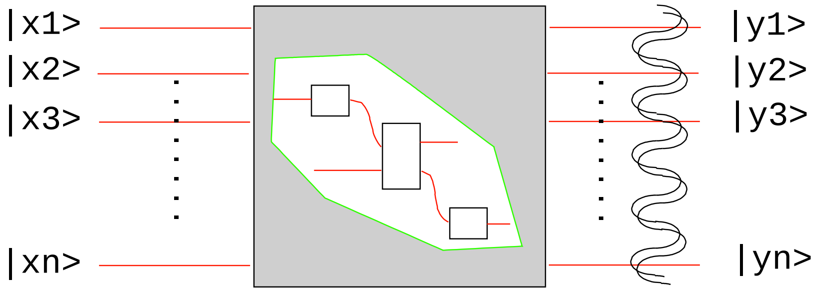

Figure 10: A generic quantum logic gate. The wavy lines mean that the output state is a generic superposition of product quantum states.

4 Elements of quantum information theory

The key idea for a working quantum computer is to decompose it into the simplest possible primitive operations or gates. The identification of universal logic gates, such as NAND, in classical computers (see Sec. 2.2) was of great help in the development of the field. A universal gate such as NAND operates locally on a very reduced number of bits, actually two. However, combining NAND gates in the appropriate number and sequence we can carry out arbitrary computations on arbitrarily many bits. This was very useful in practice for it allowed device engineers to just focus on creating only a few devices, leaving the rest to the circuit designer. The same rationale applies to a quantum computer.

Quantum registers – When a quantum computer is working, it is an evolution unitary operator that is effecting a predetermined action on a series of qubits. These qubits form the memory register of the machine or a *quantum register*. A quantum register is a string of qubits with a predetermined finite length. The space of all the possible register states makes up the Hilbert space of states associated to the quantum computer. If $\mathcal{H}$ is the Hilbert space of a single qubit and $|\Psi_i\rangle \in \mathcal{H}$, $i = 1, 2$, a given basis state, then a basis vector $|\Phi\rangle$ for the states of the quantum register is a tensor product of qubit states

$$|\Phi\rangle \;=\; |\Psi_1\rangle \otimes |\Psi_2\rangle \otimes \ldots \otimes |\Psi_n\rangle \;\in\; \mathcal{H}^{\otimes n}.$$

A quantum memory register can store multiple sequences of classical bits in superposition. This is a manifestation of the quantum parallelism and the reason of why quantum computer can, in principle, be exponentially faster than classical computers.

Quantum logical gates – A *quantum logic gate* is a unitary operator acting on the states of a certain set of qubits. If the number of such qubits is n, the quantum gate is represented by a $2^n \times 2^n$ matrix in the unitary group $\mathrm{U}(2^n)$. It is thus a *reversible* gate: we can reverse backwards the action, thereby recovering

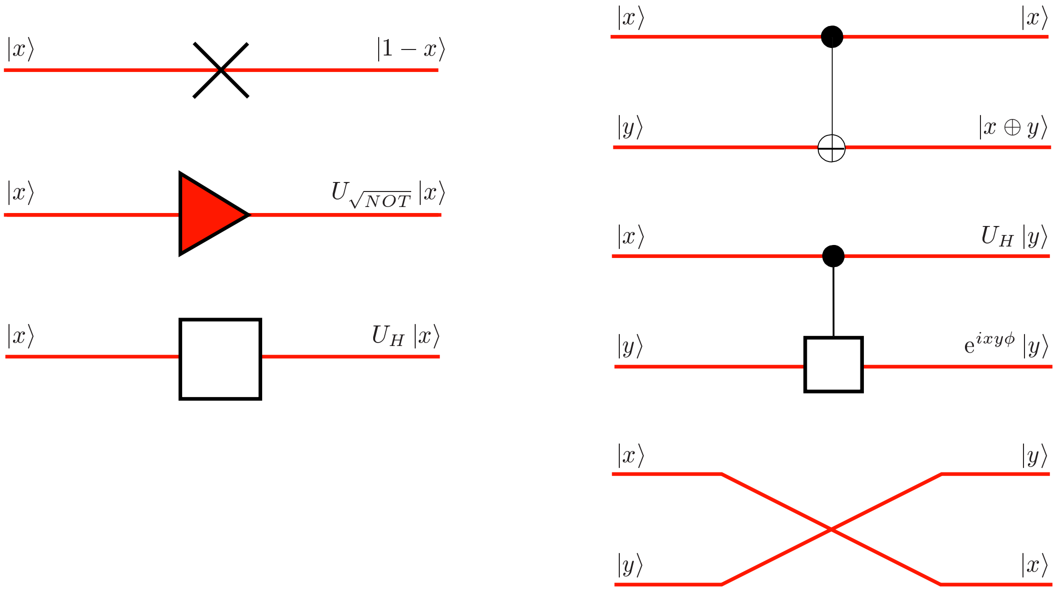

Figure 11: Right: Quantum unary gates. Top: NOT gate. Midddle: $\sqrt{\mathrm{NOT}}$ gate. Bottom: Hadamard gate. Left: Quantum binary gates. Top: CNOT gate. Middle: CPHASE gate. Bottom: SWAP gate.

