QUANTUM COMPUTING 4.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

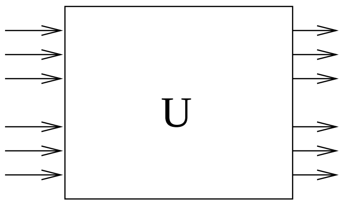
October 22, 2002

4. QUANTUM GATES and CIRCUITS

Several simple quantum gates form elementary building blocks from which any quantum circuit can be built. Quantum circuits are the most easy to deal with model of quantum computations.

QUANTUM GATES — SIMPLE EXAMPLES

Unitarity is the main new requirement quantum gates have to satisfy.



Definition 0.1 *A* **quantum gate** *with n inputs and n outputs is specified by a unitary operator $U : \mathcal{H}_{2^n} \rightarrow \mathcal{H}_{2^n}$, and it is represented by a unitary matrix A_U of degree 2^n.*

Example 0.2 *The so-called Hadamard (rotation) gates are represented by matrices*

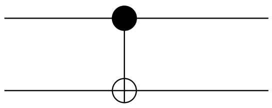
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad H' = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad H'' = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Example 0.3 *The following one parameter set of* **rotation gates** *(represented by matrices) is also often used:*

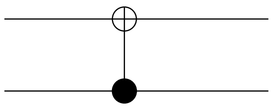
$$R_x(\theta) = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}, \quad R_y(\theta) = \begin{pmatrix} i\cos\theta & \sin\theta \\ \sin\theta & i\cos\theta \end{pmatrix},$$

$$R_z(\theta) = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix},$$

h



h



QUANTUM GATES → UNITARY MATRICES

Unitary matrix for XOR-gate

has the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

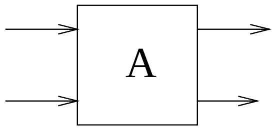
What is the unitary matrix representing the “inverse XOR gate”?

It has the form

$$\begin{pmatrix} . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \end{pmatrix}.$$

QUANTUM GATES $\rightarrow$ UNITARY MATRICES

For a quantum gate

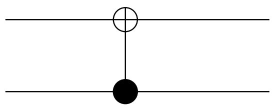


A is such a unitary matrix

	00	01	10	11
00	·	·	·	·
01	·	·	·	·
10	·	·	·	·
11	·	·	·	·

that the entry for column ij and row kl is the probability amplitude that the basis state $|ij\rangle$ transfers to the basis state $|kl\rangle$.

Example For the inverse XOR gate



the unitary matrix has the form

	00	01	10	11
00	·	·	·	·
01	·	·	·	·
10	·	·	·	·
11	·	·	·	·

$\boxed{\text{FROM GATES to UNITARY MATRICES}}$

In general, if a quantum gate has n inputs and outputs then for the corresponding unitary matrix the entry

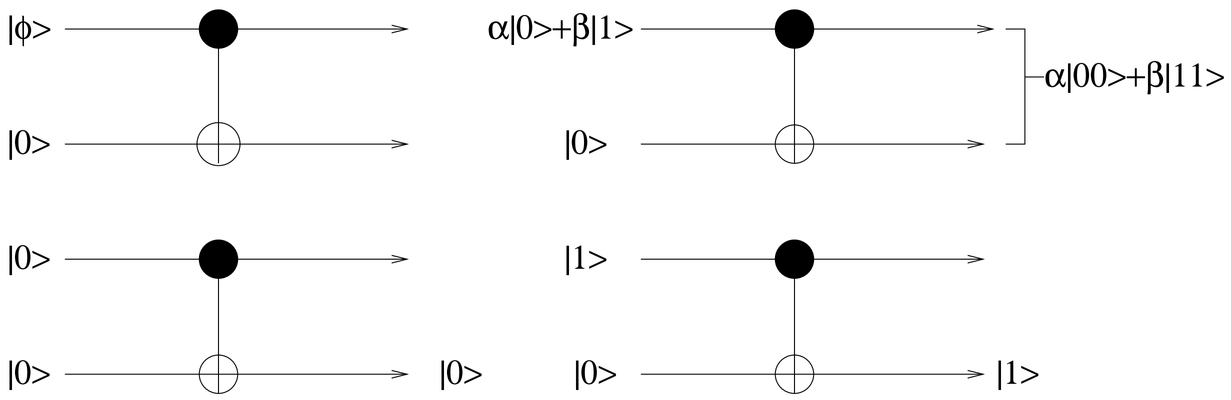
in the column $x \in \{0,1\}^n$

and

in the row $y \in \{0,1\}^n$

is the amplitude for transition from the basis state $|x\rangle$ to the basis state $|y\rangle$.

XOR GATE as a REAL WIRE



As already mentioned, of central importance for quantum computing is the XOR gate (see leftmost and topmost figure).

