Quantum Algorithms
Lecture 32
Quantum computation – task examples

Zhejiang University

Quantum Computation - Definitions and notation

Tensor product - example

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

$$|\varphi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

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

Inner product

Vectors are denoted like this: $|\psi\rangle$.

The inner product is denoted by $\langle\xi|\eta\rangle$.

If $|\xi\rangle = \sum_x a_x|x\rangle$ and $|\eta\rangle = \sum_x b_x|x\rangle$, then $\langle\xi|\eta\rangle = \sum_x {a_x}^* b_x$, where a^* is complex conjugate of a.

$|\xi_1 + \xi_2\rangle = |\xi_1\rangle + |\xi_2\rangle = \xi_1 + \xi_2$.

Example: $a = c + di$ => $a^* = c - di$.

Example of inner product:

$$|\xi\rangle = \frac{i}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$|\eta\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$$

$$\langle\xi|\eta\rangle = \frac{i}{\sqrt{2}}^* * \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}^* \frac{i}{\sqrt{2}} = -\frac{i}{2} - -\frac{i}{2} = -i$$

Operator applied to register

Let $U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$. Then the operators $U[1]$ and $U[2]$, acting on the space $B^{\otimes 2}$, are represented by these matrices:

$$U[1] = \begin{pmatrix} u_{00} & 0 & u_{01} & 0 \\ 0 & u_{00} & 0 & u_{01} \\ u_{10} & 0 & u_{11} & 0 \\ 0 & u_{10} & 0 & u_{11} \end{pmatrix}, \qquad U[2] = \begin{pmatrix} u_{00} & u_{01} & 0 & 0 \\ u_{10} & u_{11} & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}$$

The rows and columns are associated with the basis vectors arranged in the lexicographic order:

|00>, |01>, |10>, |11>.

Correspondence between classical and quantum computation

Reversible Boolean function

In what cases a function given by a Boolean circuit can be realized by a reversible circuit? Reversible circuits realize only permutations, i.e., invertible functions. This difficulty can be overcome in this way: instead of computing a general Boolean function $\mathrm{F}\colon B^n \to B^m$, we compute the permutation $F_{\bigoplus}\colon B^{n+m} \to B^{n+m}$ given by the formula $F_{\bigoplus}(x, y) = (x, y \oplus F(x))$. Then $F_{\bigoplus}(x, 0) = (x, F(x))$ contains the value of $F(x)$ we need.

$\oplus$ denotes bitwise addition modulo 2.

Controlled NOT

The gate $\circledcirc$ is usually called “Controlled NOT” for reasons that will become clear later. Note that $\circledcirc = I_{\oplus}$, where I is the identity map on a single bit. The essential meaning of the operation $\circledcirc$ is reversible copying of the bit x (if the initial value of y is 0).

$$\circledcirc : (x, y) \to (x, x \oplus y)$$

Interchange bits

The gate $\circledotimes$ allows one to interchange bits in memory, since the function $(\leftrightarrow)\colon (a,b) \to (b,a)$ can be represented as follows:

$$(\leftrightarrow)[j,k] = \circledotimes\,[j,k] \circledotimes [k,j] \circledotimes [j,k]$$

$\circledotimes\,[j,k] = [j, j \oplus k]$
$\circledotimes\,[j \oplus k, j] = [j \oplus k, j \oplus j \oplus k] = [j \oplus k, k]$
$\circledotimes\,[k, j \oplus k] = [k, k \oplus j \oplus k] = [k, j]$

Bases for quantum circuits

Complete basis

Any operator $U \in U(B)$ can be realized (without ancillas) by a constant size circuit over the basis $\{\Lambda(e^{i\phi})\colon \phi \in R\} \cup \{H\}$.

Adding CNOT operator allows to implement arbitrary unitary transformation on any number of qubits exactly.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Standard basis

In constructing quantum algorithms, we will use the following (widely adopted) standard basis.

The standard basis:

$Q = \{H, K, K^{-1}, \Lambda(\sigma^x), \Lambda^2(\sigma^x)\}$, where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

K-gate currently is widely called as the S-gate.

Standard basis allows to approximate arbitrary unitary with arbitrary precision.

Another complete basis

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Implementing NOT operator

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$X = HT^4H$$

$$T^4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Definition of quantum computation

