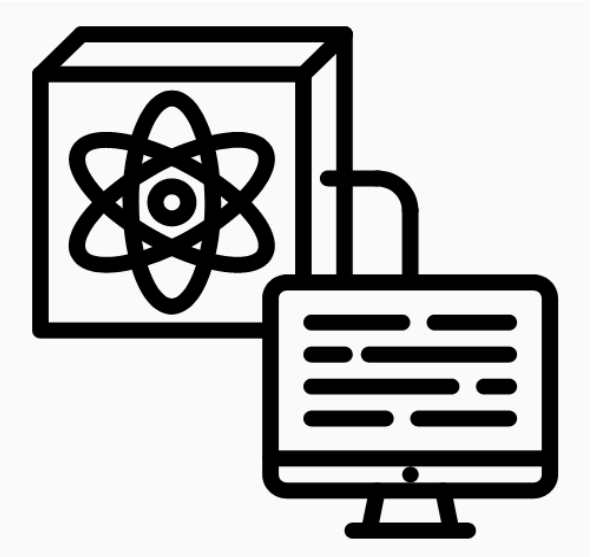
Quantum Algorithms
Lecture 9
Quantum Computation - Definitions and notation

Zhejiang University

Introduction

Quantum computers

The internal work of classical computers is based on operations with 0s and 1s, while in Nature there is possibility of performing unitary transformations (we will discuss them later). Devices (real or imaginary) using this possibility, which is described by quantum mechanics, are called quantum computers.



Power of Quantum

It is not clear a priori whether the computational power is really increased in passing from Boolean functions to unitary transformations on finite-dimensional spaces. However, there is strong evidence that such an increase is actually achieved.

Example – factoring problem. For given n, find p and q such that $n = p * q$. Quantumly – polynomial time, classically – may be exponential time.

Classical bits

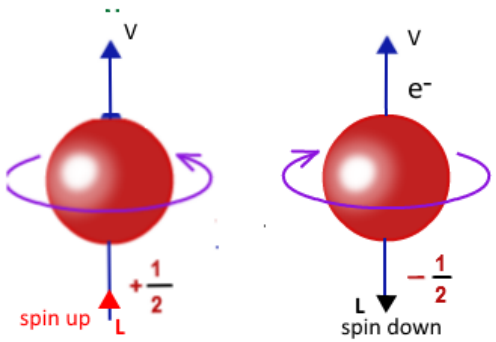
Classical computers operate with states built from a finite number of bits. The state of the whole system is given by specifying the values of all the bits (each bit 0 or 1). Therefore, the set of states $B^n = \{0,1\}^n$ is finite and has cardinality 2^n.

Quantum bits - qubits

The 2^n assignments of individual states to each qubit do not yield all possible states of the system, but they form a basis in a space of states. Arbitrary linear combinations of the basis states, with complex coefficients, are also possible.

2^n basis states $|x_1, \ldots, x_n>$

$\sum_{x_1,\ldots,x_n} c_{x_1,\ldots,x_n} |x_1, \ldots, x_n>$ is also a possible state of the system; here $c_{x_1,\ldots,x_n}$ are complex numbers called amplitudes.



Arbitrary quantum state

An arbitrary state of the system may be represented in the form

$$|\psi\rangle = \sum_{(x_1,\ldots,x_n)\in B^n} c_{x_1,\ldots,x_n} |x_1, \quad \ldots, x_n >$$

where $\sum_{(x_1,\ldots,x_n)\in B^n} \left|c_{x_1,\ldots,x_n}\right|^2 = 1.$

The state space for such a system is a linear space of dimension 2^n over the field $\mathbb{C}$ of complex numbers.