Observe that if the target qubit has the input $|0\rangle$, then this gate can be used to copy qubits $|0\rangle$ and $|1\rangle$ from the control qubit.

At the same time the gate in Figure a can be seen as a classical wire because it cannot carry on a superposition of the states.

QUANTUM CIRCUITS — SIMPLE EXAMPLES

defi A **quantum (Boolean) circuit** is a collection of quantum gates acyclically connected (by "quantum wires"). defi

A relation between a quantum circuit and the corresponding unitary matrix is far from being very transparent even for simple circuits and some experience is needed to get proper feelings in this respect.

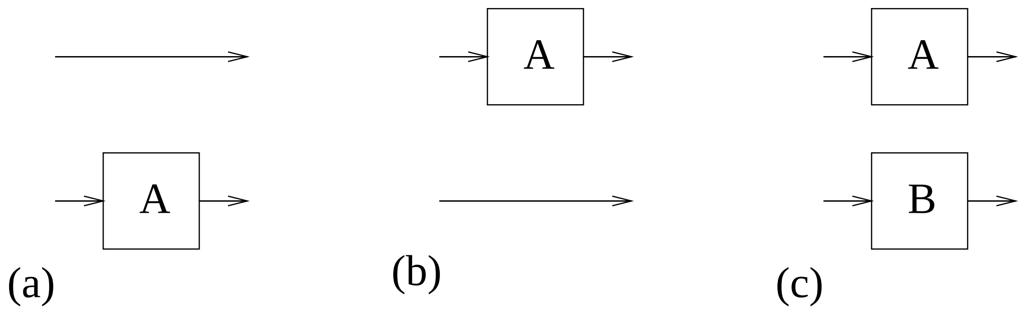


Figure 1: Elementary networks I

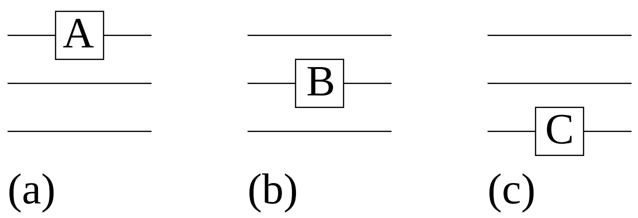


Figure 2: Elementary networks II

INVERSE XOR GATE CIRCUIT

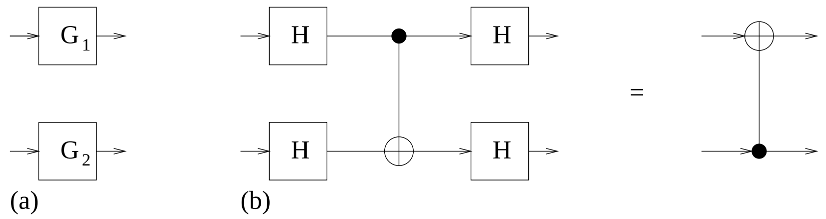


Figure 3: An implementation of the inverse of the XOR gate.

The processing in the network on the left side of the identity in Figure 3b for the input $|0\rangle|1\rangle$ can be depicted as follows:

$$\begin{array}{rcl}
|0\rangle|1\rangle & \overset{H-\text{gates}}{\longrightarrow} & |0'\rangle|1'\rangle \\
& = & \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \\
& = & \frac{1}{2}(|0\rangle|0\rangle+|1\rangle|0\rangle-|0\rangle|1\rangle-|1\rangle|1\rangle) \\
& \overset{\text{XOR gate}}{\longrightarrow} & \frac{1}{2}(|0\rangle|0\rangle+|1\rangle|1\rangle-|0\rangle|1\rangle-|1\rangle|0\rangle) \\
& = & \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \\
& = & |1'\rangle|1'\rangle \\
& \overset{H\ \text{gates}}{\longrightarrow} & |1\rangle|1\rangle.
\end{array}$$

EXAMPLE

There are various generalizations of XOR gates:

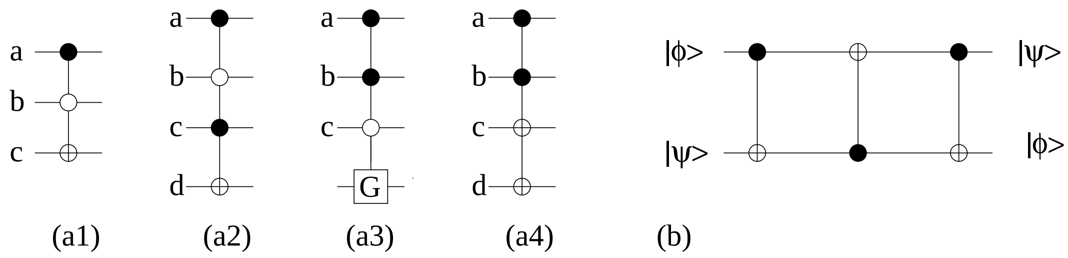


Figure 4: Generalized XOR gate notations and a quantum circuit to flip the qubits

The circuit in Figure b realizes flipping of qubits.

