

Quantum Algorithms - A short introduction

Johannes A. Buchmann

Version: August 15, 2025

Preface

This is a collection of slides for a lecture on quantum algorithms, based on my book Introduction to Quantum Algorithms, AMS Pure and Applied Undergraduate Texts 64, 2024.

I have made an effort to keep the lecture as compact as possible. The numbering of propositions, theorems, and definitions follows the numbering used in the book. This allows participants to easily find more details in the book, where complete proofs are provided.

Instructors are welcome to use a selection of these slides for their own purposes. I would be grateful to receive any corrections or suggestions.

Outline I

1. Basics

- 1.1 State spaces
- 1.2 Quantum bits
- 1.3 The Bloch sphere
- 1.4 Quantum registers
- 1.5 Composite systems
- 1.6 Entanglement
- 1.7 Some Linear Algebra
- 1.8 Measurements
- 1.9 Time Evolution
- 1.10 Mixed States and Density Operators
- 1.11 Quantum postulates for density operators
- 1.12 Tracing Out Subsystems

2. The Algorithms of Deutsch and Simon

- 2.1 The Deutsch Algorithm
- 2.2 The Deutsch-Jozsa Algorithm
- 2.3 Simon's Algorithm
- 2.4 A Generalization of Simon's algorithm

Outline II

3. Quantum Computability and Complexity

- 3.1 Single-qubit gates
- 3.2 Rotation operators and rotations on the Bloch sphere
- 3.3 Elementary single-qubit gates
- 3.4 Controlled gates
- 3.5 Universal and perfectly universal sets of quantum gates
- 3.6 Quantum complexity

4. Shor's Algorithms

- 4.1 Integer Factorization
- 4.2 Phase Estimation Using the Discrete Fourier Transform
- 4.3 Phase Estimation Using the Quantum Fourier Transform
- 4.4 Order Computation Using Phase Estimation
- 4.5 Integer Factorization by Order Computation
- 4.6 Discrete Logarithms

Outline III

5. Quantum Search and Quantum Counting

5.1 The Search Problem

5.2 Quantum search when the number of solutions is known

5.3 Grover Search for an Unknown Number of Solutions

5.4 Quantum Counting

1. Basics

1.1. State spaces

The state space postulate

Postulate 3.1.1: A closed physical system is associated with a **Hilbert space**, called the *state space* of the system. The system at a particular time is completely described by a unit vector in its state space, called the *state vector* or *state* of the physical system.

Hilbert and Euclidean spaces

A *Hilbert space* is a complete inner product space over \mathbb{R} or \mathbb{C} .

A *Euclidean space* is a finite-dimensional Hilbert space, i.e., a finite-dimensional complex inner product space.

To model quantum algorithms, only Euclidean spaces are required.

Notation:

\mathbb{H} is always a Euclidean space with inner product $\langle \cdot | \cdot \rangle$ and Euclidean length $\| \cdot \|$.

k, l, n, m are always positive integers.

The prototype of a Euclidean space: \mathbb{C}^k

$$\mathbb{C}^k = \{\vec{a} = (\alpha_0, \dots, \alpha_{k-1}) : \alpha_j \in \mathbb{C}\}.$$

The *standard basis* of \mathbb{C}^k : $(\vec{e}_0 = (1, 0 \dots, 0), \vec{e}_1 = (0, 1 \dots, 0), \dots, \vec{e}_{k-1} = (0, 0 \dots, 0, 1))$.

The *inner product* of $\vec{a} = (\alpha_0, \dots, \alpha_{k-1})$, $\vec{b} = (\beta_0, \dots, \beta_{k-1}) \in \mathbb{C}^k$: $\langle \vec{a} | \vec{b} \rangle = \sum_{j=0}^{k-1} \overline{\alpha_j} \beta_j$.

The *Euclidean length* of $\vec{a} = (\alpha_0, \dots, \alpha_{k-1}) \in \mathbb{C}^k$: $\|\vec{a}\| = \sqrt{\sum_{j=0}^{k-1} |\alpha_j|^2}$.

The *linear maps* $\mathbb{C}^l \rightarrow \mathbb{C}^k$ are represented by matrices in $\mathbb{C}^{k,l}$ where the j th column is the image of the j th standard basis vector of \mathbb{C}^l .

The bra-ket notation

Every element of \mathbb{H} is denoted by $|\varphi\rangle$ for some character φ , pronounced “ket- φ ”.

For $|\varphi\rangle \in \mathbb{H}$ we define the linear map “bra- φ ”: $\langle\varphi| : \mathbb{H} \rightarrow \mathbb{C}, |\psi\rangle \mapsto \langle\varphi|\psi\rangle$.

The character φ may be replaced by any other character, number, or even word.

The **inner product** of $|\varphi\rangle$ and $|\psi\rangle$ in \mathbb{H} is denoted by $\langle\varphi|\psi\rangle$. It is obtained by gluing $\langle\varphi|$ and $|\psi\rangle$ together.

The **Euclidean length** of $|\varphi\rangle$ is denoted by $\|\varphi\|$.

Identification of \mathbb{H} with \mathbb{C}^k

Let $B = (|b_0\rangle, \dots, |b_{k-1}\rangle)$ be an *orthonormal basis (ONB)* of \mathbb{H} , i.e., $\|b_i\| = 1$ and $\langle b_i | b_j \rangle = \delta_{i,j}$ for $0 \leq i, j < k$.

Identify \mathbb{H} and \mathbb{C}^k via the isomorphism $\mathbb{H} \rightarrow \mathbb{C}^k$, $\sum_{j=0}^{k-1} \alpha_j |b_j\rangle \mapsto (\alpha_0, \dots, \alpha_k)$.

Let \mathbb{H}' be a Euclidean space of dimension l with ONB B' .

Identify $\text{Hom}_{\mathbb{C}}(\mathbb{H}', \mathbb{H})$ with $\mathbb{C}^{(k,l)}$ via

$$\begin{array}{ccc} \mathbb{C}^l & \xrightarrow{A \in \mathbb{C}^{k \times l}} & \mathbb{C}^k \\ \updownarrow B' & & \updownarrow B \\ \mathbb{H}' & \xrightarrow{f} & \mathbb{H} \end{array}$$

1.2. Quantum bits

States of quantum bits

The state of a classical bit b is 0 or 1

The state of a *quantum bit (qubit)* Q is

$$|\varphi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle, \alpha_0, \alpha_1 \in \mathbb{C}, |\alpha_0|^2 + |\alpha_1|^2 = 1.$$

Example:

$$|x_+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |y_+\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, |z_+\rangle = |0\rangle, |h_+\rangle = \cos \frac{\pi}{8} |0\rangle + \sin \frac{\pi}{8} |1\rangle,$$

$$|x_-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, |y_-\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}, |z_-\rangle = |1\rangle, |h_-\rangle = \sin \frac{\pi}{8} |0\rangle - \cos \frac{\pi}{8} |1\rangle.$$

The state space \mathbb{H}_1 of a quantum bit

$$\mathbb{H}_1 = \{\alpha_0 |0\rangle + \alpha_1 |1\rangle : \alpha_0, \alpha_1 \in \mathbb{C}\} = \mathbb{C} |0\rangle + \mathbb{C} |1\rangle.$$

The *computational basis* of \mathbb{H}_1 is $(|0\rangle, |1\rangle)$.

The *inner product* of $|\varphi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, $|\psi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$ $\langle\varphi|\psi\rangle = \overline{\alpha_0}\beta_0 + \overline{\alpha_1}\beta_1$.

We use the isomorphism $\mathbb{H}_1 \rightarrow \mathbb{C}^2$, $\alpha_0 |0\rangle + \alpha_1 |1\rangle \mapsto (\alpha_0, \alpha_1)$ to identify \mathbb{H}_1 with \mathbb{C}^2 .

Example: $|0\rangle \cong (1, 0)$ and $|1\rangle \cong (0, 1)$.

The state space postulate for qubits

A quantum bits (qubit) is associated with the Euclidean space \mathbb{H}_1 , called the *state space* of the qubit. The qubit at a particular time is completely described by a unit vector in its state space, called the *state vector* or *state* of the qubit.

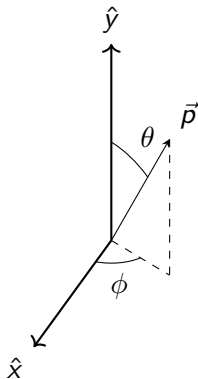
1.3. The Bloch sphere

1.3. The Bloch sphere

Spherical coordinates

Proposition 3.1.12: Let $\vec{p} \in \mathbb{R}^3$. Then there is a uniquely determined triplet (r, θ, ϕ) of real numbers, called the *(standard) spherical coordinate representation of \vec{p}* with

- ▶ $r = \|\vec{p}\|$: *radial distance*.
- ▶ $\theta \in [0, \pi]$; if $\vec{p} = \vec{0}$ then $\theta = 0$: *polar angle*.
- ▶ $\phi \in [0, 2\pi[$; if $\theta \in \{0, \pi\}$ then $\phi = 0$: *azimuthal angle*.
- ▶ $\vec{p} = r(\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta)$.



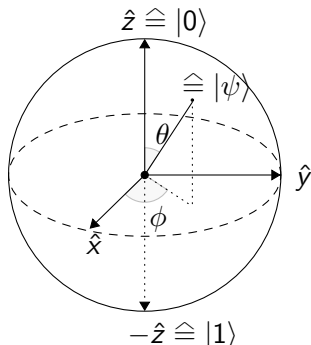
Visualization of qubit states on the Bloch sphere

The *Bloch sphere* S_1 is the unit ball in \mathbb{R}^3 .

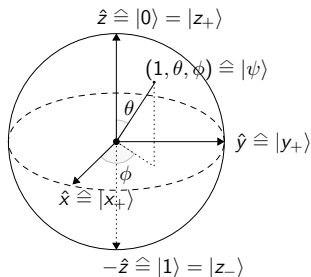
For $\vec{p} = (1, \theta, \phi) \in S_1$ set $|\psi(\vec{p})\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle$.

Proposition 3.1.18: For any quantum state $|\psi\rangle \in \mathbb{H}_1$ there is a uniquely determined point \vec{p} on the Bloch sphere and $\gamma \in [0, 2\pi[$ such that $|\psi\rangle = e^{i\gamma} |\psi(\vec{p})\rangle$. We write $\vec{p}(\psi) = \vec{p}$.

If $\vec{p} = (1, \theta, \phi)$, we set $\theta(\psi) = \theta$, $\phi(\psi) = \phi$.



Example



Points on the Bloch sphere corresponding to

$$|x_+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |y_+\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \quad |z_+\rangle = |0\rangle, \quad |z_-\rangle = |1\rangle,$$

and a general single-qubit state $|\psi\rangle$.

1.4. Quantum registers

The states of a quantum register

The *Computational basis states* of n -qubit registers are $|\vec{b}\rangle$ with $\vec{b} \in \{0, 1\}^n$.

Alternative representation: $|b\rangle_n = |\vec{b}\rangle$ with $b = \sum_{j=0}^{n-1} b_j 2^{n-j-1}$, $\vec{b} = (b_0 \cdots b_{n-1})$.

Example: $|13\rangle_4 = |1101\rangle$, $|13\rangle_5 = |01101\rangle$.

The *general state* of an n -qubit register is of the form

$$|\varphi\rangle = \sum_{\vec{b} \in \{0,1\}^n} \alpha_{\vec{b}} |\vec{b}\rangle = \sum_{b=0}^{2^n-1} \alpha_b |b\rangle_n, \text{ with } \alpha_{\vec{b}}, \alpha_b \in \mathbb{C}, \sum_{\vec{b} \in \{0,1\}^n} |\alpha_{\vec{b}}|^2 = \sum_{b=0}^{2^n-1} |\alpha_b|^2 = 1.$$

Example: The *Bell state*: $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle = \frac{1}{\sqrt{2}} |0\rangle_2 + \frac{1}{\sqrt{2}} |3\rangle_2$.

The state space \mathbb{H}_n of n -bit quantum registers

$$\mathbb{H}_n = \sum_{\vec{b} \in \{0,1\}^n} \mathbb{C} |\vec{b}\rangle = \sum_{b=0}^{2^n-1} \mathbb{C} |b\rangle_n.$$

The *inner product* of $|\varphi\rangle = \sum_{b=0}^{2^n-1} \alpha_b |b\rangle_n$ and $|\psi\rangle = \sum_{b=0}^{2^n-1} \beta_b |b\rangle_n$ is $\langle\varphi|\psi\rangle = \sum_{j=0}^{2^n-1} \overline{\alpha_j} \beta_j$.

We use $\mathbb{H}_n \rightarrow \mathbb{C}^{2^n}$, $\sum_{b=0}^{2^n-1} \alpha_b |b\rangle_n \mapsto (\alpha_0, \dots, \alpha_{2^n-1})$ to identify \mathbb{H}_n with \mathbb{C}^{2^n} .

Example: $|00\rangle \hat{=} (1, 0, 0, 0)$, $|01\rangle \hat{=} (0, 1, 0, 0)$, $|10\rangle \hat{=} (0, 0, 1, 0)$, $|11\rangle \hat{=} (0, 0, 0, 1)$.

The state space postulate for quantum registers

An n -qubit register is associated with the Euclidean space \mathbb{H}_n , called the *state space* of the register. The register at a particular time is completely described by a unit vector in its state space, called the *state vector* or *state* of the quantum register.

1.5. Composite systems

The composite systems postulate

Postulate 3.2.1: The state space of the composition of finitely many physical systems is the **tensor product** of the state spaces of the component systems. Moreover, if we have systems numbered 0 through $m - 1$ and if system i is in the state $|\psi_i\rangle$ for $0 \leq i < m$, then the composite system is in state $|\psi_0\rangle \otimes \cdots \otimes |\psi_{m-1}\rangle$.

The tensor product of two qubits

If qubit A is in state $|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and qubit B is in state $|\psi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, then the state of the composition AB of A and B is the *tensor product* of $|\varphi\rangle$ and $|\psi\rangle$:

$$|\varphi\rangle \otimes |\psi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle.$$

This is a state in \mathbb{H}_2 .

