Quantum Computing
WS 2009/10

Prof. Dr. Erich Grädel

Mathematische Grundlagen der Informatik
RWTH Aachen

Contents

1 Introduction

1.1 Historical overview

The history of quantum computing started in 1982 when Nobel laureate Richard Feynman argued that certain quantum mechanical effects cannot be simulated efficiently by classical computers. This started a debate whether these effects (in particular the parallelism which occurs inherently in quantum mechanical processes) could be employed by building a quantum computer.

Between 1985 and 1993, in a series of papers, Deutsch, Bernstein-Vazirani, Yao, and others advanced the theoretical foundations of quantum computing by providing theoretical models such as quantum Turing machines and quantum gate arrays as well as introducing complexity classes for quantum computing and several simple algorithms that could be performed by a quantum computer.

A breakthrough occurred in 1994 when Peter Shor published his factorisation algorithm for quantum computers, which runs in polynomial time. His algorithm relies on the so-called *quantum Fourier transformation*, which we will introduce later. Another example of a quantum algorithm is Grover's search algorithm (1996), that can find a *needle in a haystack* of size N in time $\mathrm{O}(\sqrt{N})$.

Despite these surprising results, quantum computing still faces several problems: There are not many more algorithms known besides the one we have mentioned, and a quantum computer of moderate size that can keep a stable state for a sufficient amount of time needs yet to be built. So far, one was only able to build a quantum computer consisting of 7 *qubits*, which successfully factorised the number $15 = 3 \cdot 5$.

1.2 An experiment

The following experiment can be conducted using easily accessible ingredients:

- a powerful light source (e.g. a *laser*),
- three polarisation filters, which polarise light horizontally, vertically, and with an angle of 45°, respectively.

If we put one or more of the polarisation filters in front of the light source, we will make the following observations:

(1) If only the horizontal polarisation filter ($\rightarrow$) is put in front of the light source, 50% of light passes through.

(2) If the vertical polarisation filter ($\uparrow$) is put in front of the horizontal filter, 50% of light passes through the first filter, but the remaining light gets blocked by the second filter.

(3) However, if the diagonal filter ($\nearrow$) is put between $\rightarrow$ and $\uparrow$, we can observe that, from the total light emitted by the source, 50% passes through the first filter, 25% passes through the first two filters, and 12.5% of the light passes through all three filters, after all.

To explain these results, we describe the polarisation state of a photon by a vector

$$|\varphi\rangle := \alpha|\uparrow\rangle + \beta|\rightarrow\rangle$$

in a 2-dimensional vector space with basis $\{|\uparrow\rangle, |\rightarrow\rangle\}$. Since the direction of such a vector is all that matters, we only consider *unit vectors*: $|\alpha|^2 + |\beta|^2 = 1$. Also note that the choice of the basis is arbitrary: Instead of $\{|\uparrow\rangle, |\rightarrow\rangle\}$, one could also take $\{|\nearrow\rangle, |\searrow\rangle\}$ or, for that matter, any pair of orthogonal unit vectors.

The *measurement* of a state corresponds to the projection of such a vector with respect to an orthonormal basis, e.g. $\{|\uparrow\rangle, |\rightarrow\rangle\}$, which is given by the present equipment: If the vector $|\varphi\rangle = \alpha|\uparrow\rangle + \beta|\rightarrow\rangle$ is measured, it is projected either to $|\uparrow\rangle$ (with probability $|\alpha|^2$) or to $|\rightarrow\rangle$ (with probability $|\beta|^2$).

After the measurement, the vector φ is "destroyed", i.e. it has been transformed into one of the basic states $|{\uparrow}\rangle$ or $|{\rightarrow}\rangle$. There is no way to gain back φ, and each successive measurement gives the same result as the first one.