To see that, denote I_{jk} the matrix obtained from the unit matrix of degree 4 by exchanging j-th and h-th columns (i.e. XOR=I_{34}).

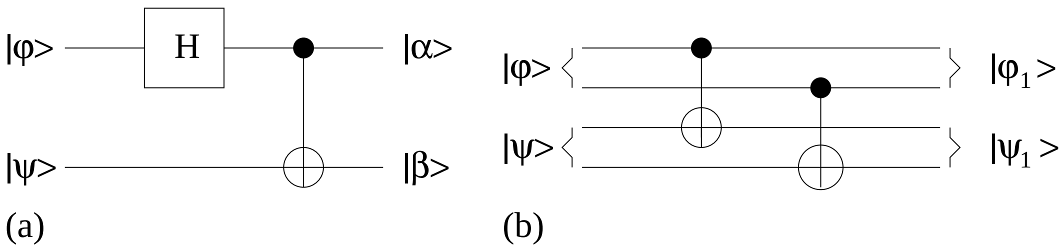
If $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\psi\rangle = \alpha'|0\rangle + \beta'|1\rangle$, then computation by the circuit in Figure b, gate by gate, corresponds to the following matrix computation:

$$I_{34}I_{24}I_{34}\begin{pmatrix}\alpha\alpha'\\ \alpha\beta'\\ \beta\alpha'\\ \beta\beta'\end{pmatrix} = I_{34}I_{24}\begin{pmatrix}\alpha\alpha'\\ \alpha\beta'\\ \beta\beta'\\ \beta\alpha'\end{pmatrix} = I_{34}\begin{pmatrix}\alpha\alpha'\\ \beta\alpha'\\ \beta\beta'\\ \alpha\beta'\end{pmatrix} = \begin{pmatrix}\alpha\alpha'\\ \beta\alpha'\\ \alpha\beta'\\ \beta\beta'\end{pmatrix} = \begin{pmatrix}\alpha'\alpha\\ \alpha'\beta\\ \beta'\alpha\\ \beta'\beta\end{pmatrix}$$

In classical circuits gates are stationary, bits move.

In quantum circuits qubits are stationary, gates need to be moved in order to be applied.

BELL STATE CIRCUITS



The circuit in Figure a produces all four Bell states for all possibilities $|\phi\rangle, |\psi\rangle \in \{|0\rangle, |1\rangle\}$.

The circuit in Figure b performs one-to-one mapping of Bell states into Bell states.

PERMUTATION CIRCUITS

Using several copies of the circuit to flip (or to transpose) two qubits one can realize any permutation of qubits. Using such a method one needs 6 gate-steps to perform permutation shown in the following figure, where such a permutation is realized, using a more complex circuit, with three ancilla qubits, but in only four gate-steps.

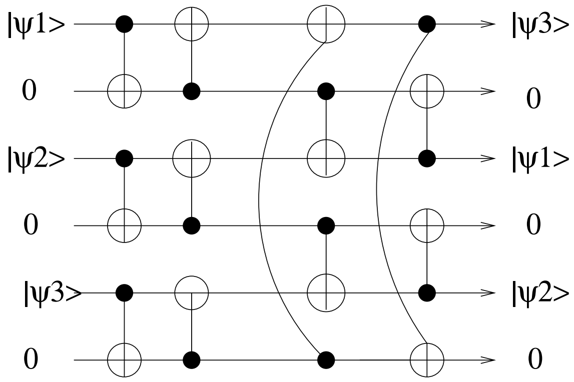
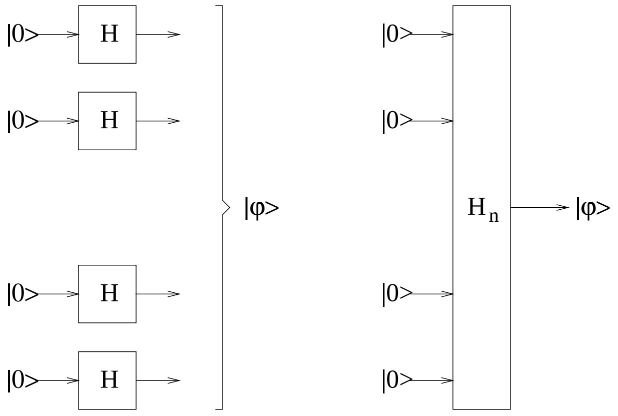


Figure 5: Permutation circuit

HADAMARD GATE

The Hadamard transform H_n is implemented by the circuit in Figure a, and Figure b contains the usual notation for the circuit for H_n.



(a) (b)

The Hadamard circuit H_n and its application to the state $|0^{(n)}\rangle$ with the outcome

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle.$$

COMPUTATIONAL MEANING OF QGATES

The computational meaning of quantum circuits is defined as follows.

