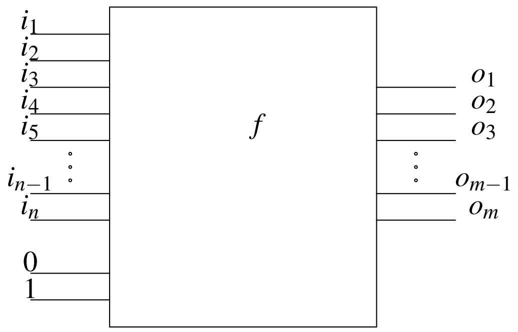
CS 294-2 Quantum Circuit Model, Solovay-Kitaev Theorem, BQP
9/11/04
Fall 2004 Lecture 4

1 Quantum Circuit Model

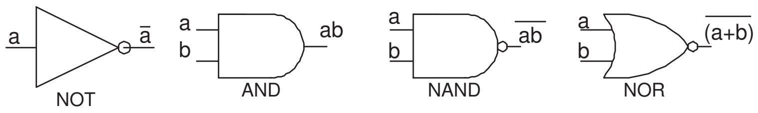
1.1 Classical Circuits - Universal Gate Sets

A classical circuit implements a multi-output boolean function $f : \{0,1\}^n \to \{0,1\}^m$, given as primitive a finite collection of gates each of which implements a boolean function on k bits for some small k. The picture of the circuit is as follows:



where the box contains a finite number of gates from the given collection.

Examples of gates that are commonly used are the following:



There exist finite gate sets that can be used to implement every multi-output boolean function. Such sets are called *universal gate sets* and the following gate sets can easily be proved universal:

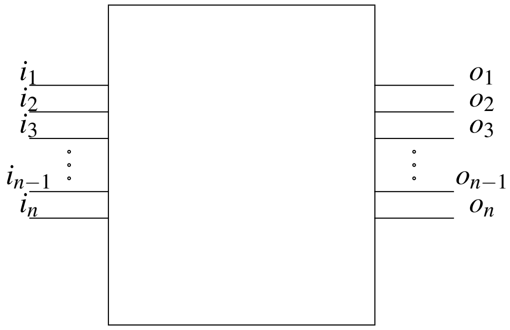
- {AND, NOT}
- {OR, NOT}
- {NAND}
- {NOR}

Every boolean function can be implemented using gates from a universal gate set. This implies that the circuit complexity (number of gates in the minimum circuit) is the same with respect to any finite universal gate set up to a constant factor.

A subtle point when we consider circuit design is the fan out. In classical circuits we can take fan out as granted, because fan out is trivially implemented in classical reality. However, this is not trivial in quantum mechanics as we'll see shortly.

1.2 Quantum Circuits

A quantum circuit implements a unitary operator in a Hilbert space $\mathbb{C}^{2^n}$, given as primitive a (usually finite) collection of gates each of which implements a unitary operator on k qubits for some small k. Unitarity implies that quantum circuits have the same number of inputs and outputs. The picture of a quantum circuit is as follows:



where the box contains a finite number of quantum gates.

Clearly no finite set of gates can generate all unitary operators. If such a set existed, then for all values of $\theta \in \Re$ we should be able to built up a quantum circuit for the operator R_θ using gates from this set. With a finite set of gates that's impossible.

It seems though that we need a notion of approximation to define universality. For that purpose we'll use the operator norm which is defined as $||B|| = \max_{|\vec{v}|=1} |B\vec{v}|$ for every operator B. Using that measure the *distance between operators U and U'* will be:

$$||U - U'|| = \max_{|\vec{v}|=1} |(U - U')\vec{v}|$$

and we'll say that *operator U' simulates operator U to within ε* if $||U - U'|| \leq \varepsilon$

After the above definitions it's interesting to see how we define the universality in quantum mechanics.