To each polarisation filter belongs a different orthonormal basis: If the angle of the filter is η, then the corresponding basis is

$$\{\sin\eta|{\uparrow}\rangle + \cos\eta|{\rightarrow}\rangle\ ,\ \cos\eta|{\uparrow}\rangle - \sin\eta|{\rightarrow}\rangle\}.$$

In particular, for both the horizontal and the vertical polarisation filter, the corresponding basis is $\{|{\nearrow}\rangle, |{\searrow}\rangle\}$, whereas for the diagonal filter $\nearrow$, the basis is

$$\{|{\nearrow}\rangle, |{\searrow}\rangle\} = \left\{\frac{1}{\sqrt{2}}(|{\uparrow}\rangle + |{\rightarrow}\rangle), \frac{1}{\sqrt{2}}(|{\uparrow}\rangle - |{\rightarrow}\rangle)\right\}$$

The photons that, after the measurement, correspond to the polarisation, pass through the filter; the others are reflected. Hence, filter $\rightarrow$ projects 50% of the photons onto $|{\rightarrow}\rangle$ and lets them pass; the other 50% are projected onto $|{\uparrow}\rangle$ and thus reflected. Filter $\uparrow$, on the other hand, reflects all photons that are projected on $|{\rightarrow}\rangle$. Hence, no light passes through this filter if it is put behind filter $\rightarrow$.

Filter $\nearrow$ projects a photon in state $|{\rightarrow}\rangle = \frac{1}{\sqrt{2}}|{\nearrow}\rangle - \frac{1}{\sqrt{2}}|{\searrow}\rangle$ with probability $\frac{1}{2}$ onto $|{\nearrow}\rangle$. Hence, if filter $\nearrow$ is put in between filter $\rightarrow$ and filter $\uparrow$, then 25% of the photons pass through the first two filters and are subsequently in state $|{\nearrow}\rangle$. Since $|{\nearrow}\rangle = \frac{1}{\sqrt{2}}|{\rightarrow}\rangle + \frac{1}{\sqrt{2}}|{\uparrow}\rangle$, half of these are projected by $\uparrow$ to $|{\uparrow}\rangle$ and can pass through.

1.3 Foundations of quantum mechanics

In general, a *state* is a complete description of a physical system. In quantum mechanics, a state is a unit vector in a *Hilbert space*.

Definition 1.1. A *Hilbert space H* is a vector space over the field $\mathbb{C}$ of complex numbers, equipped with an *inner product*

$$\langle\cdot\,|\,\cdot\rangle\colon H \times H \to \mathbb{C}$$

with the following properties:

- $\langle \psi \mid \varphi \rangle = \langle \varphi \mid \psi \rangle^*$ for all $\psi, \varphi \in H$ (for a complex number $z = a + ib$, its *conjugate* z^* is defined by $z^* = a - ib$).
- $\langle \psi \mid \psi \rangle \geq 0$ for all $\psi \in H$, and $\langle \psi \mid \psi \rangle = 0$ if and only if $\psi = 0$ (the zero vector).
- $\langle \psi \mid \alpha\varphi_1 + \beta\varphi_2 \rangle = \alpha\langle \psi \mid \varphi_1 \rangle + \beta\langle \psi \mid \varphi_2 \rangle$ for all $\psi, \varphi_1, \varphi_2 \in H$ and $\alpha, \beta \in \mathbb{C}$.

Note that, if H is a Hilbert space, then $\|\cdot\| \colon H \to \mathbb{C}$, defined by

$$\|\psi\| := \sqrt{\langle \psi \mid \psi \rangle}$$

for all $\psi \in H$, defines a *norm* on H.

Remark 1.2. For Hilbert spaces of infinite dimension, in which we are not interested here, it is also required that H is *complete* (with respect to $\|\cdot\|$), i.e. that any Cauchy sequence has a limit.

In quantum mechanics, a vector $\psi \in H$ is usually written in *Dirac notation* as $|\psi\rangle$ (read *ket* ψ). However, the zero vector is denoted by 0 (not $|0\rangle$, which might be a different vector). For a given vector $|\psi\rangle$, its *dual vector* is denoted by $\langle\psi|$ (read *bra* ψ). Formally, $\langle\psi|$ is the function from H to $\mathbb{C}$ that maps a vector $|\varphi\rangle$ to the number $\langle \psi \mid \varphi \rangle$.

