V. ELEMENTS OF QUANTUM COMPUTING

In this chapter we will work out a set of *universal quantum gates*. An excellent reference for this material is Chapter 4 of Nielsen and Chuang [3] which consists to a large extent of exercises which the reader is encouraged to solve in order to really learn the material. (However, the anticipated results of the exercises are stated clearly enough so that the lazy reader may also get along without solving the exercises.) Preskill [8], Sec. 6.2.3 discusses universal quantum gates qfrom a different (Lie-group) point of view.
Up until now two main classes of quantum algorithms can be distinguished:

- Quantum Fourier transform based algorithms. The most prominent member of this class is Shor's [11] algorithm with its exponential speedup of number factoring as compared to classical algorithms.
- Quantum searching algorithms, for example the one by Grover [27, 28] with its quadratic speedup for a "needle in a haystack" search in an unstructured data base.

We will discuss the elementary building blocks for these algorithms: quantum gates. In several steps we will show that arbitrary quantum gates can be constructed from a small number of one-and two-bit gates. To "construct" here will mean "to approximate to arbitrary precision". Note that in Chap. II we argued that using *classical reversible* gates, three-bit operations are needed to achieve universality, whereas here we will need at most two-qubit operations. This shows that quantum computing is "more powerful" than classical computing.

A. Single-qubit gates

A quantum gate in general is an arbitrary unitary operator on the Hilbert space of interest. A 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 already know the $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$ gates (Pauli matrices, with eigenvalues ±1) as well as the Hadamard gate $\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X}+\mathbf{Z})$. Important are also

$$\mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & \exp i\frac{\pi}{4} \end{pmatrix} = \exp i\frac{\pi}{8} \begin{pmatrix} \exp -i\frac{\pi}{8} & 0 \\ 0 & \exp i\frac{\pi}{8} \end{pmatrix},$$

(the $\frac{\pi}{8}$ gate) and

$$\mathbf{S} = \mathbf{T}^2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

(the phase gate). Note that $\mathbf{T}^2 = \mathbf{Z}$. We have already seen in Chap. I that

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

are nothing but "rotations" in Hilbert space. This can be generalized to

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

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 $\mathbf{R}_{\hat{n}}(\theta)$ into sine and cosine terms can be verified in a similar manner that of $\exp i\alpha\mathbf{X}$ etc in Chap. I. Obviously

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

In terms of the Bloch sphere representation of qubits, $\mathbf{R}_{\hat{n}}(\theta)$ has an interpretation as a rotation. From Chap. I 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 $\mathbf{R}_{\hat{n}}(\alpha)$ 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.
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 $\mathbf{R}_{\vec{P}}(\alpha)$ 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

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

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 Chap. I) and application of $\exp(i\alpha\vec{P}\cdot\vec{\sigma})$ just leads to an irrelevant overall phase. Tha calculation of θ' and φ' in

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

for general $\hat{n}$ is a tedious exercise in spherical geometry (just try!). For $\hat{n}=\hat{z}$, though, it is trivial, because

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

and thus

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

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

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

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

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

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

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 the next subsection is closely related to the above single-qubit $Z-Y$ decomposition. Let

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

$$\mathbf{C} = \mathbf{R}_{\hat{z}}(\frac{\delta-\beta}{2}).$$

Note that

$$\mathbf{ABC} = \mathbf{1},$$

furthermore

$$\mathbf{XYX} = -\mathbf{Y}; \quad \mathbf{XZX} = -\mathbf{Z}$$

can be used to show that

$$\mathbf{XBX} = \mathbf{R}_{\hat{y}}(\frac{\gamma}{2})\mathbf{R}_{\hat{z}}(\frac{\delta+\beta}{2})$$

and thus

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

B. 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

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

(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 roles of control and target qubits may be shifted by basis transformations (in the individual qubit Hilbert spaces). One example is shown in figure V.1. Here control and target qubits have interchanged their roles.

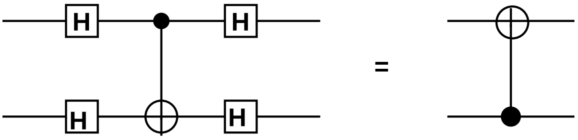


FIG. V.1: Ambiguity of control and target qubits

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 figure V.2 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.