For any quantum circuit C with input variables $x_1, \ldots, x_n$ and output variables $y_1, \ldots, y_m$, $m \leq n$ (they are to be a subset of outputs), we associate to any input $x \in \{0,1\}^n$ the probability distribution ρ_x over $\{0,1\}^m$ defined in the following way.

For any input x the final quantum state v, corresponding to all output wires, not only to those carrying output variables, has the form

$$v = \sum_{y \in \{0,1\}^m} \alpha_y |y\rangle,$$

where α_y is the amplitude obtained by the projection of v when the output variables are set to the value y, i.e. α_y is the square root of the sum of squares of amplitudes of these final outcomes having value y in the wires corresponding to output variables.

$\pi_x(y) = |\alpha_y|^2$ is the corresponding probability and $\{\pi_x \mid x \in \{0,1\}^n\}$ is said to be the distribution generated by the circuit C.

QUANTUM CIRCUITS versus QTM

One of the main results of classical computation theory says that each TM can be simulated in polynomial time by a uniform family of Boolean circuits (and vice versa).

A similar result holds also for quantum Turing machines and quantum circuits, and due to this result one uses nowadays more quantum circuits than QTM to develop quantum algorithms.

To present the corresponding result we need at first to introduce the concept of simulation of QTM by quantum circuit.

Definition 0.4 *A quantum circuit C with n input variables is said to (n,t)-simulate a QTM M, if for each $x \in \{0,1\}^n$ the probability distribution ρ_x generated by C is identical to the distribution of the configurations of M after t steps with x as input.*

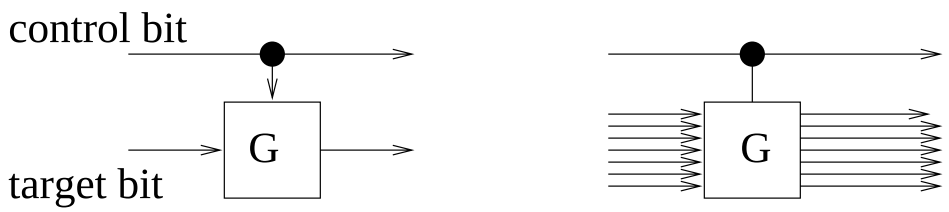
Yao (1993) has shown the following result.

Theorem 0.5 *If M is a QTM and $n, t \in \mathbf{N}^{\geq 0}$, then there exists a quantum Boolean circuit C of size (number of gates) polynomial in n and t that (n,t)-simulates M.*

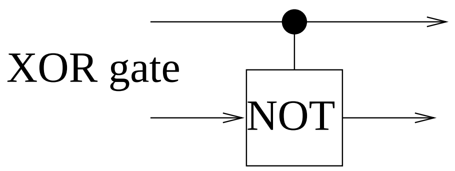
A **quantum program** is a quantum circuit together with some measurement (observation) gates/processes attached to some of the wires.

CONTROLLED QUANTUM GATES

To any quantum gate G we can design a **controlled version** CG of G as follows



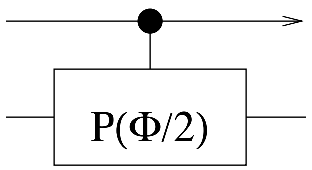
For example



If

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{or} \quad R(\theta) = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}$$

then



represents rotation of the target qubit by angle $\frac{\theta}{2}$ if the control bit is 1.

MEASUREMENT GATES

Measurement gates are not only to magnify results of quantum evolution to provide its outcomes to the classical world. They can be used also to influence, in an essential way, the whole process of quantum computation.

Consider the two quantum circuits depicted in Figure. The first one consists at first of two Hadamard gates H_n and ends with the measurement gate, with respect to the standard observable.

The second circuit has in addition a measurement gate also in between two Hadamard gates.

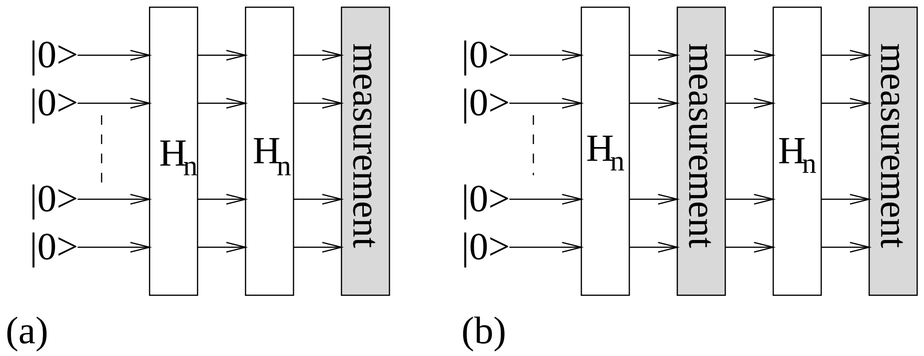


Figure 6: Measurement gates and their role

There is an essential difference between these two circuits. Which one?