Definition 1.3. An *orthonormal basis* of a Hilbert space H is a basis $\{|e_1\rangle, \dots, |e_n\rangle\}$ of H such that

$$\langle e_i \mid e_j \rangle = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases}$$

for all $i, j = 1, \dots, n$. In particular, $\|e_i\| = 1$ for all $i = 1, \dots, n$.

The elementary building blocks of a classical computer are the *bits*, which can be in one of two states 0 or 1. In quantum computing, the elementary building blocks are the *qubits*; these are superpositions of two vectors $|0\rangle$ and $|1\rangle$, which form a basis for the 2-dimensional Hilbert space H_2. (Note that any two Hilbert spaces of the same dimension are isomorphic.)

Definition 1.4. Given a basis $|0\rangle, |1\rangle$ of H_2, a *qubit* is any vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in H^2$ such that $|\alpha|^2 + |\beta|^2 = 1$.

If a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is *measured*, then with probability $|\alpha|^2$ we obtain the state $|0\rangle$, and with probability $|\beta|^2$ we obtain the state $|1\rangle$. Moreover, any successive measurement leads to the same result. Hence, although a qubit can be in one of infinitely many states, we can only extract *one* bit of classical information. This process of extraction (the *measurement*) is, in fact, a probabilistic process.

Of course, a quantum computer will normally not only have access to one qubit but to many of them. A classical system with n bits comprises 2^n states $0\cdots0$, $0\cdots1$ up to $1\cdots1$. An *n-qubit system*, on the other hand, has 2^n basic states and can reside in any superposition

$$\alpha_0|0\cdots0\rangle + \alpha_1|0\cdots1\rangle + \cdots + \alpha_{2^n-1}|1\cdots1\rangle$$

such that $\sum_{i=0}^{2^n-1}|\alpha_i|^2 = 1$. Such systems are also called *quantum registers*.

The n-qubit space H_{2^n} can be obtained from H_2 by an operation called the *tensor product*. Formally, if V and W are Hilbert spaces, then $V \otimes W$ (read V *tensor* W) is a Hilbert space of dimension $\dim V \otimes W = \dim V \cdot \dim W$. Any two vectors $|\psi\rangle \in V$ and $|\varphi\rangle \in W$ correspond to a vector $|\psi\rangle \otimes |\varphi\rangle \in V \otimes W$, and this operation is compatible with addition and scalar multiplication:

- $(|\psi_1\rangle + |\psi_2\rangle) \otimes |\varphi\rangle = |\psi_1\rangle \otimes |\varphi\rangle + |\psi_2\rangle \otimes |\varphi\rangle$;
- $|\psi\rangle \otimes (|\varphi_1\rangle + |\varphi_2\rangle) = |\psi\rangle \otimes |\varphi_1\rangle + |\psi\rangle \otimes |\varphi_2\rangle$;
- $\alpha|\psi\rangle \otimes |\varphi\rangle = |\psi\rangle \otimes \alpha|\varphi\rangle = \alpha(|\psi\rangle \otimes |\varphi\rangle)$.

In fact, if $\{v_1, \ldots, v_n\}$ is a basis of V and $\{w_1, \ldots, w_m\}$ is a basis of W, then $\{v_i \otimes w_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$ is a basis of $V \otimes W$. Note that this space is different from the *product space* $V \times W$, which is of dimension $\dim V + \dim W$. Instead of $|\psi\rangle \otimes |\varphi\rangle$, we also write $|\psi\rangle|\varphi\rangle$ or $|\psi\varphi\rangle$. We have

$$H_{2^n} = \underbrace{H_2 \otimes \cdots \otimes H_2}_{n \text{ times}},$$

and $\{|0\cdots0\rangle, |0\cdots1\rangle, \ldots, |1\cdots1\rangle\}$ is a basis of H_{2^n}. Note that

$\dim H_{2^n} = 2^n$. Hence, the dimension of the system grows exponentially in the number of qubits.