Example: $|x_+\rangle \otimes |x_-\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle-|01\rangle+|10\rangle-|11\rangle}{2}.$

The tensor product of several quantum registers

For $0 \leq j < m$ let $n_j \in \mathbb{N}$ and let

$$|\varphi_j\rangle = \sum_{\vec{b} \in \{0,1\}^{n_j}} \alpha_{\vec{b},j} |\vec{b}\rangle \in \mathbb{H}_{n_j}$$

be the state of an n_j -quantum register Q_j

Then the state of the composite system Q_0, \dots, Q_{m-1} is the *tensor product*

$$|\varphi_0\rangle \otimes \dots \otimes |\varphi_{m-1}\rangle = \sum_{\vec{b}_0 \in \{0,1\}^{n_0}} \dots \sum_{\vec{b}_{m-1} \in \{0,1\}^{n_{m-1}}} \left(\prod_{j=0}^{m-1} \alpha_{\vec{b}_j,j} \right) |\vec{b}_0|| \dots || \vec{b}_{m-1}\rangle.$$

Multilinearity of tensor products

Example: $|0\rangle \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |1\rangle = \frac{1}{\sqrt{2}} (|001\rangle + |011\rangle).$

In general:

If $n_i \in \mathbb{N}$, $|\varphi_i\rangle \in \mathbb{H}_{n_i}$ for $0 \leq i < m$, $j \in \mathbb{Z}_m$, $|\varphi\rangle, |\psi\rangle \in \mathbb{H}_{n_j}$, $\alpha \in \mathbb{C}$, then we have

$$\begin{aligned} & |\varphi_0\rangle \otimes \cdots \otimes |\varphi_{j-1}\rangle \otimes \left(\alpha(|\varphi\rangle + |\psi\rangle) \right) \otimes |\varphi_{j+1}\rangle \otimes \cdots \otimes |\varphi_{m-1}\rangle \\ &= \alpha \left(|\varphi_0\rangle \otimes \cdots \otimes |\varphi_{j-1}\rangle \otimes |\varphi\rangle \otimes |\varphi_{j+1}\rangle \otimes \cdots \otimes |\varphi_{m-1}\rangle \right. \\ &\quad \left. + |\varphi_0\rangle \otimes \cdots \otimes |\varphi_{j-1}\rangle \otimes |\psi\rangle \otimes |\varphi_{j+1}\rangle \otimes \cdots \otimes |\varphi_{m-1}\rangle \right). \end{aligned}$$

Simplified notation

$$|\varphi_0\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_{m-1}\rangle = |\varphi_0\rangle |\varphi_2\rangle \cdots |\varphi_{m-1}\rangle = \bigotimes_{j=0}^{m-1} |\varphi_j\rangle.$$

$$|\varphi_0\rangle^{\otimes m} = \bigotimes_{j=0}^{m-1} |\varphi_0\rangle.$$

Example: $\left| \underbrace{0 \dots 0}_m \right\rangle = \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_m = \underbrace{|0\rangle \cdots |0\rangle}_m = \bigotimes_{j=0}^{m-1} |0\rangle = |0\rangle^{\otimes m}.$

1.6. Entanglement

Entangled states

A state of the composition of two quantum systems is called *entangled* (with respect to this partitioning) if it cannot be written as the tensor product of states of the component systems. Otherwise, this state is called *separable* or *non-entangled*.

Example:

1. The state $|\varphi\rangle = (\frac{1}{2}(|00\rangle + i|01\rangle + |10\rangle + i|11\rangle))$ is separable because we have $|\varphi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$.
2. The Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is entangled.

The Schmidt decomposition theorem

Theorem 2.5.18: Let $\mathbb{H}(0)$ and $\mathbb{H}(1)$ be Euclidean spaces of dimension k, l , respectively, let $m = \min\{k, l\}$, and $|\varphi\rangle \in \mathbb{H} = \mathbb{H}(0) \otimes \mathbb{H}(1)$. Then there are orthonormal sequences $(|u_0\rangle, \dots, |u_{m-1}\rangle)$ in $\mathbb{H}(0)$ and $(|v_0\rangle, \dots, |v_{m-1}\rangle)$ in $\mathbb{H}(1)$ as well as $r_0, \dots, r_{m-1} \in \mathbb{R}_{\geq 0}$ such that

$$|\varphi\rangle = \sum_{i=0}^{m-1} r_i |u_i\rangle \otimes |v_i\rangle. \quad (1.6.1)$$

Up to reordering, the coefficients r_i are uniquely determined by $|\varphi\rangle$. The representation (1.6.1) is called a *Schmidt decomposition* with respect to the partitioning $\mathbb{H} = \mathbb{H}(0) \otimes \mathbb{H}(1)$. The nonzero coefficients r_i are called the *Schmidt coefficients* of φ and their number is called the *Schmidt rank* of $|\varphi\rangle$ with respect to this partitioning.

Example: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ is a Schmidt decomposition of the Bell state. Therefore, its Schmidt rank is 2, the Schmidt coefficients are both 1, and it is entangled.

Characterization of entangled states

The state of the composition of two quantum registers is separable if and only if its Schmidt rank with respect to this partitioning is 1.

1.7. Some Linear Algebra

Adjoint, involutions, normal, unitary, Hermitian matrices

$A = \begin{pmatrix} 1 & i \\ 2i & 0 \end{pmatrix}$ represents the linear map $\mathbb{H}_1 \rightarrow \mathbb{H}_1$, $|0\rangle \mapsto |0\rangle + 2i|1\rangle$, $|1\rangle \mapsto i|0\rangle$.

The *adjoint* of $A \in \mathbb{C}^{(k,k)}$ is $A^* = \overline{A^T}$; **Example:** $A = \begin{pmatrix} 1 & i \\ 2i & 0 \end{pmatrix}$, $A^* = \begin{pmatrix} 1 & -2i \\ -i & 0 \end{pmatrix}$.

A is an *involution* if A^2 is the identity, A is *normal* if $A^*A = AA^*$, A is *Hermitian* if $A^* = A$, A is *unitary* if A is invertible and $A^* = A^{-1}$,

Proposition 2.4.49: If A is Hermitian or unitary, then A is normal.

Example: The *Pauli matrix* $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is a Hermitian and unitary involution.

Outer products

The *outer product* of $|\varphi\rangle$ and $|\psi\rangle$ in \mathbb{H} is $|\varphi\rangle\langle\psi| : \mathbb{H} \rightarrow \mathbb{H}, |\xi\rangle \mapsto |\varphi\rangle\langle\psi|\xi\rangle$.

The outer product of $\vec{a}, \vec{b} \in \mathbb{C}^k$ is $\vec{a}\vec{b}^*$.

Example: The outer product of $(1, 0)$ with itself is $= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Proposition: If B is an ONB of \mathbb{H} and $|\varphi\rangle \in \mathbb{H}$, then $|\varphi\rangle = \sum_{|b\rangle \in B} |b\rangle\langle b|\varphi\rangle$.

Orthogonal projections

Proposition 2.2.44: If \mathbb{H}' is a subspace of \mathbb{H} , then \mathbb{H} is the direct sum of \mathbb{H}' and its *orthogonal complement* $(\mathbb{H}')^\perp = \{|\varphi\rangle \in \mathbb{H} : \langle\varphi|\psi\rangle = 0 \text{ for all } |\psi\rangle \in \mathbb{H}'\}$, i.e., $\mathbb{H} = \mathbb{H}' \oplus (\mathbb{H}')^\perp$.

The *orthogonal* projection of \mathbb{H} onto \mathbb{H}' is the map $\mathbb{H}' \oplus (\mathbb{H}')^\perp \rightarrow \mathbb{H}'$, $\vec{v} + \vec{w} \mapsto \vec{v}$.

Proposition 2.4.44: If B' is an ONB of \mathbb{H}' then the orthogonal projection of \mathbb{H} onto \mathbb{H}' is $\mathbb{H} \rightarrow \mathbb{H}' : |\varphi\rangle \mapsto \sum_{|b\rangle \in B'} |b\rangle \langle b|\varphi\rangle$.

The spectral theorem

Theorem 2.4.56: Let $O \in \mathbb{C}^{(k,k)}$ be a normal matrix. Let Λ be the set of eigenvalues of O . For $\lambda \in \Lambda$ denote by P_λ the orthogonal projection onto the eigenspace corresponding to λ . Then we have

$$O = \sum_{\lambda \in \Lambda} \lambda P_\lambda.$$

This representation of O is called its *spectral decomposition*.

1.8. Measurements

The measurement postulate

Postulate 3.3.1: A *projective measurement* is described by an *observable* O which is a Hermitian operator on the state space of the quantum system being observed. Let $O = \sum_{\lambda \in \Lambda} \lambda P_\lambda$ be the spectral decomposition of O . The possible outcomes of the measurement are the eigenvalues λ of the observable. When measuring O while the quantum system is in the state $|\varphi\rangle$, the probability of getting λ is $\Pr_{O,\varphi}(\lambda) = \|P_\lambda |\varphi\rangle\|^2$. If this outcome occurs, the state of the quantum system immediately after the measurement is $\frac{P_\lambda |\varphi\rangle}{\|P_\lambda |\varphi\rangle\|}$.

In the situation of the Measurement Postulate we say:

1. The observable O is measured *on the quantum system* in the state $|\varphi\rangle$.
2. After the measurement, the state of the quantum system *collapses onto* $\frac{P_\lambda |\varphi\rangle}{\|P_\lambda |\varphi\rangle\|}$.

Global phase factors

Definition 3.1.22: Let $|\varphi\rangle, |\psi\rangle \in \mathbb{H}$ and $\gamma \in \mathbb{R}$. If $|\psi\rangle = e^{i\gamma} |\varphi\rangle$, then we call $e^{i\gamma}$ a *global phase factor* and say: $|\varphi\rangle$ and $|\psi\rangle$ are *equal up to a global phase factor*.

Theorem 3.1.25: Two states of a quantum bit correspond to the same point on the Bloch sphere if and only if they only differ by a global phase factor.

Theorem 3.4.4: Let $|\varphi\rangle$ and $|\psi\rangle$ be states of a quantum system. Then the following statements are equivalent.

1. For all observables O of the quantum system, the two states give the same measurement statistics.
2. The two states differ only by a global phase factor.

Measurement in the computational basis

Let Q be an n -qubit register. Its state space is \mathbb{H}_n with the computational basis $(|\lambda\rangle)_{\lambda \in \mathbb{Z}_{2^n}}$.

Measurements in the computational basis use the observable

$$O = \sum_{\substack{\lambda \in \mathbb{Z}_{2^n} \\ \text{spectral decomposition}}} \lambda |\lambda\rangle \langle \lambda| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 2^n - 1 \end{pmatrix}.$$

A measurement of O on Q in the state $|\varphi\rangle = \sum_{\lambda \in \mathbb{Z}_{2^n}} \alpha_\lambda |\lambda\rangle$ yields $\lambda \in \mathbb{Z}_{2^n}$ with probability $|\alpha_\lambda|^2$.

If the outcome $\lambda \in \mathbb{Z}_{2^n}$ occurs, then the state of Q collapses onto $|\lambda\rangle$.

This can be generalized to any ONB $(|b_\lambda\rangle)_{\lambda \in \mathbb{Z}_{2^n}}$ of \mathbb{H}_n : Replace $|\lambda\rangle$ by $|b_\lambda\rangle$.

Partial measurements

Consider quantum system A, B with state spaces $\mathbb{H}_A, \mathbb{H}_B$ and an observable O_A of A .

Measuring O_A on $Q = AB$ in the state $|\varphi\rangle$ means measuring $O_A \otimes I_B$ on Q in the state $|\varphi\rangle$.

Example: Measuring the first qubit of a two-qubit register in the state $|\varphi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$.

The observable is $O = (0 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1|) \otimes I = 0 \cdot |0\rangle\langle 0| \otimes I + 1 \cdot |1\rangle\langle 1| \otimes I$.

If $\lambda \in \{0, 1\}$ then $\Pr_{O, \varphi}(\lambda) = \|P_\lambda |\varphi\rangle\|^2 = \left\| (|\lambda\rangle\langle \lambda| \otimes I) \frac{|00\rangle + |11\rangle}{\sqrt{2}} \right\|^2 = \left\| \frac{|\lambda\lambda\rangle}{\sqrt{2}} \right\|^2 = \frac{1}{2}$.

If the outcome is $\lambda \in \{0, 1\}$, then the state of $Q = AB$ collapses onto $|\lambda\lambda\rangle$.

Partial measurements of quantum registers in separable states

Consider quantum system A, B with state spaces $\mathbb{H}_A, \mathbb{H}_B$ and an observable O_A of A .

Theorem:

1. Measuring $O_A \otimes I_B$ on AB in the state $|\varphi\rangle = |\varphi_A\rangle \otimes |\varphi_B\rangle$ yields the same measurement statistics as measuring O_A on A in the state $|\varphi_A\rangle$.
2. Suppose that, after obtaining the outcome λ when measuring O_A on A the state of A collapses onto $|\psi_A\rangle$. Then after the same outcome of measuring $O_A \otimes I_B$ on AB the state of AB collapses onto $|\psi_A\rangle \otimes |\varphi_B\rangle$.

Example:

1. Measuring the first qubit of a quantum register in the state $\frac{|0\rangle + |1\rangle}{\sqrt{2}} |x_{-}\rangle$ gives $\lambda \in \{0, 1\}$ with probability $\frac{1}{2}$.
2. If the outcome $\lambda \in \{0, 1\}$ occurs, then the register is in the state $|\lambda\rangle |x_{-}\rangle$.

1.9. Time Evolution

The Evolution Postulate

Postulate 3.3.1: The evolution of a closed quantum system is described by a unitary transformation. More precisely, if $t, t' \in \mathbb{R}$, $t < t'$, then the state $|\varphi'\rangle$ of the quantum system at time t' is obtained from the state $|\varphi\rangle$ of the quantum system at time t as $|\varphi'\rangle = U|\varphi\rangle$ where U is a unitary operator on the state space of the quantum system that depends only on t and t' .

Properties of unitary operators

Proposition 2.4.18:: An operator U on \mathbb{H} is unitary if it has one of the following equivalent properties.

