Konstantin Sakharovskiy

Universal Quantum Gates

Bachelors Thesis in Information Technology

May 25, 2022

University of Jyväskylä

Faculty of Information Technology

Author: Konstantin Sakharovskiy

Contact information: +358442437240, kosakhro@student.jyu.fi

Supervisor: Timo Tiihonen

Title: Universal Quantum Gates

Työn nimi: Universaaliset kvanttiportit

Project: Bachelors Thesis

Page count: 48+0

Abstract:

In this thesis, structured as a literature review, we give the reader an overview of universal quantum gates, the basic elements of the circuit model of quantum computing. We outline the introductory information needed to understand quantum computing and universality, including the minimum required mathematics. We conclude with an argument for the importance of universal quantum gates for the theory and practice of quantum computing, and the need to study an exhaustive list of non-universality criteria.

Keywords: Quantum computing, Quantum Gates, Qubits

Suomenkielinen tiivistelmä: Tässä kirjallisuuskatsaukseksi rakennetussa opinnäytetyössä annamme lukijalle yleiskatsauksen kvanttilaskennan piirimallin peruselementeistä, universaaleistaporteista. Esittelemme alustavat tiedot, joihin tarvitaan kvanttilaskennan ja universaalisuuden ymmärtämiseen, mukaan lukien vaadittava minimimatematiikka. Päätämme väitteeseen universaalien kvanttiporttien tärkeydestä kvanttilaskennan teorialle ja käytännölliselle sekä tarpeeseen tutkia tyhjentävä luettelo ei-universaalisista kriteereistä.

Avainsanat: Kvanttilaskenta, Kvanttiportit, Qubitit

Preface

This work is dedicated to the innocent victims of the Russian war in Ukraine.

While I was writing this thesis, the world fell apart for me and millions of people in February 2022. It is my deep conviction that humanity's destiny is to explore outer space, learn to live with viruses, build quantum computers, cure cancer, expand the horizons of knowledge, and pursue the ideals of humanism. There is no place in the 21st century for killing children and causing suffering to countless numbers of people on far-fetched grounds. I will make every effort to help the victims and stop the bloodshed as soon as possible.

Jyväskylä, May 25, 2022

Konstantin Sakharovskiy

List of Figures

List of Tables

Contents

1 Introduction

We virtually ignore the astonishing range of scientific and practical applications that quantum mechanics undergirds: today an estimated 30 percent of the U.S. gross national product is based on inventions made possible by quantum mechanics, from semiconductors in computer chips to lasers in compact-disc players, magnetic resonance imaging in hospitals, and much more.

(Tegmark and Wheeler 2001)

Successful development of modern technology industries is impossible without detailed calculations of quantum systems, such as nanostructures, complex chemical and biological molecules, new drugs, etc. However, despite impressive progress in the study of the fundamental laws of Nature, full-scale modelling of complex quantum systems is still an impractical task. Quantum problems are computationally intractable for conventional computers. Following this pessimistic observation Feynman (1982) managed to draw a positive conclusion, stating that as nature has successfully solved these problems, we (humans) can to employ quantum systems as a new foundation for computation. Feynman concludes that devices based on quantum principles could be much more powerful than their conventional counterparts. Two years prior to that Manin (1980) expressed similar ideas. The formal description of quantum computing began with the work of Benioff (1980) and D. Deutsch (1985), who studied quantum Turing machines and the concept of universal quantum computing.

Quantum computing started attract public attention when Shor (1999) introduced a fast quantum algorithm for integer factorization, for which there is not known an efficient algorithm in classical computing. Most of this emphasis comes from the fact that many modern cryptographic systems are built on the presumption of the nonexistence of a classical algorithm. (Rivest, Shamir, and Adleman 1978). Since then, significant advances have been made, both in terms of quantum information theory and building quantum devices. We would like to point out recent successes in practical implementation: achieving quantum supremacy (Arute et al. 2019) and 127 qubit processor creation (Chow, Dial, and Gambetta 2021).

Despite the advances made in this field, the task of creating a large-scale fault-tolerant quantum machine seems extraordinarily difficult. One of the main problem is that quantum systems implementation must comply with two contradictory principles - isolation from external environment and possibility to manipulate the system, send and receive information. This leads to the phenomenon of *Quantum errors*. Another fundamental problem arise in one of the most promising model, *Quantum Gate Model* or *Quantum Circuit Model*: how to build relevant *set of gates*, by which we can implement universal quantum computer? To address these problems we could use *Universal quantum gates*. With some assumptions, the analogy with classical computation is appropriate here, when we can use *NAND* alone to implement any classical computation. The following two theoretical studies may be considered the most important for universal quantum gates:

- Proof of the effectiveness of approximating quantum gates by the Solovay-Kitaev theorem (Dawson and Nielsen 2005). A consequence of this theorem is that an arbitrary quantum circuit can be efficiently approximated to a small error by another circuit built from a desired finite universal gate set.
- According to DiVincenzo (2000) criteria, to build a quantum computer, a quantum machine must meet five compulsory conditions: controllability, measurability, initializability, enough decoherence times and availability of *universal quantum gates*.

Quantum universal gates have been an active research topic since the landmark Solovay-Kitaev theorem. Numerous studies have been conducted on how to use universal sets to implement various quantum gates with arbitrary precision (see for instance Kliuchnikov, Maslov, and Mosca 2012; Ross and Selinger 2014; Selinger 2015; Maslov et al. 2008; Amy et al. 2013; Nam et al. 2018), or on how to implement circuits onto hardware with restricted connection (see for instance Maslov et al. 2008; Bhattacharjee and Chattopadhyay 2017; Oddi and Rasconi 2018; Booth et al. 2018; Zulehner and Wille 2019; Bhattacharjee et al. 2019; Zulehner, Paler, and Wille 2018; Cowtan et al. 2019; Itoko et al. 2020; Tan and Cong 2020; Murali et al. 2019).

The primary methodology used in this thesis is a literature review. The aim of the review is to examine a collection of studies on the universal quantum gates and on related areas of this phenomenon. In this review, literature based on classical and quantum gate models is identified. The role of universal gate sets is explored. The primary goal of this work is to introduce different universal quantum gate sets to the reader and specify directions for future research.

This thesis is structured as follows:

Section 2 gives necessary preliminary information for better understanding the circuit model of quantum computing, including the minimum required mathematics and physics.

Section 3 introduces the reader to the most notable quantum gates. We decided to visualize some gates as a rotation of the Bloch Sphere for clarity.

Section 4 clarifies the notion of universality in quantum computing and gives the most significant examples. In view of the importance of universal gates for the building of quantum computers, we will provide a brief overview of the present state of the art in this field.

Section 5 provides an overall conclusion to this thesis project.

2 Preliminaries

This section provides the foundational information needed to understand quantum computing in the context of universality. Due to the scope of this thesis we will not elaborate much in important topics closely related to the universal quantum gates, such as computational complexity and quantum error correction. For interested readers, we can recommend the classical textbook of Papadimitriou (2003) and the modern approach by Arora and Barak (2009) as comprehensive sources on complexity. Nielsen and I. Chuang (2002) and Williams, Clearwater, et al. (1998) serve as an informative introduction to quantum error correction.

To understand how quantum computing works, one needs maturity in mathematics that describes its formalism. In this chapter we introduce the key aspects of its associated mathematics and provide references for more details. This chapter is structured as follows: first we discuss essential mathematical formalism in complex numbers and linear algebra, second, we introduce the core idea of quantum computing and the base element of computation, quantum bit or *qubit* and thirdly, we introduce the concept of quantum gates and quantum circuits.

2.1 Complex numbers

Parameters of a quantum system are described by complex numbers. We will see further (and this is very intriguing discovery) that universal set gates, which work with real part only, may be enough to employ all the power of quantum computation. There is a fairly debated question as to whether the use of complex numbers is a convenience or the only possible way to describe quantum mechanical systems. The imaginary unit is part of the Schrödinger's equation, which we will introduce later (2.7). But could we get by same description with real numbers or quanterions? We will give Aaronson (2004) arguments against it: since the field of complex numbers is algebraically closed, this makes a natural quantum operation, such as taking the square root of the unitary, elementary.

Comprehension of complex numbers can be a significant threshold for those wishing to explore quantum computing. Nevertheless, we decided to include an introduction to complex numbers in view of the fact that many notable quantum gates work with the imaginary part.

A complex numbers[1] $c \in \mathbb{C}$ represented as $c = a + bi$, with $a, b \in \mathbb{R}$, and imaginary unit i, with condition $i^2 = -1$. One can rewrite c as $c = re^{i\phi}$ with $r = |c| = \sqrt{a^2 + b^2}$ as c norm, the angel $\phi \in [0, 2\pi)$ that c creates with y-axis if we consider point (a, b) in the plane. Norm 1 complex numbers form a unit circle. We can represent it as Euler's formula:

$$e^{i\phi} = \cos\phi + i\sin\phi \tag{2.1}$$

The complex conjugate c^* is $a - ib$, or $c^* = re^{-i\phi}$.