As opposed to $H_2 \times H_2$, not every state in $H_2 \otimes H_2$ can be decomposed into two states of H_2. We call such states *entangled*.

Proposition 1.5. There exists a unit vector $|\psi\rangle \in H_2 \otimes H_2$ such that $|\psi\rangle \neq |\varphi_1\rangle \otimes |\varphi_2\rangle$ for any two vectors $|\varphi_1\rangle, |\varphi_2\rangle \in H_2$.

Proof. Consider, for example, $|\psi\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and assume that there exists $|\varphi_1\rangle, |\varphi_2\rangle \in H_2$ with $|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$. Then there exist $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{C}$ such that $|\varphi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$ for $i = 1, 2$. Hence,

$$\begin{aligned} |\psi\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \\ &= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \alpha_2\beta_1|10\rangle + \beta_1\beta_2|11\rangle \end{aligned}$$

Since $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ forms a basis of $H_2 \otimes H_2$, we have $\alpha_1\beta_2 = \alpha_2\beta_1 = 0$. But then, also $\alpha_1\alpha_2 = 0$ or $\beta_1\beta_2 = 0$, a contradiction. Q.E.D.

In an n-qubit system, each qubit can be measured separately. The measurement of the first qubit of an n-qubit state $|\psi\rangle = \sum_{v \in \{0,1\}^n} \alpha_v |v\rangle$ can have two outcomes:

- With probability $p = \sum_{w \in \{0,1\}^{n-1}} |\alpha_{0w}|^2$, the result of the measurement is $|0\rangle$, and $|\psi\rangle$ is projected onto the vector

$$|0\rangle \otimes \frac{1}{\sqrt{p}} \sum_{w \in \{0,1\}^{n-1}} \alpha_{0w}|w\rangle.$$

- With probability $q = \sum_{w \in \{0,1\}^{n-1}} |\alpha_{1w}|^2$, the result of the measurement is $|1\rangle$, and $|\psi\rangle$ is projected onto the vector

$$|1\rangle \otimes \frac{1}{\sqrt{q}} \sum_{w \in \{0,1\}^{n-1}} \alpha_{1w}|w\rangle.$$

A quantum-mechanical system evolves through *unitary transformations*. Formally, a linear operator $U\colon H \to H\colon |\psi\rangle \mapsto U|\psi\rangle$ is unitary if it preserves the inner product:

$$\langle U\psi \mid U\varphi\rangle = \langle \psi \mid \varphi\rangle$$

For the presentation of an operator by a matrix $U \subseteq \mathbb{C}^{n \times n}$ this means that $U^*U = UU^* = \mathrm{I}$ (the identity matrix), where U^* is the *conjugate transpose* of U, i.e. the matrix that results from U by transposing U and replacing each entry by its conjugate. In particular, every unitary transformation is invertible, i.e. *reversible*.

Finally, we can postulate that any computation of a quantum computer consists of reversible building blocks (combined with measurements). This imposes a serious limitation on quantum computers. For example, this implies that no quantum computer can simply copy around some qubits.

Theorem 1.6 (No-Cloning Theorem)**.** Let H be any Hilbert space of dimension $n > 1$. There does not exist a unitary transformation $\mathrm{Copy} : H \otimes H \to H \otimes H$ and a vector $|0\rangle \in H$ such that $\mathrm{Copy}(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$ for all $\psi \in H$.

Proof. Assume that Copy and $|0\rangle$ exist. Since $n > 1$, there exists a unit vector $|1\rangle$ that is orthogonal to $|0\rangle$. Let $\psi = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. We have:

$$\begin{aligned}\mathrm{Copy}(|\psi\rangle|0\rangle) &= \frac{1}{\sqrt{2}}(\mathrm{Copy}(|0\rangle|0\rangle) + \mathrm{Copy}(|1\rangle|0\rangle)) \\ &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)\end{aligned}$$

The latter vector is different from $|\psi\rangle|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$, a contradiction. Q.E.D.