COPYING GATES

Example 0.6 *As discussed in the previous example, the network in Figure a can be seen as generating a random bit. However, the same can do networks in Figure 7b,c.*

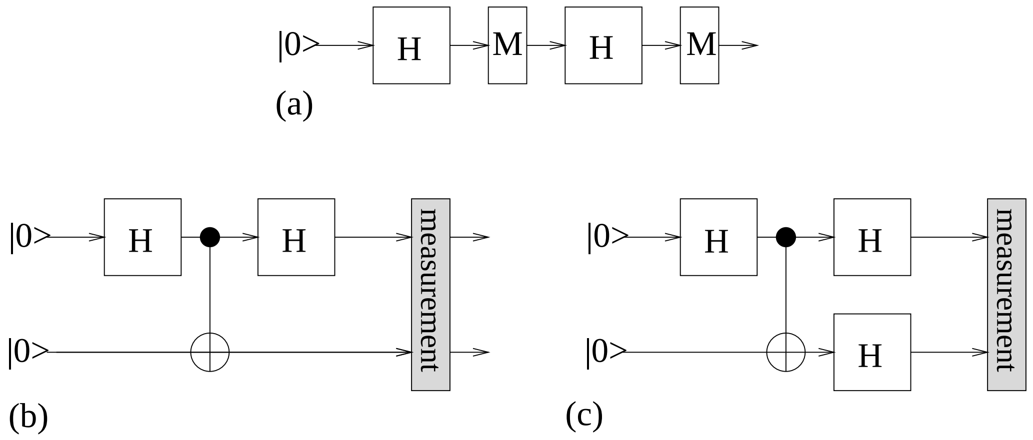


Figure 7: Power of copying circuits

In the circuit in Figure b, after the XOR gate the state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and the first bit is random. After the next application of the Hadamard gate on the first bit we get

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

and the first bit is perfectly random.

In the circuit in Figure c, after the XOR gate we find the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. After the application of Hadamard gates on both bits we get

$$(H \otimes H)(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

and the first bit is again perfectly random.

$\boxed{\text{UNIVERSAL GATES}}$

Definition 0.7 *A set of quantum gates is* **universal** *if any unitary transformation U on any qubit register can be performed, with arbitrary precision $\varepsilon > 0$, by a quantum circuit $C_{U,\varepsilon}$, consisting of the gates from that set. (In other words, the unitary matrix defined by $C_{U,\varepsilon}$ is ε-close to U.)*

A quantum gate is **universal** *if by itself it forms a universal set when supported by constant inputs $|0\rangle$ and $|1\rangle$*

SETS OF UNIVERSAL QUANTUM PRIMITIVES

Several examples of universal sets of quantum computation primitives are known.

Deutsch gate

$$D(\theta) = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i\cos\theta & \sin\theta \\ 0 & 0 & \sin\theta & i\cos\theta \end{matrix} \end{pmatrix}.$$

Barenco gate

$$A(\phi,\alpha,\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha}\cos\theta & -ie^{i(\alpha-\phi)}\sin\theta \\ 0 & 0 & -ie^{i(\alpha+\phi)}\sin\theta & e^{i\alpha}\cos\theta \end{pmatrix}.$$

Sets of universal computation primitives:

1. XOR gate and one-qubit gates;
2. GHZ state ($\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$), quantum measurement and one-qubit gates.

ENTANGLING GATES

A two-qubit gate is called **entangling** if it can create an entangled state when applied to a separable state.

Entangling gates are important. As shown by J. Brylinski and R. Brylinski (2001):

A two qubit gate forms with one-qubit gates a universal set of gates if and only if it is an entangling gate.

ENTANGLEMENT as a COMPUTATIONAL PRIMITIVE

- As shown by Gottesman and Chuang (1999), it is possible to realize any quantum computation by starting with some GHZ states $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and then performing one qubit operations and Bell measurements.
- Moreover, Rausschendorf and Briegel (2000) have shown that universal quantum computation is possible by starting with a proper multipartite entangled state (a sort of a *computational substrate*) and then performing only single qubit measurements.

BINARY ADDER

The following quantum circuit performs binary addition.