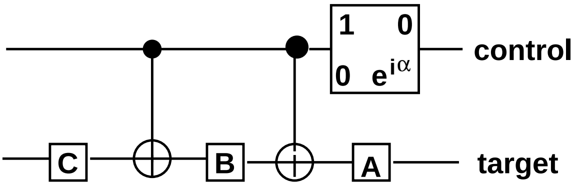


FIG. V.2: A circuit for the controlled-U gate

In higher-order controlled operations n control qubits and k target qubits are used; an important example is the Toffoli (controlled-controlled-NOT, or C^{2}NOT) gate, or more general, the C^{2}U gate for some arbitrary single-qubit $\mathbf{U}$. Actually, C^{2}U can be built from CNOT and single-qubit gates. To see this, consider the unitary operator $\mathbf{V}$, with $\mathbf{V}^2 = \mathbf{U}$ (which always exists) and build the circuit shown in figure V.3. If neither of the control qubits is set, nothing at all happens. If only one control qubit is set, $\mathbf{V}^\dagger = \mathbf{V}^{-1}$ and one $\mathbf{V}$ act on the target qubit. If both control qubits are set, $\mathbf{V}^\dagger$ is not switched on, but both $\mathbf{V}$'s are. It is interesting to note that with quantum reversible gates the Toffoli gate can be decomposed into one-

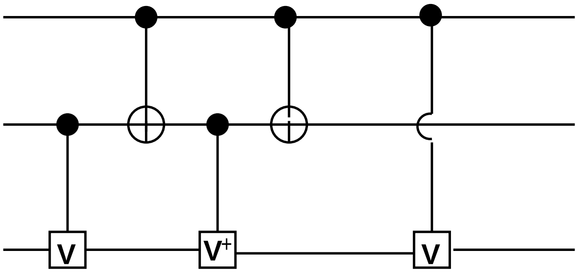


FIG. V.3: A circuit for the controlled-controlled-U gate; $\mathbf{V}^2 = \mathbf{U}$

and two-qubit gates, which is not possible classically. (Otherwise universal reversible classical computation with just one- and two-bit operations would be possible, contrary to what we discussed in Chap. II.) The Toffoli gate (and as we shall see, *any* gate) can be made from

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

gates. The Toffoli gate needs about a dozen of these more elementary gates, as shown in Fig. 4.9 of Nielsen and Chuang [3]. Also of interest is Fig. 4.10, showing how to implement C^{n}U from Toffoli and U gates.

C. 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 listed above will be shown to be universal in a three-step process.

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) (From i) and preceding subsections.) 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.

We start with step 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

$$\mathbf{U}_1 = \frac{1}{\sqrt{|a|^2+|b|^2}}\begin{pmatrix} a^* & b^* \\ b & -a \end{pmatrix}$$

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 $\mathbf{U}_1\mathbf{U}$ make sense.) Similar 2×2 matrices can be used to eliminate further elements from the first column of $\mathbf{U}$:

$$\mathbf{U}_{d-1}\mathbf{U}_{d-2}\cdots\mathbf{U}_1\mathbf{U} = \begin{pmatrix} 1 & 0 & 0 & \cdots \\ 0 & c' & . & \cdots \\ 0 & . & . & \text{(non-zero)} \\ . & & & \end{pmatrix}.$$

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

$$\mathbf{U}_k\mathbf{U}_{k-1}\cdots\mathbf{U}_1\mathbf{U} = \mathbf{1}$$

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

and thus

$$\mathbf{U} = \mathbf{U}_1^\dagger\mathbf{U}_2^\dagger\cdots\mathbf{U}_k^\dagger$$

which is the desired decomposition. (I suspect that this decomposition is fairly elementary from the point of view of Lie groups (continuous groups): The $d\times d$ unitary matrices form a Lie group $U(d)$ and can be decomposed as products of exponentials $\exp(i\alpha_i\mathbf{A}_i)$ where the $\mathbf{A}_i$ are the *generators* of the Lie group and form a *Lie algebra.* It should be possible to chose the generators of $U(d)$ so that every generator acts non-trivially only on a two-dimensional subspace, e.g. the Pauli matrices with respect to these subspaces. However, I do not know enough about Lie groups to make this connection perfectly clear.)

Step 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. We just discuss a three-qubit example: How to perform a two-level operation involving the states $|ABC\rangle = |000\rangle$ and $|111\rangle$? First, apply the Toffoli gate $\theta^{(3)}($ 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. This operation swaps $|000\rangle$ with $|001\rangle$ and leaves everything else untouched. Now, apply $\theta^{(3)}($ NOT $A, C, B)$. This swaps $|001\rangle$ with $|011\rangle$. The net effect has been to swap $|000\rangle$ with $|011\rangle$. Now, the C^{2}U 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. Similar rearrangements can always be achieved through a sequence of qubit basis states (or binary numbers) two consecutive members of which differ at one position only. (Such sequences are known as *Gray codes.*) Clearly this way of constructing arbitrary quantum gates is not always the most efficient one (involving the smallest possible number of operations), but on the other hand (see Section 4.5.4 of [3]) there are unitary n-qubit operations which involve $O(e^n)$ gates to implement.