the initial quantum state from the final one. Generically, a quantum logic gate can have any finite number of input qubits, but in practice we shall be interested in gates that are elementary for quantum computation, and those have a small number of input qubits. Diagrammatically, a quantum gate is represented by a "black box" wherein operation takes place, and a number of input (output) lines, used to wire up a set of gates, equal to the number of qubits involved in the computation (see Fig. 10). Let us see more explicitly how quantum gates look like by giving some representative gates in increasing order of complexity.

4.1 Elementary quantum logical gates

We now discuss how we can "naturally" generalize the classical reversible gates to unitary operators. The general rule is: The matrix elements of this unitary operator in the basis states have to recover the truth-tables of classical reversable logics. Before we discuss the general quantum gate, we start with some examples.

4.1.1 Unary qubit gates

1-qubit gates are are the simplest possible gates for they take one input qubit and transform it into one output qubit, see Fig. 11 for illustrations.

The quantum NOT – The *quantum* NOT gate is a one-qubit gate. Its unitary evolution operator U_{NOT} is:

$$U_{\mathrm{NOT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . \tag{4}$$

Letting U_{NOT} act on the basis states $|0\rangle$ and $|1\rangle$ we obtain the classical truth table. However, there is a basic underlying difference in between the classical NOT and U_{NOT}: the quantum gate acts on qubits while the classical gate does it on bits. This difference allows us to introduce a truly quantum one-qubit gate:

The quantum $\sqrt{\mathrm{NOT}}$ – The matrix representation the $\sqrt{\mathrm{NOT}}$ gate is

$$U_{\sqrt{\mathrm{NOT}}} = \frac{1}{2}\begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix} . \tag{5}$$

This gate, when applied twice, gives NOT. Explicitly

$$\begin{aligned} U_{\sqrt{\mathrm{NOT}}}\, U_{\sqrt{\mathrm{NOT}}} &= \frac{1}{4}\begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix} \cdot \begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix} . \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \equiv U_{\mathrm{NOT}} \end{aligned}$$

This gate has no counterpart in classical computers since it implements nontrivial superpositions of basis states, e.g. it maps

$$U_{\sqrt{\mathrm{NOT}}} : \qquad |0\rangle \longmapsto \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle .$$

The Hadamar gate – Another one-qubit gate without analogue in classical circuitry is the so called Hadamard gate H (see Sec. 1.5.4). It is defined as

$$U_{\mathrm{H}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{6}$$

4.1.2 Binary qubit gates

2-qubit gates represent the next level of complication. In fact we will need no 3-qubit gates for a complete quantum mechanical reverible logics, in contrast to the classical case. This is due to the fact that there are quantum logical gates with no classical counterparts.

The quantum XOR – The XOR (*exclusive*-OR), or CNOT (*controlled*-NOT) gate, is an example of a quantum logic gate on two qubits. It is instructive

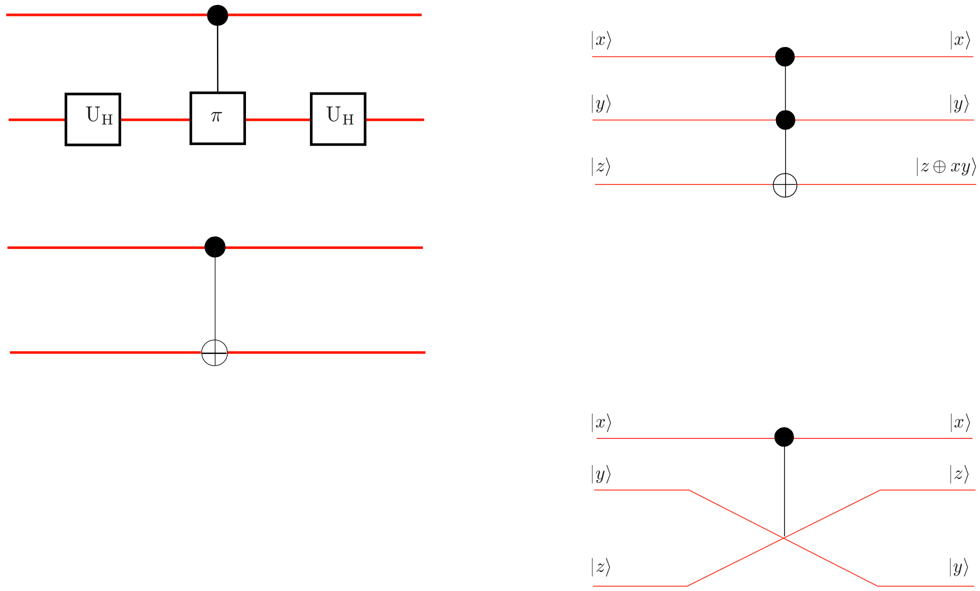

Figure 12: Left: The quantum-CNOT gate bottom is identical to a controlled-*pi* gate in combination with two Hadamar's (top). Right: The CCNOT-gate (top) and the controlled-SWAP (bottom).