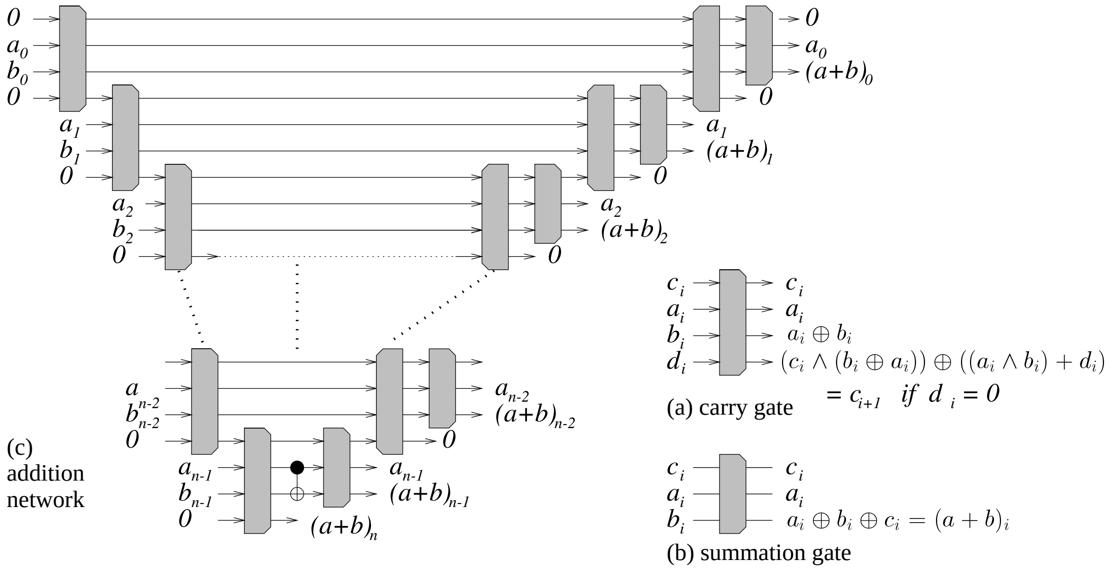
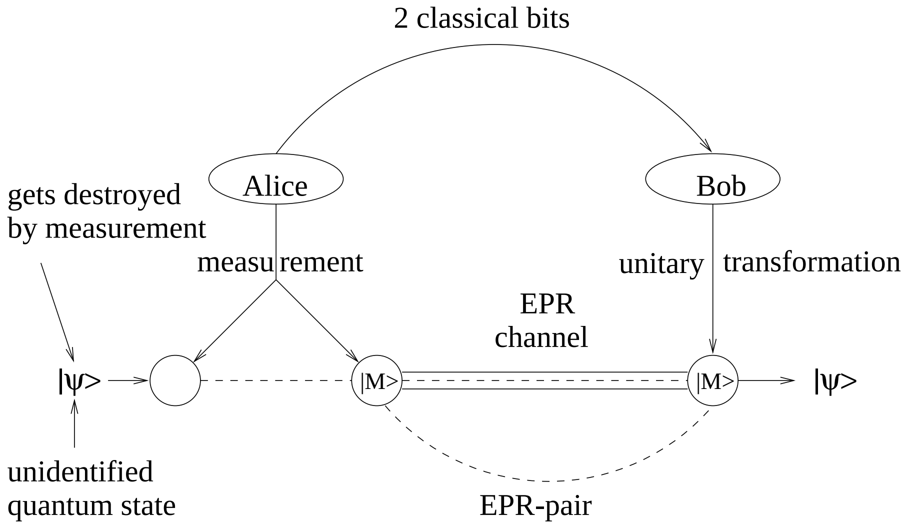


Figure 8: Quantum network for binary addition

QUANTUM TELEPORTATION

Quantum teleportation allows to transmit unknown quantum information to a very distant place in spite of impossibility to measure or to broadcast information to be transmitted.



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |EPR-pair\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Total state

$$|\psi\rangle|EPR-pair\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle$$

Measurement of the first two qubits is done with respect to the "Bell basis":

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

QUANTUM TELEPORTATION I

Total state of three particles:

$$|\psi\rangle|EPR - state\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

can be expressed as follows:

$$\begin{aligned}|\psi\rangle|EPR - state\rangle \;=\; & |\Phi^+\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) + |\Psi^+\rangle\frac{1}{\sqrt{2}}(\beta|0\rangle + \alpha|1\rangle) \\ & + |\Phi^-\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle) + |\Psi^-\rangle\frac{1}{\sqrt{2}}(-\beta|0\rangle + \alpha|1\rangle))\end{aligned}$$

and therefore the measurement of the first two particles projects the state of the Bob's particle into a "small modification " $|\psi_1\rangle$ of the unknown state $|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)$.

The unknown state $|\psi\rangle$ can therefore be obtained from $|\psi_1\rangle$ by applying one of the four operations

$$\sigma_x, \sigma_y, \sigma_z, I$$

and the result of the Bell measurement provides two bits specifying which of the above four operations should be applied.

These four bits Alice needs to send to Bob using a classical channel (by email, for example).