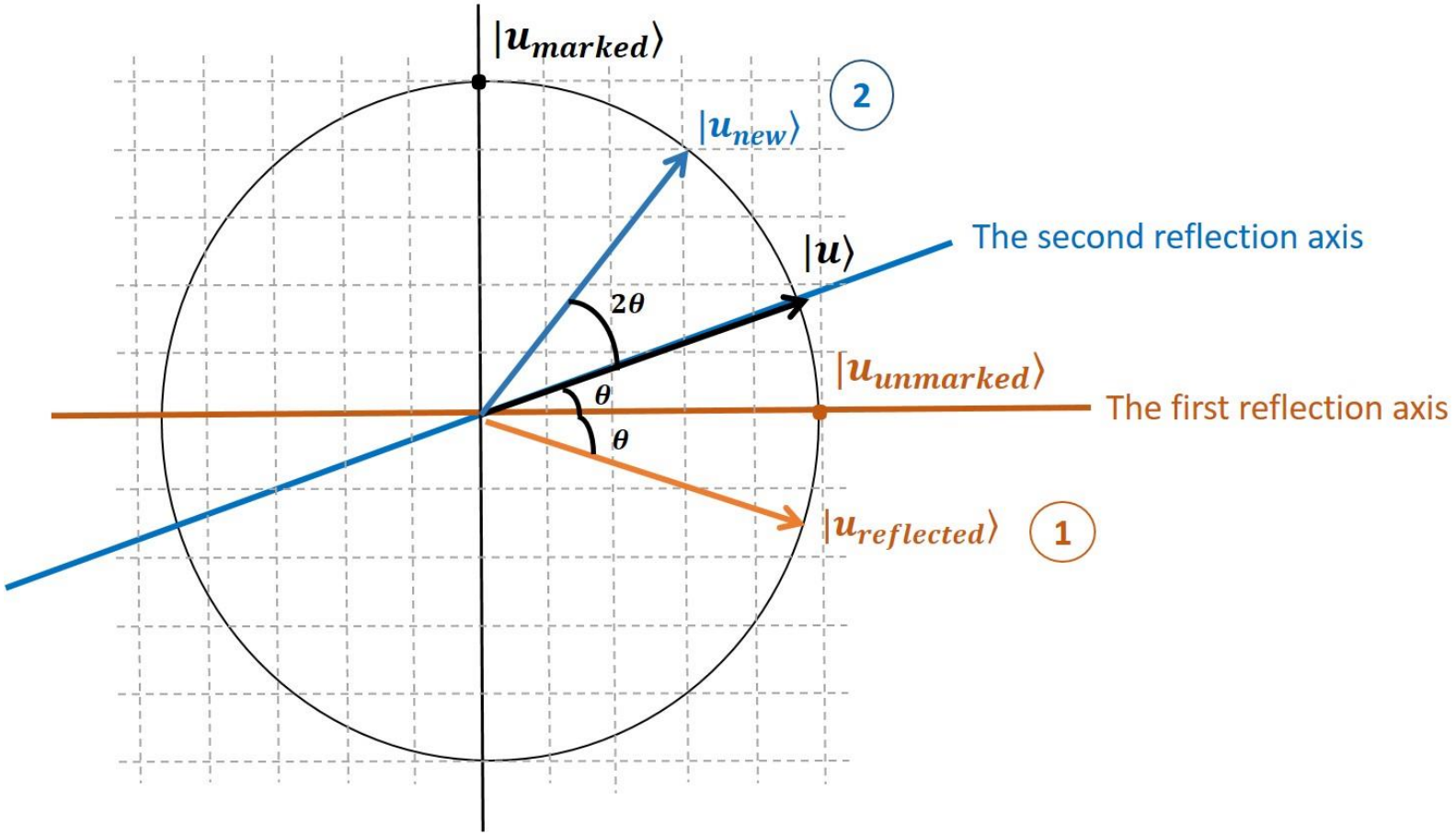
Definition

The circuit $U = U_L \cdots U_2 U_1$ computes F if for any x we have

$$\sum_z |\langle F(x), z|U|x, 0^{N-n}\rangle|^2 \geq 1 - \varepsilon$$

where ε is some fixed number smaller than $1/2$. (Note that $F(x)$ and x consist of different numbers of bits, although the total lengths of $(F(x), z)$ and $(x, 0^{N-n})$ must be equal to N.)

Grover's search - one qubit representation



Analysis – iterations

For small θ: $\theta \approx sin\theta$.

We need to rotate by $\frac{\pi}{2}$.

When one element is marked, then $\theta \approx \frac{1}{\sqrt{N}}$, each iteration rotates by 2θ.

We need to perform $\frac{\pi/2}{2/\sqrt{N}} = \frac{\pi\sqrt{N}}{4}$ iterations.

Analysis – probabilities

When we have N elements total and k of elements provide solution (are marked), then $\theta \approx \frac{\sqrt{k}}{\sqrt{N}}$. This is our starting angle.

Each iteration rotates vector by 2θ.

Probability to observe solution (marked element) if we measure after m iterations is:

$$\left(sin\left(\frac{(2m+1)\sqrt{k}}{\sqrt{N}} \right) \right)^2$$

Analysis – probabilities

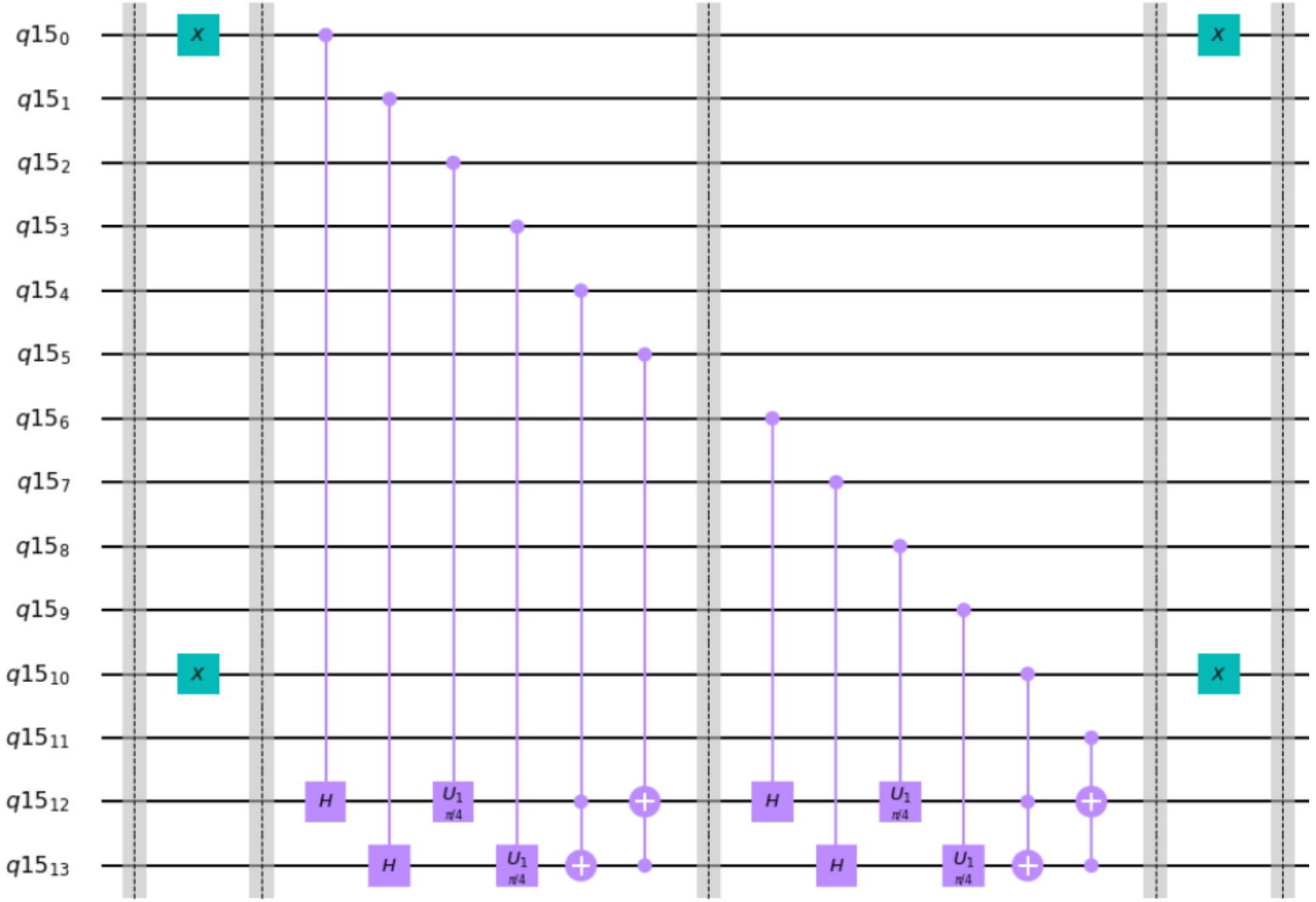
Probability to observe solution (marked element) if we measure after m iterations is:

$$\left(sin\left(\frac{(2m+1)\sqrt{k}}{\sqrt{N}} \right) \right)^2$$

Example: we have $N = 100$ elements, $k = 2$ solutions, and do $m = 3$ iterations of Grover's search. What is the probability to succeed?

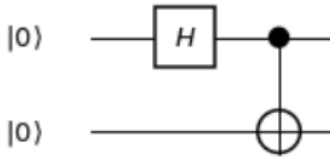
Answer: $\left(sin\left(\frac{7\sqrt{2}}{10} \right) \right)^2 = 0.94$

Universal quantum circuit



X changes qubit to state $|1\rangle$,
at the end we reverse it.

Result:



Quantum probability

Density matrix

$$\sum_k p_k \mathbf{P}(|\xi\rangle, \mathcal{M}) = \sum_k p_k \langle \xi_k | \Pi_{\mathcal{M}} | \xi_k \rangle$$

$$= \sum_k p_k \operatorname{Tr}\left(|\xi_k\rangle\langle\xi_k|\Pi_{\mathcal{M}}\right) = \operatorname{Tr}(\rho \Pi_{\mathcal{M}})$$

Here ρ denotes the density matrix $\rho = \sum_k p_k \, |\xi_k\rangle\langle\xi_k|$. The final expression here is what we take as the general definition of probability.

Actually, this is an operator rather than a matrix, although the term “density matrix” is traditional. In the sequel, we will often have in mind a matrix, i.e., an operator expressed in a particular basis.