1. U is invertible and $U^{-1} = U^*$.
2. $\langle U|\varphi\rangle, U|\psi\rangle\rangle = \langle\varphi, \psi\rangle$ for all $|\varphi\rangle, |\psi\rangle \in \mathbb{H}$.
3. $\|U|\varphi\rangle\| = \|\varphi\|$ for all $|\varphi\rangle \in \mathbb{H}$.

Quantum gates

Quantum gates: unitary operators that are the building blocks of quantum computing.

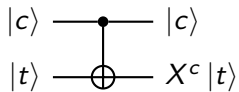
Elementary quantum gates are provided by the quantum computing platform.

The Pauli gates and the Hadamard gate

Gate	Matrix	Spectral decomposition	Image of computational basis
Pauli X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$ x_+\rangle \langle x_+ - x_-\rangle \langle x_- $	$ 0\rangle \mapsto 1\rangle, 1\rangle \mapsto 0\rangle$
Pauli Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$ y_+\rangle \langle y_+ - y_-\rangle \langle y_- $	$ 0\rangle \mapsto i 1\rangle, 1\rangle \mapsto -i 0\rangle$
Pauli Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$ z_+\rangle \langle z_+ - z_-\rangle \langle z_- $	$ 0\rangle \mapsto 0\rangle, 1\rangle \mapsto - 1\rangle$
Hadamard H	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$ h_+\rangle \langle h_+ - h_-\rangle \langle h_- $	$ 0\rangle \mapsto x_+\rangle, 1\rangle \mapsto x_-\rangle$

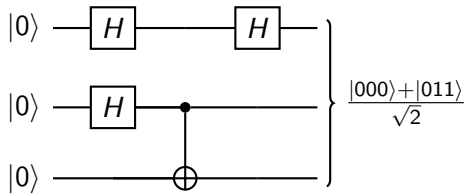
The CNOT gate

$$\text{CNOT} : \mathbb{H}_2 \rightarrow \mathbb{H}_2, \quad |c\rangle |t\rangle \mapsto |c\rangle X^c |t\rangle$$

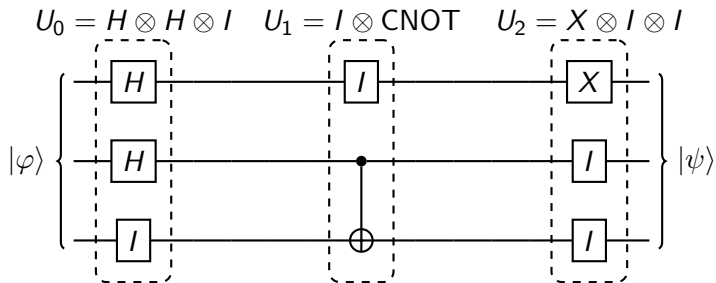


$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

A quantum circuit



The unitary operator implemented by the quantum circuit



1.10. Mixed States and Density Operators

Mixed states

Let Q be a quantum system with state space \mathbb{H} .

Definition 3.5.3:

1. A *mixed state* of Q is a sequence $((p_0, |\psi_0\rangle), \dots, (p_{l-1}, |\psi_{l-1}\rangle))$, where $l \in \mathbb{N}$, $|\psi_i\rangle$ are quantum states of Q , and $p_i \in \mathbb{R}_{\geq 0}$ for $0 \leq i < l$ such that $\sum_{i=0}^{l-1} p_i = 1$.
2. A *pure state* of Q is a quantum state in \mathbb{H} . It is identified with the mixed state $(1, |\psi\rangle)$.

Mixed states that are not pure model the situation when there is only partial knowledge about a quantum system. This should not be confused with the superposition of quantum states.

Density operators

Definition 3.5.1: A *density operator* on \mathbb{H} is a linear operator ρ on \mathbb{H} that satisfies the following conditions.

1. *Trace condition:* $\text{tr } \rho = 1$,
2. *Positivity condition:* ρ is positive semidefinite.

Proposition 3.5.4: Let $S = ((p_0, |\psi_0\rangle), \dots, (p_{l-1}, |\psi_{l-1}\rangle))$ be a mixed state of Q . Then

$$\rho_S = \sum_{i=0}^{l-1} p_i |\psi_i\rangle \langle \psi_i|$$

is a density operator on \mathbb{H} , called the *density operator of S* . Its representation matrix with respect to the computational basis of \mathbb{H} is called the *density matrix* of S .

Example: The density operator of $((\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle))$ is $\frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1|$.

Correspondence between density operators and mixed states

Proposition 3.5.8: Every density operator on \mathbb{H} is the density operator of a mixed state.

Theorem 3.5.11:

1. The density operators of two pure quantum states are equal if and only if these states are equal up to a global phase factor.
2. The density operators of two mixed states

$$((p_0, |\varphi_0\rangle), \dots, (p_{l-1}, |\varphi_{l-1}\rangle)), \quad ((q_0, |\psi_0\rangle), \dots, (q_{l-1}, |\psi_{l-1}\rangle))$$

are equal if and only if there is a unitary matrix $U \in \mathbb{C}^{(l,l)}$ with

$$(\sqrt{p_0} |\varphi_0\rangle, \dots, \sqrt{p_{l-1}} |\varphi_{l-1}\rangle) = (\sqrt{q_0} |\psi_0\rangle, \dots, \sqrt{q_{l-1}} |\psi_{l-1}\rangle)U.$$

Characterization of pure states

Theorem 3.5.15: Let ρ be a density operator on \mathbb{H} . Then the following holds.

1. ρ is a density operator of a pure state if and only if $\rho^2 = \rho$, which is true if and only if $\text{tr } \rho^2 = 1$.
2. ρ is not a density operator of a pure state if and only if $\text{tr } \rho^2 < 1$.

Example: $\rho = \frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1|$, $\rho^2 = \frac{1}{4}(|0\rangle \langle 0| + |1\rangle \langle 1|) \neq \rho$.

1.11. Quantum postulates for density operators

State Space and Composite Systems Postulates

Postulate 3.6.1: Associated with any physical system is a Hilbert space, called the state space of the system. The system is completely described by a density operator on the state space.

Postulate 3.6.2: The state space of the composition of finitely many physical systems is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 0 through $m - 1$ and if system i is in the state ρ_i where ρ_i is a density operator on the state space of the i th component system for $0 \leq i < m$, then the composite system is in the state $\rho_0 \otimes \cdots \otimes \rho_{m-1}$.

Measurement Postulate

Postulate 3.6.5: A projective measurement is described by an observable O that is a Hermitian operator on the state space of the system being observed. Let $O = \sum_{\lambda \in \Lambda} \lambda P_\lambda$ be the spectral decomposition of O . The possible outcomes of the measurement are the eigenvalues of the observable. When measuring the state ρ the probability of getting the result corresponding to λ is $\Pr_{O,\rho}(\lambda) = \text{tr}(P_\lambda \rho)$. If this outcome occurs, the state immediately after the measurement is $\frac{P_\lambda \rho P_\lambda}{\text{tr}(P_\lambda \rho)}$.

Definition 3.6.6: Let O be an observable of a quantum system with state space \mathbb{H} . Suppose that we measure this observable when the system is in a state described by the density operator ρ . Then the *expectation value of this measurement* is defined as $\text{tr}(O\rho)$.

This is the expectation value of the random variable which is the identity on Λ .

Evolution postulate

Postulate 3.6.3: The evolution of a quantum system with state space \mathbb{H} is described by a unitary transformation on \mathbb{H} . More precisely, if $t, t' \in \mathbb{R}$, $t < t'$. Assume that the state of the system at time t is described by the density operator ρ on \mathbb{H} . Then the state of the system at time t' is obtained from ρ as $\rho' = U\rho U^*$ where U is a unitary operator on \mathbb{H} that only depends on t and t' .

1.12. Tracing Out Subsystems

Partial trace

Theorem B.9.21:

Let $n_j \in \mathbb{N}$ for $0 \leq j < m$ and $J \subset \mathbb{Z}_m$. Then there is a uniquely determined linear map

$$\mathrm{tr}_J : \mathrm{End} \left(\bigotimes_{j \in \mathbb{Z}_m} \mathbb{H}_{n_j} \right) \rightarrow \mathrm{End} \left(\bigotimes_{j \in \mathbb{Z}_m \setminus J} \mathbb{H}_{n_j} \right) \quad (1.12.1)$$

with

$$\mathrm{tr}_J \left(\bigotimes_{j \in \mathbb{Z}_m} f_j \right) = \prod_{j \in J} \mathrm{tr} f_j \bigotimes_{j \in \mathbb{Z}_m \setminus J} f_j. \quad (1.12.2)$$

for all $(f_0, \dots, f_{m-1}) \in \prod_{j=0}^{m-1} \mathrm{End}(\mathbb{H}_{n_j})$.

It is called the *partial trace* over the qubits Q_j , $j \in J$.

Tracing out subsystems

A , B quantum systems with state spaces \mathbb{H}_A and \mathbb{H}_B . $\mathbb{H} = \mathbb{H}_A \otimes \mathbb{H}_B$. Assume that AB is in a mixed state with density operator ρ .

Tracing out B : B is ignored; A is in the mixed state with density operator $\rho^A = \text{tr}_B \rho$.

Example: Tracing out the second qubit of $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Density operator: $\rho = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$.

$\text{tr}_B(|pr\rangle\langle qs|) = |p\rangle\langle q| \delta_{rs}$, $p, q, r, s \in \{0, 1\}$.

$\Rightarrow \text{tr}_B(\rho) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$: the density operator of $((\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle))$.

Generalization of the example

Proposition: If AB is in state

$$|\xi\rangle = \frac{1}{\sqrt{I}} \sum_{i=0}^{I-1} |\varphi_i\rangle |\psi_i\rangle.$$

and B is traced out, where the $|\psi_i\rangle$ are orthogonal to each other, then A is in the mixed state

$$\left(\left(\frac{1}{I}, |\varphi_0\rangle \right), \dots, \left(\frac{1}{I}, |\varphi_{I-1}\rangle \right) \right).$$

2. The Algorithms of Deutsch and Simon

2.1. The Deutsch Algorithm

The classical Deutsch problem

$f : \{0, 1\} \rightarrow \{0, 1\}$.

► f *constant*, if $f(0) = f(1)$, i.e., $f(0) \oplus f(1) = 0$.

► f *balanced*, if $f(0) \neq f(1)$, i.e., $f(0) \oplus f(1) = 1$.

Input: A *black box* for f , i.e., a component with unknown and inaccessible internal workings, observable only through its input-output behavior: given $b \in \{0, 1\}$, it returns $f(b)$.

Output: $f(0) \oplus f(1)$.

Theorem: Any deterministic algorithm requires the computation of $f(0)$ and $f(1)$.

The quantum Deutsch problem

$$f : \{0, 1\} \rightarrow \{0, 1\}.$$

$$U_f : \mathbb{H}_2 \rightarrow \mathbb{H}_2, \quad |x\rangle |y\rangle \mapsto |x\rangle |f(x) \oplus y\rangle = |x\rangle X^{f(x)} |y\rangle.$$

The first qubit (*control qubit*) controls the modification of the second (*target qubit*).

Input: A black box for U_f .

Output: $f(0) \oplus f(1)$.

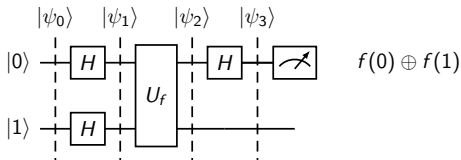
The quantum Deutsch algorithm

$$(*) \quad U_f |x\rangle |x_{-}\rangle = \frac{|x\rangle X^{f(x)} |0\rangle - |x\rangle X^{f(x)} |1\rangle}{\sqrt{2}} |x_{-}\rangle = |x\rangle (-1)^{f(x)} |x_{-}\rangle = \underbrace{(-1)^{f(x)}}_{\text{phase kickback}} |x\rangle |x_{-}\rangle.$$

superposition
+ interference:

$$U_f |x_{+}\rangle |x_{-}\rangle = \frac{U_f |0\rangle |x_{-}\rangle + U_f |1\rangle |x_{-}\rangle}{\sqrt{2}} \stackrel{(*)}{=} \frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}} |x_{-}\rangle$$

$$= (-1)^{f(0)} \frac{|0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle}{\sqrt{2}} |x_{-}\rangle = (-1)^{f(0)} H |f(0) \oplus f(1)\rangle |x_{-}\rangle$$



$$\begin{aligned} |\psi_0\rangle &= |0\rangle |1\rangle \\ |\psi_1\rangle &= |x_{+}\rangle |x_{-}\rangle \\ |\psi_2\rangle &= (-1)^{f(0)} H |f(0) \oplus f(1)\rangle |x_{-}\rangle \\ |\psi_3\rangle &= (-1)^{f(0)} |f(0) \oplus f(1)\rangle |x_{-}\rangle \end{aligned}$$

2.2. The Deutsch-Jozsa Algorithm

The classical Deutsch-Jozsa problem

$f : \{0, 1\}^n \rightarrow \{0, 1\}$ constant or balanced.

- ▶ f *constant*: $f(\vec{x})$ is the same for all $\vec{x} \in \{0, 1\}^n$,
- ▶ f *balanced*: $f(\vec{x}) = 0$ for half of the $\vec{x} \in \{0, 1\}^n$ and $f(\vec{x}) = 1$ for the other half.

Input: $n \in \mathbb{N}$ and a black box for f .

Output: "constant" or "balanced".

Theorem: Any deterministic algorithm requires – in the worst case – $2^{n-1} + 1$ evaluations of f .

The quantum Deutsch-Jozsa problem

$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ constant or balanced.

$$U_f : |\vec{x}\rangle |y\rangle \mapsto |\vec{x}\rangle X^{f(\vec{x})} |y\rangle.$$

Input: $n \in \mathbb{N}$ and a black box for U_f .

Output: "constant" or "balanced".

Auxiliary results

Lemma 1:

1. We have $H^{\otimes n} |\vec{0}\rangle^{\otimes n} = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle$.
2. For any $\vec{y} \in \{0,1\}^n$ we have $H^{\otimes n} |\vec{y}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{\vec{x} \cdot \vec{y}} |\vec{x}\rangle$.