State

of an ordinary computer

$\square \ \square \ \cdots \ \square$ bits

$x_1 \ x_2 \ \ldots \ x_n \ \ x_j \in \mathbb{B}$

of a quantum computer

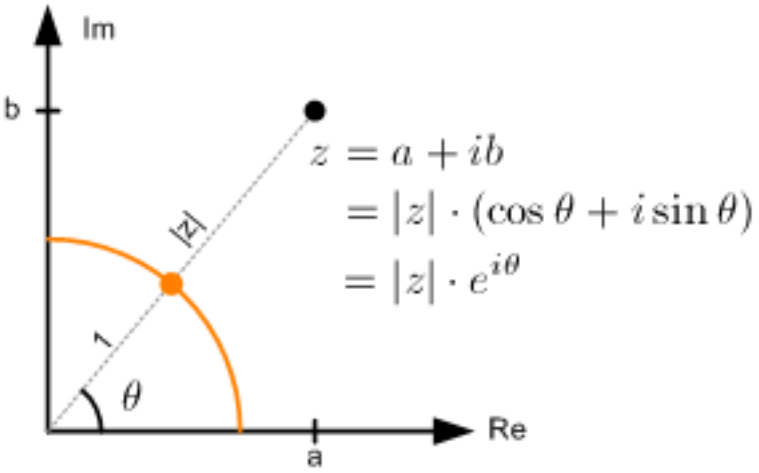
$\square \ \square \ \cdots \ \square$ qubits

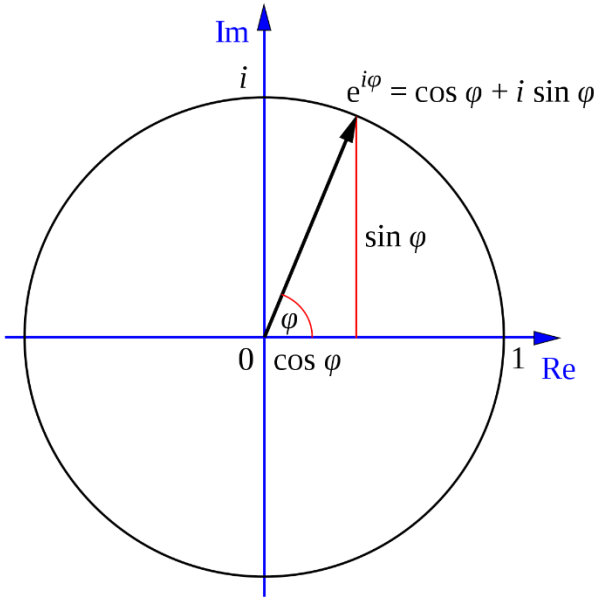
basis: $|x_1, \ x_2, \ \ldots, \ x_n\rangle, \qquad x_j \in \mathbb{B}$

arbitrary: $\sum_{x \in \mathbb{B}^n} c_x |x\rangle$, where $\sum_{x \in \mathbb{B}^n} |c_x|^2 = 1$

Global phase

If we multiply the vector $\sum_x c_x|x\rangle$ by a phase factor $e^{i\phi}$ (ϕ real), we obtain a physically indistinguishable state. Therefore, a state of a quantum computer is a unit vector defined up to a phase factor.





Transformations

Computation may be imagined as a sequence of transformations on the set of states of the system.

Classical case:	**Quantum case:**
transformations are functions from $\mathbb{B}^n$ to $\mathbb{B}^n$.	transformations are unitary operators, i.e., operators that preserve the length $\sum_{x \in \mathbb{B}^n} \lvert c_x \rvert^2$ of each vector $\sum_{x \in \mathbb{B}^n} c_x \lvert x \rangle$.

Remarks

All that has been said pertains only to isolated systems. A real quantum computer is (will be) a part of a larger system (the Universe), interacting with the remaining world. Quantum states and transformations of open systems will be considered later.

We can define both quantum Turing machines and quantum circuits. In the book the second approach is chosen, which is more convenient for a number of reasons.

The tensor product

Tensor product of qubits

A system of n qubits has a state space $\mathbb{C}^{2^n}$, which can be represented as a tensor product, $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes n}$. The factors correspond to a space of a single qubit.

Linear spaces

The tensor product of linear spaces L and M can be defined as an arbitrary space N of dimension (dim L)(dim M). The idea is that if L and M are endowed with some bases, $\{e_1, \ldots, e_l\} \subseteq L$ and $\{f_1, \ldots, f_m\} \subseteq M$, then N possesses a standard basis whose elements are associated with pairs (e_j, f_k).

Linear spaces

We denote these elements by $e_j \otimes f_k$, thus the basis is

$$\{e_j \otimes f_k : \text{j} = 1,...,\text{l};\ \text{k} = 1,...,\text{m}\}$$

Using this basis, one can define the tensor product of arbitrary two vectors, $\text{u} = \sum_j u_j e_j$ and $\text{v} = \sum_k v_k f_k$ (u_j, $v_k \in \mathbb{C}$) in such a way that the map $\otimes$: $(u, v) \rightarrow u \otimes v$ is linear in both u and v:
$u \otimes v = \sum_{j,k} \left(u_j v_k\right) e_j \otimes f_k$.

