Chapter 3

Algorithmic Appetizers

In this chapter, we discuss three small algorithms. The examples illustrate the operations that we introduced in the previous chapter. We begin with a communication protocol, which allows to communicate the state of a single quantum bit. This process is known as teleportation, a somewhat ambitious name for a simple protocol.

§1 Teleportation

Suppose that Alice wants to communicate the state of a quantum bit to Bob. The matter is complicated by the fact that the quantum state might not be known to her. This would not help her much anyway, since, in most cases, she would not be able to communicate a complete description of the state by classical communication alone.

Alice and Bob need, in addition to classical communication, another resource. If Alice and Bob share a pair of quantum bits, which are in the state

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle, \tag{3.1}$$

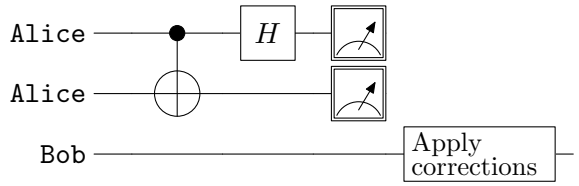
then it is not difficult to communicate the unknown quantum state, as we will show in this section. This method has been suggested by Bennett, Brassard, Crepeau, Josza, Peres, and Wootters in 1993, and is known as **teleportation**. This type of teleportation has been demonstrated in several experiments.

We need three quantum bits in the teleportation protocol. We assume that the two most significant qubits belong to Alice, and the least significant qubit belongs to Bob. Alice wants to communicate the most significant bit to Bob. We assume that this quantum bit is in the state $a|0\rangle + b|1\rangle$, but Alice

might not be aware of that, and the least two qubits are in the state (3.1). Therefore, the system is initially in the state

$$(a|0\rangle + b|1\rangle) \otimes (\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle). \tag{3.2}$$

We assume that Alice and Bob are located far apart. They can apply operations locally on the qubits in their possession and communicate over the phone. The teleportation is surprisingly simple. Alice applies a controlled-not operation $\Lambda_{2,1}(X)$, and a Hadamard gate to the most significant bit. Then she measures her quantum bits, and tells Bob what kind of gate he should apply to his quantum bit.



The controlled-not gate $\Lambda_{2,1}(X)$ transforms the state (3.2) to

$$a|0\rangle \otimes (\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle) \; + \; b|1\rangle \otimes (\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle).$$

Applying the Hadamard gate on the most significant qubit yields the state

$$\begin{aligned} &a(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle) \otimes (\tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle) \\ &+ b(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle) \otimes (\tfrac{1}{\sqrt{2}}|10\rangle + \tfrac{1}{\sqrt{2}}|01\rangle). \end{aligned}$$

The bilinear relations of the tensor product allow this state to be rewritten as follows:

$$\begin{aligned} &a(\tfrac{1}{2}|000\rangle + \tfrac{1}{2}|011\rangle + \tfrac{1}{2}|100\rangle + \tfrac{1}{2}|111\rangle) \\ &+b(\tfrac{1}{2}|001\rangle + \tfrac{1}{2}|010\rangle - \tfrac{1}{2}|101\rangle - \tfrac{1}{2}|110\rangle). \end{aligned}$$

We collect the terms with the same two most significant qubits, and use the bilinear relations of the tensor product to express this state in yet another, but still equivalent, form:

$$\begin{aligned} \frac{1}{2}\Big(&|00\rangle \otimes (a|0\rangle + b|1\rangle) + |01\rangle \otimes (a|1\rangle + b|0\rangle) \\ &+|10\rangle \otimes (a|0\rangle - b|1\rangle) + |11\rangle \otimes (a|1\rangle - b|0\rangle)\Big). \end{aligned}$$

Alice finally measures the two most significant qubits. The different measurement results and corresponding post-measurement states are shown in the following table:

Observation	Resulting State	Alice tells Bob
00	$\|00\rangle \otimes (a\|0\rangle + b\|1\rangle)$	to do nothing
01	$\|01\rangle \otimes (a\|1\rangle + b\|0\rangle)$	to apply X
10	$\|10\rangle \otimes (a\|0\rangle - b\|1\rangle)$	to apply Z
11	$\|11\rangle \otimes (a\|1\rangle - b\|0\rangle)$	to apply ZX

We note that the resulting state after the measurement can be transformed in each case into a state of the form $|x_2x_1\rangle \otimes (a|0\rangle + b|1\rangle)$, with $x_i \in \{0, 1\}$, by applying the single-qubit gate recommended by Alice. We have accomplished our goal: Alice has successfully communicated the state $a|0\rangle + b|1\rangle$ to Bob.