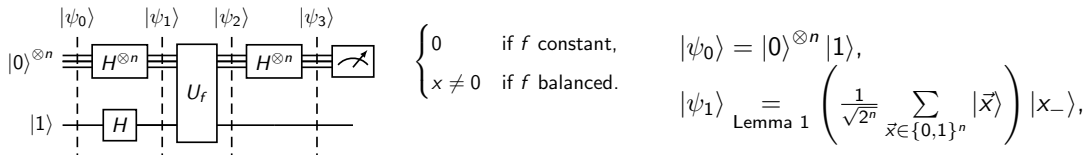
Lemma 2:

1. If f is constant, then $H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x}) \oplus f(\vec{0})} |\vec{x}\rangle \right) = |\vec{0}\rangle$
2. If f is balanced, then the coefficient of $|\vec{0}\rangle$ in the computational basis representation of $H^{\otimes n} \left(\frac{(-1)^{f(\vec{0})}}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x}) \oplus f(\vec{0})} |\vec{x}\rangle \right)$ is 0.

The quantum algorithm

$$(*) \quad U_f |\vec{x}\rangle |x_{-}\rangle = \frac{|\vec{x}\rangle X^{f(\vec{x})} |0\rangle - |\vec{x}\rangle X^{f(\vec{x})} |1\rangle}{\sqrt{2}} = |\vec{x}\rangle (-1)^{f(\vec{x})} |x_{-}\rangle = \underbrace{(-1)^{f(\vec{x})}}_{\text{phase kickback}} |\vec{x}\rangle |x_{-}\rangle.$$

Superposition + interference:



$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} U_f |\vec{x}\rangle |x_{-}\rangle \stackrel{(*)}{=} \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x})} |\vec{x}\rangle |x_{-}\rangle = \frac{(-1)^{f(\vec{0})}}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x}) \oplus f(\vec{0})} |\vec{x}\rangle |x_{-}\rangle$$

$$|\psi_3\rangle = H^{\otimes n} \left(\frac{(-1)^{f(\vec{0})}}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x}) \oplus f(\vec{0})} |\vec{x}\rangle \right) \stackrel{\text{Lemma 2}}{=} \frac{(-1)^{f(\vec{0})}}{\sqrt{2^n}} \begin{cases} |\vec{0}\rangle |x_{-}\rangle & \text{if } f \text{ is constant,} \\ \left(\sum_{\vec{x} \neq \vec{0}} \alpha_{\vec{x}} |\vec{x}\rangle \right) |x_{-}\rangle & \text{if } f \text{ is balanced.} \end{cases}$$

2.3. Simon's Algorithm

The classical version of Simon's problem

$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$: there is a *hidden string* $\vec{s} \in \{0, 1\}^n$, $\vec{s} \neq \vec{0}$, such that for all $\vec{x}, \vec{y} \in \{0, 1\}^n$ we have $f(\vec{x}) = f(\vec{y})$ if and only if $\vec{x} = \vec{y}$ or $\vec{x} = \vec{y} \oplus \vec{s}$.

Input: A black box for f .

Output: The hidden string \vec{s} .

Theorem 5.4.3: [Cle11]: Any classical probabilistic algorithm that solves Simon's problem with probability at least $3/4$ must make $\Omega(2^{n/2})$ queries to the black box for f .

The quantum version of Simon's problem

$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$: $\vec{s} \in \{0, 1\}^n$, $\vec{s} \neq \vec{0}$: $f(\vec{x}) = f(\vec{y})$ if and only if $\vec{x} \in \{\vec{y}, \vec{y} \oplus \vec{s}\}$.

$U_f : |\vec{x}\rangle |\vec{y}\rangle \mapsto |\vec{x}\rangle |f(\vec{x}) \oplus \vec{y}\rangle$.

Input: A black box for U_f ; **Output:** The hidden string \vec{s} .

Idea of the algorithm:

- ▶ Construct a quantum circuit Q_f that computes random elements of \vec{s}^\perp with the uniform distribution and uses U_f once.
- ▶ Invoking Q_f $n - 1$ times gives a sequence W in \vec{s}^\perp of length $n - 1$.
- ▶ With probability $\prod_{k=1}^{n-1} \left(1 - \frac{1}{2^k}\right) \geq 1/4$, W is a basis of \vec{s}^\perp . In this case, \vec{s} is the uniquely determined solution of the $W^T \vec{s} = \vec{0}$.

The quantum circuit $Q(U_f)$

$$(*1) \quad H^{\otimes n} |\vec{z}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{w} \in \{0,1\}^n} (-1)^{\vec{z} \cdot \vec{w}} |\vec{w}\rangle \Rightarrow |\vec{z}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{w} \in \{0,1\}^n} (-1)^{\vec{z} \cdot \vec{w}} H^{\otimes n} |\vec{w}\rangle.$$

$$(*2) \quad U_f |\vec{z}\rangle |\vec{0}\rangle = |\vec{z}\rangle |f(\vec{z}) \oplus \vec{0}\rangle = |\vec{z}\rangle |f(\vec{z})\rangle; \quad U_f |\vec{z} \oplus \vec{s}\rangle |\vec{0}\rangle = |\vec{z} \oplus \vec{s}\rangle |f(\vec{z})\rangle$$

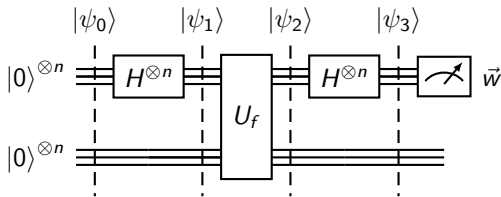
$$(*3) \quad U_f \frac{|\vec{z}\rangle + |\vec{z} \oplus \vec{s}\rangle}{\sqrt{2}} |0\rangle^{\otimes n} \underset{(*2)}{=} \frac{|\vec{z}\rangle + |\vec{z} \oplus \vec{s}\rangle}{\sqrt{2}} |f(\vec{z})\rangle \underset{(*1)}{=} \frac{1}{\sqrt{2^{n-1}}} \sum_{\vec{w} \in \vec{s}^\perp} (-1)^{\vec{z} \cdot \vec{w}} H^{\otimes n} |\vec{w}\rangle |f(\vec{z})\rangle$$

Choose I such that $\{0,1\}^n = \bigcup_{\vec{z} \in I} \{\vec{z}, \vec{s} \oplus \vec{z}\}$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{\vec{z} \in I} \frac{|\vec{z}\rangle + |\vec{z} \oplus \vec{s}\rangle}{\sqrt{2}} |0\rangle^{\otimes n},$$

$$|\psi_2\rangle \underset{(*3)}{=} \sum_{\vec{z} \in I} \sum_{\vec{w} \in \vec{s}^\perp} \frac{(-1)^{\vec{z} \cdot \vec{w}}}{2^{n-1}} H^{\otimes n} |\vec{w}\rangle |f(\vec{z})\rangle,$$

$$|\psi_3\rangle = \sum_{\vec{z} \in I} \sum_{\vec{w} \in \vec{s}^\perp} \frac{(-1)^{\vec{z} \cdot \vec{w}}}{2^n} |\vec{w}\rangle |f(\vec{z})\rangle.$$



Measuring the first register of $|\psi_3\rangle$ gives each $\vec{w} \in \vec{s}^\perp$ with probability $1/2^{n-1}$.

Success probability and complexity of Simon's algorithm

Theorem: The success probability of Simon's algorithm is at least $1/4$. It requires $n - 1$ applications of U_f and $O(n^3)$ other operations.

2.4. A Generalization of Simon's algorithm

Generalization of Simon's problem

$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$: There is a *hidden subspace* S of $\{0, 1\}^n$ such that $f(\vec{x}) = f(\vec{y})$ if and only if $\vec{x} = \vec{y} \oplus \vec{s}$ for some $\vec{s} \in S$.

Input: A black box implementing U_f and the dimension m of S .

Output: A basis of the hidden subspace S .

Generalized Simon's algorithm

```
1:  $W \leftarrow ()$ 
2: for  $j = 1$  to  $n - m$  do
3:    $\vec{w}_j \leftarrow Q(U_f)$ 
4:    $W \leftarrow W \parallel (\vec{w}_j)$ 
5: end for
6:  $r \leftarrow \text{rank } W$ 
7: if  $r = n - m$  then
8:   Find a basis  $B$  of the kernel of  $W$ 
9:   return  $B$ 
10: else
11:   return "Failure"
12: end if
```

Complexity of the Generalized Simon's Algorithm

The generalized Simon's algorithm returns a basis of the hidden subgroup S with probability at least $1/4$. It uses m applications of U_f and $O(n^3)$ other operations.

3. Quantum Computability and Complexity

3.1. Single-qubit gates

The unitary and the special unitary group

The *unitary group of rank 2* is $U(2) = \{\text{unitary operators on } \mathbb{H}_1\}$.

The *special unitary group of rank 2* is $SU(2) = \{U \in U(2) : \det U = 1\}$.

Example: The operators

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

are in $U(2)$ but not in $SU(2)$.

But iH , iX , iY , and iZ are in $SU(2)$.

Rotation operators

Set $\sigma = (X, Y, Z)$ and for $\vec{p} = (p_x, p_y, p_z) \in \mathbb{R}^3$ set $\vec{p} \cdot \sigma = p_x X + p_y Y + p_z Z$.

Proposition 4.3.3: For all unit vectors $\hat{w} \in \mathbb{R}^3$ and $\gamma \in \mathbb{R}$

$$R_{\hat{w}}(\gamma) = e^{-i\gamma \hat{w} \cdot \sigma / 2} = \cos \frac{\gamma}{2} I - i \sin \frac{\gamma}{2} \hat{w} \cdot \sigma$$

is a unitary operator on \mathbb{H}_1 with determinant 1, called a *rotation operator*.

Theorem 4.3.15: The set of rotation operators is $SU(2)$.

3.2. Rotation operators and rotations on the Bloch sphere

The orthogonal and special orthogonal group

$O \in \mathbb{R}^{(3,3)}$ is called *orthogonal* if O is invertible and $O^{-1} = O^T$.

The *orthogonal group of order 3* is $O(3) = \{\text{orthogonal matrices in } \mathbb{R}^3\}$.

The *special orthogonal group of order 3* is $SO(3) = \{O \in O(3) : \det O = 1\}$.

General spherical coordinates

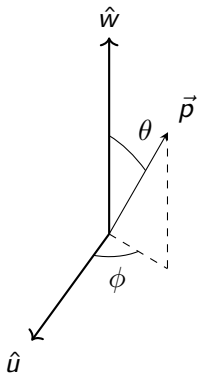
Let \hat{u}, \hat{w} be orthogonal unit vectors and let $\vec{p} \in \mathbb{R}^3$.

Theorem 4.2.8: There is a uniquely determined unit vector \hat{v} such that $B = (\hat{u}, \hat{v}, \hat{w})$ is in $SO(3)$.

Definition 4.2.10: *The spherical coordinate representation of \vec{p} w.r.t. (\hat{u}, \hat{w})* is the standard spherical coordinate representation (r, θ, ϕ) of $B^{-1}\vec{p}$. It satisfies

- ▶ $r = \|\vec{p}\|$: *radial distance*.
- ▶ $\theta \in [0, \pi]$; if $\vec{p} = \vec{0}$ then $\theta = 0$: *polar angle*.
- ▶ $\phi \in [0, 2\pi[$; if $\theta \in \{0, \pi\}$ then $\phi = 0$: *azimuthal angle*.
- ▶ $B^{-1}\vec{p} = r(\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta)$.

\hat{w} is called the *zenith* and \hat{u} the *azimuth reference*.



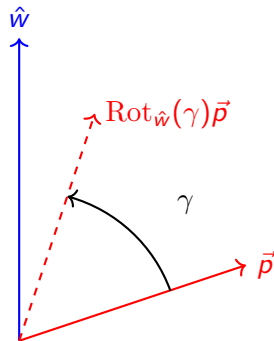
Rotations in \mathbb{R}^3

Theorem 4.2.21: Let $\hat{u}, \hat{w} \in \mathbb{R}^3$ be orthogonal unit vectors and let $\gamma \in \mathbb{R}$. The map $\text{Rot}_{\hat{w}}(\gamma) : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ that sends $\vec{p} \in \mathbb{R}^3$ with spherical coordinates (r, θ, ϕ) w.r.t. (\hat{u}, \hat{w}) to the vector in \mathbb{R}^3 with the following spherical coordinates w.r.t. (\hat{u}, \hat{w})

$$\begin{cases} (r, \theta, \phi) & \text{if } \theta \in \{0, \pi\}, \\ (r, \theta, (\phi + \gamma) \bmod 2\pi) & \text{otherwise.} \end{cases}$$

depends only on \hat{w} and γ and is independent of \hat{u} . It is called the *rotation about the axis \hat{w} through the angle γ* .

Theorem 4.2.22: The set of rotations in \mathbb{R}^3 is $\text{SO}(3)$.



Correspondence between rotation operators and rotations

Theorem 4.3.20: For $U \in \text{SU}(2)$, $U = R_{\hat{w}}(\gamma)$ with a unit vector $\hat{w} \in \mathbb{R}^3$ and $\gamma \in \mathbb{R}$ set $\text{Rot}(U) = \text{Rot}_{\hat{w}}(\gamma)$. Then the following holds

1. $\text{Rot} : \text{SU}(2) \rightarrow \text{SO}(3)$, $U \mapsto \text{Rot}(U)$ is a well-defined, surjective group homomorphism with kernel $\pm I$.
2. For all $U \in \text{SU}(2)$ and all quantum states $|\psi\rangle$ in \mathbb{H}_1 , the point on the Bloch sphere corresponding to $U|\psi\rangle$ is $\vec{p}(U|\psi\rangle) = \text{Rot}(U)\vec{p}(\psi)$.

Example: $\text{Rot}(iX) = \text{Rot}_{\hat{x}}(\pi)$, $\text{Rot}(iY) = \text{Rot}_{\hat{y}}(\pi)$, $\text{Rot}(iZ) = \text{Rot}_{\hat{z}}(\pi)$.