QUANTUM TELEPORTATION II

If the first two particles of the state

$$\begin{aligned}|\psi\rangle|EPR - state\rangle \; &= \; |\Phi^+\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) + |\Psi^+\rangle\frac{1}{\sqrt{2}}(\beta|0\rangle + \alpha|1\rangle) \\ &\quad + |\Phi^-\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle) + |\Psi^-\rangle\frac{1}{\sqrt{2}}(-\beta|0\rangle + \alpha|1\rangle))\end{aligned}$$

are measured with respect to the Bell basis then Bob's particle gets into the mixed state

$$(\frac{1}{4}, \alpha|0\rangle + \beta|1\rangle) \oplus (\frac{1}{4}, \alpha|0\rangle - \beta|1\rangle) \oplus (\frac{1}{4}, \beta|0\rangle + \alpha|1\rangle) \oplus (\frac{1}{4}, \beta|0\rangle - \alpha|1\rangle)$$

to which corresponds the density matrix

$$\frac{1}{4}\begin{pmatrix} \alpha \\ \beta* \end{pmatrix}(\alpha^*, \beta^*) + \frac{1}{4}\begin{pmatrix} \alpha \\ -\beta \end{pmatrix}(\alpha^*, -\beta^*) + \frac{1}{4}\begin{pmatrix} \beta \\ \alpha \end{pmatrix}(\beta^*, \alpha^*) + \frac{1}{4}\begin{pmatrix} \beta \\ -\alpha \end{pmatrix}(\beta^*, -\alpha^* \; = \frac{1}{2}$$

The resulting density matrix is identical to the density matrix for the mixed state:

$$(\frac{1}{2}, |0\rangle) \oplus (\frac{1}{2}, |1\rangle).$$

Indeed, the density matrix for the last mixed state has the form:

$$\frac{1}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix}(1, 0) + \frac{1}{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}(0, 1) = \frac{1}{2}I.$$

QUANTUM TELEPORTATION — COMMENTS

- Alice can be seen as dividing information contained in $|\psi\rangle$ into

  quantum information - transmitted through EPR channel

  and

  classical information - transmitted through a classical channel

- In a quantum teleportation an unknown quantum state $|\phi\rangle$ can be disambled into, and later reconstructed from, two classical bit-states and an maximally entangled pure quantum state.

- Using quantum teleportation an unknown quantum state can be *teleported* from one place to another by a sender who does not need to know — for teleportation itself — neither the state to be teleported nor the location of the intended receiver.

- The teleportation procedure cannot be used to transmit information faster than light

  but

  it can be argued that quantum information presented in unknown state is transmitted instantaneously (except two random bits to be transmitted at the speed of light at most).

- EPR channel is irreversibly destroyed during the teleportation process.

QUANTUM TELEPORTATION CIRCUIT

Consider the circuit

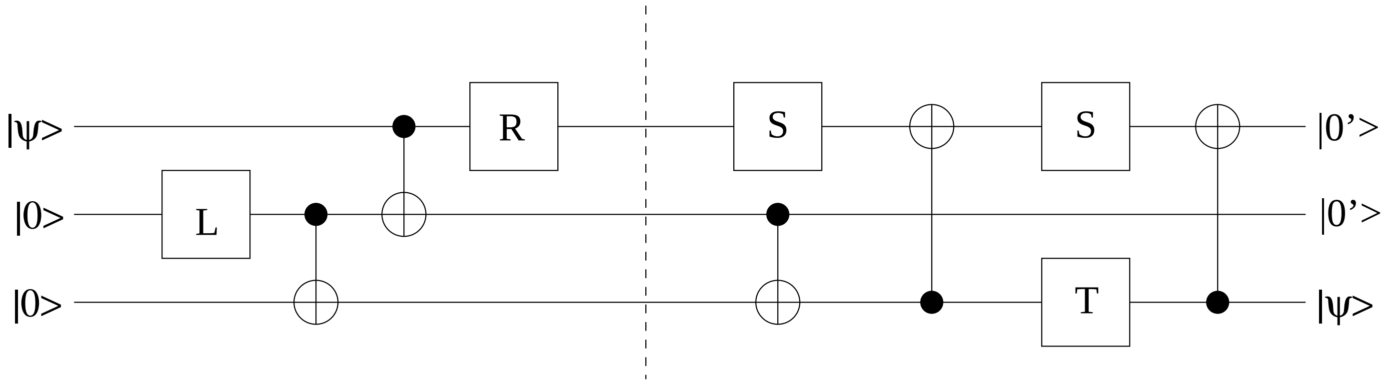


Figure 9: Brassard's teleportation circuit

where L, R, S, and T are the gates implementing the following unitary transformations

$$R = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad L = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad S = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \quad T = \begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}$$

Let $|\psi\rangle$ be a qubit state. If the state $|\psi 00\rangle$ is processed by the circuit from Figure 12, then the output will be $|0'0'\psi\rangle$.

In the state of the circuit at the dashed line all three qubits are entangled.

A measurement of the two up most qubits at the dashed line provides random classical bits, say u, v.