2.2 Essential linear algebra

It is a good idea to brush up on the basics of linear algebra, including concepts like vectors, matrices, and linear subspaces. It is quite difficult to fit such a vast area in the introduction and we use the following sources for inspiration (De Wolf 2019; Barak 2017). Linear functions over complex numbers can be used to model quantum mechanical operations. The most common concepts we employ for quantum are:

- We call $U : \mathbb{C}^N \to \mathbb{C}^N$ a linear function if $U(\alpha u + \beta v) = \alpha U(u) + \beta U(v)$, for $u, v \in \mathbb{C}^N$ and $\alpha, \beta \in \mathbb{C}$.
- We define $\langle u, v \rangle = \sum_{i \in [N]} u_i v_i$ as the inner product of vectors $u, v \in \mathbb{C}^N$. We also define $\|u\| = \sqrt{\langle u, u \rangle} = \sqrt{\sum_{i \in [N]} u_i^2}$ as the norm of $u \in \mathbb{C}^N$. If $\|u\| = 1$ it is a unit vector.
- For $\langle u, v \rangle = 0$ condition of orthogonality of vectors $u, v \in \mathbb{C}^N$. A set of N vectors $v_0, v_1, \ldots, v_{N-1}$ subject to $\|v_i\| = 1$ for $i \in [N]$ and $\langle v_i, v_j \rangle = 0$ for $i \neq j$ forms an orthonormal basis for $\mathbb{C}^N$.
- If l is a vector in $\mathbb{C}^n$ and $v_0, \ldots, v_{N-1}$ is an orthonormal basis for $\mathbb{C}^N$, then there are coefficients $\alpha_0, \ldots, \alpha_{N-1}$ such that $l = \alpha_0 v_0 + \cdots + \alpha_{N-1} v_{N-1}$. Consequently, the value $U(l)$ is determined by the values $U(v_0)$, …, $U(v_{N-1})$. Moreover, $\|l\| = \sqrt{\sum_{i \in [N]} \alpha_i^2}$.
- We define $N \times N$ matrix $M(U)$ as a linear function $U : \mathbb{C}^N \to \mathbb{C}^N$ with the coordinate in the i-th row and j-th column of $M(U)$ (that is $M(U)_{i,j}$) is equal to $\langle e_i, F(e_j) \rangle$.

1. The mathematical abstraction of complex numbers can be very difficult to grasp. Some visualization helps to understand: we warmly recommend the series of video explanations at the 3Blue1Brown YouTube channel by Grant Sanderson https://www.youtube.com/c/3blue1brown/featured

- We call a linear function $U : \mathbb{C}^N \rightarrow \mathbb{C}^N$ unitary if such that $\|U(l)\| = \|l\|$ for every l. Important properties of unitary functions:
  - function U is unitary iff $UU^* = I$ where * (or physicists use the notation †) is the conjugate transpose operator and I is the $N \times N$ identity matrix.
  - $U^* = U^{-1}$
  - both the rows and columns of $A(U)$ form an orthonormal basis.
- We denote by $A \otimes B$ the tensor product of linear spaces A and B. For all $a \in A$ and $b \in B$ the following condition is true $a \otimes b$ is in the space $A \otimes B$.

  Let $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & \cdots & b_{1q} \\ \vdots & \ddots & \vdots \\ b_{p1} & \cdots & b_{pq} \end{pmatrix}$

  then their tensor product matrix will be written in the basis formed by the tensor product of the bases:

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}$$

  Notable properties:

  - $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$
  - $dim(A \otimes B) = dim(A) \cdot dim(B)$.
  - $A \otimes (B \otimes C) = (A \otimes B) \otimes C$
  - $c(A \otimes B) = (cA) \otimes B = A \otimes (cB)$, $c \in \mathbb{C}$
  - $(A \otimes B)^* = A^* \otimes B^*$.
  - $A \otimes (B + C) = (A \otimes B) + (A \otimes C)$

  Tensor products can also be used to combine different vector spaces. Consider vector spaces V and V' with dimension d and d' and $\{v_1, \ldots, v_d\}$ and $\{v'_1, \ldots, v'_{d'}\}$ as bases, the tensor product of that space is the $d \cdot d'$-dimensional space $W = V \otimes V'$ spanned by $\{v_i \otimes v'_j \mid 1 \leq i \leq d, 1 \leq j \leq d'\}$.
- *Pauli matrices*, a set of 2×2 when performing quantum computation, it is necessary

to use both Hermitian and unitary complex matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.2}$$

Notable properties of Pauli matrices: eigenvalue $\lambda \in \{1, -1\}$. If $A, B \in \{X, Y, Z\}$, then $AB = -BA$. A set of $\{X, Y, Z, I\}$ form an orthonormal base for $M_{2\times2}(\mathbb{C})$.

- *Dirac notation* to denote quantum states. *bra* defines $\langle\phi| = \phi$ and *ket* defines $|\phi\rangle = \phi^\dagger$, so bra and ket are conjugate transposes of each other. For $|\phi\rangle, |\psi\rangle \in \mathbb{C}^n$ and $A \in M_{n.n}(\mathbb{C})$:
  - for inner products products we use $\langle v|w\rangle$.
  - orthonormal set of eigenvectors $\{v_i\}$ and unitarily diagonalizable matrix A equal $A = \sum_i \lambda_i |v_i\rangle \langle v_i|$
  - some abbreviations that are easy to read but could cause ambiguity $|v\rangle\langle v| \otimes |w\rangle\langle w| = (|v\rangle \otimes |w\rangle)(\langle v| \otimes \langle w|)$, the latter is often abbreviated to $|v\rangle \otimes |w\rangle \langle v| \otimes \langle w|$
  - $(U|v\rangle)^\dagger = \langle v|U^\dagger$ and $(|u\rangle \otimes |v\rangle)^\dagger = \langle u| \otimes \langle v|$

2.3 Quantum computing

Models of quantum computation By quantum computing and quantum computer we refer to the *Quantum Circuit Model*. There are several models of quantum computation which differ in terms of the quantum effects and resources they employ to implement quantum computation, as well as their simplicity (and even the possibility in principle [2]) of implementation in hardware. The polynomial equivalence of these models has been established: one paradigm of quantum computation can be used to execute quantum computation in another model with a polynomial increase in resources at the most. Thus, from a theoretical point of view, it does not matter which model to use. For the sake of completeness, we refer to the most significant works in this area:

- Yao (1993) proved that *Quantum Circuit Model* can efficiently simulate the *Quantum Turing Machine*.

2. it seems very unlikely that a *Quantum Turing Machine* could be built, since a sequential model is fundamentally incapable of operating fault tolerantly in the presence of noise. (Aharonov and Ben-Or 1996)

- Aharonov et al. (2008), Kempe, Kitaev, and Regev (2006) and Siu (2005) showed that *Quantum Adiabatic Model* can efficiently simulate *Quantum Circuit Model* and vice versa.
- Raussendorf and Briegel (2001) demonstrated *Quantum Circuit Model* and *One-Way model* equivalence.
- *Non-Abelian anyons* can simulate efficiently *Quantum Circuit Model* and could also be efficiently simulated by *Quantum Circuit Model* (Kitaev 2003; Freedman, Kitaev, and Wang 2002)

Key differences between classical deterministic and quantum computing Quantum machines approach to solve computational problems is different to conventional computers. Quantum devices can be in a large number of states simultaneously, while conventional devices can only be in one state at a time. Before we move on to a more in-depth presentation of the theory, let us highlight four things, to which we refer more than once in this thesis: superposition, entanglement, uncertainty and interference.

- *Superposition.* A fundamental principle of quantum mechanics, according to which if states $|0\rangle$ and $|1\rangle$ are possible for some quantum system, then any linear combination of them $|\phi\rangle = c_0 |0\rangle + c_1 |1\rangle$ with complex coefficients c_0, c_1 is also possible, which is called a superposition of states $|0\rangle$ and $|1\rangle$. Considering universal sets of quantum gates we will see that possibility to put a quantum system into superposition is a necessary condition of universality.
- *Entanglement.* Quantum entanglement is a phenomenon in which quantum states of several particles turn out to be interrelated regardless of distance between them and the state of each quantum entangled particle cannot be described independently of the states of others. Quantum entanglement is the fundamental distinction between the classical and quantum worlds (Bell 1964): entanglement is a fundamental property of quantum mechanics that does not exist in classical mechanics. Just as in the case of superposition, the possibility of bringing a quantum system into an entangled state is an essential condition for universal sets,
- *Uncertainty.* The information limitation of quantum systems leads to the necessity of

their statistical description. According to quantum mechanics, the state of a physical system is specified by means of such objects as the wave function and the density matrix, which allow one to correctly calculate the probabilities of outcomes of any future measurements. Thus, one of the most important characteristics of quantum computing turns out to be the probabilistic aspect.

- *Interference.* One very important difference from the classical world is the effect of quantum interference. We encounter it always when there is more than one path to get a result. As a consequence of this phenomenon, each of the paths simultaneously interacts with others, increasing the probability of the outcome by constructive interaction or decreasing the probability by destructive interaction, like ripples on water, when waves add up or amplify or absorb each other.

Qubit We use an arbitrary two-level quantum system for implementation of *qubit* (quantum bit), the base element of quantum computers [3]. Qubits can be ions, atoms, electrons, photons, atomic nuclei spins, superconductor structures and many other physical systems. The coding of a state $|0\rangle$ or $|1\rangle$ can be done e.g. with spin (spin up and spin down) or the polarization of a photon (vertical polarization and horizontal polarization).

Bloch sphere representation of a qubit Consider the action of a single quantum gate on a single qubit. A classical bit can be in either the zero or one state. In comparison, a quantum bit may exist in a *quantum superposition* of $|0\rangle$ and $|1\rangle$. We can represent this state as a point on the surface of the Bloch sphere (Bloch October 1946). Applying a quantum gate could be generalized as a rotation of this sphere around some axis.