1.4 Quantum gates and quantum gate arrays

Definition 1.7. A *quantum gate* on m qubits is a unitary transformation $U : H_{2^m} \to H_{2^m}$ on the Hilbert space $H_{2^m} = H_2 \otimes \cdots \otimes H_2$ of dimension 2^m.

For $m = 1$, a quantum gate is a unitary transformation $U : H_2 \to H_2$. Consider the standard basis $|0\rangle, |1\rangle$ of H_2. The transformation U is uniquely determined by its behaviour on the basis vectors:

$$U\colon |0\rangle \mapsto a|0\rangle + b|1\rangle$$

$$|1\rangle \mapsto c|0\rangle + d|1\rangle,$$

As usual in linear algebra, we write these vectors as column vectors $\binom{a}{b}$ and $\binom{c}{d}$, respectively. Hence, the application of U on the basis vectors $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$ corresponds to a multiplication of the matrix

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

with these vectors. That U is unitary is expressed by the matrix equation

$$\begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Example 1.8.

(1) The *not* gate is given by the matrix

$$M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We have $M_\neg|0\rangle = |1\rangle$ and $M_\neg|1\rangle = |0\rangle$.

(2) Consider the matrix

$$M = \frac{1}{2}\begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix}.$$

M is unitary since

$$\begin{aligned} M^*M &= \frac{1}{4}\begin{pmatrix} 1-\mathrm{i} & 1+\mathrm{i} \\ 1+\mathrm{i} & 1-\mathrm{i} \end{pmatrix}\begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix} \\ &= \frac{1}{4}\begin{pmatrix} 2(1-\mathrm{i}^2) & (1-\mathrm{i})^2+(1+\mathrm{i})^2 \\ (1-\mathrm{i})^2+(1+\mathrm{i})^2 & 2(1-\mathrm{i}^2) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Moreover, we have

$$M^2 = \frac{1}{4}\begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = M_{\neg}\,.$$

Hence, M is a square root of $M_{\neg}$, and we write $M = \sqrt{M_{\neg}}\,$.

(3) The *Hadamard transformation* is given by the matrix

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

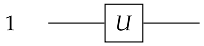
It transforms the standard basis $|0\rangle, |1\rangle$ into the *Hadamard basis* (also called the *Fourier basis*)

$$\begin{aligned} |0'\rangle &= \mathrm{H}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1'\rangle &= \mathrm{H}\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

(see Section 1.2) and back:

$$\begin{aligned} \mathrm{H}\,|0'\rangle &= \mathrm{H}\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \\ \mathrm{H}\,|1'\rangle &= \mathrm{H}\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \end{aligned}$$

We denote the operation of a quantum gate U on 1 qubit as follows:



Other important gates on 1 qubit are

$$\mathrm{S} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix} \quad \text{(Phase)}$$

and

$$\mathrm{T} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/4} \end{pmatrix}.$$

Note that $\mathrm{S} = \mathrm{T}^2$.

For $m = 2$, we are dealing with 2-qubit gates, which are of the form $U : H_4 \to H_4$. The standard basis of H_4 is $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, or as coordinates

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

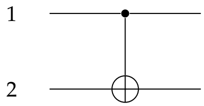
Example 1.9. The *controlled not* gate (CNOT) is given by the matrix

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

We have:

$$M_{\text{CNOT}}|00\rangle = |00\rangle, \qquad M_{\text{CNOT}}|01\rangle = |01\rangle,$$
$$M_{\text{CNOT}}|10\rangle = |11\rangle, \qquad M_{\text{CNOT}}|11\rangle = |10\rangle.$$

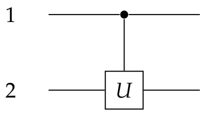
Hence, $M_{\text{CNOT}}|ij\rangle = |i\rangle \otimes |i \oplus j\rangle$ ($\oplus$ denotes *exclusive or*, i.e. $i \oplus j = 1$ if and only if $i \neq j$). The operation of CNOT on 2 qubits is denoted as follows:



In general, if U is a unitary transformation on 1 qubit, then we can define a unitary transformation C-U (read *controlled* U) on 2 qubits as follows:

$$\text{C-}U|ij\rangle = |i\rangle \otimes \begin{cases} U|j\rangle & \text{if } i = 1,\\ |j\rangle & \text{if } i = 0.\end{cases}$$

Graphically, this operation is denoted as follows:



If U is represented by the matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$, then C-$U$ is represented by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & c \\ 0 & 0 & b & d \end{pmatrix}.$$

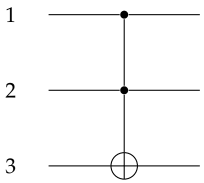
For $m = 3$, an interesting gate is C-CNOT, better known as the *Toffoli gate* Tf, which is defined as follows:

$$\mathrm{Tf}\,|ijk\rangle = |ij\rangle \otimes |ij \oplus k\rangle.$$

The corresponding matrix is

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

Graphically, this operation is denoted as follows:



Of course, it is also possible to consider the Toffoli gate as a classical gate

$$\mathrm{Tf}\colon \{0,1\}^3 \to \{0,1\}^3\colon (i,j,k) \mapsto (i,j,ij \oplus k).$$

In fact, every classical circuit can be simulated by a circuit consisting of Tf gates only. For $f : \{0,1\}^n \to \{0,1\}^n$ consider the reversible function

$$f' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n : (x,y) \mapsto (x, f(x) \oplus y).$$

We show that any reversible function can be computed by a circuit consisting of Tf gates.

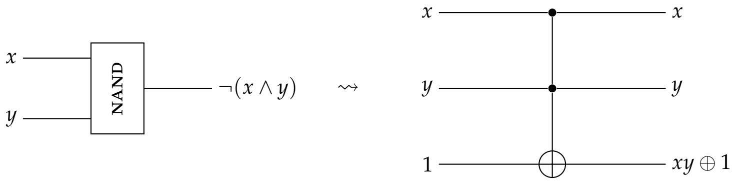
More formally, we say that a set Ω of reversible gates is *complete* (for classical reversible computation) if, given any reversible function $g : \{0,1\}^n \to \{0,1\}^n$, we can construct a circuit consisting of gates in Ω only that computes a function $h : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n \times \{0,1\}^k$ such that for a fixed $u \in \{0,1\}^k$ we have

$$h(x,u) = (g(x), v)$$

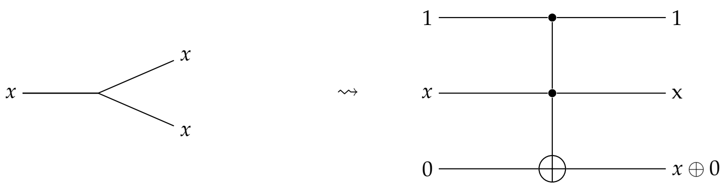
for all $x \in \{0,1\}^n$.

Theorem 1.10. $\{\mathrm{Tf}\}$ is complete (for classical reversible computation).

Proof. We use the fact that every function can be computed by (classical) circuit consisting of NAND gates. Then, we can replace each NAND gate with inputs x and y by a Toffoli gate with inputs x, y and 1 (Note that $xy \oplus 1 = \neg(x \wedge y)$):

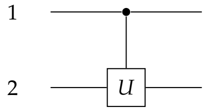


Similarly, we can replace every branching with input x by a Toffoli gate with inputs 1, x and 0 (Note that $x \oplus 0 = x$):

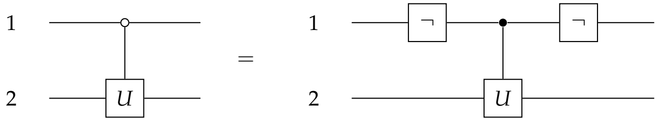


Q.E.D.