Task with density matrix

Suppose we have the following quantum state:

$$\rho = \frac{1}{4}\begin{pmatrix}0\\1\end{pmatrix} + \frac{3}{4}\begin{pmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{pmatrix}$$

Calculating the density matrix:

$$\rho = \frac{1}{4}\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} + \frac{3}{4}\begin{pmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{pmatrix}\begin{pmatrix}1/\sqrt{2} & -1/\sqrt{2}\end{pmatrix}$$

$$= \begin{pmatrix}0 & 0\\0 & 1/4\end{pmatrix} + \begin{pmatrix}3/8 & -3/8\\-3/8 & 3/8\end{pmatrix} = \begin{pmatrix}3/8 & -3/8\\-3/8 & 5/8\end{pmatrix}$$

Task with density matrix

$$\rho = \begin{pmatrix} {}^{3}/_{8} & -{}^{3}/_{8} \\ -{}^{3}/_{8} & {}^{5}/_{8} \end{pmatrix}$$

Applying operator (Hadamard) $\mathrm{U} = \begin{pmatrix} {}^{1}/_{\sqrt{2}} & {}^{1}/_{\sqrt{2}} \\ {}^{1}/_{\sqrt{2}} & -{}^{1}/_{\sqrt{2}} \end{pmatrix}$

$$U\rho U^{+}$$

$$= \begin{pmatrix} {}^{1}/_{\sqrt{2}} & {}^{1}/_{\sqrt{2}} \\ {}^{1}/_{\sqrt{2}} & -{}^{1}/_{\sqrt{2}} \end{pmatrix} \begin{pmatrix} {}^{3}/_{8} & -{}^{3}/_{8} \\ -{}^{3}/_{8} & {}^{5}/_{8} \end{pmatrix} \begin{pmatrix} {}^{1}/_{\sqrt{2}} & {}^{1}/_{\sqrt{2}} \\ {}^{1}/_{\sqrt{2}} & -{}^{1}/_{\sqrt{2}} \end{pmatrix}$$

$$= \begin{pmatrix} 1/8 & -1/8 \\ -1/8 & 7/8 \end{pmatrix}$$

Task with density matrix

$$\rho = \begin{pmatrix} 1/8 & -1/8 \\ -1/8 & 7/8 \end{pmatrix}$$

Probability to measure state 0:

$$\Pi_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$Pr = Tr(\rho\Pi_0) = Tr\left(\begin{pmatrix} \frac{1}{8} & 0 \\ -\frac{1}{8} & 0 \end{pmatrix}\right) = 1/8$$

Physically realizable transformations of density matrices

Physically realizable superoperator

We postulate that a physically realizable superoperator is a composition of an arbitrary number of transformations of types 2 and 3 (type 1 is a special case of 3).

1. $\rho \xrightarrow{U} U\rho U^{\dagger}$
2. $Tr_F\colon \rho \to Tr_F \rho$
3. $V \cdot V^{\dagger}\colon \rho \to V\rho V^{\dagger}$

Probability

Suppose we use a supplementary subsystem. After we no longer need it, we can discard it to the trash and, in counting the probability, take the partial trace over the state space of the supplementary subsystem.

Or else we may hold all the trash until the very end and consider the probability of an event of the form $M_1 \otimes N_2$ (once we have stopped using the second subsystem, no details of its existence are of any importance to us and we are not interested in what precisely happens to it in the trash bin). As already stated, these probabilities are equal:

$$P(\rho, M_1 \otimes N_2) = P(Tr_{N_2}\rho, M_1)$$

Irreversible degradation

The term “decoherence” is generally used to denote irreversible degradation of a quantum state caused by its interaction with the environment. This could be an arbitrary physically realizable superoperator that takes pure states to mixed states. For the purpose of our discussion, decoherence means the specific superoperator D that “forgets” off-diagonal matrix elements:

$$\rho = \sum_{j,k} \rho_{jk} \, |j\rangle\langle k| \xrightarrow{D} \sum_{k} \rho_{kk} \, |k\rangle\langle k|$$

Irreversible degradation

$$\rho = \sum_{j,k} \rho_{jk} |j\rangle\langle k| \xrightarrow{D} \sum_{k} \rho_{kk} |k\rangle\langle k|$$

This superoperator is also known as an extreme case of a “phase damping channel”. We will show that it is physically realizable. For simplicity, let us assume that D acts on a single qubit.

Action of D

The action of D on a density matrix ρ can be performed in three steps. First, we append a null qubit:

$$\rho \rightarrow \rho \otimes |0\rangle\langle 0|$$

Then we “copy” the original qubit into the ancilla. This can be achieved by applying the operator

$$\Lambda(\sigma^x)\colon |a, b\rangle \rightarrow |a, a \oplus b\rangle$$

Action of D

We get

$$\rho \otimes |0\rangle\langle 0| \xrightarrow{\Lambda(\sigma^x)} \sum_k \rho_{jk} |j,j\rangle\langle k,k|$$

Finally, we take the partial trace over the ancilla, which yields the diagonal matrix

$$\sum_k \rho_{kk} |k\rangle\langle k|$$

Projective measurement

A superoperator: $\rho \mapsto \sum_j \mathbf{P}(\rho, \mathcal{L}_j) \cdot \left(\gamma^{(j)}, j\right)$

$$\gamma^{(j)} = \frac{\Pi_{\mathcal{L}_j} \rho \Pi_{\mathcal{L}_j}}{\mathbf{P}(\rho, \mathcal{L}_j)}$$

$P(\rho, L_j)$ is the probability of getting a specified outcome j. Then our quantum system will be in according state $\gamma^{(j)}$.