If these two bits are "returned" into the circuit, i.e. if the computation of the circuit to the right of the dashed line starts with input $|uvz\rangle$, where z is the state of the third qubit of the dashed line, then the output of the circuit will be $|uv\psi\rangle$.

TELEPORTATION using TELEPORTATION CIRCUIT

In case qubits can be stored one can use teleportation circuit for teleportation as follows:

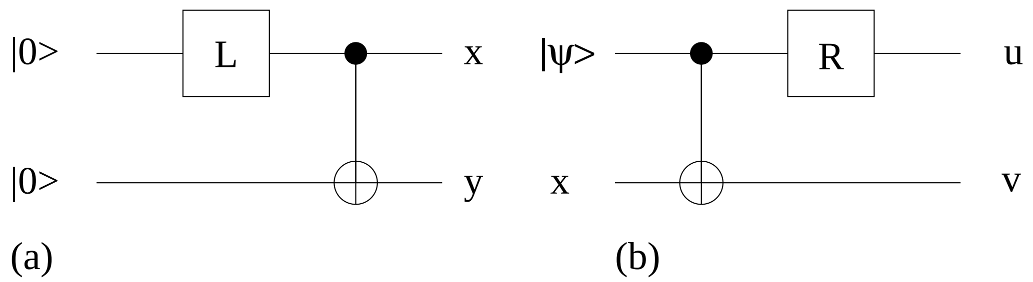


Figure 10: Two teleportation circuits of Alice and Bob

By using two lower wires and the first gates Alice gets, see Figure a, at the output the state

$$\frac{1}{2}(|00\rangle + |11\rangle)$$

.

Alice keeps x in her memory and sends y to Bob.

Assume that at some time later Alice receives a qubit in an unknown state $|\psi\rangle$.

To teleport $|\psi\rangle$ to Bob, Alice takes x from her quantum memory an uses the second part of the teleportation circuit, see Figure b, to produce two classical bits u, v that are then sent to Bob.

To finish teleportation Bob uses u, v and the last part of the teleportation circuit to get $|\psi\rangle$ on the third wire.

$\boxed{\text{EXTRAS}}$

SUPEROPERATOR GATES

In spite of the fact that the model of quantum circuits from page 7 is fundamental for processing pure quantum states of an isolated quantum system, circuits processing density matrices with superoperator-gates defined below, are of increasing (practical) importance. They better correspond to computations in noisy environments.

Definition 0.8 *A superoperator gate G of type (k, l) is a completely positive map which maps density matrices on k qubits to density matrices on l qubits. Its action on a density matrix ρ will be denoted symbolically by $G \circ \rho$.*

Two important special cases of superoperator gates are unitary and measurement gates.

In the case of a unitary gate U the corresponding operator is $U \cdot U^*$. For a pure state $|\phi\rangle$, U maps $\rho = |\phi\rangle\langle\phi|$ into $U \circ \rho = U\rho U^*$.

A measurement gate represents a probabilistic projection into a set of mutually orthogonal subspaces, which produces a mixed state. Superoperators are in general not reversible.

SUPEROPERATOR CIRCUITS

There is a well-known and well-understood relation between superoperators and unitary operators.

Lemma 0.9 *The following conditions are equivalent for any two Hilbert spaces H_n and H_m and sets of linear operators $\mathcal{L}(H_n)$ and $\mathcal{L}(H_m)$.*

1. *A superoperator $T : \mathcal{L}(H_n) \rightarrow \mathcal{L}(H_m)$ is trace-preserving and completely positive.*
2. *There is a Hilbert space F with $\mathrm{dim}(F) \leq \mathrm{dim}(H_n)\,\mathrm{dim}(H_m)$, and a unitary embedding $E : H_n \rightarrow H_n \otimes F$ such $T\rho = Tr_F(E\rho E^*)$ for all $\rho \in \mathcal{L}(H_n)$.*

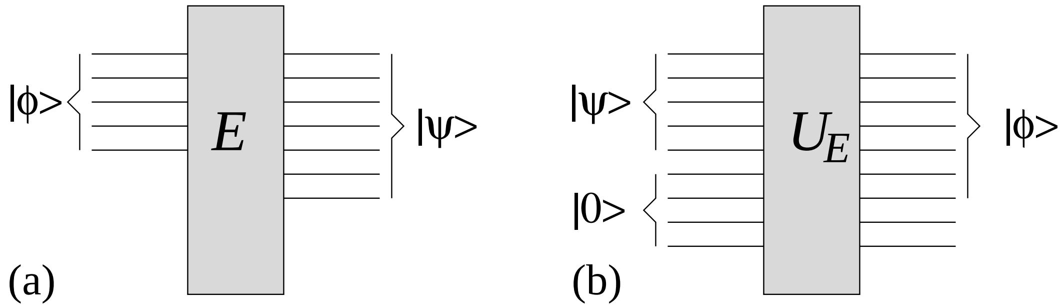


Figure 11: Encoder as superoperator and its unitary embedding