Entanglement. Let $\mathbf{C}^n$ and $\mathbf{C}^m$ be state spaces of two quantum systems. A state of $\mathbf{C}^n \otimes \mathbf{C}^m$ that can be written in the form $v \otimes w$, for some $v \in \mathbf{C}^n$ and $w \in \mathbf{C}^m$, is called **decomposable**. If a state is not decomposable, then it is called an **entangled state**. Teleportation and many other protocols in quantum computing use entanglement as a resource.

Exercise 3.1 Show that the state (3.1) is an entangled state.

There exists a simple criterion that allows us to decide whether an arbitrary state in $\mathbf{C}^2 \otimes \mathbf{C}^2$ is entangled or not. We have to check only a single invariant of the state to decide this question.

Exercise 3.2 Prove that the state $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ is decomposable if and only if the coefficients satisfy $\alpha\delta - \beta\gamma = 0$.

The state (3.1) is called an **Einstein-Podolsky-Rosen state**, or **EPR state** for short. This state received considerable attention after the famous critique on quantum mechanics by Einstein, Podolsky, and Rosen; particularly in Bohm's interpretation. However, there is nothing sacred about this state, and it is, of course, possible to use other entangled states for teleportation.

Exercise 3.3 Suppose that Alice and Bob share the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{e^{i\theta}}{\sqrt{2}}|11\rangle$, $\theta \in \mathbf{R}$. Assume that Alice wants to use her teleport circuit to communicate an unknown state $a|0\rangle + b|1\rangle$ of some quantum bit to Bob. Assuming that they both know θ, what kind of operations does Bob have to apply when he learns Alice's measurement results? Derive all steps carefully.

If the state shared by Alice and Bob is not entangled, then teleportation is not possible. However, not every entangled state can be used in for teleportation. We will show later that the shared state has to be a so-called maximally entangled state.

Extensions. Suppose that Alice wants to communicate the state of a system of several quantum bits to Bob. Can she teleport one qubit at a time? We contend that this is the case. To prove this claim, we assume that Alice has $n+1$ quantum bits, which are in the state

$$\sum_{k=0}^{2^n-1} \sum_{j=0}^{1} a_{kj} |k\rangle \otimes |j\rangle \in \mathbf{C}^{2^n} \otimes \mathbf{C}^2. \tag{3.3}$$

If Alice wants to communicate this state to Bob using the teleportation protocol, then she needs to share $n+1$ EPR pairs with Bob. It would be tedious to give a direct proof that this approach works. We show instead that teleportation is faithful in the following sense: If Alice teleports a single qubit, then Alice's remaining n qubits, and the qubit that Bob has received, are in the state (3.3), and these $n+1$ qubits are not entangled with the remaining part of the system. It follows that we can teleport one qubit at a time.

It remains to show that the teleportation of one qubit will preserve the state (3.3), except that one qubit is transferred from Alice to Bob. The intial state of the system is

$$\sum_{k=0}^{2^n-1} \sum_{j=0}^{1} a_{kj} |k\rangle \otimes |j\rangle \otimes (\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle).$$

Note that it suffices to consider one EPR state to teleport a single qubit. We now repeat the exact same teleportation protocol as before. Intially, Alice applies the controlled-not gates $\Lambda_{2,1}(X)$; this yields the state

$$\sum_{k=0}^{2^n-1} \Big(a_{k0}|k\rangle \otimes |0\rangle \otimes (\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle) + a_{k1}|k\rangle \otimes |1\rangle \otimes (\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle) \Big).$$

Then she applies the Hadamard gate on the qubit at position 2, which yields the state

$$\sum_{k=0}^{2^n-1} \Big(a_{k0}|k\rangle \otimes \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + a_{k1}|j\rangle \otimes \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle) \Big).$$

We want to measure the qubits at positions 1 and 2. We use the bilinear relations of the tensor product to rewrite this state in the more convenient, but equivalent, form

$$\sum_{k=0}^{2^n-1} \frac{1}{2}\Big(|k\rangle \otimes |00\rangle \otimes (a_{k0}|0\rangle + a_{k1}|1\rangle) \\ +|k\rangle \otimes |01\rangle \otimes (a_{k0}|1\rangle + a_{k1}|0\rangle) \\ +|k\rangle \otimes |10\rangle \otimes (a_{k0}|0\rangle - a_{k1}|1\rangle) \\ +|k\rangle \otimes |11\rangle \otimes (a_{k0}|1\rangle - a_{k1}|0\rangle)\Big).$$

Suppose that Alice measures the qubits at positions 2 and 1. If she observes x_2 and x_1, respectively, and informs Bob to apply $Z^{x_2}X^{x_1}$, then after applying Bob's correction operations, we get

$$\sum_{k=0}^{2^n-1}\sum_{j=0}^{1} |k\rangle \otimes |x_2x_1\rangle \otimes a_{kj}|j\rangle = \sum_{k=0}^{2^n-1}\sum_{j=0}^{1} a_{kj}|k\rangle \otimes |x_2x_1\rangle \otimes |j\rangle.$$

We note that Alice's n most significant qubits, and Bob's least significant qubit are in the state (3.3), and that these qubits are not entangled with the qubits at positions 1 and 2.