For qubit $|\psi\rangle$ and $c_0, c_1 \in \mathbb{C}$, s.t. $|c_0|^2 + |c_1|^2 = 1$ we could represent the state as:

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle \tag{2.3}$$

and rewrite this using 2.1 with $\alpha, \theta, \phi \in \mathbb{R}$:

3. in this review we are limited to a two-level system. *Qudit*, a d-level computational unit requires a special study. Nevertheless, we do not expect any dramatic changes here in terms of quantum computational universality

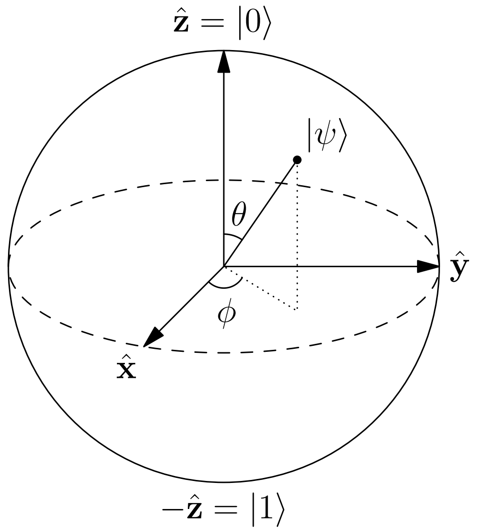


Figure 1. Bloch Sphere represents a state of a single qubit.

$$|\psi\rangle = e^{i\alpha}\left(\cos\left(\tfrac{1}{2}\theta\right)|0\rangle + e^{i\phi}\sin\left(\tfrac{1}{2}\theta\right)|1\rangle\right) \tag{2.4}$$

We could omit the global phase $e^{i\alpha}$ and rewrite using $\simeq$ to point the equivalence up to a global phase.

$$|\psi\rangle \simeq \cos\left(\tfrac{1}{2}\theta\right)|0\rangle + e^{i\phi}\sin\left(\tfrac{1}{2}\theta\right)|1\rangle \tag{2.5}$$

One can note θ and ϕ as coordinates on the Bloch sphere, with the corresponding angles relative to $\widehat{x}$ and $\widehat{z}$ axes, in addition $0 \leq \phi < 2\pi$ and $0 \leq \theta \leq \pi$.

The vector can be used to find the point on the three-dimensional unit sphere.

$$\widehat{\psi} = (\sin\theta\cos\phi,\ \sin\theta\sin\phi,\ \cos\theta) \tag{2.6}$$

On the top of the Bloch sphere's is $|0\rangle$ state and $|1\rangle$ state is at the bottom by convention. Note that the orthogonal states (the basis for representing a qubit) are on opposite sides of the Bloch sphere.

2.4 Quantum logic gates

Quantum gates are much more diverse than their classical counterparts. With a sequence of quantum logic gates we can implement any quantum computation. Quantum gates can control arbitrary multiqubit states in *superposition* which can be *entangled*, while classical gates control classical bit values only 0 or 1.

Some essential physics Different physical phenomena are used to create quantum gates, which are related to qubit embodiment technology among other things.

For instance, if qubits are implemented by ion trap technology, the logic is based on the application of laser pulses with different parameters that manipulate the atomic state. Or, if a quantum system is represented by photons, quantum gates can be implemented by different beam splitters and phase shifters.

Due to the fact that quantum gates realize the evolution of a quantum mechanical system, we can describe the transformation they perform by Schrödinger's[4] equation with Hamiltonian $\mathscr{H}$ which is describing physical forces.

$$i\hbar\partial|\psi\rangle/\partial t = \mathscr{H}|\psi\rangle \tag{2.7}$$

Equations for quantum gates describe the physical processes by which they are realized, and hence unitary matrices describe quantum gates.

$$U = e^{-i\mathscr{H}t/\hbar}. \tag{2.8}$$

Due to unitarity of quantum evolution (in absence of disturbances) we observe the following evolution of quantum system from state $|\psi(0)\rangle$ to state $|\psi(t)\rangle$ in time t

$$|\psi(t)\rangle = e^{-i\mathscr{H}t/\hbar}|\psi(0)\rangle = U|\psi(0)\rangle \tag{2.9}$$

Here we see such a remarkable property of quantum computation as reversibility. It is a consequence of the fact that quantum logic gates are always described by a unitary matrix. Of

4. perhaps the most famous physicist since Einstein in pop culture thanks to the famous $|cat\rangle = c_1|dead\rangle + c_2|alive\rangle$ paradox (which in our opinion is often misinterpreted)

course, this is true until interference with the system: a measurement or unplanned influence with the environment, causing an error. Note how much importance such phenomena as measurement or error has in the quantum world compared to classical computation, where measurements (bit-reading) can be made whenever needed without consequences and error correction is an unnoticeable chore.

The remarkable consequences of unitarity Let us also specify the properties of quantum gates in consequence of their unitarity in accordance with these definitions 2.2

- $U^{\dagger} = U^{-1}$ and both are also unitary.
- $U^{\dagger}U = 1$.
- $|det(U)| = |det(U^{\dagger})| = |det(U^{-1})| = 1$.
- both the rows and columns of U form an orthonormal basis.

2.5 General quantum circuits and unitary purification

Quantum circuit could be represented as a graph, where gates encoded by nodes and qubits, on which the gates act, encoded by edges.

Let us take look at an example of a famous scheme, which is *entangling* two qubits by evolving them from the state $|00\rangle$ to the Bell state.

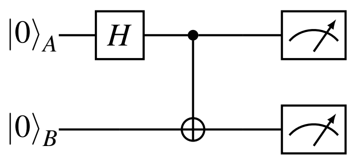
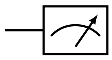


Figure 2. Bell state preparation and measurement

We will go into more detail later on about the gates' action on the qubits, now we briefly describe how to read the circuit example given in figure 2. We should read from left to right - this is evolution of the quantum system by convention. At the beginning of each qubit wire (line), the starting state of the qubit is shown. In this example we have 2 qubits in state $|00\rangle = |0\rangle_A \otimes |0\rangle_B$. Then the gate H acts on the qubit A and no action on the qubit B

(it also equals the action of I - identity or "no-action" gate, which is not usually displayed). This can be written as $H \otimes I$ gate action on two qubits. Then we apply $CNOT$ gate on two qubits where • on the qubit A means "control" and $\oplus$ on the qubit B means "target". Finally measurement gates  applied on both qubits.

Quantum circuit purification As we have already seen that quantum operations are unitary. In *General quantum circuits* a number of non-unitary operations should be performed to get a result or to implement some algorithms. Given in Fig. 3 examples of non-unitary gates.

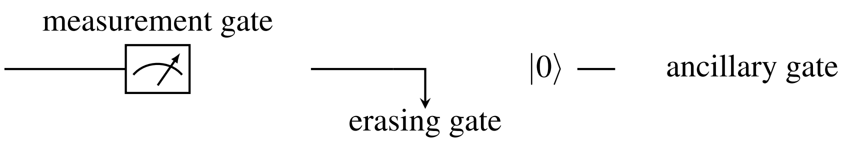


Figure 3. Gates representing non-unitary operations

The unitary purification can be used to explain the link between general and unitary quantum circuits. *Stinespring Dilation* (Stinespring 1955), states that larger systems of unitary operations could realize general quantum operations. In this study we do not include non-unitary gates in the set of universal gates, undoubtedly aware of their need for practical implementation.

3 Quantum gates

A neutral term *notable* is a good fit in describing quantum gates most commonly used in the theory and practice of quantum computing. Here we will consequently present notable quantum gates acting on 1 qubit, 2 qubits, and 3 qubits [1]. Relevant comments concerning the inclusion of presented quantum gates into universal sets will be given in the course of the presentation. This is the most extensive and difficult chapter to comprehend, but we have tried to simplify by visualizing the action of the single-qubit gate on the Bloch sphere. We use not yet finished material by Crooks (2020) as an excellent source of data and aid to visualize the Bloch sphere rotation with three axes.

3.1 Notable 1-qubit gates

In classical computation only two 1-bit gates are available to us: $\{NOT, IDENTITY\}$ if we do not take into account constant functions, which are ancillary in some sense. Quantum computation gives us an incredibly vast picture. Let us focus on the most important gates.

3.1.1 Pauli

Pauli operators, which we introduced earlier 2.2 could be implemented by four 1-qubit gates I, X, Y, and Z. Physicists use the following notation: $I = \sigma_0$, $X = \sigma_1$, $Y = \sigma_2$, $Z = \sigma_3$.

I gate $-\boxed{I}-$ The identity matrix represents the gate on a single qubit which means no action. When a gate is applied to any state, it is not changed: $I\,|\psi\rangle = |\psi\rangle$.

X gate $-\boxed{X}-$ The X could be seen as a half-turn around the $\widehat{x}$ axis in the Bloch sphere. In the basis $|0\rangle, |1\rangle$ it is the same as NOT in classical computation. With respect to basis, X

1. Here we should immediately note that the number of quantum gates even just for one qubit is uncountable. Furthermore, as we should see below there exist uncountably many universal sets of quantum gates! Trying to cover everything would make the work incredibly boring, therefore, we will limit ourselves to the most notable gates which will be useful for building up the most notable universal sets.

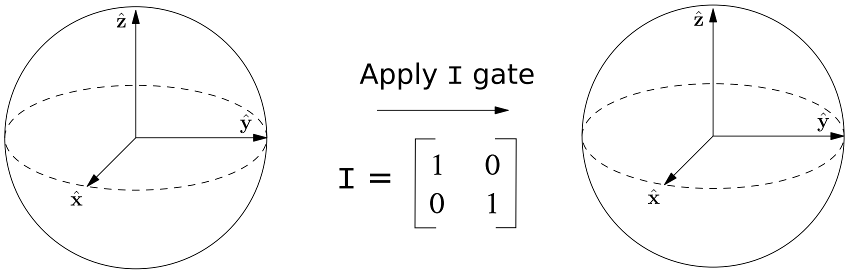


Figure 4. Identity gate on the Bloch Sphere.

gate interchanges the state, so that $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$.

Despite the similar behaviour in the computational basis with the classical computation, it is wrong to consider X-gate as quantum NOT gate. A general quantum NOT gate does not exist.