Step 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). Imagine 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

$$n\alpha \mod 2\pi \quad (n = 0(1)\infty)$$

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

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

If we can implement two such irrational rotations about mutually orthogonal axes we can perfom arbitrary rotations due to the Z-Y-Z decomposition property already mentioned. This is exactly the route followed by Boykin et al. [29]; a simplified (and, in my view, not entirely correct) version is presented in Section 4.5.3 of [3]. Here I will just give a sketch of the calculation, leaving the dull details to you.

Recall the fundamental multiplication laws for Pauli matrices:

$$\mathbf{X}^2 = \mathbf{Y}^2 = \mathbf{Z}^2 = \mathbf{1}, \quad \mathbf{XY} = i\mathbf{Z} = -\mathbf{YX} \quad \text{etc.}$$

With

$$\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z})$$

we obtain

$$\mathbf{HXH} = \mathbf{Z}, \quad \mathbf{HZH} = \mathbf{X}.$$

Furthermore recall

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

$(\vec{\sigma} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z}))$ the rotation of the Bloch sphere about the unit vector $\hat{n}$ by an angle θ, and the $\frac{\pi}{8}$ gate

$$\mathbf{T} = e^{i\frac{\pi}{8}}\begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} = e^{i\frac{\pi}{8}}e^{-i\frac{\pi}{8}\mathbf{Z}} = \mathbf{Z}^{\frac{1}{4}}$$

$$\Rightarrow \mathbf{HTH} = e^{i\frac{\pi}{8}}e^{-i\frac{\pi}{8}\mathbf{X}} = \mathbf{X}^{\frac{1}{4}}.$$

Now multiply

$$\mathbf{Z}^{-\frac{1}{4}}\mathbf{X}^{\frac{1}{4}} = e^{i\frac{\pi}{8}\mathbf{Z}}e^{-i\frac{\pi}{8}\mathbf{X}} = \left(\cos\left(\frac{\pi}{8}\right)\mathbf{1} + i\sin\left(\frac{\pi}{8}\right)\mathbf{Z}\right)\left(\cos\left(\frac{\pi}{8}\right)\mathbf{1} - i\sin\left(\frac{\pi}{8}\right)\mathbf{X}\right) =$$

$$\cos^2\left(\frac{\pi}{8}\right)\mathbf{1} - i\sin\left(\frac{\pi}{8}\right)\left(\cos\left(\frac{\pi}{8}\right)\mathbf{X} - \sin\left(\frac{\pi}{8}\right)\mathbf{Y} - \cos\left(\frac{\pi}{8}\right)\mathbf{Z}\right) = \cos^2\left(\frac{\pi}{8}\right)\mathbf{1} - i\sin\left(\frac{\pi}{8}\right)\vec{n}\cdot\vec{\sigma}$$

where

$$\vec{n} = \left(\cos\left(\frac{\pi}{8}\right), -\sin\left(\frac{\pi}{8}\right), -\cos\left(\frac{\pi}{8}\right)\right).$$

With $\hat{n} = \frac{\vec{n}}{|\vec{n}|}$ this can be written as

$$\mathbf{Z}^{-\frac{1}{4}}\mathbf{X}^{\frac{1}{4}} = \cos\alpha\mathbf{1} - i\sin\alpha\,\hat{n}\cdot\vec{\sigma}$$

where

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

Invoking some theorems from algebra and number theory it can be shown that α is an irrational multiple of 2π.

This was the first of the two rotations we need. The second one is

$$\mathbf{H}^{-\frac{1}{2}}\mathbf{Z}^{-\frac{1}{4}}\mathbf{X}^{\frac{1}{4}}\mathbf{H}^{\frac{1}{2}},$$

where

$$\mathbf{H}^{-\frac{1}{2}} = \frac{e^{-i\frac{\pi}{4}}}{\sqrt{2}}(\mathbf{1} + i\mathbf{H}).$$

Now we can work out

$$\mathbf{H}^{-\frac{1}{2}}\mathbf{X}\mathbf{H}^{\frac{1}{2}} = \frac{1}{2}(\mathbf{X} + \mathbf{Z} - \sqrt{2}\mathbf{Y})$$

$$\mathbf{H}^{-\frac{1}{2}}\mathbf{Y}\mathbf{H}^{\frac{1}{2}} = \frac{1}{\sqrt{2}}(\mathbf{X} - \mathbf{Z})$$

$$\mathbf{H}^{-\frac{1}{2}}\mathbf{Z}\mathbf{H}^{\frac{1}{2}} = \frac{1}{2}(\mathbf{X}+\mathbf{Z}+\sqrt{2}\mathbf{Y}),$$

and finally

$$\mathbf{H}^{-\frac{1}{2}}\mathbf{Z}^{-\frac{1}{4}}\mathbf{X}^{\frac{1}{4}}\mathbf{H}^{\frac{1}{2}} = \cos^2\left(\frac{\pi}{8}\right)\mathbf{1} - i\sin\left(\frac{\pi}{8}\right)\vec{m}\cdot\vec{\sigma}$$