Projective measurement

If we measure the pure state $\rho = |\xi\rangle\langle\xi|$, then $\gamma^{(j)} = \left|\eta_j\right\rangle\left\langle\eta_j\right|$, where

$$|\eta_j\rangle = \frac{\Pi_{\mathcal{L}_j}|\xi\rangle}{\sqrt{\mathbf{P}(|\xi\rangle, \mathcal{L}_j)}}$$

In last expression division by $\sqrt{P(|\xi\rangle, L_j)}$ is done as a normalization, so we get mathematically a valid quantum system.

Example of a measurement

Copy a qubit (relative to the classical basis) and apply the decoherence superoperator to the copy. $\Pi_{L_0} = |0\rangle\langle 0|, \Pi_{L_1} = |1\rangle\langle 1|$

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \mapsto \rho_{00} \cdot \Big(|0\rangle\langle 0|, 0\Big) + \rho_{11} \cdot \Big(|1\rangle\langle 1|, 1\Big)$$

The measurement superoperator in such case looks like this.

Measuring operators

Measuring operator

$$W = \sum_j \Pi_{L_j} \otimes U_j$$

We have a state space $N \otimes K$, $N = \bigotimes_{j \in \{1,\dots,r\}} L_j$ (pairwise orthogonal subspaces), Π_{L_j} is a projection on a subspace L_j, $U_j \in L(K)$.

We have projections in space N, if a system appears in subspace L_j, then U_j is applied to subspace K.

Measuring

We want to measure $\rho \in L(N)$.
First, add subsystem: joint state is $\rho \otimes |0\rangle\langle 0|$.
Then, apply $W = \sum_j \Pi_{L_j} \otimes U_j$.

$$W\left(\rho \otimes |0^m\rangle\langle 0^m|\right)W^\dagger = \sum_j \left(\Pi_{\mathcal{L}_j}\rho\Pi_{\mathcal{L}_j}\right) \otimes \left(U_j|0\rangle\langle 0|U_j^\dagger\right)$$

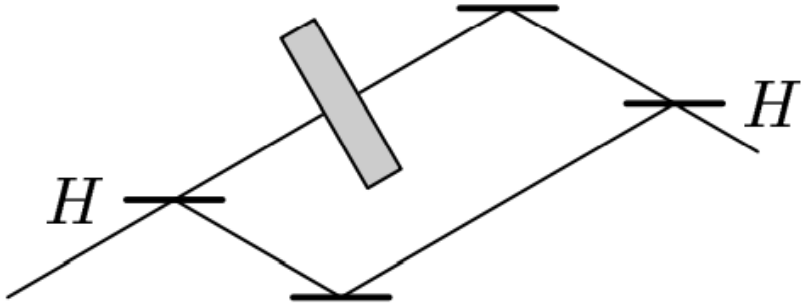
Properties of projection were considered:

- $\Pi^\dagger = \Pi$
- $\Pi^2 = \Pi$

Mathematical variant

$$\Xi(U) = (H \otimes I)\Lambda(U)(H \otimes I)\colon B^{\otimes N} \to B^{\otimes N}$$

$$\boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



If the initial vector has the form $|\psi\rangle = |\eta\rangle \otimes |\xi\rangle$ ($|\xi\rangle \in L_j$), then $\Xi(U)|\psi\rangle = |\eta'\rangle \otimes |\xi\rangle$, where

$$|\eta'\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \lambda_j \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}|\eta\rangle = \frac{1}{2}\begin{pmatrix} 1+\lambda_j & 1-\lambda_j \\ 1-\lambda_j & 1+\lambda_j \end{pmatrix}|\eta\rangle$$

Mathematical variant

$$|\eta'\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \lambda_j\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}|\eta\rangle = \frac{1}{2}\begin{pmatrix}1+\lambda_j & 1-\lambda_j\\ 1-\lambda_j & 1+\lambda_j\end{pmatrix}|\eta\rangle$$

Here λ_j is a phase shift applied to the qubit $|\eta'\rangle$, so that amplitude of state $|1\rangle$ is multiplied by $\lambda_j = e^{\pi i \varphi_j}$.

$$\Xi(U) = \sum_j \overbrace{\frac{1}{2}\begin{pmatrix}1+\lambda_j & 1-\lambda_j\\ 1-\lambda_j & 1+\lambda_j\end{pmatrix}}^{R_j} \otimes \Pi_{\mathcal{L}_j}$$

We obtain the following conditional probabilities:

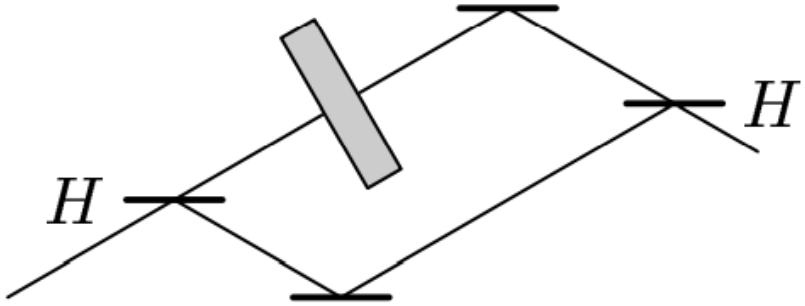
$$\mathbf{P}(0|j) = \left|\langle 0|R_j|0\rangle\right|^2 = \left|\frac{1+\lambda_j}{2}\right|^2 = \frac{1+\cos(2\pi\varphi)}{2}$$

Quantum algorithms for Abelian groups

Operator for measuring eigenvalues

$$\Xi(U) = (H \otimes I)\Lambda(U)(H \otimes I)\colon B^{\otimes N} \to B^{\otimes N}$$

$$\boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



If the initial vector has the form $|\psi\rangle = |\eta\rangle \otimes |\xi\rangle$ ($|\xi\rangle \in L_j$), then $\Xi(U)|\psi\rangle = |\eta'\rangle \otimes |\xi\rangle$, where

$$|\eta'\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \lambda_j \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}|\eta\rangle = \frac{1}{2}\begin{pmatrix} 1+\lambda_j & 1-\lambda_j \\ 1-\lambda_j & 1+\lambda_j \end{pmatrix}|\eta\rangle$$

Operator for measuring eigenvalues

We have $\lambda_k = e^{2\pi i \phi_k}$, so we have:

$$\Xi(U_a) = \sum_k V_k \otimes \Pi_{\mathcal{L}_k}, \quad V_k = \frac{1}{2}\begin{pmatrix} 1+e^{2\pi i\varphi_k} & 1-e^{2\pi i\varphi_k} \\ 1-e^{2\pi i\varphi_k} & 1+e^{2\pi i\varphi_k} \end{pmatrix}$$

and its action in the form

$$|0\rangle \otimes |\xi_k\rangle \xmapsto{\Xi(U_a)} \left(\frac{1+e^{2\pi i\varphi_k}}{2}|0\rangle + \frac{1-e^{2\pi i\varphi_k}}{2}|1\rangle\right) \otimes |\xi_k\rangle$$

Operator for measuring eigenvalues

$$|0\rangle \otimes |\xi_k\rangle \xrightarrow{\Xi(U_a)} \left(\frac{1 + e^{2\pi i \varphi_k}}{2} |0\rangle + \frac{1 - e^{2\pi i \varphi_k}}{2} |1\rangle \right) \otimes |\xi_k\rangle$$

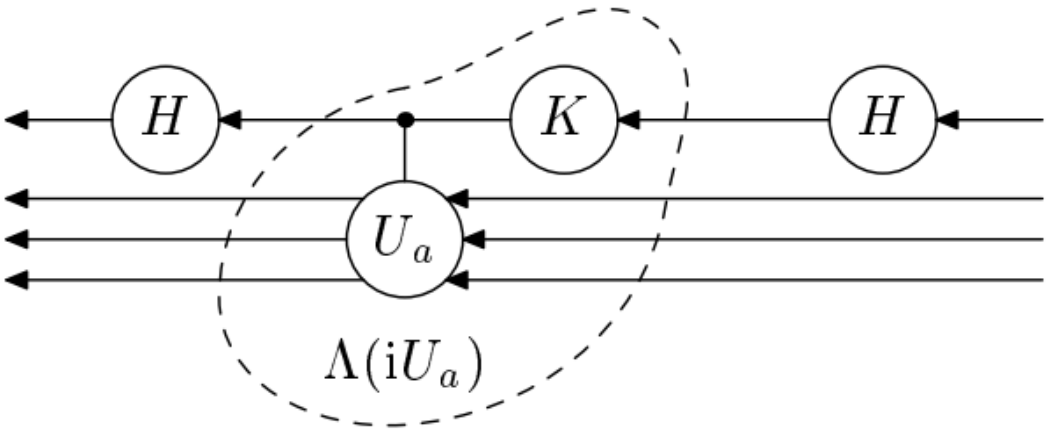
We get conditional probabilities for the first qubit:

$$\mathbf{P}(0|k) = \left| \frac{1 + e^{2\pi i \varphi_k}}{2} \right|^2 = \frac{1 + \cos(2\pi\varphi_k)}{2}, \qquad \mathbf{P}(1|k) = \frac{1 - \cos(2\pi\varphi_k)}{2}$$

Although the conditional probabilities depend on ϕ_k, they do not allow one to distinguish between $\phi_k = \phi$ and $\phi_k = -\phi$ (like in case of global phase). That is why another type of measurement is needed.

Another operator - improvement

We will use the operator $\Xi(iU_a)$. $K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ is from the standard basis.