to give the unitary action $U_{\mathrm{XOR,CNOT}}$ of this gate in several forms. Its action on the two-qubit basis states is defined by the classical truth table for CNOT:

$$U_{\mathrm{CNOT}}|00\rangle = |00\rangle, \quad U_{\mathrm{CNOT}}|10\rangle = |11\rangle \ , \tag{7}$$

$$U_{\mathrm{CNOT}}|01\rangle = |01\rangle, \quad U_{\mathrm{CNOT}}|11\rangle = |10\rangle. \tag{8}$$

From this definition we see that the name of this gate is quite apparent for it means that it executes a NOT operation on the second qubit conditioned to have the first qubit in the state $|1\rangle$. Its matrix representation is

$$U_{\mathrm{CNOT}} \; = \; U_{\mathrm{XOR}} \; = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} .$$

The diagrammatic representation of the CNOT gate is shown in Fig. 11. We shall see how this quantum CNOT gate plays a paramount role in both the theory and experimental realization of quantum computers. It allows implementing conditional logic at a quantum level.

The controlled phase gate – Unlike the CNOT gate, there are two-qubit gates with no analogue classical gate. One example is the *controlled-phase* gate or CPHASE:

$$U_{\mathrm{CP}(\phi)} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{e}^{\mathrm{i}\phi} \end{pmatrix} \tag{9}$$

It implements a conditional phase-shift $\mathrm{e}^{\mathrm{i}\phi}$ on the second qubit.

An important result is that we can reproduce the CNOT gate with a controlled-phase gate of $\phi = \pi$ and two Hadamards transforms on the target qubits as shown in Fig. 12. This is a simply consequence of the relation

$$\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} .$$

SWAP and $\sqrt{\mathrm{SWAP}}$ – Other interesting two-qubit gates are the SWAP gate, which interchanges the states of the two qubits, and the $\sqrt{\mathrm{SWAP}}$ gate, whose matrix representations are

$$U_{\mathrm{SWAP}} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} , \qquad U_{\sqrt{\mathrm{SWAP}}} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1+\mathrm{i}}{2} & \frac{1-\mathrm{i}}{2} & 0 \\ 0 & \frac{1-\mathrm{i}}{2} & \frac{1+\mathrm{i}}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

4.1.3 3-Qubit Gates

An immediate extension of the CNOT construction to three-qubits yields the CCNOT gate (or $\mathrm{C}^2\mathrm{NOT}$),[‡] which is also called Toffoli gate:

$$(x, y, z) \longmapsto (x, y, z \text{ XOR } xy) .$$

The matrix representation is a one-qubit extension of the CNOT gate (see Fig. 12), namely

$$U_{\mathrm{CCNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} . \tag{10}$$

The associated truth table is:

[‡] Controlled-controlled-not gate.

x	y	z	x'	y'	z'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Fredkin gate – Another instance of a three-qubit gate is the Fredkin gate. It is a *controlled*-SWAP operation, schematically shown in Fig. 12 and represented by the matrix

$$U_{\mathrm{F}} \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

4.2 The generic single-qubit gate

The generic single-qubit gate is a unitary 2×2 matrix, usually considered with respect to the "computational basis states"

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \;=\; |\uparrow\rangle \;=\; |0\rangle$$

and

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \;=\; |\downarrow\rangle \;=\; |1\rangle .$$

We have already discussed the Pauli-matrices $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$, as well as the Hadamard gate $\mathbf{H} = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X}+\mathbf{Z})$. Important are also the $\pi/8$-gate

$$\mathbf{T} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & \exp i\frac{\pi}{4} \end{pmatrix} \;=\; \exp\left(\mathbf{i}\frac{\pi}{\mathbf{8}}\right) \begin{pmatrix} \exp -i\frac{\pi}{8} & 0 \\ 0 & \exp i\frac{\pi}{8} \end{pmatrix} \tag{11}$$

and the phase-gate

$$\mathbf{S} \;=\; \mathbf{T^2} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} . \tag{12}$$

Note that $\mathbf{S^2} = \mathbf{Z}$.