3.3. Elementary single-qubit gates

$R_{\hat{x}}$, $R_{\hat{y}}$, and $R_{\hat{z}}$

Proposition 4.3.8:

1. If $\gamma \in \mathbb{R}$, then

$$R_{\hat{x}}(\gamma) = \begin{pmatrix} \cos \frac{\gamma}{2} & -i \sin \frac{\gamma}{2} \\ -i \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{pmatrix}, R_{\hat{y}}(\gamma) = \begin{pmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{pmatrix}, R_{\hat{z}}(\gamma) = \begin{pmatrix} e^{-i\frac{\gamma}{2}} & 0 \\ 0 & e^{i\frac{\gamma}{2}} \end{pmatrix}.$$

2. $R_{\hat{x}}(\pi) = -iX$, $R_{\hat{y}}(\pi) = iY$, $R_{\hat{z}}(\pi) = -iZ$ and $H = XR_{\hat{y}}\left(\frac{\pi}{2}\right)$.

Implementation of $R_{\hat{x}}$, $R_{\hat{y}}$, and $R_{\hat{z}}$

The rotation operators $R_{\hat{x}}$, $R_{\hat{y}}$, and $R_{\hat{z}}$ can be implemented in hardware, e.g., by the methods below.

- ▶ Superconducting qubits (e.g., transmon qubits used by IBM, Google, Rigetti) implement single-qubit rotations using microwave pulses.
- ▶ Trapped-ion quantum computers (e.g., IonQ, Honeywell, Alpine Quantum Technologies) use laser pulses to manipulate qubit states.
- ▶ Neutral atom quantum computers (e.g., QuEra, ColdQuanta) use laser beams to trap and manipulate neutral atoms.
- ▶ Quantum dots (e.g., Intel, Silicon Quantum Computing) implement rotation gates using electric and magnetic fields.
- ▶ In Nuclear Magnetic Resonance (NMR) quantum computing, radiofrequency pulses induce spin rotations.

Decomposition of rotations and rotation operators

Theorem 4.2.30, 4.3.31:

1. For any $O \in \text{SO}(3)$ there are $\alpha, \beta, \gamma \in \mathbb{R}$ with $O = \text{Rot}_{\hat{z}}(\alpha) \text{Rot}_{\hat{y}}(\beta) \text{Rot}_{\hat{z}}(\gamma)$.
The real numbers α, β, γ are called *Euler angels* of O .
2. For any $U \in \text{U}(2)$ there are $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ with $U = e^{i\delta} R_{\hat{z}}(\alpha) R_{\hat{y}}(\beta) R_{\hat{z}}(\gamma)$. If $U \in \text{SU}(2)$, then such a representation exists with $\delta = 0$.

Phase shift gates

Phase shift gate: $P(\gamma) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\gamma} \end{pmatrix} = e^{i\frac{\gamma}{2}} R_{\hat{z}}(\gamma), \gamma \in \mathbb{R}.$

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix} = e^{\frac{2\pi i}{2^{k+1}}} R_{\hat{z}}\left(\frac{2\pi}{2^k}\right).$$

$\pi/8$ gate: $T = R_3 = P\left(\frac{\pi}{4}\right) = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = e^{\frac{\pi i}{8}} \begin{pmatrix} e^{-\frac{\pi i}{8}} & 0 \\ 0 & e^{\frac{\pi i}{8}} \end{pmatrix}.$

Phase gate $S = R_2 = P\left(\frac{\pi}{2}\right) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = T^2.$

Elementary single-qubit gates

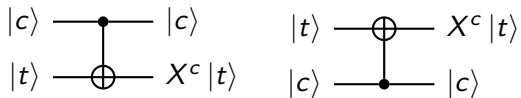
The operators $R_{\hat{y}}(\gamma)$ and $R_{\hat{z}}(\gamma)$, $\gamma \in \mathbb{C}$, are sufficient to construct all single-qubit gates.

But to simplify the description of quantum algorithms we assume that the following single-qubit operators are *elementary*, i.e., provided by the quantum computing platform. Each of them can be implemented using $O(1)$ of the above rotation operators.

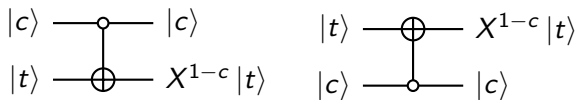
- ▶ The operators $e^{i\phi}R_{\hat{w}}(\gamma)$ with known rotation axis $\hat{w} \in \mathbb{R}^3$, rotation angle $\gamma \in [0, 2\pi[$, and phase $\phi \in [0, 2\pi[$.
- ▶ This includes the Pauli gates, the Hadamard gate, the phase shift gates, the gates R_k for $k \in \mathbb{N}$, the phase gate, and the $\pi/8$ gate.

3.4. Controlled gates

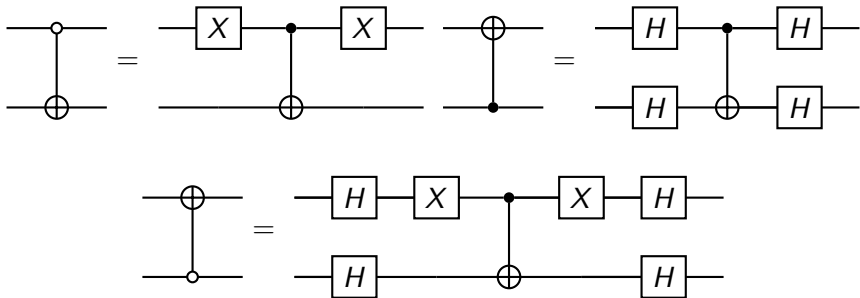
CNOT gates



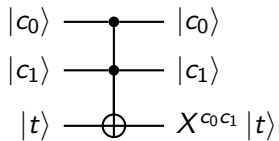
Standard CNOT



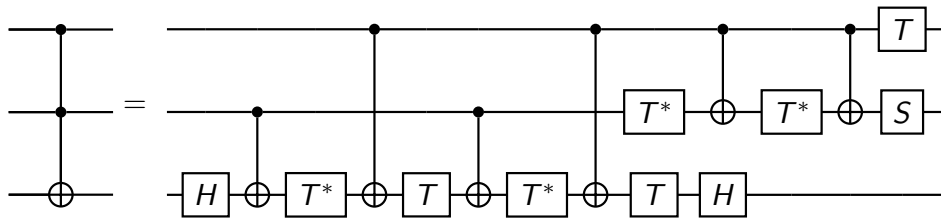
Implementation of the non-standard CNOT gates



The quantum Toffoli or CCNOT gate CCNOT



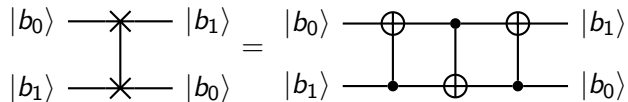
Implementation of the CCNOT gate



CCNOT gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix} = e^{\frac{\pi i}{8}} R_{\hat{z}}\left(\frac{\pi}{4}\right), \quad S = T^2 = e^{\frac{\pi i}{4}} R_{\hat{z}}\left(\frac{\pi}{2}\right), \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = X R_{\hat{y}}\left(\frac{\pi}{2}\right).$$

The quantum swap gate

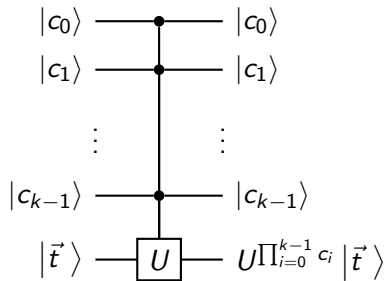


Proposition: The implementation of the SWAP gate requires three CNOT gates.

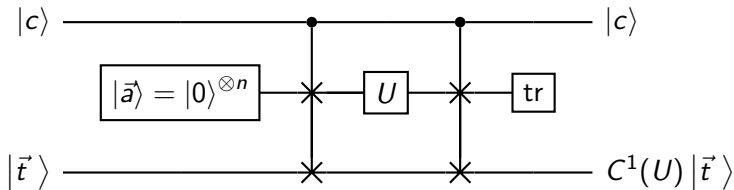
Proposition 4.5.2: For $\pi \in S_n$, the *permutation operator*

$U_\pi |b_0 \cdots b_{n-1}\rangle = |b_{\pi(0)} \cdots b_{\pi(n-1)}\rangle$ can be implemented using $O(n)$ CNOT gates.

$$C^k(U)$$



Implementation of $C^1(U)$

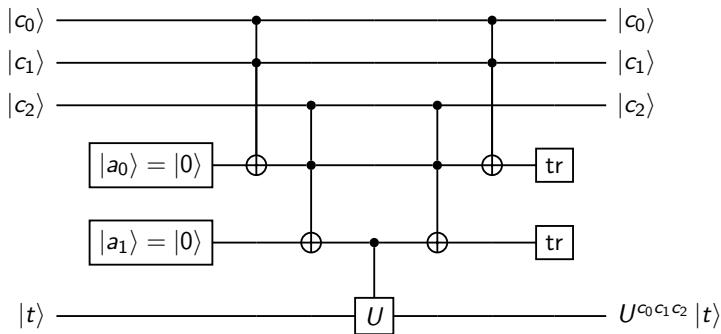


Proposition: The implementation of $C^1(U)$ requires $6n$ CCNOT gates, n ancilla and erasure gates, and one U gate.

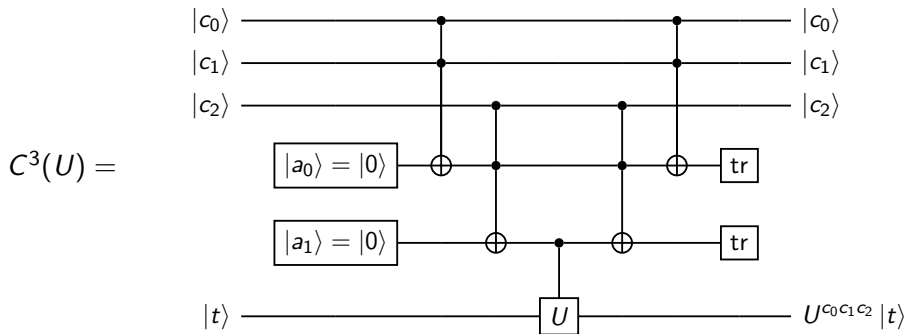
Ancilla and erasure gates

$$U \in \text{End}(\mathbb{H}_1), C^3(U) : \mathbb{H}_4 \rightarrow \mathbb{H}_4, |c_0 c_1 c_2 t\rangle \mapsto |c_0 c_1 c_2\rangle X^{c_0 c_1 c_2} |t\rangle.$$

The following circuit implements $C^3(U)$. It uses *ancilla and erasure gates*.



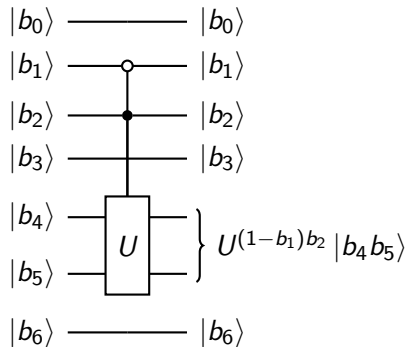
Implementation of $C^k(U)$, $k \geq 2$



Proposition 4.9.10: The implementation of $C^k(U)$ requires $k - 1$ ancilla and erasure gates, $2(k - 1)$ CNOT gates, and one $C^1(U)$ gate.

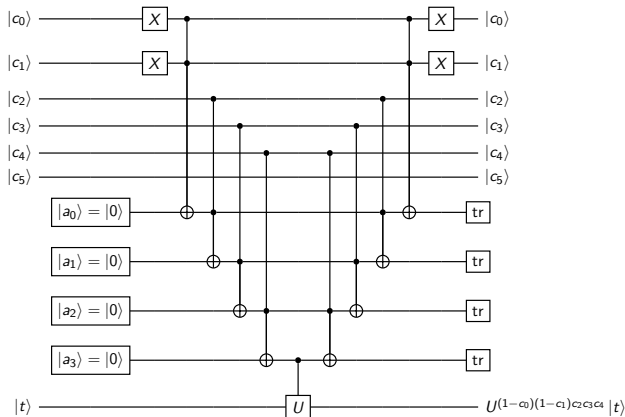
General controlled operators

Example:



Implementation of general controlled operators

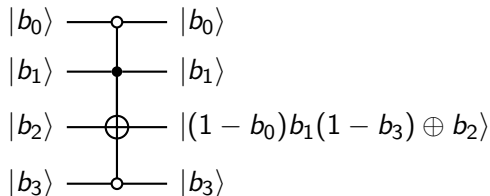
$$C^{\{0,1\},\{2,3,4\},6} =$$



Theorem 4.9.13: The implementation of $C^{C_0, C_1, T}$ requires $O(|C_0| + |C_1| + |T|)$ Pauli X , CCNOT, ancillary and erasure gates as well as one $C^1(U)$ gate.

Quantum transposition operators

The operator $\text{TRANS}^{(01*0)}$, which exchanges $|0100\rangle$ and $|0110\rangle$:



Theorem 4.9.15: Any transposition operator on \mathbb{H}_n can be implemented using $O(|C_0| + |C_1| + |T|)$ Pauli X , CCNOT, ancillary and erasure gates as well as one $C^1(U)$ gate.

3.5. Universal and perfectly universal sets of quantum gates

Perfectly universal sets of quantum gates

Definition 4.8.5: A set S of quantum gates is called *perfectly universal* if for all $n \in \mathbb{N}$, any unitary operator on \mathbb{H}_n can, up to a global factor, be implemented by a quantum circuit that uses only gates from S , ancillary gates, and erasure gates.

Definition 4.10.1: A *two-level operator* on \mathbb{H}_n is a unitary operator that maps at least $n - 2$ elements of the computational basis of \mathbb{H}_n to themselves.

Theorem 4.10.4: The set of all two-level operators is perfectly universal.

Theorem 4.10.12: Any two-level operator can be implemented by a quantum circuit that uses $O(n^2)$ unitary single-qubit, standard CNOT, ancilla, and erasure gates.