The encircled part of the diagram realizes the operator $\Lambda(iU_a)$. Indeed, K multiplies only $|1\rangle$ by i, but this is just the case where the operator U_a is applied (by the definition of $\Lambda(U_a)$).

Another operator - analysis

For the operator $\Xi(iU_a)$ the conditional probabilities are

$$\mathbf{P}(0|k) = \frac{1 - \sin(2\pi\varphi_k)}{2}, \qquad \mathbf{P}(1|k) = \frac{1 + \sin(2\pi\varphi_k)}{2}$$

The complexity of the realization of the operators $\Xi(U_a)$ and $\Xi(iU_a)$ depends on the complexity of the operator $\Lambda(U_a)$, which is not much higher than the complexity of the operator U. Thus, $\Xi(U_a)$ and $\Xi(iU_a)$ can be realized by quantum circuits of size $O(n^2)$ in the standard basis.

Example

Suppose that we have $\lambda_k = e^{2\pi i * 0.2}$ for our operator U, and so we apply $\Xi(U)$ to $|0\rangle \otimes |\xi\rangle$:

$$\Xi(U)(|0\rangle \otimes |\xi\rangle)$$

$$= \left(\frac{1 + e^{2\pi i * 0.2}}{2}|0\rangle + \frac{1 - e^{2\pi i * 0.2}}{2}|1\rangle\right) \otimes |\xi\rangle$$

We get conditional probabilities:

$$P(0) = \frac{1 + \cos(2\pi * 0.2)}{2} = \frac{1 + 0.309}{2} = 0.6545$$

and

$$P(1) = \frac{1 - \cos(2\pi * 0.2)}{2} = 0.3455$$

Example

Suppose that we have $\lambda_k = e^{2\pi i * 0.2}$ for our operator U, and so we apply $\Xi(iU)$ to $|0\rangle \otimes |\xi\rangle$

We get conditional probabilities:

$$P(0) = \frac{1 - \sin(2\pi * 0.2)}{2} = \frac{1 - 0.95}{2} = 0.025$$

and

$$P(1) = \frac{1 + \sin(2\pi * 0.2)}{2} = 0.975$$

Procedure for finding a nontrivial divisor

Input. An integer y ($y > 1$).

Step 1. Check y for parity. If y is even, then give the answer "2"; otherwise proceed to Step 2.

Step 2. Check whether y is the k-th power of an integer for $k = 2, \ldots, \log_2 y$. If $y = m^k$, then give the answer "m"; otherwise proceed to Step 3.

Step 3. Choose an integer a randomly and uniformly between 1 and $y - 1$. Compute $b = \gcd(a, \boldsymbol{y})$ (say, by Euclid's algorithm). If $b > 1$, then give the answer "b"; otherwise proceed to Step 4.

Procedure for finding a nontrivial divisor

Step 4. Compute $r = per_y(a)$ (using the period finding algorithm that we assume we have). If r is odd, then the answer is "y is prime" (which means that we give up finding a nontrivial divisor). Otherwise proceed to Step 5.

Step 5. Compute $d = \gcd(a^{r/2} - 1, y)$. If $d > 1$, then the answer is "d"; otherwise the answer is "y is prime".

Procedure for finding a nontrivial divisor

Step 4. Compute $r = per_y(a)$.

Step 5. Compute $d = \gcd(a^{r/2} - 1, y)$. If $d > 1$, then the answer is "d"; otherwise the answer is "y is prime".

For example, if $y = 21$ and:

- if $a = 2$, algorithm will find $d = 7$: $r = 6$, because $2^6 = 64 = 1(mod\ 21)$; $\gcd(2^3 - 1,21) = 7$.
- if $a = 5$ will fail to find $d > 1$: $r = 6$, because $5^6 = 64 = 1(mod\ 21)$; $\gcd(5^3 - 1, y) = \gcd(124,21) = 1$

The quantum analogue of NP: the class BQNP

BQNP definition

A function $F\colon B^n \to \{0,1,\text{“}undefined\text{”}\}$ belongs to the class BQNP if there exists a polynomial classical algorithm that computes a function $x \to Z(x)$, where $Z(x)$ is a description of a quantum circuit, realizing an operator $U_x\colon B^{\otimes N_x} \to B^{\otimes N_x}$ such that

$$F(x)=1 \implies \exists\,|\xi\rangle \in \mathcal{B}^{\otimes m_x}\ \mathbf{P}\Big(U_x|\xi\rangle \otimes |0^{N_x-m_x}\rangle,\ \mathcal{M}\Big) \geq p_1,$$

$$F(x)=0 \implies \forall\,|\xi\rangle \in \mathcal{B}^{\otimes m_x}\ \mathbf{P}\Big(U_x|\xi\rangle \otimes |0^{N_x-m_x}\rangle,\ \mathcal{M}\Big) \leq p_0.$$

k-local Hamiltonian

An operator H: $B^{\otimes n} \to B^{\otimes n}$ is called a k-local Hamiltonian if it is expressible in the form

$$H = \sum_j H_j[S_j]$$

where each term $H_j \in L(B^{\otimes |S_j|})$ is a Hermitian operator acting on a set of qubits S_j, $|S_j| \leq k$.