Tensor product - example

$$|\psi\rangle = a|0\rangle + b|1\rangle$$
$$|\varphi\rangle = c|0\rangle + d|1\rangle$$
$$|\psi\rangle \otimes |\varphi\rangle = (ac)|0\rangle \otimes |0\rangle + (ad)|0\rangle \otimes |1\rangle + (bc)|1\rangle \otimes |0\rangle + (bd)|1\rangle \otimes |1\rangle$$

Pedestrian definition

Previous definition is not invariant, i.e., it depends on the choice of bases in L and M. An invariant definition is abstract and hard to grasp, but it is indispensable if we really want to prove something.

Universality property

The tensor product of two spaces, L and M, is a space $N = L \otimes M$, together with a bilinear map $H\colon L \times M \to N$ (also denoted by $\otimes$, i.e., $u \otimes v = H(u, v)$) which satisfy the following universality property:

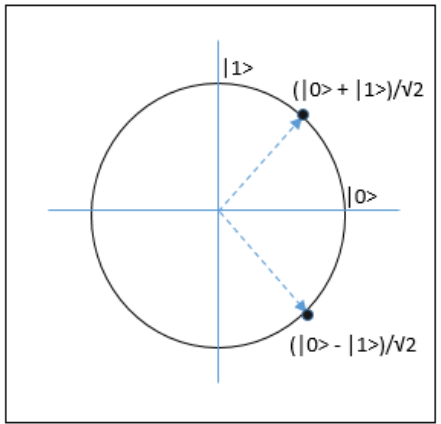
for any space S and any bilinear function $F\colon L \times M \to S$, there is a unique linear function $G\colon L \otimes M \to S$ such that $F(u, v) = G(u \otimes v)$ (for every pair of $u \in L$, $v \in M$.)

Linear algebra in Dirac's notation

Classical basis

Prechosen classical basis: $\{|0\rangle, |1\rangle\}$ for $\mathbb{C}^2$, and $\{|x_1, \dots, x_n\rangle, : x_j \in B\}$ for $(\mathbb{C}^2)^{\otimes n}$. The space $\mathbb{C}^2$ furnished with a basis is denoted by B. The basis is considered orthonormal, which yields an inner product on the space of states.

Orthonormal basis - formed by orthonormal vectors. Vectors are orthonormal if they are orthogonal (or perpendicular along a line) unit vectors (length of vector is equal to 1).



Amplitudes

The coefficients $c_{x_1,\ldots,x_n}$ of the decomposition of a vector $|\psi\rangle$ relative to this basis are called amplitudes. Their physical meaning is that the square of the absolute value $\left|c_{x_1,\ldots,x_n}\right|^2$ of the amplitude is interpreted as the probability of finding the system in the given state of the basis.

$$\sum_{(x_1,\ldots,x_n)\in B^n}\left|c_{x_1,\ldots,x_n}\right|^2 = 1.$$

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:

$|\xi\rangle = a|0\rangle + b|1\rangle$

$|\eta\rangle = c|0\rangle + d|1\rangle$

$\langle\xi|\eta\rangle = a^*c + b^*d$

Hermitian

The inner product is Hermitian. It is conjugate-linear in the first argument and linear in the second:

$$\langle \xi_1 + \xi_2 | \eta \rangle = \langle \xi_1 | \eta \rangle + \langle \xi_2 | \eta \rangle$$
$$\langle \xi | \eta_1 + \eta_2 \rangle = \langle \xi | \eta_1 \rangle + \langle \xi | \eta_2 \rangle$$
$$\langle c\xi | \eta \rangle = c^* \langle \xi | \eta \rangle$$
$$\langle \xi | c\eta \rangle = c \langle \xi | \eta \rangle$$

Bra- and ket- vectors

$$\langle\xi| = {c_0}^*\langle 0| + {c_1}^*\langle 1| = ({c_0}^*, {c_1}^*)$$

$$|\xi\rangle = c_0|0\rangle + c_1|1\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

Bra- and ket-vectors are in a one-to-one correspondence to one another. (Nonetheless, it is necessary to distinguish them in some way — and it is just for this purpose the angle brackets were introduced.)