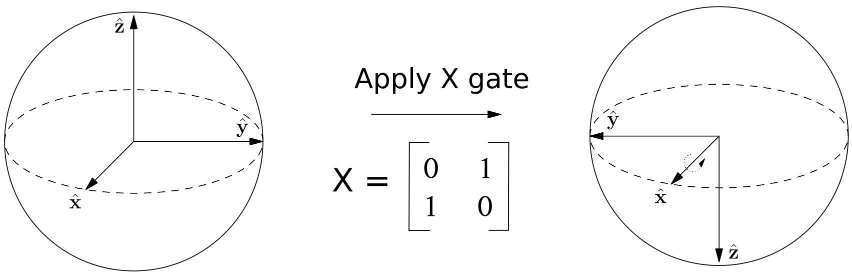


Figure 5. X gate on the Bloch Sphere.

Y gate $-\boxed{Y}-$

The Y could be seen as a half-turn around the $\widehat{y}$ axis in the Bloch sphere. In the basis it change zero to one and make a phase flip $Y|0\rangle = +i|1\rangle$ and $Y|1\rangle = -i|0\rangle$.

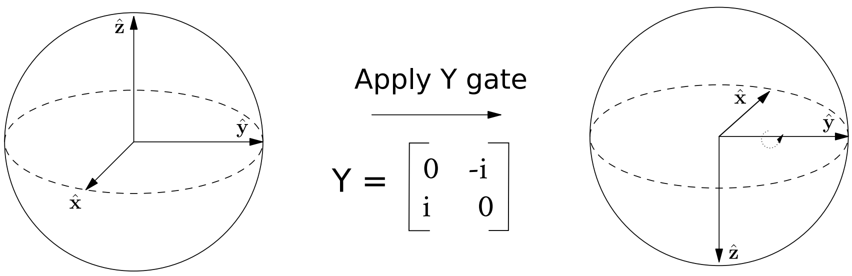


Figure 6. Y gate on the Bloch Sphere.

Z gate $\boxed{Z}$ The Z could be seen as a half-turn around the $\widehat{z}$ axis in the Bloch sphere. In the basis it make a phase flip $Z|0\rangle = +i|0\rangle$ and $Z|1\rangle = -i|1\rangle$

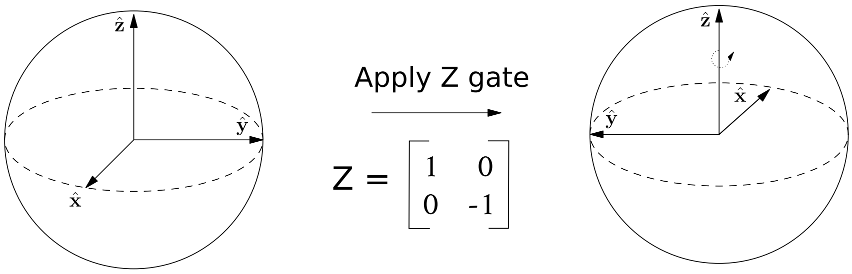


Figure 7. Z gate on the Bloch Sphere.

3.1.2 Rotations

One can rotate vector by any angle around the Bloch sphere's corresponding axis with rotation operator gates R_x, R_y, and R_z. They are formed by taking a power of the Pauli operators.

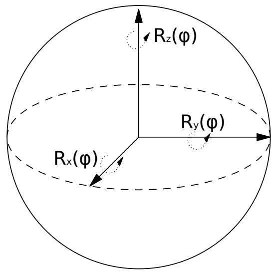


Figure 8. Rotation gates on the Bloch Sphere.

If $A^2 = I$ then $e^{i\phi A} = \cos(\phi)\, I + i\sin(\phi)\, A$. We can use Euler formula 2.1:

$$\begin{aligned} e^{i\phi A} &= I + i\phi A - \frac{\phi^2}{2!}I - i\frac{\phi^3}{3!}A - \frac{\phi^4}{4!}I - i\frac{\phi^5}{5!}A + + \cdots \\ &= \left(1 - \frac{\phi^2}{2!} + \frac{\phi^4}{4!} - \cdots\right) I + \left(\phi - \frac{\phi^3}{3!} + \frac{\phi^5}{5!} - \cdots\right) A \\ &= \cos(\phi)\, I + i\sin(\phi)\, A \end{aligned} \tag{3.1}$$

Gate R_x $\boxed{R_x(\phi)}$ angle ϕ rotation around $\widehat{x}$.

$$R_x(\phi) = \begin{bmatrix} \cos\left(\frac{1}{2}\phi\right) & -i\sin\left(\frac{1}{2}\phi\right) \\ -i\sin\left(\frac{1}{2}\phi\right) & \cos\left(\frac{1}{2}\phi\right) \end{bmatrix} \tag{3.2}$$

Gate R_y $-\boxed{R_y(\phi)}-$ angle ϕ rotation around $\hat{y}$.

$$R_y(\phi) = \begin{bmatrix} \cos\left(\frac{1}{2}\phi\right) & -\sin\left(\frac{1}{2}\phi\right) \\ \sin\left(\frac{1}{2}\phi\right) & \cos\left(\frac{1}{2}\phi\right) \end{bmatrix} \tag{3.3}$$

Gate R_z $-\boxed{R_z(\phi)}-$ angle ϕ rotation around $\hat{z}$.

$$R_z(\phi) = \begin{bmatrix} e^{-i\frac{1}{2}\phi} & 0 \\ 0 & e^{+i\frac{1}{2}\phi} \end{bmatrix} \tag{3.4}$$

Gate $R_{\vec{n}}$ $-\boxed{R_{\vec{n}}(\phi)}-$ angle ϕ rotation around an arbitrary axis represented by vector $\vec{n}$, where $n_x^2 + n_y^2 + n_z^2 = 1$.

$$\begin{aligned} R_{\vec{n}}(\phi) &= e^{-i\frac{1}{2}\phi(n_xX+n_yY+n_zZ)} \\ &= \cos\left(\tfrac{1}{2}\phi\right)I - i\sin\left(\tfrac{1}{2}\phi\right)(n_xX + n_yY + n_zZ) \\ &= \begin{bmatrix} \cos\left(\frac{1}{2}\phi\right) - in_z\sin\left(\frac{1}{2}\phi\right) & -n_y\sin\left(\frac{1}{2}\phi\right) - in_x\sin\left(\frac{1}{2}\phi\right) \\ n_y\sin\left(\frac{1}{2}\phi\right) - in_x\sin\left(\frac{1}{2}\phi\right) & \cos\left(\frac{1}{2}\phi\right) + in_z\sin\left(\frac{1}{2}\phi\right) \end{bmatrix} \end{aligned}$$

This is, in a sense, a generalization of the one-qubit quantum gate because one could implement any gate as a rotation of some angle around some axis. This gate, although not universal itself, can form universal sets with any entangling two-qubit quantum gate.

P gate $-\boxed{P}-$ The gate map the basis states $|1\rangle$ to $e^{i\theta}|1\rangle$ and $|0\rangle$ to $|0\rangle$ state.

$$P(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

Important P gate fractions The Z gate has its own notations for discrete fractional powers. We meet them in quantum Fourier transform as controlled operations.

$$\begin{aligned} P_k &= \begin{bmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^k} \end{bmatrix} \\ &= P(2\pi/2^k) = Z^{2^{1-k}} \\ P_1 &= Z \text{ (half turn around the z axis)} \\ P_2 &= S \text{ (quarter turn around the z axis)} \\ P_3 &= T \text{ (eighth turn around the z axis)} \end{aligned}$$

T gate $-\boxed{T}-$ Let us take a closer look at the very important 4-th root of the Z gate: $T^4 = Z$.

$$\begin{aligned} T &= Z^{\frac{1}{4}} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} \end{aligned}$$

An eight turn around the $\widehat{z}$ axis.

The critical insight is that T gate, in combination with H gate introduced below, produces two distinct rotations on the Bloch sphere with *irrational* π angles. This enables for dense filling of the Bloch sphere's surface by combinations of $\{T, H\}$ gates only, approximating any one-qubit unitary operator with the desired error.

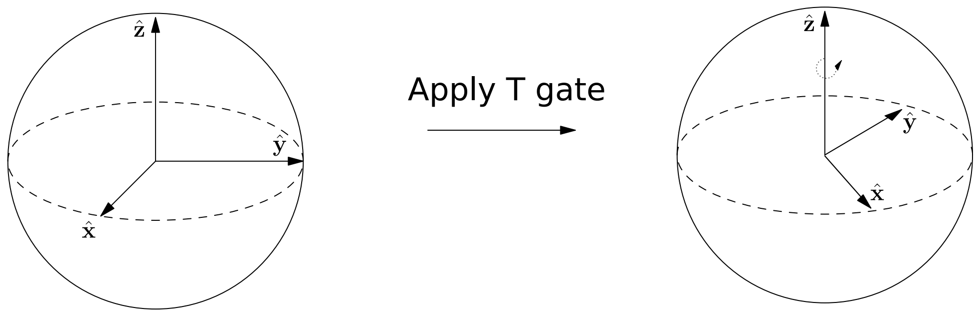


Figure 9. Bloch Sphere represents the acting of T gate.

H, Hadamard gate $-\boxed{H}-$ This gate is consider to be the most important of all 1-qubit gates. It could be seen as a π rotation around the axis $\frac{1}{\sqrt{2}}(\hat{x}+\hat{z})$. This axis lies between the Z and X. H matrix is both Hermitian and unitary, hence the inverse of itself and the square is the identity $HH = I$

$$\begin{aligned} H &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ &\simeq R_{\vec{n}}(\pi), \quad \vec{n} = \frac{1}{\sqrt{2}}(1,0,1) \end{aligned}$$

Bloch axes: H gate exchanging x and z, inverting y: $HXH = Z$, $HZH = X$, $HYH = -Y$.