In addition, authors put a normalization condition, namely, $0 \leq H_j \leq 1$, meaning that both H_j and $I - H_j$ are nonnegative.

The local Hamiltonian

z={description of a k-local Hamiltonian H, a, b} where $k = O(1)$, $0 \leq a < b$, $b - a = \Omega(n^{-\alpha})$ ($\alpha > 0$ is a constant). Then

- $F(x) = 1 \iff H$ has an eigenvalue not exceeding a,
- $F(x) = 0 \iff$ all eigenvalues of H are greater than b.

LH belongs to BQNP

$$H = \sum_j H_j[S_j]$$

Authors construct a circuit W that can be applied to a state $|\eta\rangle \in B^{\otimes n}$ so as to produce a result 1 or 0 (“yes” or “no”): it says whether Arthur accepts the submitted state or not.

The answer "yes" will occur with probability $p = 1 - r^{-1}\langle\eta|H|\eta\rangle$.

Number of terms r means how many such $H_j[S_j]$ we have.

Example

Suppose that we have 1-local Hamiltonian

$$H = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

And state $|\eta\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

The answer "yes" will occur with probability $p = 1 - 2^{-1}\langle\eta|H|\eta\rangle = 1 - \frac{\langle\eta|H|\eta\rangle}{2}$.

Example

$$\langle \eta | H | \eta \rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 1 + 0 + 0 + 0 = 1$$

The answer "yes" will occur with probability $p = 1 - \frac{1}{2} = \frac{1}{2}$.

Classical and quantum codes

Classical code example

$$M_3 = \{(0,0,0), (1,1,1)\} \subseteq B^3$$

$$d(M) = \min\{d(x1, x2): x1, x2 \in M, x1 \neq x2\}$$

For the code M_3 the code distance is 3.

A code M corrects k errors if and only if $d(M) > 2k$.

One error for $(0,0,0)$ results in one of the following state: $(1,0,0)$, $(0,1,0)$, $(0,0,1)$

One error for $(1,1,1)$ results in one of the following state: $(0,1,1)$, $(1,0,1)$, $(1,1,0)$

We can easily distinguish between first 3 cases and last 2 cases. Using Majority function.

Hamming code example

We pick $r = 2$, so we get code $(2^r - 1, 2^r - 1 - r) = (3,1)$.

So code consists of 3-bit strings, and according to Hamming code check sums, we get

x**1**0 + x**1**1 = 0

x0**1** + x1**1** = 0

Strings 000 and 111 satisfy both conditions, so we get a code that is equal to repetition code.

Toric code example

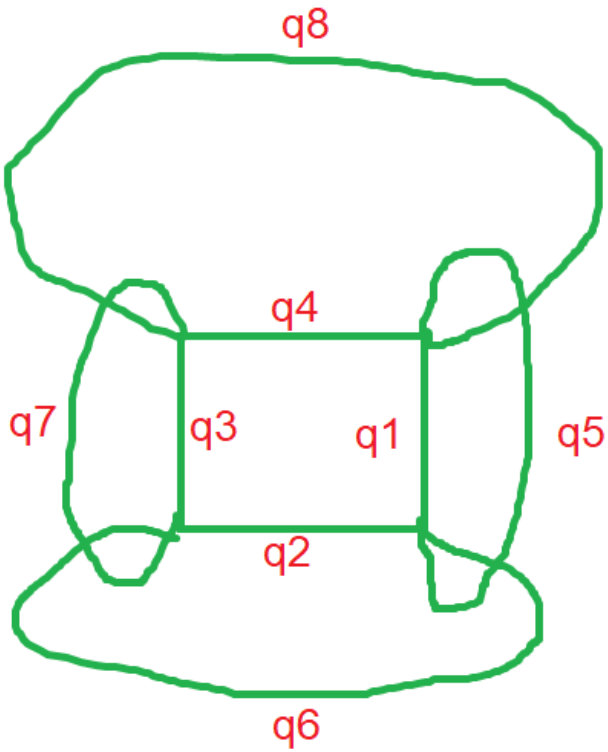
We have $r = 2$, which means 2×2 lattice on a torus. We have $2r^2 = 8$ qubits.

Type I operators:

$\sigma_1^x \sigma_4^x \sigma_5^x \sigma_8^x$, $\sigma_1^x \sigma_2^x \sigma_5^x \sigma_6^x$, $\sigma_2^x \sigma_6^x \sigma_7^x \sigma_3^x$, $\sigma_3^x \sigma_4^x \sigma_7^x \sigma_8^x$

Type II operators:

$\sigma_1^z \sigma_2^z \sigma_3^z \sigma_4^z$, $\sigma_1^z \sigma_6^z \sigma_3^z \sigma_8^z$, $\sigma_5^z \sigma_2^z \sigma_7^z \sigma_4^z$, $\sigma_5^z \sigma_6^z \sigma_7^z \sigma_8^z$



Thank you for your attention!