We can summarize our findings as follows: If Alice wants to communicate the state of $n+1$ quantum bits, then she can do that by applying the teleportation protocol $n+1$ times. If the system is initially in the state

$$\sum_{k=0}^{2^n-1}\sum_{l=0}^{1} a_{kj}|k\rangle \otimes |j\rangle \otimes \bigotimes_{i=0}^{n}(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle),$$

then after applying $2n+2$ gate operations and $2n+2$ measurements on Alice's side, and up to $2n+2$ operations on Bob's side, they manage to transfer the state (3.3) to Bob.

Remark. Note that the protocol simply communicates quantum states, and it does not teleport matter. You find many exaggerated conclusions in publications about teleportation – watching episodes of Star Trek seems to have side effects.

§2 Deutsch's Problem

Suppose that you are given a black box that contains an implementation of a boolean function $f\colon \mathbf{F}_2 \to \mathbf{F}_2$. Your task is to determine the parity

$f(0) \oplus f(1)$, the sum of $f(0)$ and $f(1)$ modulo 2. The goal is to solve this task with a minimal number of calls to the black box.

The classical solution to this problem requires two calls to the black box, since the function might be constant or not. In the quantum version, you are given an implementation of f as a quantum circuit on two quantum bits,

$$|x_1\rangle \otimes |x_0\rangle \mapsto |x_1\rangle \otimes |x_0 \oplus f(x_1)\rangle, \tag{3.4}$$

with $x_1, x_0 \in \mathbf{F}_2 = \{0, 1\}$. The quantum version can be solved with a single call to the black box. The problem and its solution were suggested by Deutsch in 1985; it is historically one of the first quantum algorithms.

Exercise 3.4 Give implementations of the quantum circuit (3.4) for the constant functions (a) $f(0) = f(1) = 0$, and (b) $f(0) = f(1) = 1$, as well as for the balanced functions (c) $f(0) = 0$, $f(1) = 1$, and (d) $f(0) = 1$, $f(1) = 0$.

Let B denote the unitary map on $\mathbf{C}^4$ determined by (3.4). We will derive the solution in some small steps. It is clear that we have to take advantage of the superposition principle to evaluate the boolean function simultaneously for both possible input arguments. The solution to Deutsch's problem uses an additional trick, which allows us to encode the value of $f(x)$ into a phase factor. Suppose that the least significant bit is in the state $1/\sqrt{2}(|0\rangle - |1\rangle)$, then

$$B\left(|x_1\rangle \otimes \big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\big)\right) = |x_1\rangle \otimes \big(\frac{1}{\sqrt{2}}|f(x_1)\rangle - \frac{1}{\sqrt{2}}|1 \oplus f(x_1)\rangle\big) =: v_{x_1}$$

for all $x_1 \in \{0, 1\}$. If the value of $f(x_1)$ is zero, then the input state remains invariant; otherwise, B affects a change of sign. Explicitly,

$$v_{x_1} = (-1)^{f(x_1)}|x_1\rangle \otimes \big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\big).$$

We can now use the superposition principle. If we choose $1/\sqrt{2}(|0\rangle + |1\rangle)$ for the most significant qubit, then we obtain the result $1/\sqrt{2}(v_0 + v_1)$ since the black box B is linear. To put this in a different way, we get

$$B\left(\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)\right) = \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle).$$

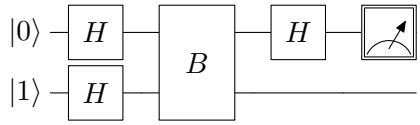
The goal was to discriminate between functions, which satisfy $f(0) \oplus f(1) = 0$, and functions satisfying $f(0) \oplus f(1) = 1$. The previous state is equivalent to

$$\begin{cases} \pm\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) & \text{if } f(0) \oplus f(1) = 0, \\ \pm\frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) & \text{if } f(0) \oplus f(1) = 1. \end{cases}$$

If we apply the Hadamard gate on the most significant qubit, then we get

$$\begin{cases} \pm|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } f(0) \oplus f(1) = 0, \\ \pm|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } f(0) \oplus f(1) = 1. \end{cases}$$

We measure the most significant qubit now. If the function in the black box satisfies $f(0) \oplus f(1) = 0$, then we will observe 0 with certainty. If f satisfies $f(0) \oplus f(1) = 1$, then we will observe 1. Note that the algorithm is completely deterministic. We can summarize the algorithm that we have developed as follows:



The reader should pause here for a moment and retrace each step in the circuit diagram. The first two Hadamard gates prepare the superposition of the input and the state which allows the encoding of the value of $f(x)$ into a phase factor.