We shall call a set G of quantum gates universal if:

$$\forall U \text{ (unitary operator on k qubits) }, \forall \varepsilon > 0, \exists g_1, g_2, \ldots, g_l \in G : ||U - U_{g_1} U_{g_2} \ldots U_{g_l}|| \leq \varepsilon$$

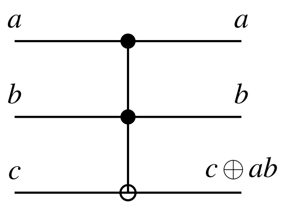
where by U_{g_i} ("usage of g_i") we represent the tensor product of the gate g_i with the identity operator for an appropriate number of qubits so that U_{g_i} is a unitary operator for k qubits whereas g_i might be a unitary operator for less than k qubits.

1.3 Known Universal Gate Families for Quantum Mechanics

The following families of circuits are universal:

- CNOT, all 1-qubit gates
- CNOT gate, Hadamard gate, suitable phase flips
- Tofolli gate, Hadamard gate

where the Tofolli gate (or C-CNOT gate for "controlled-controlled NOT gate") is a three-qubit gate that complements the third bit if the first two control bits are both 1.



2 Solovay-Kitaev Theorem

The Solovay-Kitaev theorem states the following:

If $G \subseteq SU(d)$ is a universal family of gates (where $SU(d)$ is the group of unitary operators in a d-dimensional Hilbert space), G is closed under inverse (i.e. $g \in G \Leftrightarrow g^{-1} \in G$) and G generates a dense subset of SU(d), then $\forall U \in SU(d), \varepsilon > 0, \exists g_1, g_2, \ldots, g_l \in G : ||U - U_{g_1}U_{g_2}\ldots U_{g_l}|| \leq \varepsilon$ and $l = O(\log^2 1/\varepsilon)$

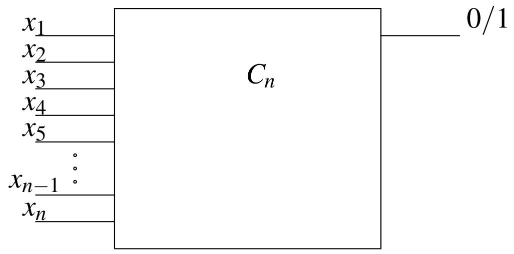
3 Complexity Classes - Class BQP

3.1 Class P - Polynomial Time

A definition of the class P in terms of circuits is the following:

$L \in P$ iff there is a family $\mathfrak{F} = \{C_n\}_{n\in\mathbb{N}}$ of circuits such that:

- $|C_n| \leq poly(n), \forall n \in \mathbb{N}$
- there is a polynomial time Turing Machine that on input 1^n outputs C_n (*Uniformity Condition*)
- if $|x| = n$ then $C_n(x) = (c \in L?)$



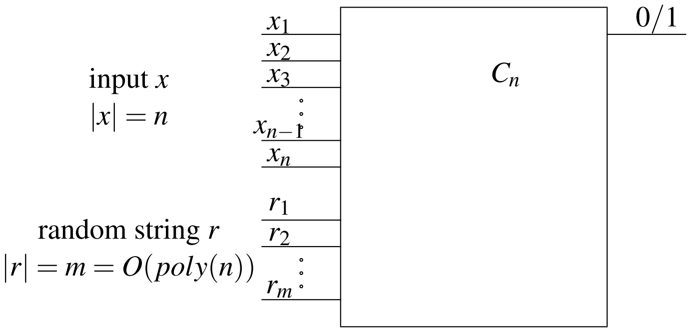
3.2 Class BPP - Bounded Error Polynomial Time

A definition of the class BPP in terms of circuits is the following:

$L \in BPP$ iff there is a family $\mathfrak{F} = \{C_n\}_{n\in\mathbb{N}}$ of circuits such that:

- every circuit C_n has an input x of $|x| = n$ bits and a random input r of $|r| = O(poly(n))$ bits

- $|C_n| \leq poly(n), \forall n \in \mathbb{N}$
- there is a polynomial time Turing Machine that on input 1^n outputs C_n (*Uniformity Condition*)
- moreover:
  - if $x \in L$ and $|x| = n$ then $Pr[C_n(x,r) = \text{"}yes\text{"}] \geq 2/3$
  - if $x \notin L$ and $|x| = n$ then $Pr[C_n(x,r) = \text{"}no\text{"}] \geq 2/3$