4.2.1 SU-rotations

The group of all hermitian 2×2 matrizes are call the SU-group, its generator are the Pauli-matrizes which form a Lie-Algebra. In particular, we have already seen in Sec. 1.5.4 that

$$\exp i\alpha\mathbf{X}\ , \qquad \exp i\beta\mathbf{Y}\ , \qquad \exp i\gamma\mathbf{Z}$$

are nothing but "rotations" (about the main axis) in Hilbert space. The general rotation is

$$\mathbf{R}_{\hat{\mathbf{n}}}(\theta) \;=\; \exp\left(-\mathbf{i}\theta\frac{\hat{\mathbf{n}}\cdot\vec{\sigma}}{\mathbf{2}}\right) \;=\; \cos\left(\frac{\theta}{\mathbf{2}}\right)\mathbf{1} - \mathbf{i}\sin\left(\frac{\theta}{\mathbf{2}}\right)\hat{\mathbf{n}}\cdot\vec{\sigma}$$

where $\vec{\sigma} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ and $\hat{n}$ is a unit vector. Consequently $(\hat{n}\cdot\vec{\sigma})^2 = \mathbf{1}$ and the decomposition of $\mathbf{R}_{\hat{\mathbf{n}}}(\theta)$ into sine and cosine terms can be verified in a similar manner that of $\exp(i\alpha\mathbf{X})$ in Sec. 1.5.4. Obviously

$$\mathbf{R}^{\dagger}_{\hat{\mathbf{n}}}(\theta) \;=\; \mathbf{R}_{\hat{\mathbf{n}}}(-\theta) \;=\; \mathbf{R}^{-\mathbf{1}}_{\hat{\mathbf{n}}}(\theta)\ .$$

In terms of the Bloch sphere representation of qubits, $\mathbf{R}_{\hat{\mathbf{n}}}(\theta)$ has an interpretation as a rotation. From Sec. 1.5.4 we recall the general pure single-qubit state

$$|\theta,\varphi\rangle \;=\; \exp\left(-i\frac{\varphi}{2}\right)\cos\frac{\theta}{2}|\uparrow\rangle + \exp\left(i\frac{\varphi}{2}\right)\sin\frac{\theta}{2}|\downarrow\rangle$$

$$(0 \le \theta \le \pi; 0 \le \varphi \le 2\pi).$$

The angles θ and φ characterize a point

$$\vec{P} \;=\; (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

on the Bloch sphere. The effect of $\mathbf{R}_{\hat{\mathbf{n}}}(\alpha)$ on the "state" $\vec{P}$ is then a rotation of $\vec{P}$ by an angle α about the $\hat{n}$ axis of the Bloch sphere.

Some examples – We will not prove that statement in general here but only make it plausible. If the statement is true, then, for example, the special transformation $\mathbf{R}_{\vec{\mathbf{P}}}(\alpha)$ should leave the state $|\theta,\varphi\rangle$ (characterized by the Bloch vector $\vec{P}$ invariant (for arbitrary α) because $\vec{P}$ is the axis of rotation. To see that, write

$$\mathbf{R}_{\vec{\mathbf{P}}}(\alpha) = \exp\left(\mathbf{i}\frac{\alpha}{\mathbf{2}}\vec{\mathbf{P}}\cdot\vec{\sigma}\right)$$

where

$$\vec{P}\cdot\vec{\sigma} \;=\; \sin\theta\cos\varphi\mathbf{X} + \sin\theta\sin\varphi\mathbf{Y} + \cos\theta\mathbf{Z}$$

$$= \begin{pmatrix} \cos\theta & \sin\theta\cos\varphi - i\sin\theta\sin\varphi \\ \sin\theta\cos\varphi + i\sin\theta\sin\varphi & -\cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta e^{-i\varphi} \\ \sin\theta e^{i\varphi} & -\cos\theta \end{pmatrix}.$$

Now we attempt

$$\vec{P}\cdot\vec{\sigma}|\theta,\varphi\rangle \;=\; \begin{pmatrix} \cos\theta & \sin\theta e^{-i\varphi} \\ \sin\theta e^{i\varphi} & -\cos\theta \end{pmatrix} \begin{pmatrix} e^{-i\frac{\varphi}{2}}\cos\frac{\theta}{2} \\ e^{i\frac{\varphi}{2}}\sin\frac{\theta}{2} \end{pmatrix}$$

$$= \begin{pmatrix} \cos\theta e^{-i\frac{\varphi}{2}}\cos\frac{\theta}{2} + \sin\theta e^{-i\frac{\varphi}{2}}\sin\frac{\theta}{2} \\ \sin\theta e^{i\frac{\varphi}{2}}\cos\frac{\theta}{2} - \cos\theta e^{i\frac{\varphi}{2}}\sin\frac{\theta}{2} \end{pmatrix} \;=\; \begin{pmatrix} e^{-i\frac{\varphi}{2}}\cos\frac{\theta}{2} \\ e^{i\frac{\varphi}{2}}\sin\frac{\theta}{2} \end{pmatrix} \;=\; |\theta,\varphi\rangle.$$

Thus $|\theta,\varphi\rangle$ is an eigenvector of $\vec{P}\cdot\vec{\sigma}$ with eigenvalue 1 (as already mentioned in Sec. 1.5.4) and application of $\exp(i\alpha\vec{P}\cdot\vec{\sigma})$ just leads to an irrelevant overall phase.

