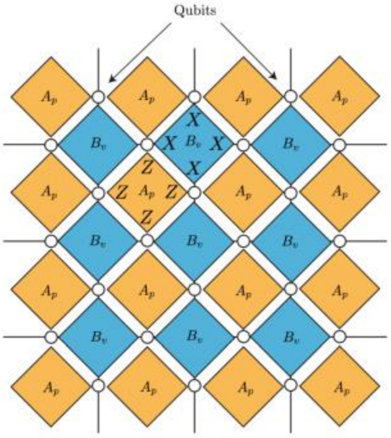
- Arbitrarily accurate quantum computation can be achieved with logic gates that introduce errors provided the errors are below a certain threshold
- Errors occur:
  - While states are encoded

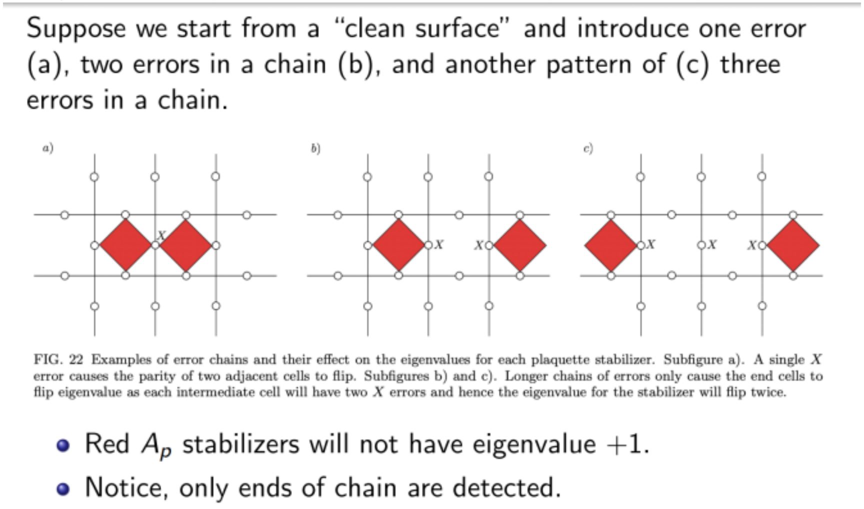
- 
    - While quantum logic is being carried out
    - While states are being measured
- To provide error correction
    - Replace each qubit in the original circuit with an encoded block of qubits
    - Replace each gate with a gate on encoded states
    - Perform error correction periodically on the encoded states with a separate set of circuits
- Fault tolerance:
    - Considers accumulation and propagation of errors in quantum circuit design
    - Definition: If only one component in the procedure fails, then the failure causes at most one error in each encoded block of qubits output from the procedure.
        - Component means: gates, measurements, quantum quiescent time evolution
    - Performing error-correction alone is not sufficient for fault-tolerance because encoded gates can cause errors to propagate. Errors in the encoded control qubit can cause errors in the encoded target qubits
    - Fault tolerant gates: failure in any physical qubit's operation in the procedure for performing the encoded gate produces errors in a small number of physical qubits in the encoded data
        - $H, S, CNOT, T$ can all be contructed using fault-tolerant procedures.
        - The complete set can be implemented with arbitrarily high precision
    - The action of error correction is to obtain a probability of error of $cp^2$ where $p$ is the probability of failure of individual components in the circuit
        - We want $cp^2 < p$, i.e. $p < \frac{1}{c}$.
- Concatenation:
    - When we recursively apply the error correction procedure. That is, make all of the physical qubits, in the first stage of encoding logical qubits
    - Example
        - Basic qubit: $|0\rangle, |1\rangle$.
        - Level 1: $|000\rangle, |111\rangle$
        - Level 2 concatenation: $|000000000\rangle$, $|111111111\rangle$ (9 physical qubits to make 1 logical qubit).
    - If the error rate of logical qubits is $p$, then the failure rate after error correction is at most $cp^2$. Concatenating the code once yields an error probability of $c\left(cp^2\right)^2 = \left(cp\right)^4/c$
    - After $k$ levels of concatenation, the error probability is $\left(cp\right)^{2^k}/c$.
        - The overhead is poly-logarithmic.

## Threshold theorem

- Suppose we wish to achieve an accuracy of $\epsilon$ in our algorithm which contains $p(n)$ gates where $p(n)$ is a polynomial in $n$. To accomplish this, each gate must have an accuracy of $\frac{\epsilon}{p(n)}$, and the number of concatenations required is $\frac{(cp)^{2^k}}{c} \le \frac{\epsilon}{p(n)}$, provided that $p < p_{th} = c^{-1}$, such a $k$ exists.
    - Let $\tilde{\epsilon}$ be the probability of error for a single operation
    - $p(correct) = 1 - \tilde{\epsilon}$ for one operation.
    - $p(correct) = (1 - \tilde{\epsilon})^{p(n)} \approx 1 - p(n)\tilde{\epsilon} + O\left(\tilde{\epsilon}^2\right)$, error for $p(n)$ operations is $p(n)\tilde{\epsilon}$.
- For errors below the threshold, the error is reduced exponentially with the number of qubits in the concatenated code $2^g$, when $p < p_{th}$.
- The value of the threshold depends on the code used and the architecture which includes considerations such as connectivity
- Most common now: $[7,1,3]$ (Steane code) on 2D nearest neighbor, with threshold $O\left(10^{-5}\right)$.
    - Can only do 2 qubit logic if and only if the 2 qubits are the nearest neighbor.
- Current revolution: topological cluster, surface code, color code

## Surface code

- A topological error correction code which has low connectivity and tolerates a lot of errors
- Code is implemented using stabilizers (on superconducting qubits, spin qubit…)
  - $A_p = \bigotimes_{j \in b(p)} Z_j$.
    - $b(p) =$ four qubits surrounding each face, $+1$ eigenstates of the operator $A_p$.
  - $B_v = \bigotimes_{j \in s(v)} X_j$.
    - $s(v) =$ four qubits surrounding each vertex, $+1$ eigenstates of the operator $B_v$.
  - 

    - An $N \times N$ lattice defined by horizontal and vertical lines contains $2^N$ qubits
    - A clean surface with no errors has $+1$ eigenvalues for all stabilizers
- The code is desirable because
  - It requires only nearest neighbor two-qubit gates
  - It tolerates a large error up to 1% for each gate
- Introducing errors
  - 

    Suppose we start from a "clean surface" and introduce one error (a), two errors in a chain (b), and another pattern of (c) three errors in a chain.

    FIG. 22 Examples of error chains and their effect on the eigenvalues for each plaquette stabilizer. Subfigure a). A single $X$ error causes the parity of two adjacent cells to flip. Subfigures b) and c). Longer chains of errors only cause the end cells to flip eigenvalue as each intermediate cell will have two $X$ errors and hence the eigenvalue for the stabilizer will flip twice.

    - Red $A_p$ stabilizers will not have eigenvalue $+1$.
    - Notice, only ends of chain are detected.
  - (a), $X$ is the error, red part has eigenvalue -1.
  - c, errors in one line is more likely.
  - When we get to edges, things may get complicated
- Surface code cannot detect two bit flip in one small region due to the stabilizer