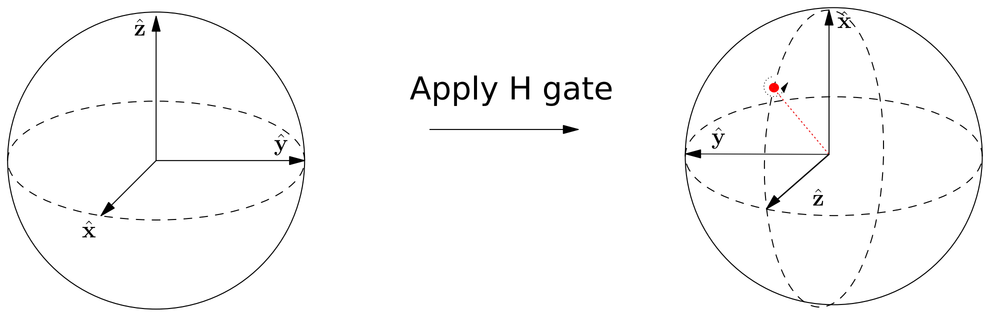


Figure 10. H gate on the Bloch Sphere (note the rotation axe lies between $\hat{x}$ and $\hat{z}$ axes) .

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \tag{3.5}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \tag{3.6}$$

It is conventional to use a proprietary notation for these states, $|+\rangle$ and $|-\rangle$. Moreover, it can be used as a basis for measurements instead of $|0\rangle$ and $|1\rangle$

The Hadamard gate is important because we can use it to convert the qubit from basis state to uniform superposed state. This is likewise true for the state of many qubits. For n qubits in the basic $|0\rangle$ state after applying H to each one, we get superposition with an exponential increase in the variables required to describe:

$$H|0\rangle \otimes H|0\rangle \otimes \cdots \otimes H|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle \tag{3.7}$$

3.2 Pauli generalization and Clifford gates

We could generalize Pauli gates for multiqubits operations. The Clifford group is defined as the group of unitaries that normalise the Pauli group, which is defined as follows:

$$\mathbf{P}_n = \left\{ e^{i\theta\pi/2} \sigma_{j_1} \otimes \cdots \otimes \sigma_{j_n} \mid \theta = 0,1,2,3, j_k = 0,1,2,3 \right\}.$$

Elements in the Clifford group are Clifford gates: Pauli gates themselves, quarter turns (square roots) of Pauli gates (S for instance), Hadamard are examples of Clifford gates. What is important for our study is that Clifford gates are *not universal*. It is impossible to implement an arbitrary qubit only by Clifford gates: $\widehat{x}, \widehat{y}, \widehat{z}$ axes maps back to the group. We could obtain a universal set if we add one non-Clifford gate. T-gate for instance forms the well-known $Clifford + T$ universal set.

3.3 Notable 2-qubit gates

Due to the exponential growth of the parameters it is impossible to visualize quantum gates with 2 or more qubits (except parallel gates), we will basically give a representation in the form of matrices. Let us briefly outline the formalism of the matrix action on a system of 2 qubits. For a 2-qubit system of qubit $|\psi\rangle$ and qubit $|\phi\rangle$ and $c_{00}, c_{01}, c_{10}, c_{11} \in \mathbb{C}$, s.t.

$|c_{00}|^2+|c_{01}|^2+|c_{10}|^2+|c_{11}|^2=1$, we could represent the state as a vector:

$$|\psi\phi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle \rightarrow \begin{bmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{bmatrix} \quad (3.8)$$

Consider the action of $H \otimes H$ two-qubit gate (applying two Hadamard gates in parallel) on a two-qubit system in the state $|00\rangle$ which can be described by the vector $\left[\begin{smallmatrix} 1 \\ 0 \\ 0 \\ 0 \end{smallmatrix}\right]$. Using tensor product and matrix multiplication we can write it:

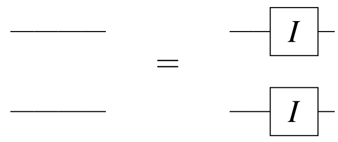
$$\begin{aligned} H \otimes H|00\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} |00\rangle \\ &= \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \\ &= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \end{aligned}$$

Hence the qubits have been changed from the basic state using a gate to the superposition state with an equal probability $(\frac{1}{2})^2 = 25\%$ of observing any of 4 possible states. This generalization of the Hadamard gate we have discussed in 1-qubit gates introduction. (3.7).

3.3.1 Non-entangling gates

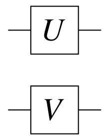
Identity gate (Clifford gate) The same as 1-qubit identity gate it has no action.

$$I_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} =$$



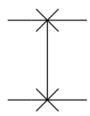
Separable gates (parallel gates) $U \otimes V$ any two-qubit gate which can be represented as a tensor product of two one-qubit gates ($I \otimes I$ in case of 2-qubit identity gate)

$$U \otimes V = \begin{bmatrix} u_{11}V & u_{12}V \\ u_{21}V & u_{22}V \end{bmatrix} =$$



SWAP gate (Clifford group) This gate exchanges two qubits, defined by the matrix:

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} =$$



Let us look how *SWAP* acts on the four basic states of a two-qubit system:

$$SWAP|00\rangle = |00\rangle$$
$$SWAP|01\rangle = |10\rangle$$
$$SWAP|10\rangle = |01\rangle$$
$$SWAP|11\rangle = |11\rangle$$

We can use *SWAP* gate to move qubits close to each other on the real quantum machine. The *SWAP* gate can be decomposed into summation form:

$$\text{SWAP} = \frac{I \otimes I + X \otimes X + Y \otimes Y + Z \otimes Z}{2}$$

The *SWAP* gate is Hermitian and unitary; Therefore we have

$$\text{SWAP} = e^{i\frac{\pi}{2}(I-\text{SWAP})} = e^{i\frac{\pi}{4}} R_{xx}(\pi/2) R_{yy}(\pi/2) R_{zz}(\pi/2)$$

.

3.3.2 Entangling gates and controlled operations

We have already discussed entanglement as a key difference between the quantum world and the classical world. We are now taking a closer look at the arguments why creating entanglement is an essential part of universality. Any pure (unentangled) state of n qubits could be represented as:

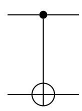
$$(\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \otimes \cdots \otimes (\alpha_n |0\rangle + \beta_n |1\rangle)$$

the resources needed to describe such a state are linear to n, i.e. can easily be implemented on a classical computer. On the other hand for entangled states we need 2^n, an exponential amount of resources:

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Controlled-Not gate, CNOT (Clifford group) [2].

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



Action of the *CNOT* gate on the four basic states of a two-qubit system, where we can see the effect of the gate on the second qubit only if the first qubit is in state 1:

2. In quantum computing *control* operations are significantly different from classical in that there are no operations of reading the controlling qubit as such (otherwise, according to the laws of quantum mechanics, which preserve linearity, the qubit would collapse into one of the ground states with a certain probability) instead, both qubits go into some, usually entangled, state

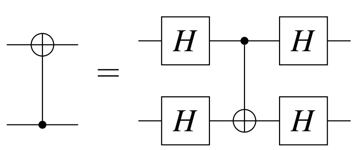
$$
\begin{aligned}
CNOT|00\rangle &= |00\rangle \\
CNOT|01\rangle &= |01\rangle \\
CNOT|10\rangle &= |11\rangle \\
CNOT|11\rangle &= |10\rangle
\end{aligned}
$$

Remember that the first qubit can be in a superposition state. The 2-qubit system then changes to a state of entanglement. We will give examples of action of the *CNOT* gate if the first control qubit is in $|+\rangle$ or $|-\rangle$ states, resulting in generation of *Bell states*, one of which we have previously introduced (see 2):

$$
\begin{aligned}
CNOT|+0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle \\
CNOT|+1\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi^+\rangle \\
CNOT|-0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle \\
CNOT|-1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Psi^-\rangle
\end{aligned}
$$

These states are extremely important in quantum information theory because they represent maximum entanglement on minimum number of qubits.

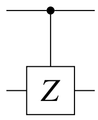
With CNOT the control could be inverted using Hadamard "sandwich".



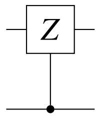
$$
= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}
$$

CZ gate (Clifford group) This gate is often used in decomposition of circuits. We should also note the natural implementation in linear optical.

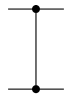
$$\mathsf{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} =$$



$=$

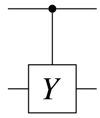


$=$



Controlled-Y, CY gate

$$\mathsf{CY} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & +i & 0 \end{bmatrix} =$$

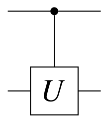


Barenco gate A 2-qubit which was first proved by Barenco (1995) to be universal.

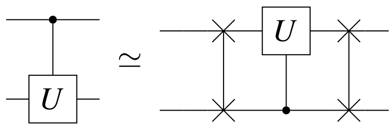
$$\mathsf{Barenco}(\phi, \alpha, \theta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha}\cos(\theta) & -ie^{i(\alpha-\phi)}\sin(\theta) \\ 0 & 0 & -ie^{i(\alpha+\phi)}\sin(\theta) & e^{i\alpha}\cos(\theta) \end{bmatrix} \tag{3.9}$$

Controlled-U gates The controlled 2-qubit gates can be generalized with the CU gate, where $U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{11} \end{pmatrix}$ is an arbitrary single qubit gate.

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{bmatrix} =$$



Given that we have already introduced a SWAP quantum gate, we can always do this trick if we need to interchange controlling and controlled qubits.