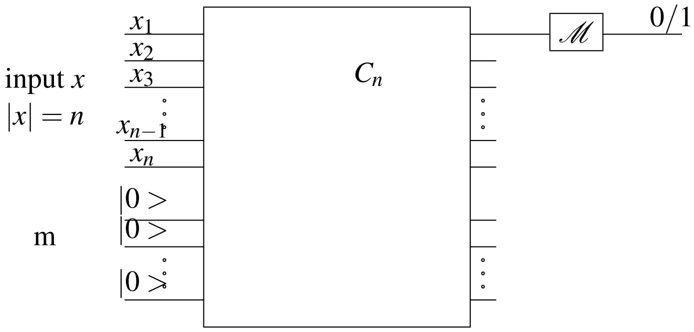


3.3 Class BQP - Bounded Error Quantum Polynomial Time

A definition of the class BQP in terms of circuits is the following:

$L \in BQP$ iff there is a family $\mathfrak{F} = \{C_n \in SU(n)\}_{n \in \mathbb{N}}$ of quantum circuits (unitary operators) such that:

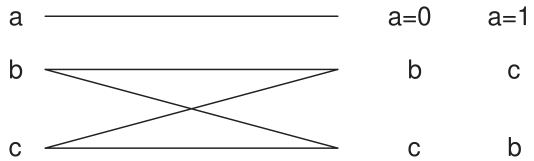
- every circuit C_n has an input x of $|x| = n$ bits and $m = O(poly(n))$ additional inputs of value $|0>$
- the output of the computation is considered to be the outcome of the measurement on the first output of the circuit
- $|C_n| \leq poly(n), \forall n \in \mathbb{N}$
- there is a polynomial time Turing Machine that on input 1^n outputs C_n (*Uniformity Condition*)
- moreover:
  - if $x \in L$ and $|x| = n$ then $Pr[measure = 1] \geq 2/3$
  - if $x \notin L$ and $|x| = n$ then $Pr[measure = 0] \geq 2/3$



3.4 Reversibility and $P \subseteq BQP$

Quantum evolution is unitary and every quantum circuit K corresponds to a unitary operator U_K in some Hilbert space. U_K being unitary means that $U_K U_K^\dagger = U_K^\dagger U_K = I$, which means that U_K has an inverse operator. Thus every quantum circuit is reversible.

This is not the case for classical circuits, however. For example if we have an AND gate, then going from two input bits to one output bit involves some loss of information, which makes reversibility infeasible. However, starting from a nonreversible circuit we can construct a reversible circuit that does the same computation but may require more inputs or outputs than the initial nonreversible circuit. There are a number of ways to do this and here we will show how to do it using the controlled swap gate (Fredkin gate). The controlled swap gate on input (a,b,c) outputs (a,b,c), if $a=0$, and (a,c,b), if $a=1$. It's obvious that the controlled swap gate is the inverse of itself. We use the following notation for the controlled swap gate.



Since the set of classical gates $\{AND, NOT\}$ is universal, every classical circuit can be built using these two gates, as well as possibly fanning out. Thus, in order to prove that every classical circuit can be extended to a reversible one, we only have to show that we can simulate the AND and NOT gates, as well as fan out, using the controlled swap gate. The extra inputs that we supposed will come in handy.

In order to simulate the NOT gate via the controlled swap gate we can give the latter the triplet $(a, b=0, c=1)$ as input. Then at the third output we always get a'.

In order to simulate the AND gate via the controlled swap gate we can give the latter the triplet $(a, b, c=0)$ as input. Then at the third output we always get ab.

Finally, in order to fan out as permitted in classical circuits via the controlled swap gate, we can give the latter the triplet $(a, b=0, c=1)$ as input. Then the first and second outputs always have the value a.

It's obvious that the reversible circuit that corresponds to a classical circuit and is constructed in the above way will have exactly the same output as the classical one on classical inputs. Thus, the above construction shows as well that $P \subseteq BQP$.