Recall that C-U executes U on the target qubit if and only if the control qubit is set to 1:



We can switch the gate's behaviour by introducing two $\neg$ gates:



The resulting operation executes U if the control qubit is set to 0:

$$|ij\rangle \mapsto |i\rangle \otimes \begin{cases} U|j\rangle & \text{if } j = 0, \\ |j\rangle & \text{if } j = 1. \end{cases}$$

Formally, the parallel execution of two unitary transformations corresponds to a tensor product of their matrices.

Definition 1.11. Let

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & \cdots & b_{1s} \\ \vdots & & \vdots \\ a_{r1} & \cdots & b_{rs} \end{pmatrix}$$

be two matrices of sizes $m \times n$ and $r \times s$, respectively. The matrix

$$A \otimes B := \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}$$

of size $mr \times ns$ is called the *tensor product* of A and B.

Proposition 1.12. Let A and B be two 2×2 matrices that represent quantum gates on one qubit. Then, the simultaneous action of A on the first and B on the second qubit is represented by $A \otimes B$.

Proof. We have to check what the simultaneous action of A and B does to the basis vectors $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ of H_4. If

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \text{ and } B = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix},$$

then the basis vector $|ij\rangle$ is mapped to

$$\begin{aligned} A|i\rangle \otimes B|j\rangle &= (a_{0i}|0\rangle + a_{1i}|1\rangle) \otimes (b_{0j}|0\rangle + b_{1j}|1\rangle) \\ &= a_{0i}b_{0j}|00\rangle + a_{0i}b_{1j}|01\rangle + a_{1i}b_{0j}|10\rangle + a_{1i}b_{1j}|11\rangle \end{aligned}$$

Hence, in the matrix representing this operation the column corresponding to $|ij\rangle$ is

$$\begin{pmatrix} a_{0i}b_{0j} \\ a_{0i}b_{1j} \\ a_{1i}b_{0j} \\ a_{1i}b_{1j} \end{pmatrix}$$

This is indeed the column that corresponds to $|ij\rangle$ in

$$A \otimes B = \begin{pmatrix} a_{00}b_{00} & a_{00}b_{01} & a_{01}b_{00} & a_{01}b_{01} \\ a_{00}b_{10} & a_{00}b_{11} & a_{01}b_{10} & a_{01}b_{11} \\ a_{10}b_{00} & a_{10}b_{01} & a_{11}b_{00} & a_{11}b_{01} \\ a_{10}b_{10} & a_{10}b_{11} & a_{11}b_{10} & a_{11}b_{11} \end{pmatrix}.$$

Q.E.D.

This correspondence does not only hold for transformations on H_2 but for transformation on any Hilbert space: If A and B are unitary transformation on two Hilbert spaces V and W, then $A \otimes B$ defines the unitary transformation on $V \otimes W$ that corresponds to the simultaneous (or sequential) composition of A and B (the order does not matter). Moreover, $A \otimes B$ does not introduce any entanglement.

Example 1.13. Let $A = B = \mathrm{H}$ the Hadamard transformation. Then

$$\begin{aligned} \mathrm{H} \otimes \mathrm{H} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} (\mathrm{H} \otimes \mathrm{H})|ij\rangle &= \frac{1}{2}\big(|00\rangle + (-1)^j|01\rangle + (-1)^i|01\rangle + (-1)^{i+j}|11\rangle\big) \\ &= \frac{1}{2}\big(|0\rangle + (-1)^i|1\rangle\big) \otimes \big(|0\rangle + (-1)^j|1\rangle\big), \end{aligned}$$

a non-entangled state, which is not a surprise given that $|ij\rangle$ is not entangled and that $\mathrm{H} \otimes \mathrm{H}$ stands for the simultaneous action of H on each qubit.

On the other, hand M_{CNOT} cannot be represented as a tensor product of two 2×2 matrices. To see this, consider the operation of M_{CNOT} on the non-entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$. We have $M_{\text{CNOT}}|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and we know that this is an entangled state. Hence, M_{CNOT} cannot possibly be equal to a tensor product of two 2×2 matrices.