$$\langle c\xi| = c^*\langle\xi|$$

Linear operator A

$\langle\xi|A|\eta\rangle$ can be interpreted in two ways:

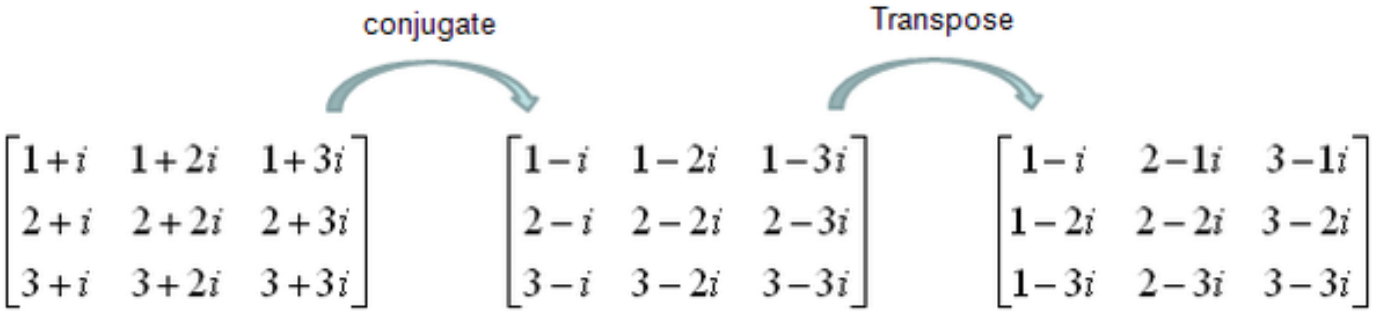
- product of $\langle\xi|$ and $A|\eta\rangle$;
- product of $\langle\xi|A$ and $|\eta\rangle$.

Linear functional $\langle\psi| = \langle\xi|A$, so we get $|\psi\rangle = A^\dagger|\xi\rangle$, $\langle\psi| = \langle A^\dagger\xi|$.

$A^\dagger$ is Hermitian adjoint to A.

$\langle A^\dagger\xi|\eta\rangle = \langle\xi|A|\eta\rangle$

Hermitian adjoint:



Operators as matrices

Operators can be specified as matrices relative to the classical basis (or any other orthonormal basis):

$A = \sum_{j,k} a_{j,k} |j\rangle \langle k|$, where $a_{j,k} = \langle j|A|k\rangle$.

$|j\rangle\langle k|$ is a linear operator $(|j\rangle\langle k|)|\xi\rangle = \langle k|\xi\rangle|j\rangle$.

Linear operators

The set of linear operators on a space M is denoted by $L(M)$. Sometimes we will have to consider linear maps between different spaces, say, from N to M. The space of such maps is denoted by $L(N, M)$. It is naturally isomorphic to $M \otimes N^*$: the isomorphism takes an operator $\sum_{j,k} a_{j,k} |j\rangle \langle k| \in L(N, M)$ to the vector $\sum_{j,k} a_{j,k} |j\rangle \otimes \langle k| \in M \otimes N^*$.

Unitary operator

A unitary operator on a space M is an invertible operator that preserves the inner product. The condition

$$\langle \eta|\xi\rangle = \langle U\eta|U|\xi\rangle = \left\langle \eta\middle|U^{\dagger}U\middle|\xi\right\rangle$$

is equivalent to $U^{\dagger}U = I$ (where I is the identity operator). Since the space M has finite dimension, the above condition implies that $|detU| = 1$, so the existence of U^{-1} follows automatically. Unitary operators can also be characterized by the property $U^{-1} = U^{\dagger}$. The set of unitary operators is denoted by $U(M)$.

Inner product

Our definition of the inner product in $B^{\otimes n}$ is consistent with the tensor product:

$$(\langle\xi_1| \otimes \langle\xi_2|)(|\eta_1\rangle \otimes |\eta_2\rangle) = \langle\xi_1|\eta_1\rangle\langle\xi_2|\eta_2\rangle$$

Tensor product of operators

It is an operator acting on the tensor product of the spaces on which the factors act. The action is defined by the rule

$(\mathrm{A} \otimes \mathrm{B})|\xi\rangle \otimes |\eta\rangle = \mathrm{A}|\xi\rangle \otimes B|\eta\rangle$.