Rotations aroune $\hat{z}$ – The calculation of θ' and φ' in

$$|\theta',\varphi'\rangle \;=\; \mathbf{R}_{\hat{\mathbf{n}}}(\alpha)|\theta,\varphi\rangle$$

for general $\hat{n}$ is a tedious exercise in spherical geometry. $\hat{n}=\hat{z}$, though, it is trivial, because

$$\mathbf{R}_{\hat{\mathbf{z}}}(\alpha) \;=\; \exp(\mathbf{i}\frac{\alpha}{\mathbf{2}}\mathbf{Z}) \;=\; \begin{pmatrix} e^{i\frac{\alpha}{2}} & 0 \\ 0 & e^{-i\frac{\alpha}{2}} \end{pmatrix}$$

and thus

$$\mathbf{R}_{\hat{\mathbf{z}}}(\alpha)|\theta,\varphi\rangle \;=\; \begin{pmatrix} e^{i\frac{\alpha}{2}} & 0 \\ 0 & e^{-i\frac{\alpha}{2}} \end{pmatrix} \begin{pmatrix} e^{-i\frac{\varphi}{2}\cos\frac{\theta}{2}} \\ e^{i\frac{\varphi}{2}\sin\frac{\theta}{2}} \end{pmatrix} \;=\; \begin{pmatrix} e^{-i\frac{\varphi-\alpha}{2}\cos\frac{\theta}{2}} \\ e^{i\frac{\varphi-\alpha}{2}\sin\frac{\theta}{2}} \end{pmatrix} \;=\; |\theta,\varphi-\alpha\rangle\;,$$

as expected.

4.2.2 Representation of the generic single-qubit operator

Any unitary single-qubit operator can be written in the form

$$\mathbf{U} \;=\; \mathbf{e}^{\mathbf{i}\alpha}\mathbf{R}_{\hat{\mathbf{n}}}(\theta).$$

It is often desirable to employ only rotations about the coordinate axes instead of rotations about arbitrary axes $\hat{n}$. This is indeed possible:

$$\mathbf{U} \;=\; \mathbf{e}^{\mathbf{i}\alpha}\,\mathbf{R}_{\hat{\mathbf{z}}}(\beta)\,\mathbf{R}_{\hat{\mathbf{y}}}(\gamma)\,\mathbf{R}_{\hat{\mathbf{z}}}(\delta)\;. \tag{13}$$

For any unitary $\mathbf{U}$ suitable values of $\alpha\cdots\delta$ can be found. A similar decomposition with $\hat{x}$ instead of $\hat{z}$ can also be found. Another decomposition which will be used in Sec. 4.4 is closely related to the above single-qubit $Z-Y$ decomposition. Let

$$\mathbf{A}=\mathbf{R}_{\hat{\mathbf{z}}}(\beta)\mathbf{R}_{\hat{\mathbf{y}}}(\frac{\gamma}{\mathbf{2}})\;;\qquad \mathbf{B}=\mathbf{R}_{\hat{\mathbf{y}}}(-\frac{\gamma}{\mathbf{2}})\mathbf{R}_{\hat{\mathbf{z}}}(-\frac{\delta+\beta}{\mathbf{2}})\;;\qquad \mathbf{C}=\mathbf{R}_{\hat{\mathbf{z}}}(\frac{\delta-\beta}{\mathbf{2}})\;.$$

Note that

$$\mathbf{ABC} \;=\; \mathbf{1}\;.$$

One can prove that

$$e^{i\alpha}\,\mathbf{AXBXC} \;=\; \mathbf{e}^{\mathbf{i}\alpha}\,\mathbf{R}_{\hat{\mathbf{z}}}(\beta)\,\mathbf{R}_{\hat{\mathbf{y}}}(\gamma)\,\mathbf{R}_{\hat{\mathbf{z}}}(\delta) \;=\; \mathbf{U}\;. \tag{14}$$

This relation will be used further below in order to show that every 2-qubit gate can be decomposed in quantum-CNOT gates and single-qubit gates.