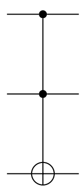


3.4 Notable 3-qubit gates

Despite the fact that 2-qubit gates are sufficient to build a universal quantum gate set, we include 3-qubit gates in this review for the three reasons. Firstly, because of the historical context: $\{DEUTSCH\}$ was the first universal set proved by D. E. Deutsch (1989) (this set contains only one gate). Secondly, $TOFFOLI$ and $FREDKIN$ have connections to universal sets in classical computation. Thirdly, 3-qubit gates direct implementation can simplify complicated quantum circuits and improve the fidelity of large-scale quantum computers (Müller et al. 2011).

Toffoli gate (controlled-controlled-not, CCNOT) Introduced by Toffoli (1980). In contrast to $CNOT$ this gate has 1 target and 2 control qubits. It is universal for classical reversible computation. One of the remarkable discoveries is that the set $\{TOFFOLI, H\}$ is universal for quantum computation (Aharonov 2003). This is particularly striking taking into account that both gates have only the real part, i.e. we can not implement for instance $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$ or any other gate, acting on imaginary part, with this set of gates.

$$\text{TOFFOLI} = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{bmatrix} =$$

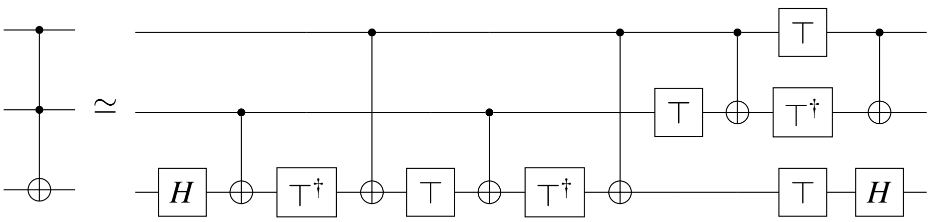


Let us look how $TOFFOLI$ acts on the eight basic states of a three-qubit system:

$$TOFFOLI|000\rangle = |000\rangle$$
$$TOFFOLI|001\rangle = |001\rangle$$
$$TOFFOLI|010\rangle = |010\rangle$$
$$TOFFOLI|011\rangle = |011\rangle$$
$$TOFFOLI|100\rangle = |100\rangle$$
$$TOFFOLI|101\rangle = |101\rangle$$
$$TOFFOLI|110\rangle = |111\rangle$$
$$TOFFOLI|111\rangle = |110\rangle$$

One can see that $TOFFOLI$ apply $X - gate$ to the rightmost qubit if first two qubits are in $|11\rangle$ state. Just as in the case of $CNOT$, control qubits and target qubit could be in superposition. We emphasise once again that there is no physical equivalency between control operation in classical and quantum world, since control qubits are not reading.

Using the set of quantum gates $\{CNOT, T, H\}$ we could implement $TOFFOLI$ (Nielsen and I. Chuang 2002).

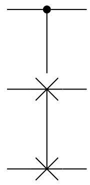


And since this set contains H, it is also universal for quantum computing. Furthermore, because of the T gate in this set, all quantum states are available to us.

Fredkin gate (controlled-swap, CSWAP) Introduced by Fredkin and Toffoli (1982). This gate swaps two qubits with a third qubit as a control. It has conservative universality in classical reversible computation (preserving Hamming weight) (Aaronson, Grier, and Schaeffer

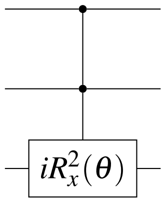
2015).

$$\mathrm{CSWAP} = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \end{bmatrix} =$$



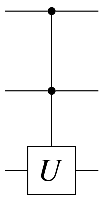
DEUTSCH gate A universal quantum gate of historical significance implements double controlled operation on the target gate $i\mathsf{R_x}^2(\theta)$.

$$\mathsf{DEUTSCH}(\theta) = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&i\cos(\theta)&\sin(\theta) \\ 0&0&0&0&0&0&\sin(\theta)&i\cos(\theta) \end{bmatrix} =$$

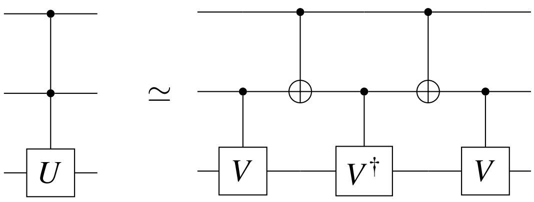


Double controlled-U, CCU gates double controlled gates generalization is the CCU gate. This includes $\mathsf{I}_3, \mathsf{TOFFOLI}, \mathsf{FREDKIN}, \mathsf{DEUTSCH}$ gates, and all three qubits controlled gates for an arbitrary 1-qubit gate $U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}$

$$CCU = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&U_{11}&U_{12} \\ 0&0&0&0&0&0&U_{21}&U_{22} \end{bmatrix} =$$



CCU gates decomposition Barenco et al. (1995) showed an explicit sequence of two bit gates which constructs any matrix on three qubits for $U = V^2$.



Therefore, 2-qubit gates are universal.

4 Universal gates

The pervasiveness of universality - that is, the likelihood that a small number of simple operations already generate all operations in some relevant class - is one of the central phenomena in computer science. It appears, among other places, in the ability of simple logic gates to generate all Boolean functions (and of simple quantum gates to generate all unitary transformations); and in the simplicity of the rule sets that lead to Turing-universality, or to formal systems to which Gödels theorems apply.

(Aaronson, Grier, and Schaeffer 2015)

Before we move on to the consideration of specific universal sets, let us emphasize again the importance of universality in relation to quantum computing:

- From a theorist point of view universality gives a sufficient level of abstraction. This allows the construction of theories and inferences to be made without regard to the limitations of physical realization. Quantum information science is still in its infancy and quantum machines are still imperfect, thus it would be a significant limitation to have to wait for the results of experiments in areas such as Quantum complexity theory.
- From a practical point of view (i.e. building quantum machines) the importance of universal gates is that the work of quantum machine engineers becomes easier. If it is possible to accomplish the entire potential of quantum computing with a limited number of gates, then it is enough to focus on how to implement them to be sure of achieving success. Additionally, it is worthwhile to design a specific universal gate set, among the uncountable number of possibilities, that may be easier to implement physically.
- The perspective of quantum error correction. In experimental physics it is possible to perform any single qubit unitary, for example to produce an arbitrary rotation of the Bloch sphere with act on an atom by setting laser parameters. For fault-tolerant quantum computing, it is important that we consider a finite set of instructions, because although there are countless physical unitaries that can be implemented in hardware,

the ones we can make fault-tolerant are just a discrete set.

In previous chapters we have explored the principles of quantum computing and presented the most notable quantum gates. A discussion has been made for the significant gates in terms of universality. In this chapter, we will define the concept of universality more rigorously and systematize universal sets in relation to the different types of universality.

Universal sets for irreversible classical computations and their reversible counterparts will be presented first (we will use *Boolean circuit model*, which is polynomially equivalent to other models of classical computation, e.g. *Turing machine*). Following this, we outline the meaning of universality and describe a key discovery in this area - the Solovey-Kitaev theorem. Then we systematize the most notable universal sets of quantum gates. And at the end we will show some examples of practical implementation.

4.1 Universal gates in classical computation

We will take the first step in describing universality with classical computing. In some ways it is more comprehensible and the area is substantially worked out. For example, we know here not only the complete universality criteria, but also a complete description where universality fails. And this is done both for irreversible classical computations (Post 1941) and for reversible classical computations (Aaronson, Grier, and Schaeffer 2015).

Irreversible classical computation By classical computation we mean a finite sequence of simple operations on bits - input bits and a circuit applied to them. As in quantum computing, the operation is referred to as a gate. Each vertex of the graph encode a gate, and edges encode bits flow. We argue that the gate set is "universal," which means that every Boolean function on any number of bits may be expressed using elements from this set. Some notable examples: $\{AND, NOT, OR\}$, $\{NAND\}$, $\{NOR\}$ However universality has limitations in the classical world, here are some non universal sets $\{NOT, OR\}$, $\{AND, OR\}$, $\{NOT, XOR\}$. Remember that in quantum computing we have agreed not to include gates such as erasure or ancillary in a set of universal gates. True, this happens in the context of maintaining unitarity. Here we act symmetrically, although obviously such gates are very common in the classical world.

Reversible classical computation The main difference between reversible and irreversible computation is that we should be able to map output bits to input bits. Reversible gates are universal if any reversible computation may be expressed in any number of bits. One example of a universal reversible gate was previously discussed in quantum: $TOFFOLI$ gate (see Chapter 3 - Quantum gates). For instance it can simulate $NAND$, preserving reversibility (we need an ancillary bit). Just as in the case of irreversible computation, universality is not an intrinsic attribute of reversible gates. $CNOT, NOT$ are examples of gates which are not universal or $FREDKIN$ which is not universal in a strong sense.

For the irreversible version of classical computation there are 2-bit universal gates. However, for reversible computation we need 3-bit gates at least to achieve universality. Another important observation: all reversible gates in classical computation are permutation matrices and are unitary by definition. This is why we can use $TOFFOLI$ both in quantum and classical. However, the nature of the actions is different, as there is no reading of the control qubit - instead it is about entangling the states of all the qubits involved.

4.2 Types of universality in quantum gates

We operate with the definitions set out in the textbook by Preskill (1998)

Definition 4.1. *gate set G is universal if unitary transformations that can be constructed as quantum circuits using this gate set are dense in the unitary group $U(2^n)$, up to an overall phase. For any $V \in U(2^n)$ and any $\sigma > 0$, there is a unitary $\widetilde{V}$ achieved by a finite circuit such that $||V - \widetilde{V}||_{sup} \leq \sigma$*

Now we will show a distinction between different kinds of universality.