Let us revisit the Hadamard transformation H, defined by the matrix

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

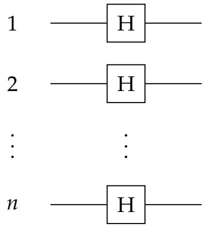
and consider the operation

$$\mathrm{H}^{\otimes n} = \underbrace{\mathrm{H} \otimes \cdots \otimes \mathrm{H}}_{n \text{ times}}$$

on n qubits. We have:

$$\begin{aligned} \mathrm{H}^{\otimes n} |0 \ldots 0\rangle &= \mathrm{H}|0\rangle \otimes \cdots \otimes \mathrm{H}|0\rangle \\ &= \frac{1}{\sqrt{2^n}} \big((|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle) \big) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle. \end{aligned}$$

Hence, the first basis vector $|0 \ldots 0\rangle$ is transformed into a uniform superposition of all the 2^n basis vectors. Graphically, this operation is denoted as follows:



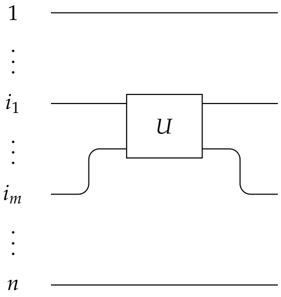
Definition 1.14. Let Ω be a set of quantum gates. A *quantum gate array (QGA)* (or a *quantum circuit*) on n qubits over Ω is a unitary transformation, which is composed out of quantum gates in Ω.

Note that mathematically there is no difference between a quantum gate and a QGA: both are unitary transformations. The idea is that, while a QGA may operate on a large number of qubits, a quantum gate may only operate on a small number of qubits.

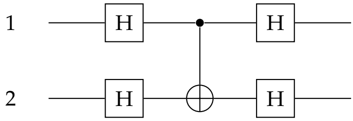
The basic step in building a quantum gate array is letting a single gate U operate on a selected number of qubits, say the qubits $i_1, \dots, i_m$. Mathematically, this operation (on n qubits) can be described by the unitary transformation

$$\mathrm{P}^{-1}_{i_1 \dots i_m} (U \otimes \mathrm{I}_{2^{n-m}})\, \mathrm{P}_{i_1 \dots i_m}$$

where $\mathrm{I}_{2^{n-m}}$ is the identity mapping on $H_{2^{n-m}}$ and $\mathrm{P}_{i_1 \dots i_m}$ is the transformation that permutes the qubits $1, \dots, m$ with the qubits $i_1, \dots, i_m$.



Example 1.15. Consider the following QGA consisting of Hadamard and CNOT gates:



The corresponding unitary transformation is $U = \mathrm{H}^{\otimes 2} \cdot M_{\text{CNOT}} \cdot \mathrm{H}^{\otimes 2}$. We claim that $U = \mathrm{P}^{-1}_{21}\, M_{\text{CNOT}}\, \mathrm{P}_{21}$, the operation of M_{CNOT} on the qubits 2 and 1 (instead of 1 and 2). Let $M = M_{\text{CNOT}}$. Then:

$$\begin{aligned} U|ij\rangle &= \mathrm{H}^{\otimes 2} \cdot M\Big(\frac{1}{2}\big(|0\rangle + (-1)^i|1\rangle\big) \otimes \big(|0\rangle + (-1)^j|1\rangle\big)\Big) \\ &= \mathrm{H}^{\otimes 2} \cdot M\Big(\frac{1}{2}\big(|00\rangle + (-1)^j|01\rangle + (-1)^i|10\rangle + (-1)^{i+j}|11\rangle\big)\Big) \end{aligned}$$

$$
\begin{aligned}
&= \mathrm{H}^{\otimes 2} \left(\frac{1}{2} \left(|00\rangle + (-1)^{j} |01\rangle + (-1)^{i+j} |10\rangle + (-1)^{i} |11\rangle \right) \right) \\
&= \mathrm{H}^{\otimes 2}\, \mathrm{H}^{\otimes 2} \left(|i \oplus j\rangle \otimes |j\rangle \right) \\
&= |i \oplus j\rangle \otimes |j\rangle
\end{aligned}
$$