4.3 Controlled gates

These multi-qubi gates have one or more *control qubits* and *target qubits*. The simplest example is the well-known controlled NOT; in matrix notation with respect to the usual computational basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ it reads

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{X} \end{pmatrix} \tag{15}$$

(using an obvious block matrix notation). Replacing $\mathbf{X}$ by an arbitrary unitary single-qubit operation $\mathbf{U}$, we arrive at the *controlled-U* (CU) gate.

The CU gate can be implemented using CNOT and single-qubit gates. The idea is to use the "$AXBXC'$" decomposition and apply $e^{i\alpha}\mathbf{AXBXC} = \mathbf{U}$ if the control qubit is set and $\mathbf{ABC} = \mathbf{1}$ if not. The circuit in Fig. 13 does the trick. Obviously the $e^{i\alpha}$ phase factor as well as the two NOT ($= \mathbf{X}$) operations are only active if the control qubit is set.

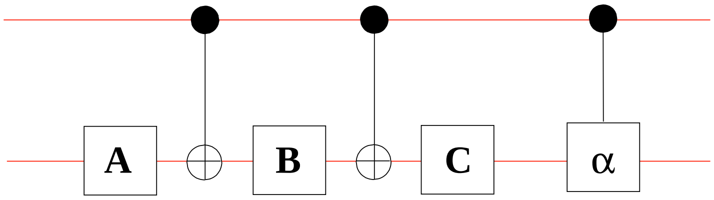

Figure 13: A circuit for the controlled-U gate, using the decompostion (14), three CNOT-gates (15) and the controlled phase-shift gate CPHASE (9).

4.4 Universal quantum gates

A set of gates is called universal, if any unitary operation may be approximated to arbitrary accuracy by a quantum circuit involving only these gates. The set of four gates

- Hadamard,
- phase,
- CNOT,
- and $\frac{\pi}{8}$

are universal. It is essential for the possiblilty of building real quantum computer that this set is (A) finite and (B) does contain only single-qubit and two-qubit gates. The reason that no three-qubit gate is needed, as for classical reversible logic, lies in the fact that quantum-gates which do not have a classical counterpart can be constructed.

Outline of proof – We will show by a three-step process that above four gates are universal:

(i) Any unitary operator can be expressed (exactly) as a product of unitary operators affecting only two computational basis states: "Two-level gates are universal."

(ii) Any unitary operator may be expressed (exactly) using single-qubit and CNOT gates: "Single-qubit and CNOT gates are universal."

(iii) Single-qubit operations may be *approximated* to arbitrary accuracy using Hadamard, phase, and $\frac{\pi}{8}$ gates.

4.4.1 (i) Two-level gates are universal

Any $d \times d$ unitary matrix $\mathbf{U}$ can be written as a product of (at most) $\frac{d(d-1)}{2}$ two-level unitary matrices (that is, unitary matrices which act non-trivially only on at most two vector components).

This can be shown as follows. Concentrate on the top left corner of the unitary matrix

$$\mathbf{U} = \begin{pmatrix} a & d & \cdots \\ b & c & \cdots \\ . & . & \cdots \end{pmatrix}.$$

The 2×2 unitary matrix

$$\mathbf{U_1} = \frac{\mathbf{1}}{\sqrt{|\mathbf{a}|^2 + |\mathbf{b}|^2}} \begin{pmatrix} a^* & b^* \\ b & -a \end{pmatrix}$$

eliminates the second element in the first column of $\mathbf{U}$:

$$\mathbf{U_1} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a' \\ 0 \end{pmatrix}.$$

(Of course we use $\mathbf{U_1}$, supplemented by a $(d-2) \times (d-2)$ unit matrix so that products like $\mathbf{U_1 U}$ make sense.) Similar 2×2 matrices can be used to eliminate further elements from the first column of $\mathbf{U}$:

$$\mathbf{U_{d-1} U_{d-2} \cdots U_1 U} = \begin{pmatrix} 1 & 0 & 0 & \cdots \\ 0 & c' & . & \cdots \\ 0 & . & . & \text{(non-zero)} \\ . & & & \end{pmatrix}.$$

Note that initially the first column had unit norm because $\mathbf{U}$ is unitary. We have applied only unitary (that is, norm-preserving) operations so the end result is still a unit vector but has only one non-zero component, which must be 1. (A phase can be eliminated.) Due to unitarity (of a product of unitary matrices) all elements in the first row other than the leftmost one must also vanish.

The elimination process can be continued in other columns and finally

$$\mathbf{U_k U_{k-1} \cdots U_1 U} \;=\; \mathbf{1}$$

$$\left(k \leq \frac{d(d-1)}{2} = (d-1) + (d-2) + \cdots + 2 + 1\right),$$

and thus

$$\mathbf{U} \;=\; \mathbf{U_1^\dagger U_2^\dagger \cdots U_k^\dagger}$$

which is the desired decomposition.