If the operators are given in the matrix form relative to some basis $\mathrm{A} = \sum_{j,k} a_{j,k}|j\rangle\langle k|$ and $\mathrm{B} = \sum_{j,k} b_{j,k}|j\rangle\langle k|$, then the matrix elements of the operator $C = A \otimes B$ have the form $c_{(j,k)(l,m)} = a_{j,l}b_{k,m}$.

Quantum gates and circuits

Elementary transformation

Computation consists of transformations, regarded as elementary and performed one at a time.

Elementary transformation **in the classical case:** a map from $\mathbb{B}^n$ to $\mathbb{B}^n$ which alters and depends upon a small number (not depending on n) of bits; the remaining bits are not used.

Elementary transformation **in the quantum case**: the tensor product of an arbitrary unitary operator acting on a small number ($r = O(1)$) of qubits, denoted altogether by $\mathcal{B}^{\otimes r}$, and the identity operator acting on the remaining qubits.

Operator applied to register

The tensor product of an operator U acting on an ordered set A of qubits and the identity operator acting on the remaining qubits, is denoted by $U[A]$. In this situation, we say that the operator U is applied to the register A. This definition is somewhat vague, but the formal construction of the operator $U[A]$ is pretty straightforward.

Operator applied to register

First, let us define $X[A]$ when A consists of just one qubit, say p. In this case, $X[p] = I_{B^{\otimes(p-1)}} \otimes X \otimes I_{B^{\otimes(n-p)}}$. Note that $X[p]$ and $Y[q]$ commute if $p \neq q$. In the general case $A = (p1, \ldots, pr)$, we can represent U as:

$U = \sum_m X_{m,1} \otimes \cdots \otimes X_{m,r}$,

where $X_{m,1}, \ldots, X_{m,r} \in L(B)$ are arbitrary one-qubit operators. Then, by definition

$$U[p1, \ldots, pr] = \sum_m X_{m,1}[p1] \ldots X_{m,r}[pr]$$

Operator applied to register

The result does not depend on the choice of the representation $U = \sum_m X_{m,1} \otimes \cdots \otimes X_{m,r}$ due to the universality property of the tensor product. In the case at hand, we have a multilinear map $F(X_{m,1}, \ldots, X_{m,r}) = X_{m,1}[p1] \ldots X_{m,r}[pr]$, whereas the corresponding linear map
$G\colon U \to U[p1, \ldots, pr]\colon L(B^{\otimes r}) \to L(B^{\otimes n})$
is given by $U[p1, \ldots, pr] = \sum_m X_{m,1}[p1] \ldots X_{m,r}[pr]$

Example

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>.

Complexity – elementary step

At this point the computational complexity begins, which makes quantum computers so powerful. Let U act on two qubits, i.e., U is a 4×4 matrix. Then $U[1,2] = U \bigotimes I$ is a matrix of size $2^n \times 2^n$ that consists of 2^{n-2} copies of U placed along the principal diagonal. This matrix represents one elementary step.

Complexity – exponential power

When we apply several such operators to various pairs of qubits, the result will appear considerably more complicated. There is no obvious way of determining this result, apart from direct multiplication of the corresponding matrices. Inasmuch as the size of the matrices is exponentially large, exponential time is required for their multiplication.

Calculation in poly-space

Chapter 12.3 from
https://arxiv.org/abs/1907.09415

It is possible to simulate quantum computation without the need to store amplitudes of all 2^n states for n qubits. The chapter shows that quantum system can actually be simulated efficiently in terms of space, though not necessarily in terms of time.

Calculation in poly-space

We remark, however, that the calculation of matrix elements is possible with polynomially bounded memory. Suppose we need to find the matrix element U_{xy} of the operator

$$U = U^{(l)}[j_l, k_l]U^{(l-1)}[j_{l-1}, k_{l-1}] \cdots U^{(2)}[j_2, k_2]U^{(1)}[j_1, k_1].$$