with

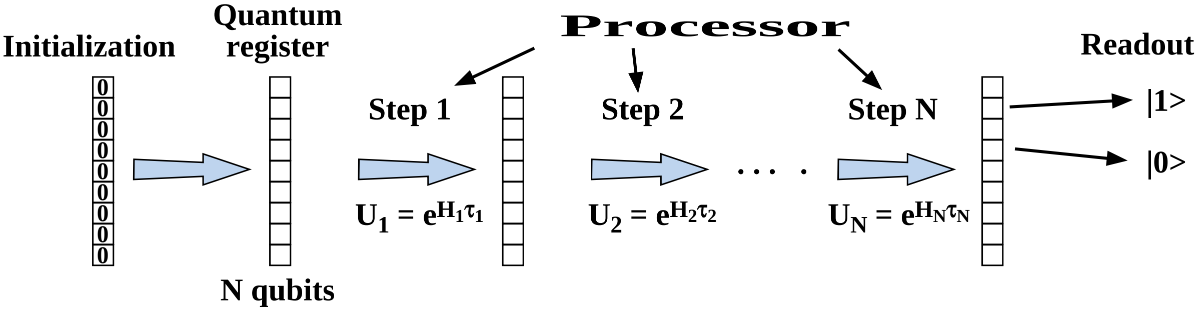
$$\vec{m} = \left(-\frac{1}{\sqrt{2}}\sin\left(\frac{\pi}{8}\right), \sqrt{2}\cos\left(\frac{\pi}{8}\right), \frac{1}{\sqrt{2}}\sin\left(\frac{\pi}{8}\right)\right)$$

from which we see that $\vec{m}^2 = \vec{n}^2$ and $\vec{m}\cdot\vec{n} = 0$. This is again a rotation by the same angle α as before, about an axis orthogonal to the previous axis $\hat{n}$.
The construction in [3] uses the rotations $\mathbf{X}^{\frac{1}{4}}\mathbf{Z}^{\frac{1}{4}}$ and $\mathbf{H}\mathbf{X}^{\frac{1}{4}}\mathbf{Z}^{\frac{1}{4}}\mathbf{H} = \mathbf{Z}^{\frac{1}{4}}\mathbf{X}^{\frac{1}{4}}$, which are quite similar to those used above, but unfortunately the axes of rotation are not orthogonal to each other but only at an angle of 32.65°. In that case the simple Z-Y-Z decomposition of an arbitrary rotation into three factors is not possible, but a decomposition into more than three factors still is.

VI. IMPLEMENTATIONS: HOW TO BUILD QUANTUM COMPUTERS

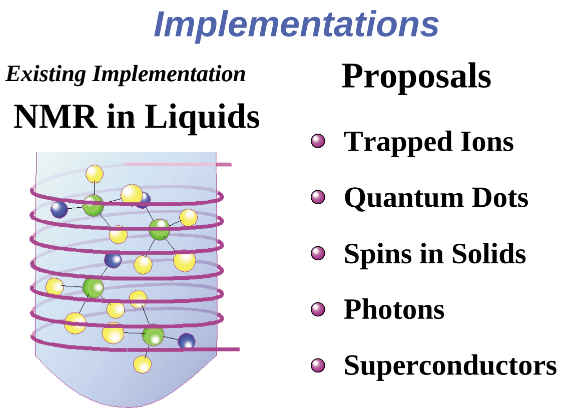
A. General requirements

Any implementation has to define a quantum mechanical system that provides the quantum register containing N qubits. For a "useful" quantum computer, N should be at least 400, better 1000; limitations on the number N of identifiable qubits will therefore be an important consideration.



These qubits must be initialized into a well defined state, typically into a ground state $|0>$. This is necessarily a dissipative process. The implementation must then provide a mechanism for applying computational steps to the quantum register. Each of these steps will be implemented by a unitary operation defined by a Hamiltonian H_i that is applied for a time τ_i. After the last processing step, the resulting state of the quantum register must be determined, i.e. the result of the computation must be read out. This would typically correspond to an ideal quantum mechanical measurement, i.e. the projection onto the eigenstate of the corresponding observable. Readout has to be done on each qubit separately.

Today, a single implementation of a quantum computer exists, which uses nuclear spin states of molecules in solution, i.e. liquid-state NMR. Details of this implementation will be discussed in one of the following subsections. In addition, there is a long list of proposed implementations, which includes, as qubits, nuclear and electronic spins, photons, trapped ions, as well as various states of quantum confined structures, mostly in semiconductors, and superconducting devices such as Josephson junctions.



B. DiVincenzo's five criteria

DiVincenzo [30] gives five requirements that a quantum computer must fulfill:

1) A scalable physical system with well characterized qubits. An implementation or embodiment of qubits corresponds to a physical system that has at least two energy levels that can be identified with the two log-