§3 Hidden Subgroup Problems

Deutsch's problem is an instance of a hidden subgroup problem. The hidden subgroup problem is often considered as the Holy Grail of quantum computing and has inspired a considerable amount of research. We need some terminology before we can state this problem. Recall that a **group** is a non-empty set G with a composition operation $\circ\colon G \times G \to G$, such that

G1 $((x \circ y) \circ z) = (x \circ (y \circ z))$ holds for all $x, y, z \in G$;

G2 there exists an element $e \in G$ such that $e \circ x = x \circ e = x$ for all $x \in G$;

G3 for each $x \in G$, there exists an $x^{-1} \in G$ such $x \circ x^{-1} = x^{-1} \circ x = e$.

Axiom G1 states that the composition is associative, and G2 that there exists an identity (or neutral) element. Note that this identity element is uniquely determined. The axiom G3 states that each element x in G has an inverse element.

Exercise 3.5 Show that (a) the integers $\mathbf{Z}$ with addition as composition is a group; (b) the set $\mathbf{Z}/n\mathbf{Z} = \{0, \cdots n-1\}$ of integers with addition modulo n is a group; (c) the set $\mathrm{GL}(n, \mathbf{R})$ of all real invertible $n \times n$ matrices is a group with matrix multiplications as composition. Explicitly determine the inverses and the identity element in all cases.

A subset H of G is called a **subgroup** of G if and only if it forms a group under the restriction of the composition $\circ$ to H. If S is a subset of G, then $\langle S \rangle$ denotes the smallest subgroup of G containing S. If there exists a finite set S such that $\langle S \rangle = G$, then G is called a **finitely generated group**.

Exercise 3.6 Determine all subgroups of the group $\mathbf{Z}/6\mathbf{Z}$.

Exercise 3.7 Determine which of the following groups are finitely generated: (a) the additive group of integer $\mathbf{Z}$, (b) the group $\mathbf{Z}/n\mathbf{Z}$. If possible, give an explicit set of generators.

We can formulate the problem as follows:

> **The Hidden Subgroup Problem:** Let $f\colon G \to X$ be a black box function from a finitely generated group G to a finite set X such that
>
> $$f(x) = f(y) \quad \text{if and only if} \quad y^{-1}x \in H, \tag{3.5}$$
>
> where H is some initially unknown subgroup of G. Your task is to find a generating set S of H.

The hidden subgroup problem serves as a yardstick measuring the progress in quantum computing. Various instances have been solved, and some see numerous examples in the following chapters.

We have already mentioned that Deutsch's problem can be viewed as a special case of the hidden subgroup problem. Indeed, let the group $G = \mathbf{Z}/2\mathbf{Z}$ and the set $X = \mathbf{Z}/2\mathbf{Z}$. We have two possible subgroups of G, namely $H = \{0, 1\}$ and $H = \{0\}$. If the hidden subgroup $H = \{0\}$, then the constraint (3.5) implies that f has to be a balanced function. If $H = \{0, 1\}$, then f has to be a constant function.

Exercise 3.8 Assume that $f\colon \mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ is a black box function for a hidden subgroup problem. Enumerate all potential hidden subgroups H of $G = \mathbf{Z}/4\mathbf{Z}$ that can be encoded by black box functions of this type.

Exercise 3.9 Let $f\colon \mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ be a black box function for a hidden subgroup problem. Assume that the black box is realized by a quantum circuit, which implements the map $|x_1x_0\rangle \otimes |y\rangle \mapsto |x_1x_0\rangle \otimes |y \oplus f(x_1, x_0)\rangle$, with $x_1, x_0, y \in \mathbf{F}_2$. We assume that the binary string x_1x_0 encodes the number $2x_1 + x_0$. Design a quantum circuit, which solves this hidden subgroup problem.

Almost all quantum algorithms that have an exponential speed-up over the best classical algorithms known to date can be formulated as hidden subgroup problems, or some closely related variation of this problem.