4.4.2 (ii) Single-qubit and CNOT gates are universal

This is because we can use them to build the arbitrary two level gates discussed in the previous step. The basic idea is simple: Transform the Hilbert space such that the two relevant basis states become the basis states of one qubit, perform the desired single-qubit operation on that qubit, and transform back to the original basis. The basis reshuffling can be achieved via higher-order controlled-NOT operations, which in turn can be reduced to simple CNOT operations.

Example GHZ-states – We just discuss a three-qubit example: How to perform a two-level operation involving the states, $|ABC\rangle = |000\rangle$ and $|111\rangle$. These states are called GHZ-states (Greenberger, Horne and Zeilinger) and can be used for three-qubit entanglements.

First, apply the CCNOT Toffoli gate $\theta^{(3)}$ on NOT A, NOT B, c. The first two qubits are control qubits which in this case must be 0, the last one is the target. We can see from the matrix representation (10) that this operation swaps $|000\rangle$ with $|001\rangle$ and leaves everything else untouched:

Now, apply $\theta^{(3)}($ NOT $A, C, B)$, the second qubit is now the target. This swaps $|001\rangle$ with $|011\rangle$. The net effect has been to swap $|000\rangle$ with $|011\rangle$. Now, the the controlled controlled phase gate C^{2}PHASE (a three-qubit gneralization of the CPHASE-gate (9)) can be applied, perfoming the operation $\mathbf{U}$ on qubit A, provided both B and C are 1. Finally the basis states can be rearranged in their original order.

4.4.3 (iii) Hadamard, phase and $\frac{\pi}{8}$ are (approximately) universal single-qubit gates

Recall that the most general single-qubit gate is a rotation of the Bloch sphere by an arbitrary angle about an arbitrary axis (combined with a trivial phase factor).

It is clearly impossible to reduce *exactly* a set of matrices, dependent on two real variables, onto a *finite* set of universal matrices.

Imagine though that we could implement a rotation about some axis $\hat{n}$ by an angle α which is an *irrational* multiple of 2π. Due to irrationality, the angles

$$(n\alpha)\mathrm{modulo}(2\pi) \qquad (n = 0(1)\infty)$$

are dense in $[0, 2\pi]$ and thus an arbitrary rotation about $\hat{n}$ can be approximated to arbitrary precision ϵ by repeating the α rotation:

$$\mathbf{R}_{\hat{\mathbf{n}}}(\beta) \;=\; (\mathbf{R}_{\hat{\mathbf{n}}}(\alpha))^{\nu} + \mathbf{O}(\epsilon) \; . \tag{16}$$

Irrational rotations – If we can implement two such irrational rotations (16) about mutually orthogonal axes we can perfom arbitrary rotations due to the Z-Y-Z decomposition property (13). This is exactly the route followed by Boykin et al. [32]. We will not give the (lengthy) proof here, we just note that the angle $\pi/8$ enters the rotation matrizes via

$$\cos(\alpha) \;=\; \cos^2\left(\frac{\pi}{8}\right) \;=\; \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) .$$

Invoking some theorems from algebra and number theory it can be shown that α is an irrational multiple of 2π. That is the reason the $\pi/8$ gate does the job.

References

[1] Michael Brooks. *Quantum Computing and Communications*. Springer, New York, 1999. 152 pp.

[2] Jozef Gruska. *Quantum computing*. McGraw-Hill, London, 2000. 439 pp.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge Univ. Press, Cambridge, 2001. 676 pp.

[4] Colin P. Williams and Scott H. Clearwater. *Explorations in quantum computing*. Springer, New York, 1998. 307 pp, CD-ROM, DM 98.00.

[5] A. Steane. Quantum computing. *Rep. Prog. Phys.*, 61:117–173, 1998.

[6] Dorit Aharonov. Quantum computation. In Dietrich Stauffer, editor, *Annual Reviews of Computational Physics VI*, pages 259–346. World Scientific, 1999. Preprint quant-ph/9812037.

[7] A. Galindo and M. A. Martin-Delgado. Information and computation: Classical and quantum aspects, 2002. Rev. Mod. Phys., to appear. Preprint quant-ph/0112105.

[8] John Preskill. Quantum computation. http://theory.caltech.edu/ preskill/ph229/, 1997. 413 pp.

[9] Paul Benioff. Quantum mechanical Hamiltonian models of Turing machines. *J. Stat. Phys.*, 29:515, 1982.

[10] Y. Lecerf. Machines de Turing reversibles. Compters Rendus **257**, 1597, 1963.

[11] Richard P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[12] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, Piscataway, NJ, 1994. IEEE Press.

[13] Stephan Mertens. Computational complexity for physicists. Lecture given at the DPG school on "Quantum Computing", 2000. Preprint cond-mat/0012185.