It is obvious that

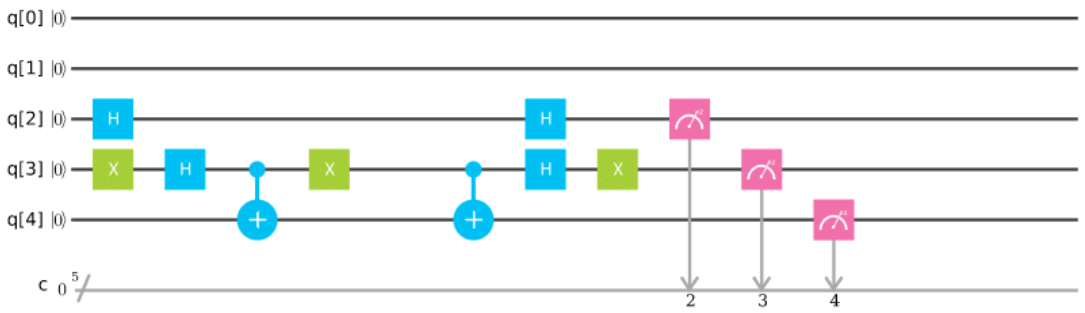
$$\left(U^{(l)} \cdots U^{(1)}\right)_{x_l x_0} = \sum_{x_{l-1},\ldots,x_1} U^{(l)}_{x_l x_{l-1}} \cdots U^{(1)}_{x_1 x_0}.$$

(Here $x_0, \ldots, x_l$ are n-bit strings.) To compute this sum, it suffices to allocate $l-1$ registers for keeping the current values of $x_{l-1}, \ldots, x_1$, one register for keeping the partial sum, and some constant number of registers for the calculation of the product $U^{(l)}_{x_l x_{l-1}} \cdots U^{(1)}_{x_1 x_0}$.

Quantum circuit

Let A be a fixed set of unitary operators. (We call A a basis, or a gate set, whereas its elements are called gates.) A quantum circuit over the basis A is a sequence $U_1[A_1], \ldots, U_L[A_L]$, where $U_j \in A$, and A_j is an ordered set of qubits.

The operator realized by the circuit is $U = U_L[A_L] \cdots U_1[A_1]$ (U: $B^{\otimes n} \to B^{\otimes n}$). The number L is called the size of the circuit.



Inversion operators

We usually assume that A is closed under inversion: if $X \in A$, then $X^{-1} \in A$. In this case U and U^{-1} are realized by circuits of the same size.

Depth of the circuit

Note that several gates, say $U_{j_1}, \ldots, U_{j_s}$, can be applied simultaneously to disjoint sets of qubits (such that $A_{j_a} \cap A_{j_b} = \emptyset$ if $a \neq b$). We say that a circuit has depth $\leq d$ if it can be arranged in d layers of simultaneously applied gates.

Depth of the circuit

The depth can be also characterized as the maximum length of a path from input to output. (By a path we mean a sequence of gates $U_{k_1}, \ldots, U_{k_d}$ $(k_1 < \cdots < k_d)$ such that each pair of adjacent gates, k_l and k_{l+1}, share a qubit they act upon, but no other gate acts on this qubit between the applications of U_{k_l} and $U_{k_{l+1}}$.)

Ancilla qubits

The previous definition is not perfect because it ignores the possibility to use additional qubits (ancillas) in the computational process. Therefore we give yet another definition.

Ancillas can be considered as extra qubits that are not included into input/output.

QC with ancillas

Operator realized by a quantum circuit using ancillas is an operator U: $B^{\otimes n} \to B^{\otimes n}$ such that the product $W = U_L[A_L] \cdots U_1[A_1]$, acting on N qubits ($N \geq n$), satisfies the condition $W(|\xi\rangle \otimes |0^{N-n}\rangle) = (U|\xi\rangle) \otimes |0^{N-n}\rangle$ for any vector $|\xi\rangle \in B^{\otimes n}$.

QC with ancillas

In this manner we "borrow" additional memory, filled with zeros, that we must ultimately return to its prior state. What sense does such a definition make? Why is it necessary to insist that the additional qubits return to the state $|0^{N-n}\rangle$? Actually, this condition is rather technical.

QC with ancillas

It is important that at the end of the computation the quantum state is a product state, i.e., has the form $|\xi'\rangle \otimes |\eta'\rangle$ (with arbitrary $|\eta'\rangle$). If this is the case, then the first subsystem will be in the specified state $|\xi'\rangle$, so that the second subsystem (the added memory) may be forgotten. In the opposite case, the joint state of the two subsystems will be entangled, so that the first subsystem cannot be separated from the second.

Thank you for your attention!