Theorem 4.10.6: $U(2) \cup \{\text{CNOT}\}$ is perfectly universal for quantum computing.

Universal sets of quantum gates

Definition 4.8.2: Let U and V be unitary operators on \mathbb{H}_n . The *error, when V is implemented instead of U* is $E(U, V) = \sup\{\|(U - V)|\varphi\rangle\| : |\varphi\rangle \in \mathbb{H}_n, \langle\varphi|\varphi\rangle = 1\}$.

Definition 4.8.2: Let S be a set of unitary quantum gates.

1. We say that S is *universal* for a set T of unitary quantum operators, if for all $\epsilon \in \mathbb{R}_{>0}$ and all $U \in T$ there is a unitary operator V that can be implemented up to a global phase factor by a quantum circuit that uses only gates from S and satisfies $E(U, V) < \epsilon$.
2. We say that S is *universal for quantum computation*, if S is universal for the set of all unitary quantum operators.

A universal set of quantum operators

Theorem 4.11.2: The set that contains the Hadamard and the $\pi/8$ gate is universal for the set of all unitary single-qubit operators.

Theorem 4.11.12: (Solovay-Kitaev Theorem [DN06]) Let G be a finite set of rotation gates containing its own inverses which is universal for the set of all rotation operators. Then for all $\epsilon \in \mathbb{R}_{>0}$ and all rotation operators U there is $l \in \mathbb{N}$ and a sequence V_0, \dots, V_{l-1} such that $l = O(\log^c 1/\epsilon)$ such $E\left(U, \prod_{i=0}^{l-1} V_i\right) < \epsilon$.

Theorem 4.11.1: The set that contains the Hadamard, $\pi/8$, and the standard CNOT gate is universal for quantum computation.

3.6. Quantum complexity

Elementary quantum gates and the complexity of quantum circuits

The *set of elementary quantum gates* contains all elementary single-qubit gates, the CNOT and the CCNOT gates, as well as the ancilla and erasure gate.

The *gate complexity of a quantum circuit* is the number of elementary quantum gates required to implement it.

Quantum algorithms and their complexity

Definition 4.12.4: A quantum algorithm is a probabilistic algorithm that may use quantum circuits with classical output as subroutines.

Definition 4.12.11: The complexity of a quantum algorithm is the number of bit operations used by the classical part plus the number of elementary quantum gates used by quantum circuits that are invoked by the quantum algorithm.

4. Shor's Algorithms

4.1. Integer Factorization

The integer factorization problem

Input: An odd composite integer N .

Output: A proper divisor of N .

Example: $N = F_7 = 2^{128} + 1$; the smallest proper divisor is 59649589127497217.

The idea of Shor's algorithm

- ▶ Choose $a \in \mathbb{Z}_N$ randomly with the uniform distribution.
- ▶ If $\gcd(a, N) > 1$, then $\gcd(a, N)$ is a proper divisor of N .
- ▶ Else, if $r = \text{order}_N a$ is even and $a^{r/2} \not\equiv -1 \pmod N$, then N divides $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$ but neither of the factors $(a^{r/2} - 1)$ and $(a^{r/2} + 1)$. Therefore, $\gcd(a^{r/2} - 1, N)$ is a proper divisor of N .

Example: $N = 15$, $a = 2$, $r = 4$, $a^{r/2} = 4 \not\equiv -1 \pmod{15}$, $\gcd(a^{r/2} - 1, N) = \gcd(3, 15) = 3$.

We will show the following:

- ▶ $\gcd(a, N) = 1 \Rightarrow r = \text{order}_N a$ can be computed in quantum polynomial time.
- ▶ The probability of r having one of the above properties is sufficiently high.

How to find the order r of a modulo N ?

- ▶ $n \leftarrow \lceil 2 \log_2 N \rceil + 1$
- ▶ Unitary operator $U_a : \mathbb{H}_n \rightarrow \mathbb{H}_n$, $|x\rangle_n \mapsto \begin{cases} |ax \bmod N\rangle_n & \text{if } 0 \leq x < N, \\ |x\rangle_n & \text{if } N \leq x < 2^n. \end{cases}$
- ▶ For $0 \leq k < r$, $|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r}s} |a^s \bmod N\rangle_n$ is an eigenstate of U_a with eigenvalue $e^{2\pi i \frac{k}{r}}$. The *phase* of this eigenvalue is $2\pi \frac{k}{r}$.
- ▶ Quantum phase estimation gives $x_1, x_2 \in \mathbb{Z}_{2^n}$ with $\frac{x_1}{2^n} \approx \frac{k_1}{r}$ and $\frac{x_2}{2^n} \approx \frac{k_2}{r}$.
- ▶ The *continued fraction expansion* of $\frac{x_j}{2^n}$ gives the reduced representation $\frac{m_j}{r_j}$ of $\frac{k_j}{r}$ for $j = 1, 2$ and with high probability, we have $r = \text{lcm}(r_1, r_2)$.

4.2. Phase Estimation Using the Discrete Fourier Transform

The phase estimation problem

Input: $L \in \mathbb{N}$, a black-box for $f(y) = e^{2\pi i \omega y}$, $\omega \in \mathbb{R}$.

Output: $x \in \mathbb{Z}_L$ such that $\frac{x}{L} \approx \omega \bmod 1$.

The discrete Fourier transform (DFT)

Definition: The *discrete Fourier transform (DFT)* of order N is $\text{DFT}_N = (e^{-2\pi i \frac{xy}{N}})_{0 \leq x, y < N}$.

Proposition: $\frac{1}{\sqrt{N}} \text{DFT}_N$ is unitary with inverse $\frac{1}{\sqrt{N}} \text{DFT}_N^* = \frac{1}{\sqrt{N}} (e^{2\pi i \frac{xy}{N}})_{0 \leq x, y < N}$.

Example: $\text{DFT}_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$,

Definition: The *discrete Fourier transform (DFT)* of $\vec{a} = (a_0, \dots, a_{N-1}) \in \mathbb{C}^N$ is the sequence $(A_0, \dots, A_{N-1}) = \text{DFT}_N \vec{a}$. Its entries are called the *Fourier coefficients* of \vec{a} .

Example: The DFT of $(1, -1, 1, -1)$ is $(0, 0, 4, 0)$.

Solving the phase estimation problem using the DFT

- ▶ Compute $\vec{a} = (a_0, \dots, a_N)$, where $a_y = e^{2\pi i \omega y}$ for $0 \leq y < N$.
- ▶ Compute $(A_0, \dots, A_N) = \text{DFT}_N \vec{a}$.

Lemma: If $\omega = \frac{k}{N}$, then $A_x = \begin{cases} N & \text{for } x \equiv k \pmod{N}, \\ 0 & \text{otherwise.} \end{cases}$.

- ▶ If $\omega = \frac{k}{N}$, find the index k of the nonzero Fourier coefficient. Then $\omega \equiv \frac{k}{N} \pmod{1}$.

Example: $N = 4$, $\omega = \frac{1}{2}$, $\vec{a} = (1, -1, 1, -1)$, $\vec{A} = (0, 0, 4, 0)$, $k = 2$, $\frac{k}{N} = \omega$.

- ▶ If $N\omega \notin \mathbb{Z}$, then $\omega \pmod{1} \approx \frac{k}{N}$ where k is the index of the largest $|A_x|$.

Example with $N\omega \notin \mathbb{Z}$

$$\omega = 0.3, N = 16, \vec{a} = (e^{2\pi i \omega y})_{0 \leq y < 16}, \vec{A} = \text{DFT}_{16} \vec{a}.$$

k	0	1	2	3	4	5	6	7
$ A_k $	0.7	0.9	1.1	1.7	3.8	15.0	2.5	1.4
k	8	9	10	11	12	13	14	15
$ A_k $	1.0	0.8	0.7	0.6	0.6	0.6	0.6	0.6

The index of the largest $|A_k|$ is $k = 5$ and $\frac{k}{N} = 0.31 \approx 0.3 = \omega$.

This requires the computation of all elements of \vec{A} .

4.3. Phase Estimation Using the Quantum Fourier Transform

The quantum phase estimation problem

Input: $m, n \in \mathbb{N}$, black-box for a unitary operator U on \mathbb{H}_m , and an eigenstate $|\psi\rangle$ of U with eigenvalue $e^{2\pi i\omega}$, $\omega \in \mathbb{R}$.

Output: $x \in \mathbb{Z}_{2^n}$ such that $\frac{x}{2^n} \approx \omega \bmod 1$.

In the sequel: $m, n \in \mathbb{N}$, $\omega \in \mathbb{R}$.

Outline of the quantum algorithm

Recall the [classical exponential algorithm](#):

1. Compute $\vec{a} = (a_y) = (e^{2\pi i \omega y})_{0 \leq y < 2^n}$ and $\vec{A} = (A_x) = \text{DFT}_{2^n} \vec{a}$.
2. Find x such that $|A_x|$ is maximum. Then $\frac{x}{2^n} \approx \omega \bmod 1$.

Definition 6.2.5: $\text{QFT}_n = \frac{1}{\sqrt{2^n}} \text{DFT}_{2^n}^{-1}$.

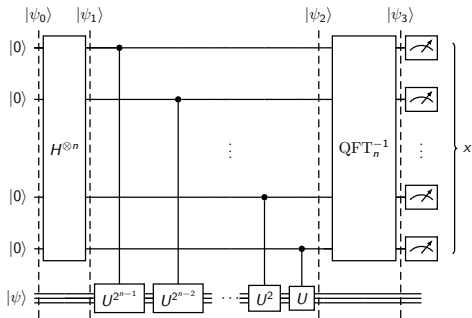
The quantum algorithm:

1. Compute the states $|\psi_n(\omega)\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} a_y |y\rangle_n$ and $\text{QFT}_n^{-1} |\psi_n(\omega)\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} A_x |x\rangle_n$.
2. Measure and obtain $x \in \mathbb{Z}_{2^n}$ with probability $|A_x|^2$. The probability is maximum for x with $\frac{x}{2^n} \approx \omega \bmod 1$.

We will show that step 1 can be performed in [quantum polynomial time](#).

A quantum circuit for $\text{QFT}_n^{-1} |\psi_n(\omega)\rangle$

Proposition 6.2.3: $|\psi_n(\omega)\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle_n = \bigotimes_{j=0}^{n-1} \frac{|0\rangle + e^{2\pi i \cdot 2^{n-j-1} \omega} |1\rangle}{\sqrt{2}}.$



$$|\psi_1\rangle = \bigotimes_{j=0}^{n-1} \frac{|0\rangle + |1\rangle}{\sqrt{2}} |\psi\rangle$$

$$|\psi_2\rangle = \bigotimes_{j=0}^{n-1} C(U^{2^n-j-1}) \frac{|0\rangle + |1\rangle}{\sqrt{2}} |\psi\rangle$$

$$= \bigotimes_{j=0}^{n-1} \frac{|0\rangle + e^{2\pi i \cdot 2^{n-j-1} \omega} |1\rangle}{\sqrt{2}} |\psi\rangle = |\psi_n(\omega)\rangle |\psi\rangle$$

$$|\psi_3\rangle = \text{QFT}_n^{-1} |\psi_n(\omega)\rangle$$

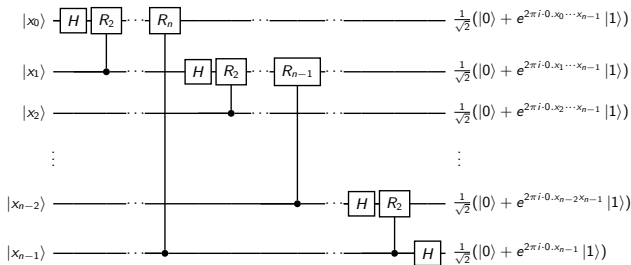
The implementation requires $O(n^2)$ elementary gates and the operators U^{2^k} , $0 \leq k < n$. A generic implementation of the U^{2^k} , $0 \leq k < n$, requires $\sum_{k=0}^{n-1} 2^k = 2^n - 1$ U gates.

A quantum circuit for QFT_n

Proposition 6.2.11:

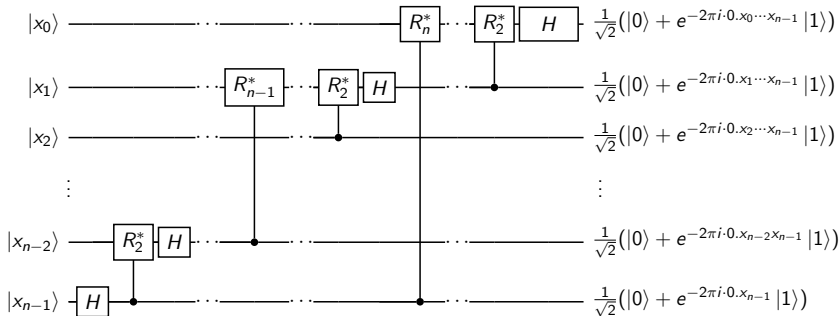
$$\text{QFT}_n |x_0 \cdots x_{n-1}\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} = \bigotimes_{j=0}^{n-1} \frac{|0\rangle + e^{2\pi i \cdot 0 \cdot x_{n-j-1}} |1\rangle}{\sqrt{2}}, x = \sum_{j=0}^{n-1} x_j 2^{n-j-1}.$$

$$R_k : \frac{|0\rangle + \alpha |1\rangle}{\sqrt{2}} \mapsto \frac{|0\rangle + \alpha e^{2\pi i \cdot \frac{1}{2^k}} |1\rangle}{\sqrt{2}} \Rightarrow \text{QFT}_n |x_0 \cdots x_{n-1}\rangle = \bigotimes_{j=0}^{n-1} R_{n-j}^{x_{n-j-1}} \cdots R_2^{x_{j+1}} H \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$



The order of the output qubits must be reversed. The gate complexity is $O(n^2)$.

A quantum circuit for QFT_n^{-1}



The order of the output qubits must be reversed. The gate complexity is $O(n^2)$.

Approximation quality and probability

$$\lfloor r \rfloor: -\frac{1}{2} < r - z \leq \frac{1}{2}, \Delta(\omega, n, x) = \omega - \frac{x}{2^n} - \left[\omega - \frac{x}{2^n} \right].$$

Theorem 6.3.7: Let x be the outcome of measuring $\text{QFT}_n^{-1} |\psi_n(\omega)\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} A_x |x\rangle_n$.