[14] Barenco, A., C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter. *"Elementary gates for quantum computation"*, Phys. Rev. A **52**, 3457-3467 (1995).

[15] Barenco, A., D. Deutsch, A. Ekert and R. Jozsa. *"Conditional quantum dynamics and logic gates"*, Phys. Rev. Lett. **74**, 4083-6 (1995).

[16] Alonzo Church. An unsolvable problem of elementary number theory. *Am. J. Math.*, 58:345–363, 1936.

[17] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc. Ser.*, 42:230, 1936. See also ibidem 43, 544.

[18] Douglas R. Hofstadter. *Gdel, Escher, Bach: An Eternal Golden Braid*. Basic Books, New York, 1979. 777 pp.

[19] Leo Szilard. ber die Entropieverminderung in einem thermodynamischen System bei Eingriffen intelligenter Wesen. *Z. Physik*, 53:840–856, 1929.

[20] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal Res Dev*, 5:183–191, 1961.

[21] Seth Lloyd. Ultimate physical limits to computation. *Nature*, 406:1047–1054, 2000.

[22] N. Margolus and L.B. Levitin. title. In T. Toffoli, M. Biafore, and J. Le?o, editors, *Proceedings of the Fourth Workshop on Physics and Computation PhysComp96 (New England Complex Systems Institute, Boston, MA, 1996)*. North-Holland, 1998. Physica D Vol. 120.

[23] Richard P. Feynman. *Feynman Lectures on Computing*, chapter 6, Quantum Mechanical Computers. Addison-Wesley, 1996. Originally published in Optics News, February 1985, pp. 11-20; see also Found. Phys. **16**, 507-532 (1986).

[24] P. Jordan and E. Wigner. Über das Paulische Äquivalenzverbot. *Z. Physik*, 47:631–651, 1928.

[25] Jian-Wei Pan, Dik Bouwmeester, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. *Nature*, 403:515–519, 2000.

[26] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe. Experimental entanglement of four particles. *Nature*, 404:256–259, 2001.

[27] Rainer Blatt. Push-button entanglement. *Nature*, 404:231–232, 2001.

[28] Brian Julsgaard, Alexander Kozhekin, and Eugene S. Polzik. Experimental long-lived entanglement of two macroscopic objects. *Nature*, 413:400–403, 2001.

[29] J. Ignacio Cirac. Quantum physics: Entangled atomic samples. *Nature*, 413:375–377, 2001.

[30] L. Grover. (title). In *Proc. 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219, New York, 1996. ACM Press.

[31] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, 1997. Preprint quant-ph/9706033.

[32] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing, 1999. Preprint quant-ph/9906054.

[33] D.P. DiVincenzo. The physical implementation of quantum computation. *Fortschr. Phys.*, 48:771–783, 2000. Preprint quant-ph/0002077.

[34] C.E. Hughes and S. Wimperis. Bounds on spin dynamics and the design of multiple-pulse NMR experiments. *J. Chem. Phys.*, 106:2105–2117, 1997.

[35] J. Stoustrup, O. Schedletzky, S.J. Glaser, C. Griesinger, N.C. Nielsen, and O.W. Sorensen. Generalized bound on quantum dynamics: efficiency of unitary transformations between non-hermitian states. *Phys. Rev. Lett.*, 74:2921–2924, 1995.

[36] J. H. Smet, R. A. Deutschmann, F. Ertl, W. Wegscheider, G. Abstreiter, and K. von Klitzing. Gate-voltage control of spin interactions between electrons and nuclei in a semiconductor. *Nature*, 415:281–286, 2002.

[37] J. Kikkawa. Eavesdropping on spin talk. *Nature*, 415:273–274, 2002.

[38] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[39] D. Dieks. Communication by EPR devices. *Phys. Lett. A*, 92:271–271, 1982.

[40] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[41] C.H. Bennettr. Logical reversability of computation. *IBM J. Res. Dev.* **17**, 525-532, 1973.

[42] C.H. Bennett and S.J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[43] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India, December 1984)*, pages 175–179, New York, 1984. IEEE.

[44] H. Zbinden, J.D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittle. Interferometry with Faraday mirrors and quantum cryptography. *Electron. Lett.*, 33:586–588, 1997.

[45] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[46] G.M. Palma, K.-A. Suominen, and A.K. Ekert. Quantum computers and dissipation. *Proc. Roy. Soc. A*, 452:567–584, 1996.

[47] D.A. Lidar, I.L. Chuang, and K.B. Whaley. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, 81:2594–2597, 1998.

[48] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, 2000.

[49] L. Viola, E.M. Fortunato, M.A. Pravia, E. Knill, R. Laflamme, and D.G. Cory. Experimental realization of noiseless subsystems for quantum information processing. *Science*, 293:2059–2063, 2001.