Exact universality We consider some class of quantum gates in an uncountable set. Exact universality means that by building circuits from those gates we can implement exactly any unitary. For example, the set of all 2-qubit gates is exactly universal. In other words if we have any unitary that we want to reach acting on n qubits, then by putting together a suitable circuit of gates, where each gate just acts on a pair of qubits, we can realize that unitary exactly. Second example: the set of all single qubit gates is exactly universal if we add one entangling two qubit gate.

Generic universality Now we set back constraints of a finite set. In fact a single 2-qubit gate in almost all cases is universal (except non-entangling gates and gates of measure zero in $U(4)$). So universality is a very general thing.

Particular universality Here we look at particular universal gate sets. The main idea here is to see that they are universal or try to understand why it is true that there are finite gate sets which are universal. Here is an example: $\{H, T, CNOT\}$. If one can implement a $CNOT$ gate and two single qubit gates H which flips the x and z basis and T which rotates by $\frac{\pi}{4}$ about the z axis, that is universal.

Encoded universality Sometimes we settle for something less than universality called encoded universality. If we can not come arbitrarily close to all the unitaries acting on n qubits, but some subgroups of the unitaries. But as long as that is an exponentially large subgroup then that is good enough for accessing the power of quantum computation. We have already given an example: $\{H, TOFFOLI\}$

What we set out earlier is mainly only concerned with the reachability of arbitrary unitaries, next we will discuss what resources are needed to do this.

Solovay-Kitaev Theorem We give here the formulation of this important theorem according to Nielsen and I. L. Chuang (1997).

Theorem 1. Let $\mathscr{G}$ be a finite set of elements in $U(2)$ containing its own inverses (so $g \in \mathscr{G}>$ implies $g^{-1} \in \mathscr{G}$) and such that the group $\langle\mathscr{G}\rangle$ they generate is dense in $SU(2)$. Consider some $\varepsilon > 0$. Then there is a constant c such that for any $U \in \mathrm{SU}(2)$, there is a sequence S of gates from $\mathscr{G}$ of length $O(\log^c(1/\varepsilon))$ such that $\|S - U\| \leq \varepsilon$. That is, S approximates U to operator norm error.

In other words, if we simulate a gate from one universal set using gates from a another universal set, then the resources required for this are growing rather moderately $\log^c(1/\varepsilon)$ So all closed under inverse universal gate sets fill in the space of all unitaries $SU(2)$ very quickly.

4.3 Notable universal quantum gate sets

We have seen how much universality in the world of quantum computing differs from the classical world, which is not surprising. What is really striking here is that the number of universal sets is uncountable. To some extent, it is more difficult to define what are criteria for quantum gate sets for fail to be universal. From what we have observed it this paper, we can list criteria of encoded[1] non-universality:

1. There is no *entangling* gate in the set.
2. There is no gate in the set, which create *superposition*.
3. Gates in the set implement a discrete subset of unitary transformations, gates taken only from $Clifford$ set for instance.

Meeting at least one of these criteria leads to the fact that this set is not universal. Note that this list is about universality in a weaker sense. We are not dealing with approximation of all unitaries, but the goal is to achieve all the power of quantum computers.

In the Table 1 we have systematized the universal sets we have reviewed.

4.4 Universal quantum gates implementation

At the end of this chapter, we will give a short overview of how universal sets are implemented on the real quantum machines. These are intended to be preliminary examples, as we acknowledge there are many variants of such practical implementations. Such important processes as compilation and transpilation, mapping logical gates to physical gates, are outside the scope of this review.

1. this is why we do not mention imaginary gate absence

Universal quantum gate set	Type of universality	Application area
All 2-qubit gates	exact	Uncountable set, not technically feasible, but important for building other universal sets
All 1-qubit gates + *any* entangling gate	exact	Not technically feasible, using in theory
$\{DEUTSCH\}$	particular	First proved to be universal. Difficult to implement because of the large number of parameters to be controlled
$\{BARENCO\}$	particular	First proved to be universal use in theory
Any 2-qubit gate, except zero measure in $U(4)$	generic	Shows that universality is a very general thing, it is even hard to avoid it.
$\{H,T,CNOT\}$	particular	Special important in fault-tolerant quantum theory
$\{H,TOFFOLI\}$	particular (encoded)	Does not work with an imaginary part, but gives all the power of quantum computing. Implementation of TOFFOLI is not known.

Table 1. Universal gates discussed in this study

Quantum platforms use various physical gates. Although a universal set of gates such as $\{H,T,CNOT\}$ is very important in theoretical terms, the implementation on real quantum machines is different. Also certain computations can be more efficiently implemented with additional gates to the universal set. A Pauli rotation with an arbitrary angle and an entangling gate with a variable or at maximal entangle is commonly employed in many quantum computation at the physical level of universal gate set. Table 2 gives examples of entangling gates implementation on the most advanced at the moment quantum platforms.

Quantum platform	Key entangling gate
Trapped ion systems	Mølmer-Sørenson gate $\begin{bmatrix} \cos\left(\frac{\phi}{2}\right) & 0 & 0 & -i\sin\left(\frac{\phi}{2}\right) \\ 0 & \cos\left(\frac{\phi}{2}\right) & -i\sin\left(\frac{\phi}{2}\right) & 0 \\ 0 & -i\sin\left(\frac{\phi}{2}\right) & \cos\left(\frac{\phi}{2}\right) & 0 \\ -i\sin\left(\frac{\phi}{2}\right) & 0 & 0 & \cos\left(\frac{\phi}{2}\right) \end{bmatrix}$
Superconductors IBM	Cross-Resonance gate $\begin{bmatrix} \cos\left(\frac{1}{2}\theta\right) & 0 & -i\sin\left(\frac{1}{2}\theta\right) & 0 \\ 0 & \cos\left(\frac{1}{2}\theta\right) & 0 & i\sin\left(\frac{1}{2}\theta\right) \\ -i\sin\left(\frac{1}{2}\theta\right) & 0 & \cos\left(\frac{1}{2}\theta\right) & 0 \\ 0 & i\sin\left(\frac{1}{2}\theta\right) & 0 & \cos\left(\frac{1}{2}\theta\right) \end{bmatrix}$
Superconductors Google Sycamore	fSim gate $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i(\delta_+ + \delta_-)}\cos(\theta) & -ie^{i(\delta_+ - \delta_{-,off})}\sin(\theta) & 0 \\ 0 & -ie^{i(\delta_+ + \delta_{-,off})}\sin(\theta) & e^{i(\delta_+ - \delta_-)}\cos(\theta) & 0 \\ 0 & 0 & 0 & e^{i(2\delta_+ - \phi)} \end{bmatrix}$

Table 2. Entangling gates implementation on different quantum platforms

5 Conclusion

This project argues in favour of the importance of universal quantum gates for both theory and practice and highlights the key difference to the universal gates in classical computing. In conclusion we summarise the most notable findings.

Linear Algebra, the basic language for describing quantum mechanics, is crucial for understanding quantum computing in general and universal quantum gates particular. In addition, probability theory, number theory, functional analysis, group theory and many other areas of mathematics are essential to a better understanding of quantum algorithms. Whereas in classical computation we mostly need discrete mathematics: logic, sets, graphs.

By Quantum Computer we refer Quantum Circuit Model in this paper and argue that it does not matter which model is taken as the basis, as polynomial equivalence between different models of quantum computing has been proved. In favour of considering the Quantum Circuit Model, the fact that most real quantum machines implement this model. We give examples of the most advanced solutions.

We stress the key differences between the quantum world and the classical world, directly affecting the computation models built on their basis. The *probabilistic* aspect and the *interference* are properties of quantum systems by default. The *entanglement* and *superposition* must be implemented in quantum gates to achieve universality.

We outline the necessary formalism of quantum computer: qubit, quantum gate, quantum circuit, as well as the key property of unitarity. For universal quantum gates (gate sets) we define the following important properties:

- The number of universal gates is actually uncountable and universality is very common: for example almost any 2-qubit gate is universal.
- The presence of an entangling gate and a gate that leads to superposition is a prerequisite for universality.
- One universal set can effectively (in polynomial time) implement another universal set.

- Complex numbers are native to describing quantum systems and quantum computing, but to achieve the full power of quantum computing one can get away with gates that work only with real numbers. For a broader problem to approximate a unitary, we definitely need complex matrices.
- Sets, naturally limited in terms of universality, can become universal with some addition. For instance, if we augment $Clifford$ with T gate, that allows together to make turns on an irrational π angle.
- The practical implementation of universal gates takes into account the specific features of quantum mechanical systems. For example CZ gate is natural in linear optics, while MølmerSørensen gate used in trapped ion.
- Universality is also common in the classical world. However, despite the apparent similarities between classical universal set $\{TOFFOLI\}$ and quantum universal set $\{TOFFOLI, H\}$, there is an important difference, apart from the addition of a superposition-creating H. In classical computing $TOFFOLI$ is just a permutation matrix, while in quantum it is a unitary entangling transformation.
- A research gap was found: the lack of a complete list of non-universality criteria, this could be a quite hot research topic.

We stress again here that universality does not imply that any operation on qubits can be performed quickly via approximation. Such a condition cannot be met since elementary gates operate on a fixed number of qubits, making it impossible. From counting arguments one can see that the efficient expressible operations on qubits capture just a fraction of the potential operations. The fundamental topic of quantum complexity theory is which operation can be described efficiently by elementary gates.