1. If $2^n \omega \in \mathbb{Z}$, then $x \equiv 2^n \omega \pmod{2^n}$ with probability 1.
2. $|\Delta(\omega, n, x)| \leq \frac{1}{2^{n+1}}$ with probability at least $\frac{4}{\pi^2}$.
3. $|\Delta(\omega, n, x)| < \frac{1}{2^n}$ with probability at least $\frac{8}{\pi^2}$.

A formula for $|A_x|^2$

Proposition 6.3.4:

1. If $2^n\omega \in \mathbb{Z}$, then $|A_x| = 2^{2n}$ for $x = 2^n\omega \bmod 2^n$ and $A_x = 0$ for all other $x \in \mathbb{Z}_{2^n}$.
2. If $2^n\omega \notin \mathbb{Z}$, then for all $x \in \mathbb{Z}_{2^n}$

$$|A_x|^2 = \frac{\sin^2(2^n\pi\Delta(\omega, n, x))}{\sin^2(\pi\Delta(\omega, n, x))}.$$

Proof: $\Delta = \Delta(\omega, n, x)$, $x \in \mathbb{Z}_{2^n}$.

$$|A_x|^2 = \left| \sum_{y=0}^{N-1} e^{2\pi i \Delta y} \right|^2 = \begin{cases} 1 & \text{if } 2^n\omega \in \mathbb{Z}, x = 2^n\omega, \\ 0 & \text{if } 2^n\omega \in \mathbb{Z}, x \neq 2^n\omega, \\ \left| \frac{1-e^{2\pi i 2^n \Delta}}{1-e^{2\pi i \Delta}} \right|^2 = \frac{\sin^2(2^n\pi\Delta)}{\sin^2(\pi\Delta)} & \text{if } 2^n\omega \notin \mathbb{Z}. \end{cases}$$

Proof of the theorem on Frame 138

1. Follows from 1. in the theorem of Frame 139.

2. Set $x = \lfloor 2^n \omega \rfloor \bmod 2^n$, $\theta = |2^n \Delta(\omega, n, x)|$. Then $|\theta| \leq \frac{1}{2}$.

$|\sin x| \leq |x|$ for $x \in \mathbb{R}$ and $|\sin \pi x| \geq 2|x|$ for $|x| \leq 1/2$. implies

$$\frac{1}{2^{2n}} |A_x|^2 = \frac{1}{2^{2n}} \frac{\sin^2(\pi\theta)}{\sin^2(\pi\theta/2^n)} \geq \frac{1}{2^{2n}} \frac{(2\theta)^2}{(\pi\theta/2^n)^2} = \frac{4}{\pi^2}.$$

3. There is $x' \in \{x \pm 1\}$ such that $2^n |\Delta(\omega, n, x')| = 1 - \theta$ and $|\Delta(\omega, n, x')| < \frac{1}{2^n}$.

[Yun23]: $\sin^2(\pi\theta) \left(\frac{1}{\theta^2} + \frac{1}{(1-\theta)^2} \right) \geq 8$ for $0 < \theta < 1$.

$$\frac{1}{2^{2n}} (|A_x|^2 + |A_{x'}|^2) = \frac{\sin^2(\pi\theta)}{2^{2n}} \left(\frac{1}{\sin^2 \frac{\pi\theta}{2^n}} + \frac{1}{\sin^2 \frac{\pi(1-\theta)}{2^n}} \right) \geq \frac{\sin^2(\pi\theta)}{\pi^2} \left(\frac{1}{\theta^2} + \frac{1}{(1-\theta)^2} \right) \geq \frac{8}{\pi^2}.$$

4.4. Order Computation Using Phase Estimation

The order problem

Input: $N \in \mathbb{N}$, $N > 1$, $a \in \mathbb{Z}_N^*$. **Output:** $r = \min\{s \in \mathbb{N} : a^s \equiv 1 \pmod{N}\}$.

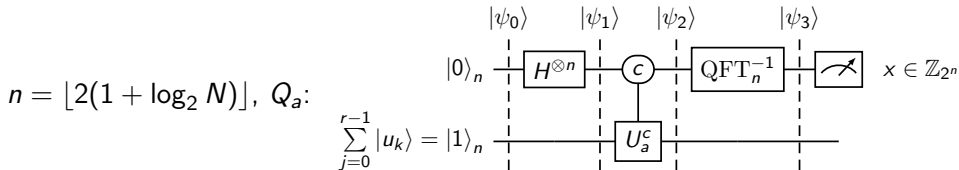
Definition 6.4.2: $U_a : |x\rangle_n \mapsto \begin{cases} |ax \bmod N\rangle_n & \text{if } 0 \leq x < N, \\ |x\rangle_n & \text{if } N \leq x < 2^n. \end{cases}$

Proposition 6.4.4: For $0 \leq k < r$, $|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{ks}{r}}$ is an eigenstate of U_a with eigenvalue $e^{2\pi i \frac{k}{r}}$.

It is not known how to prepare the eigenstates $|u_k\rangle$ efficiently but:

Proposition 6.4.5: $\sum_{j=0}^{r-1} |u_k\rangle = |1\rangle_n$.

The quantum order algorithm and its success probability



- ▶ For $j = 1, 2$:
 - ▶ Apply Q_a ; return value $x_j \in \mathbb{Z}_{2^n}$.
 - ▶ **Proposition 6.4.8:** With probability $\geq \frac{8}{r\pi^2}$, there is $k_j \in \mathbb{Z}_r$ with $\left| \frac{x_j}{2^n} - \frac{k_j}{r} \right| < \frac{1}{2^n}$. If this happens, exactly one of the convergents of the CFA of $\frac{x_j}{2^n}$ is the reduced representation $\frac{m_j}{r_j}$ of $\frac{k_j}{r}$. Record r_j .
- ▶ **Lemma 6.4.11:** If r_1, r_2 are found and $\gcd(k_1, k_2, r) = 1$, then $r = \text{lcm}(r_1, r_2)$.
- ▶ **Proposition 6.4.12:** This happens with conditional probability $\geq \frac{989731}{1628176}$.
- ▶ **Theorem 6.4.8:** The total success probability is $\geq \frac{989731}{1628176} \frac{64}{\pi^4} > 0.399$.

Time complexity of the order algorithm

- ▶ $N \in \mathbb{N}$, $a \in \mathbb{Z}_N^*$, $n = \lfloor 2(1 + \log_2 N) \rfloor = O(\log N)$.
- ▶ Q_a is used twice. Output $x_j \in \mathbb{Z}_{2^n}$ for $j = 1, 2$. Complexity:
 - ▶ Bottleneck: Implementation of $|c\rangle_n |\varphi\rangle \mapsto |c\rangle_n U_a^c |\varphi\rangle$.
 - ▶ But: $U_a : |x\rangle_n \mapsto \begin{cases} |ax \bmod N\rangle_n & \text{if } 0 \leq x < N, \\ |x\rangle_n & \text{if } N \leq x < 2^n. \end{cases}$

Therefore, square and multiply can be used.
 - ▶ **Proposition 6.4.18:** Gate complexity: $O(n^3) = O((\log N)^3)$.
- ▶ CFA is applied to $\frac{x_j}{2^n}$ for $j = 1, 2$. All convergents are computed and compared.
- ▶ **Proposition A.3.28:** Complexity $O(n^2) = O((\log N)^2)$.
- ▶ $\text{lcm}(r_1, r_2)$ is computed. Complexity $O(n^2) = O((\log N)^2)$.
- ▶ **Theorem 6.4.8:** Total complexity: $O((\log N)^3)$.

4.5. Integer Factorization by Order Computation

Shor's factoring algorithm

Input: An odd composite $N \in \mathbb{N}$

- ▶ $a \leftarrow \text{randomInt}(N)$; $d \leftarrow \text{gcd}(a, N)$
- ▶ If $d > 1$, return d .
- ▶ $n \leftarrow \lceil 2 \log_2 N \rceil + 1$
- ▶ $r \leftarrow \text{FindOrder}(N, a, n)$
- ▶ If $r = \text{"FAILURE"}$ or $r \not\equiv 0 \pmod{2}$, return "FAILURE"
- ▶ $b \leftarrow a^{r/2} \pmod{N}$; $d \leftarrow \text{gcd}(b - 1, N)$
- ▶ If $d = 1$, return "FAILURE"
- ▶ Return d .

Success probability

- ▶ Case I: $\gcd(a, r) > 1$ with probability $\frac{N - \varphi(N)}{N}$.
- ▶ Case II:
 1. $\gcd(a, N) = 1$ with probability $\frac{\varphi(N)}{N}$.
 2. Theorem 6.4.8: $r = \text{order}_N(a)$ is found with probability ≥ 0.399 .
 3. Proposition 6.5.6: r is even and $a^{r/2} \not\equiv -1 \pmod{N}$ with probability $\geq \frac{1}{2}$.
- ▶ Total probability $\geq \underbrace{\frac{N - \varphi(N)}{N}}_{\text{Case I}} \underbrace{\frac{\varphi(N)}{N}}_{1.} \cdot \underbrace{0.399}_{2.} \cdot \underbrace{\frac{1}{2}}_{3.} > 0.199$.

Time complexity

- ▶ $\gcd(a, N)$: $O((\log N)^2)$.
- ▶ **Theorem 6.4.8:** $\text{FindOrder}(N, a, n)$: $O((\log N)^3)$.
- ▶ $\gcd(a^{r/2} - 1, N)$: $O((\log N)^2)$.
- ▶ Total complexity: $O((\log N)^3)$.

Prime number decomposition

Theorem: The prime number decomposition of a positive integer can be found in quantum polynomial time.

4.6. Discrete Logarithms

The discrete logarithm problem (DLP)

Input: Elements a, b in a finite group G such that $b = a^t$, $t \in \mathbb{Z}_r$ and $r = \text{order}_G a$.

Output: The exponent t , called the *discrete logarithm* of b to the base a .

The discrete logarithm problem in \mathbb{Z}_N^* :

Input: $N \in \mathbb{N}$, $N \geq 3$, $a, b \in \mathbb{Z}_N^*$ such that $b \equiv a^t \pmod{N}$, $t \in \mathbb{Z}_r$, $r = \text{order}_N a$.

Output: The *discrete logarithm t of b to the base a modulo N* .

Reduction to bases of prime order

Let G be a finite group of known order $|G|$.

1. The quantum factoring algorithm finds the prime number decomposition of $|G|$ in polynomial time.
2. The *Pohlig-Hellman algorithm* (see [Buc04] Section 10.5.) reduces the general DL problem to the problem of computing discrete logarithms for basis elements of prime order in polynomial time.

The quantum DL algorithm

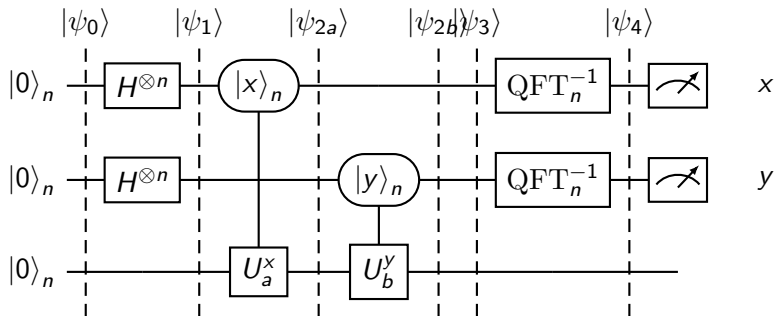
$N \in \mathbb{N}$, $N \geq 3$. Quantum factorization allows computing $\varphi(N) = |\mathbb{Z}_N^*|$ and its prime factorization in polynomial time and reducing DL problems in \mathbb{Z}_N^* to DL problems to bases whose order is a prime number.

So consider DLP: $a, b \in \mathbb{Z}_N^*$, $b \equiv a^t \pmod N$ where $t \in \mathbb{Z}_r$ and $r = \text{order}_N a \in \mathbb{P}$.

$$U_c : |x\rangle_n \mapsto \begin{cases} |cx \bmod N\rangle_n & \text{if } 0 \leq x < N, \\ |x\rangle_n & \text{if } N \leq x < 2^n, \end{cases}, \quad |u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r}s} |a^s \bmod N\rangle_n.$$

1. $|u_k\rangle$ is an eigenstate of U_a with eigenvalue $e^{2\pi i \frac{k}{r}}$.
2. $|u_k\rangle$ is an eigenstate of $U_{a^t} = U_b$ with eigenvalue $e^{2\pi i \frac{tk}{r}}$.
3. Simultaneous quantum phase estimation gives $\frac{k}{r}$ and $\frac{kt}{r}$ for some $k \in \mathbb{Z}_r^*$.
4. $t \equiv k^{-1} \pmod r$.

The quantum circuit Q_{DL}



Success probability and complexity

Theorem 6.6.3: On input of $N \in \mathbb{N}$, $a, b \in \mathbb{Z}_N^*$, the order r of a modulo N which is a prime number and $b \equiv a^t \pmod{N}$ for some $t \in \mathbb{Z}_r^*$, the quantum discrete logarithm algorithm returns t with probability at least $64(r-1)/r\pi^4 > 0.328$. Its running time is $O((\log N)^3)$.

5. Quantum Search and Quantum Counting

5.1. The Search Problem

The classical search problem

Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$, $M = |f^{-1}\{1\}| > 0$.

Input: A black-box for f . **Output:** $\vec{x} \in \{0, 1\}^n$ with $f(\vec{x}) = 1$.

Theorem A: any deterministic algorithm requires in the worst case $2^n - M + 1$ evaluations of f

Theorem A: any probabilistic algorithm that evaluates f at most k times has a success probability of at most $\frac{Mk}{2^n}$ if $k \leq \frac{2^n}{M}$.

The quantum search problem

Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$, $M = |f^{-1}\{1\}| > 0$. Assume that $M > 0$.

Let $U_f : \mathbb{H}_{n+1} \rightarrow \mathbb{H}_{n+1}$, $|\vec{x}\rangle |y\rangle \mapsto |\vec{x}\rangle X^{f(\vec{x})} |y\rangle$

Input: n and a black-box for U_f .