§4 A Small Search Algorithm

Suppose that we are given a black box function $f\colon \mathbf{F}_2^n \to \mathbf{F}_2$ such that $f(s) = 1$ for some $s \in \mathbf{F}_2^2$, and $f(x) = 0$ otherwise. We want to find this element s satisfying the search criterion $f(s) = 1$. Classically, we need to evaluate $f(x)$ more than two times to find s with probability greater than $1/2$. We discuss in this section a quantum algorithm that allows us to find s with probability 1 using a single evaluation of the black box function.

We assume that the black box function is given in form of a quantum circuit, which realizes the unitary map B_f given by

$$|x_1x_0\rangle \otimes |y\rangle \mapsto |x_1x_0\rangle \otimes |y \oplus f(x_1, x_0)\rangle,$$

where $x_1, x_0, y \in \mathbf{F}_2$. We evaluate B_f on a superposition of all inputs, and encode the result as a sign change. We accomplish this by initializing with $|0\rangle \otimes |0\rangle \otimes |1\rangle$, and by applying Hadamard gates to all three qubits; these operations generate the state

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

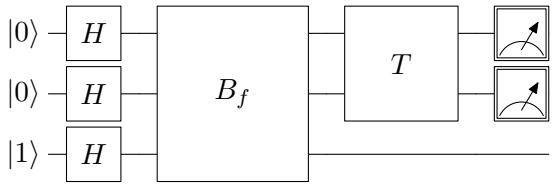
Applying B_f to this state yields one of the following four possible results:

$f(s) = 1$	resulting state
$s = 00$	$\frac{1}{2}(-\|00\rangle + \|01\rangle + \|10\rangle + \|11\rangle) \otimes \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$,
$s = 01$	$\frac{1}{2}(\|00\rangle - \|01\rangle + \|10\rangle + \|11\rangle) \otimes \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$,
$s = 10$	$\frac{1}{2}(\|00\rangle + \|01\rangle - \|10\rangle + \|11\rangle) \otimes \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$,
$s = 11$	$\frac{1}{2}(\|00\rangle + \|01\rangle + \|10\rangle - \|11\rangle) \otimes \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$.

We note that the four states are orthogonal. Therefore, it is possible to find a base change T transforming the two most significant qubits into the computational bases states. The coordinate transform is given by

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

After this base change, we can measure the result in the computational basis. The resulting circuit is

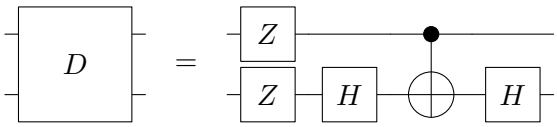


Notice that if the search string is $s = (x_1, x_0)$, then we will observe the two bits (x_1, x_0) in the measurement.

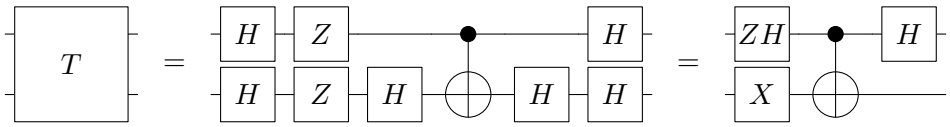
It remains to realize the base change T by a sequence of quantum gates. Note that

$$T = (H \otimes H)\,\mathrm{diag}(1, -1, -1, -1)(H \otimes H).$$

This is easily verified by a direct computation. The diagonal matrix $D = \mathrm{diag}(1, -1, -1, -1)$ can be realized by the circuit



Therefore, we can implement T by



It is possible to generalize this search problem to n quantum bits. A quantum algorithm to solve this problem was published by Grover in 1996. We will discuss his algorithm in detail in one of the following chapters.

§5 Summary

- **Teleportation** is a communication protocol that allows to communicate the state of n quantum bits from Alice to Bob, if they share n EPR pairs.
- **Deutsch's problem** asks to evaluate the parity $f(0) \oplus f(1)$ of a boolean black box function $f\colon \mathbf{F}_2 \to \mathbf{F}_2$. A quantum algorithm can solve this task with a single evaluation of the black box function.
- The **hidden subgroup problem** asks us to find a generating set of an unknown subgroup H of a finitely generated group G, given a black box function f that maps elements of the group G to a finite set X such that $f(x)$ and $f(y)$ are the same if and only if $y^{-1}x \in H$.
- Let $f\colon \mathbf{F}_2^2 \to \mathbf{F}_2$ be a black box function, which is constant zero except on one argument. The **search algorithm** allows us to find this argument with a single evaluation of f. This algorithm was suggested by Grover in 1996.