In this paper we talk about computational complexity only in the context of polynomial resource growth as a measure of efficiency. Nevertheless, the connection between universal gates and complexity theory is much closer. The hypothesis of inequality between the classes of efficient classical (probabilistic) computation BPP and efficient quantum computation BQP is widely accepted. If the hypothesis turns out to be wrong and problems from the BQP class can be solved on a probabilistic classical universal machine, then $\{NAND\}$ is universal for quantum computation if we add ancillary random bits.

Bibliography

Aaronson, Scott. 2004. "Is quantum mechanics an island in theoryspace?" *arXiv preprint quant-ph/0401062.*

Aaronson, Scott, Daniel Grier, and Luke Schaeffer. 2015. "The classification of reversible bit operations". *arXiv preprint arXiv:1504.05155.*

Aharonov, Dorit. 2003. "A simple proof that Toffoli and Hadamard are quantum universal". *arXiv preprint quant-ph/0301040.*

Aharonov, Dorit, and Michael Ben-Or. 1996. "Polynomial simulations of decohered quantum computers". In *Proceedings of 37th Conference on Foundations of Computer Science,* 46–55. IEEE.

Aharonov, Dorit, Wim Van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev. 2008. "Adiabatic quantum computation is equivalent to standard quantum computation". *SIAM review* 50 (4): 755–787.

Amy, Matthew, Dmitri Maslov, Michele Mosca, and Martin Roetteler. 2013. "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits". *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 32 (6): 818–830.

Arora, Sanjeev, and Boaz Barak. 2009. *Computational complexity: a modern approach.* Cambridge University Press.

Arute, Frank, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. 2019. "Quantum supremacy using a programmable superconducting processor". *Nature* 574 (7779): 505–510.

Barak, Boaz. 2017. "Introduction to Theoretical Computer Science". *Under preperation.*

Barenco, Adriano. 1995. "A universal two-bit gate for quantum computation". *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 449 (1937): 679–683.

Barenco, Adriano, Charles H Bennett, Richard Cleve, David P DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A Smolin, and Harald Weinfurter. 1995. "Elementary gates for quantum computation". *Physical review A* 52 (5): 3457.

Bell, John S. 1964. "On the einstein podolsky rosen paradox". *Physics Physique Fizika* 1 (3): 195.

Benioff, Paul. 1980. "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". *Journal of statistical physics* 22 (5): 563–591.

Bhattacharjee, Debjyoti, and Anupam Chattopadhyay. 2017. "Depth-optimal quantum circuit placement for arbitrary topologies". *arXiv preprint arXiv:1703.08540.*

Bhattacharjee, Debjyoti, Abdullah Ash Saki, Mahabubul Alam, Anupam Chattopadhyay, and Swaroop Ghosh. 2019. "MUQUT: Multi-constraint quantum circuit mapping on NISQ computers". In *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD),* 1–7. IEEE.

Bloch, F. October 1946. "Nuclear Induction". *Phys. Rev.* 70 (7-8): 460–474. https://doi.org/10.1103/PhysRev.70.460. https://link.aps.org/doi/10.1103/PhysRev.70.460.

Booth, Kyle EC, Minh Do, J Christopher Beck, Eleanor Rieffel, Davide Venturelli, and Jeremy Frank. 2018. "Comparing and integrating constraint programming and temporal planning for quantum circuit compilation". In *Twenty-Eighth international conference on automated planning and scheduling.*

Chow, Jerry, Oliver Dial, and Jay Gambetta. 2021. "IBM Quantum breaks the 100-qubit processor barrier". *IBM Research Blog, available in https://research. ibm. com/blog/127-qubit-quantum-process-or-eagle.*

Cowtan, Alexander, Silas Dilkes, Ross Duncan, Alexandre Krajenbrink, Will Simmons, and Seyon Sivarajah. 2019. "On the qubit routing problem". *arXiv preprint arXiv:1902.08091.*

Crooks, Gavin E. 2020. "Gates, states, and circuits".

Dawson, Christopher M, and Michael A Nielsen. 2005. "The solovay-kitaev algorithm". *arXiv preprint quant-ph/0505030.*

De Wolf, Ronald. 2019. “Quantum computing: Lecture notes”. *arXiv preprint arXiv:1907.09415.*

Deutsch, David. 1985. “Quantum theory, the Church–Turing principle and the universal quantum computer”. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400 (1818): 97–117.

Deutsch, David Elieser. 1989. “Quantum computational networks”. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 425 (1868): 73–90.

DiVincenzo, David P. 2000. “The physical implementation of quantum computation”. *Fortschritte der Physik: Progress of Physics* 48 (9-11): 771–783.

Feynman, R.P. 1982. “Simulating physics with computers”. Cited By 2994, *International Journal of Theoretical Physics* 21 (6-7): 467–488. https://doi.org/10.1007/BF02650179.

Fredkin, Edward, and Tommaso Toffoli. 1982. “Conservative logic”. *International Journal of theoretical physics* 21 (3): 219–253.

Freedman, Michael H, Alexei Kitaev, and Zhenghan Wang. 2002. “Simulation of topological field theoriesű by quantum computers”. *Communications in Mathematical Physics* 227 (3): 587–603.

Itoko, Toshinari, Rudy Raymond, Takashi Imamichi, and Atsushi Matsuo. 2020. “Optimization of quantum circuit mapping using gate transformation and commutation”. *Integration* 70:43–50.

Kempe, Julia, Alexei Kitaev, and Oded Regev. 2006. “The complexity of the local Hamiltonian problem”. *Siam journal on computing* 35 (5): 1070–1097.

Kitaev, A Yu. 2003. “Fault-tolerant quantum computation by anyons”. *Annals of Physics* 303 (1): 2–30.

Kliuchnikov, Vadym, Dmitri Maslov, and Michele Mosca. 2012. “Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates”. *arXiv preprint arXiv:1206.5236.*

Manin, Yuri. 1980. “Computable and uncomputable”. *Sovetskoye Radio, Moscow* 128.

Maslov, Dmitri, Gerhard W Dueck, D Michael Miller, and Camille Negrevergne. 2008. "Quantum circuit simplification and level compaction". *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 27 (3): 436–444.

Müller, M, Klemens Hammerer, YL Zhou, Christian F Roos, and P Zoller. 2011. "Simulating open quantum systems: from many-body interactions to stabilizer pumping". *New Journal of Physics* 13 (8): 085007.

Murali, Prakash, Norbert Matthias Linke, Margaret Martonosi, Ali Javadi Abhari, Nhung Hong Nguyen, and Cinthia Huerta Alderete. 2019. "Full-stack, real-system quantum computer studies: Architectural comparisons and design insights". In *2019 ACM/IEEE 46th Annual International Symposium on Computer Architecture (ISCA),* 527–540. IEEE.

Nam, Yunseong, Neil J Ross, Yuan Su, Andrew M Childs, and Dmitri Maslov. 2018. "Automated optimization of large quantum circuits with continuous parameters". *npj Quantum Information* 4 (1): 1–12.

Nielsen, Michael A, and Isaac Chuang. 2002. *Quantum computation and quantum information.*

Nielsen, Michael A, and Isaac L Chuang. 1997. "Programmable quantum gate arrays". *Physical Review Letters* 79 (2): 321.

Oddi, Angelo, and Riccardo Rasconi. 2018. "Greedy randomized search for scalable compilation of quantum circuits". In *International Conference on the Integration of Constraint Programming, Artificial Intelligence, and Operations Research,* 446–461. Springer.

Papadimitriou, Christos H. 2003. *Computational complexity.* John Wiley / Sons Ltd.

Post, EL. 1941. "The two-valued iterative systems of mathematical logic. Number 5 in Annals of Math". *Studies. Princeton Univ. Press.*

Preskill, John. 1998. "Lecture notes for physics 229: Quantum information and computation". *California Institute of Technology* 16 (1): 1–8.

Raussendorf, Robert, and Hans Briegel. 2001. "Computational model underlying the one-way quantum computer". *arXiv preprint quant-ph/0108067.*

Rivest, Ronald L, Adi Shamir, and Leonard Adleman. 1978. “A method for obtaining digital signatures and public-key cryptosystems”. *Communications of the ACM* 21 (2): 120–126.

Ross, Neil J, and Peter Selinger. 2014. “Optimal ancilla-free Clifford+ T approximation of z-rotations”. *arXiv preprint arXiv:1403.2975.*

Selinger, Peter. 2015. “Generators and relations for n-qubit Clifford operators”. *Logical Methods in Computer Science* 11.

Shor, Peter W. 1999. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”. *SIAM review* 41 (2): 303–332.

Siu, M Stewart. 2005. “From quantum circuits to adiabatic algorithms”. *Physical Review A* 71 (6): 062314.

Stinespring, W Forrest. 1955. “Positive functions on C*-algebras”. *Proceedings of the American Mathematical Society* 6 (2): 211–216.

Tan, Bochen, and Jason Cong. 2020. “Optimality study of existing quantum computing layout synthesis tools”. *IEEE Transactions on Computers* 70 (9): 1363–1373.

Tegmark, Max, and John Archibald Wheeler. 2001. “100 years of quantum mysteries”. *Scientific American* 284 (2): 68–75.

Toffoli, Tommaso. 1980. “Reversible computing”. In *International colloquium on automata, languages, and programming,* 632–644. Springer.

Williams, Colin P, Scott H Clearwater, et al. 1998. *Explorations in quantum computing.* Springer.

Yao, A Chi-Chih. 1993. “Quantum circuit complexity”. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science,* 352–361. IEEE.

Zulehner, Alwin, Alexandru Paler, and Robert Wille. 2018. “An efficient methodology for mapping quantum circuits to the IBM QX architectures”. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 38 (7): 1226–1236.

Zulehner, Alwin, and Robert Wille. 2019. "Compiling SU (4) quantum circuits to IBM QX architectures". In *Proceedings of the 24th Asia and South Pacific Design Automation Conference,* 185–190.