Output: $\vec{x} \in \{0, 1\}^n$ with $f(\vec{x}) = 1$.

5.2. Quantum search when the number of solutions is known

Idea of the algorithm

$f : \{0, 1\}^n \rightarrow \{0, 1\}$, $M = |f^{-1}\{1\}| > 0$ is known. $N = 2^n$.

$$|s_0\rangle = \frac{1}{\sqrt{N-M}} \sum_{\vec{x} \in \{0,1\}^n, f(\vec{x})=0} |\vec{x}\rangle, \quad |s_1\rangle = \frac{1}{\sqrt{M}} \sum_{\vec{x} \in \{0,1\}^n, f(\vec{x})=1} |\vec{x}\rangle,$$

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle = \sqrt{\frac{N-M}{N}} |s_0\rangle + \sqrt{\frac{M}{N}} |s_1\rangle = \cos \theta |s_0\rangle + \sin \theta |s_1\rangle, \quad \theta = \arcsin \sqrt{\frac{M}{N}}.$$

1. Construct $|s\rangle = H^{\otimes n} |0\rangle^{\otimes n}$.
2. Measure $|s\rangle$: The result is $\vec{x} \in \{0, 1\}^n$ such that $f(\vec{x}) = 1$ with probability $\frac{M}{N}$.

We will show how to amplify the amplitude of $|s_1\rangle$.

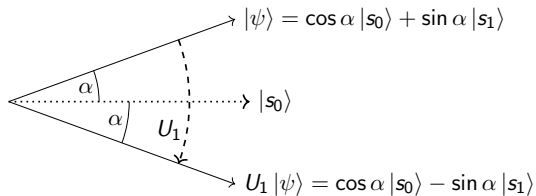
The operator U_1

$$|s_0\rangle = \frac{1}{\sqrt{N-M}} \sum_{f(\vec{x})=0} |\vec{x}\rangle, |s_1\rangle = \frac{1}{\sqrt{M}} \sum_{f(\vec{x})=1} |\vec{x}\rangle, \theta = \arcsin \sqrt{\frac{M}{N}}.$$

Proposition 7.1.9:

$$U_1 = I - 2 |s_1\rangle \langle s_1|$$

is the reflection:



The operator U_s

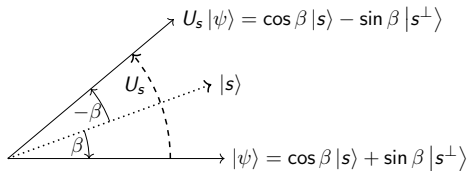
$$|s_0\rangle = \frac{1}{\sqrt{N-M}} \sum_{f(\vec{x})=0} |\vec{x}\rangle, \quad |s_1\rangle = \frac{1}{\sqrt{M}} \sum_{f(\vec{x})=1} |\vec{x}\rangle,$$

$$|s\rangle = \cos \theta |s_0\rangle + \sin \theta |s_1\rangle, \quad |s^\perp\rangle = -\sin \theta |s_0\rangle + \cos \theta |s_1\rangle, \quad \theta = \arcsin \sqrt{\frac{M}{N}}.$$

Proposition 7.1.12:

$$U_s = 2 |s\rangle \langle s| - I$$

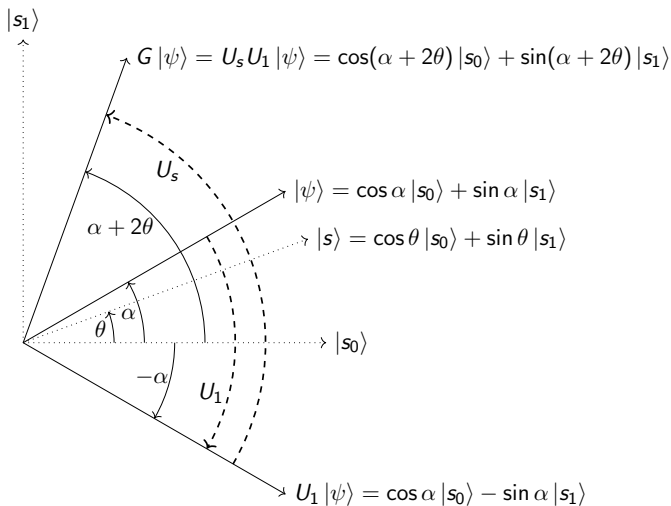
is the reflection



The Grover iterator G

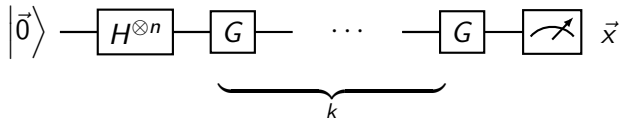
Proposition 7.1.16:

$G = U_s U_1$ has the property:



Amplitude amplification

Proposition 7.1.16: $G \cos \alpha |s_0\rangle + \sin \alpha |s_1\rangle = \cos(\alpha + 2\theta) |s_0\rangle + \sin(\alpha + 2\theta) |s_1\rangle$



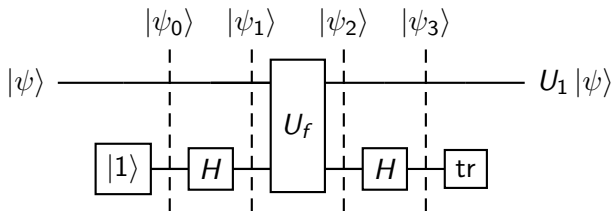
- ▶ $G^k H^{\otimes n} |0\rangle^{\otimes n} = G^k |s\rangle = \cos(2k+1)\theta |s_0\rangle + \sin(2k+1)\theta |s_1\rangle$.
- ▶ Measuring $G^k |s\rangle$ gives \vec{x} such that $f(\vec{x}) = 1$ with probability $\sin^2(2k+1)\theta$.
- ▶ Make $\sin^2(2k+1)$ as large as possible!
- ▶ $k = \lfloor \frac{\pi}{4\theta} \rfloor \leq \frac{\pi}{4} \sqrt{\frac{N}{M}} \Rightarrow$ **Theorem 7.1.21:** $\sin^2(2k+1)\theta \geq 1 - \frac{M}{N}$.
- ▶ For small M , this gives a quadratic speedup compared to brute force search.

Complexity of Grover's algorithm

Grover algorithm: measure $G^k H^{\otimes n} |\vec{0}\rangle$, $G = U_s U_1$, $k = \lfloor \frac{\pi}{4\theta} \rfloor$, $\theta = \arcsin \sqrt{\frac{M}{N}}$.

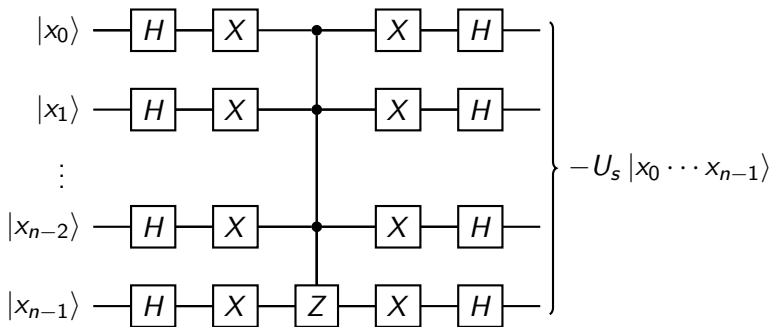
1. $|\arcsin y| \geq |y|$ for all $y \in [-1, 1] \Rightarrow k \leq \frac{\pi}{4 \arcsin \sqrt{M/N}} \leq \frac{\pi}{4} \sqrt{\frac{N}{M}}$
2. U_1 can be implemented using the U_f gate and 4 elementary gates.
3. U_s can be implemented using $O(n)$ elementary gates.
4. $\Rightarrow G$ can be implemented using one U_f gate and $O(n)$ elementary gates.
5. 2. and 5. \Rightarrow **Theorem 7.1.21**: The algorithm uses U_f at most $\frac{\pi}{4} \sqrt{\frac{N}{M}}$ times and $O\left(\log N \sqrt{\frac{N}{M}}\right)$ additional elementary gates.

Quantum circuit for U_1



Gate complexity: One U_f gate and 4 elementary gates.

Quantum circuit for U_s



Gate complexity: $O(n)$ elementary gates.

5.3. Grover Search for an Unknown Number of Solutions

The algorithm

```
1:  $l \leftarrow 1; \lambda \leftarrow 6/5$ 
2: repeat
3:    $m \leftarrow \lfloor \min\{l, \sqrt{N}\} \rfloor$ 
4:    $k \leftarrow \text{randomInt}(m)$ 
5:   Measure  $G^k H^{\otimes n} |\vec{0}\rangle$ , the result being  $\vec{x} \in \{0, 1\}^n$ 
6:    $l = \lambda l$ 
7: until  $f(\vec{x}) = 1$ 
8: return  $\vec{x}$ 
```

Theorem 7.1.23: Assume that $M \leq \frac{3N}{4}$. Then the expected number of applications of the Grover iterator and thus of the operator U_f required by the algorithm on frame 170 to find a solution of the search problem is at most $9\sqrt{\frac{N}{M}}$. The expected running time of the algorithm is $\left(\sqrt{\frac{N}{M}}\right)^{1+o(1)}$.

5.4. Quantum Counting

The counting problem

Input: $n \in \mathbb{N}$ and a black-box for a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$

Output: The number $M = |f^{-1}(1)|$ of solutions of the search problem.

The idea

$$|s_0\rangle = \frac{1}{\sqrt{N}} \sum_{f(\vec{x})=0} |\vec{x}\rangle, \quad |s_1\rangle = \frac{1}{\sqrt{N}} \sum_{f(\vec{x})=1} |\vec{x}\rangle, \quad P = \mathbb{C}|s_0\rangle + \mathbb{C}|s_1\rangle$$

$$|s_+\rangle = \frac{|s_1\rangle + i|s_0\rangle}{\sqrt{2}}, \quad |s_-\rangle = \frac{|s_1\rangle - i|s_0\rangle}{\sqrt{2}}, \quad \theta = \arcsin\left(\sqrt{\frac{M}{N}}\right).$$

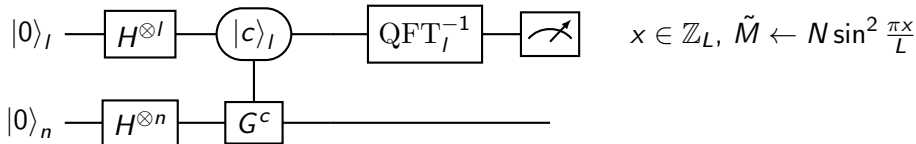
Proposition 7.2.2:

1. $(|s_+\rangle, |s_-\rangle)$ is an ONB of eigenstates of $G|_P$ with eigenvalues $e^{2i\theta}$, $e^{-2i\theta}$, resp.
2. $|s\rangle = \frac{-i}{\sqrt{2}} (e^{i\theta} |s_+\rangle - e^{-i\theta} |s_-\rangle)$.

$M = N \sin^2 \theta$ is determined by approximating one of the phases $\pm 2\theta$.

Approximate quantum counting

Choose a precision parameter $l \in \mathbb{N}$. Set $N = 2^n$, $L = 2^l$.



Theorem 7.2.5:

1. If $M = 0$, then $\tilde{M} = 0$ with probability 1.
2. If $M \neq 0$, then $\left| \tilde{M} - M \right| < 2\pi \frac{\sqrt{M(N-M)}}{L} + \frac{\pi^2 N}{L^2}$ with probability at least $\frac{8}{\pi^2}$.
3. The algorithm requires $O(L)$ applications of U_f and $O(Ln^2)$ additional elementary operations.

Quantum counting with preselected error ϵ

```
1:  $l \leftarrow 0$ 
2: repeat
3:    $l \leftarrow l + 1$ ;  $\tilde{M} \leftarrow \text{QCount}(n, U_f, l)$ 
4: until  $\tilde{M} \neq 0$  or  $2^l \geq 2\sqrt{N}$ 
5:  $l \leftarrow l + \left\lceil \log_2 \frac{20\pi^2}{\epsilon} \right\rceil$ ;  $\tilde{M} \leftarrow \text{QCount}(n, U_f, l)$ 
6: return  $\hat{M} \leftarrow \left\lfloor \tilde{M} \right\rfloor$ 
```

Theorem 7.2.7:





1. If $M = 0$, then $\hat{M} = 0$ with probability 1.
2. With probability at least $\frac{2}{3}$ we have $|\hat{M} - M| < \epsilon M$.
3. The algorithm requires $O\left(\frac{\sqrt{N}}{\epsilon}\right)$ applications of U_f and $O\left(\frac{n^2\sqrt{N}}{\epsilon}\right)$ additional elementary operations.

Exact quantum counting

- 1: $\tilde{M}_1 \leftarrow \text{ApproxQCount}(n, U_f, \frac{1}{2})$
- 2: $l \leftarrow \left\lceil \log_2 26\sqrt{\tilde{M}_1 N} \right\rceil$
- 3: $\tilde{M}_2 \leftarrow \text{QCount}(n, U_f, l)$
- 4: **return** $M \leftarrow \left\lfloor \tilde{M}_2 \right\rfloor$

Theorem 7.2.9: The algorithm returns $M = |f^{-1}(1)|$ with probability at least $\frac{1}{2}$. It requires $O(\sqrt{MN})$ applications of U_f and $O(n^2\sqrt{MN})$ additional elementary operations.

Bibliography I

-  Johannes Buchmann, *Introduction to cryptography*, 2nd ed., Undergraduate texts in mathematics, Springer, New York, 2004.
-  Richard Cleve, *Classical lower bounds for simon's problem*, <https://cs.uwaterloo.ca/~cleve/courses/F11CS667/SimonClassicalLB.pdf>, 2011.
-  C.M. Dawson and M.A. Nielsen, *The Solovay-Kitaev algorithm*, Quantum Information and Computation **6** (2006), no. 1, 81–95.
-  Ho Yun, *Redheffer: Trig to quantum error bounds*, arXiv e-prints (2023), arXiv–2310.