Quantum Computing Cheatsheet

Edoardo Riggio

June 26, 2022

Quantum Computing - S.P. 2022
Computer Science
Università della Svizzera Italiana, Lugano

Contents

1 What is Quantum Informatics **2**
- 1.1 Information and Physics . . . 2
- 1.2 Second Law of Thermodynamics . . . 2
- 1.3 The Stern/Gerlach Experiment . . . 2
- 1.4 Superposition . . . 4
- 1.5 Quantum Key Distribution . . . 4
- 1.6 The Double-Slit Experiment . . . 5
- 1.7 The Mach/Zehnder Interferometer . . . 5
- 1.8 Quantum Bit . . . 6
  - 1.8.1 Hadamard Gate . . . 7
  - 1.8.2 Square Root of NOT . . . 7
- 1.9 Deutsch's Algorithm . . . 7
- 1.10 The Aspect/Gisin/Zelinger Experiments . . . 9
  - 1.10.1 Einstein/Podolsky/Rosen's Claim . . . 9
  - 1.10.2 Bell's Claim . . . 9

2 Information is Physical **9**
- 2.1 Thermodynamics and Entropy . . . 9
  - 2.1.1 First Law . . . 9
  - 2.1.2 Second Law . . . 10
- 2.2 Information Theory . . . 10
  - 2.2.1 Standard Model of Communication . . . 10
  - 2.2.2 The Game of 20 Questions . . . 10
- 2.3 Entropy . . . 11
- 2.4 Bit Analogy . . . 12
- 2.5 Landauer's Principle . . . 12
- 2.6 The Converse of Landauer's Principle . . . 12
- 2.7 Bennett's Solution to Maxwell's Demon . . . 13
- 2.8 Reversible Computing . . . 13
- 2.9 Toffoli Gate . . . 14

3 Key Experiments and Postulates of Quantum Physics **15**
- 3.1 Black-Body Radiation . . . 15
  - 3.1.1 Classical Mechanics . . . 15
  - 3.1.2 Quantum Mechanics . . . 17
- 3.2 Photoelectric Effect . . . 17
  - 3.2.1 Classical Mechanics . . . 17
  - 3.2.2 Quantum Mechanics . . . 17
- 3.3 Wave-Particle Dualism . . . 18
  - 3.3.1 Schrödinger's Equation . . . 18
- 3.4 Postulates of Quantum Theory . . . 19
  - 3.4.1 The State . . . 19
  - 3.4.2 The Time Evolution . . . 19
  - 3.4.3 The Observables . . . 19

3.4.4 Joint Systems and Composition . . . 19
3.4.5 Astraction and Simplification . . . 20
3.4.6 The Trace . . . 21
3.4.7 Density Matrix . . . 21
3.4.8 The Time Evolution . . . 21
3.4.9 The Probability . . . 21
3.4.10 Pure States . . . 21
3.4.11 Separability and Entanglement . . . 22
3.5 CNOT Gate . . . 22
3.6 Cloning, Pseudo-Cloning, and Pseudo-Measurements . . . 22

4 Quantum Communication **23**
4.1 Teleportation . . . 23
4.1.1 Circuit . . . 24
4.1.2 Quantum Repeaters . . . 24
4.2 Superdense Coding . . . 25

5 Simple Algorithms **25**
5.1 n Qbits . . . 25
5.2 The Secret Mask . . . 26
5.3 Deutsch/Josza Algorithm . . . 28

6 Glossary **30**
6.1 Magnetic Dipole Moment . . . 30
6.2 Singlet . . . 30
6.3 Hilbert Spaces . . . 30
6.4 Hermitian Operator . . . 30
6.5 Unitary Operator . . . 30
6.6 Superposition . . . 30

1 What is Quantum Informatics

1.1 Information and Physics

Experience, observation, and physical discourse are in the form of information. "It from Bit" – John Wheeler

Information representation, processing, and transmission are physical processes. "Information is physical" – Rolf Landauer

The representation of a bit must be physical. Moreover, digitalization comes very naturally with **quantization**. In classical physics, digitalization has to be enforced somehow (e.g., switched).

1.2 Second Law of Thermodynamics

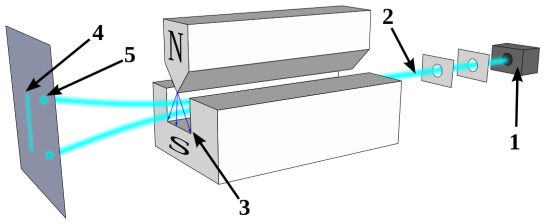
The second law of thermodynamics states that, in a closed system, entropy does not increase.

Entropy can be defined as a measure of disorder. Given n binary memory cells containing random bits, if we erase all of the bits – i.e., set them to 0 – then the entropy in the set of memory cells drops.

1.3 The Stern/Gerlach Experiment

This experiment was proposed in 1921 by Otto Stern and later carried out in 1922 by Walther Gerlach.

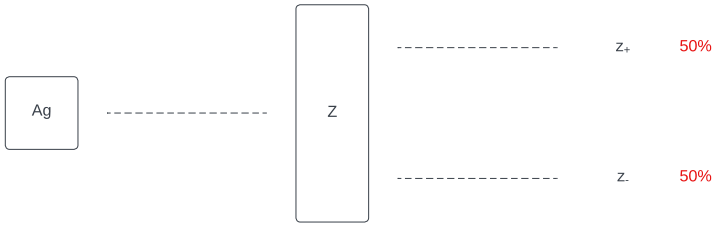
This is one of the most important experiments to understand the structure and properties of the basic building block of quantum information processing, the **Qbit**.



This experiment consisted of the measurement of the **magnetic dipole moment** of silver atoms. These silver atoms are sent as a stream (2) from an oven (1). Each atom is deflected from the path through an inhomogeneous magnetic field (3) and deflected from the path (5). This deflection is proportional to its dipole in the direction of the magnets.

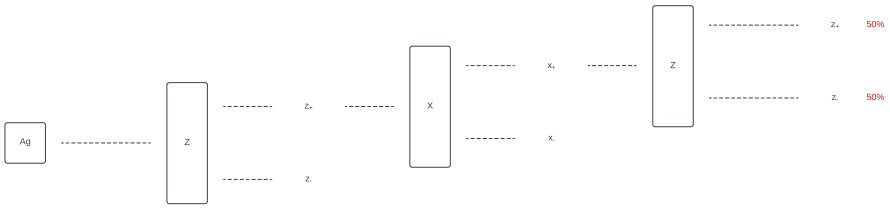
This experiment revealed no detection in the middle of the screen (4) but rather two sharp peaks at equal distances from the center (5). The quantity measured by the experiment is known in quantum mechanics as **spin**.

In the case of a single measurement, for example, in the z-direction, it will result in two identical rays.



If the exact measurement is repeated for only one of the rays – say z_+, then all the atoms are deflected again in the + direction.

Finally, if the magnet is rotated and a x-direction measurement of the z_+ ray is made, another z-direction measurement, a 50-50 distribution. This puts the stability and the independence of the properties in question.



1.4 Superposition

Quantum superposition is a fundamental principle of quantum mechanics. It states that any two – or more – quantum states can be added together, and the result will be another valid quantum state.

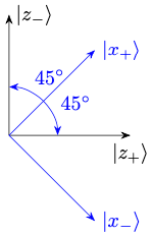
The question of whether a silver atom is in the state $|z_-\rangle$ or in the state $|z_+\rangle$ are complementary to one another. They can be regarded as two answers to the same question – i.e., the Z measurement.

If after performing an X measurement, we want to know whether the silver atom is in a state $|x_+\rangle$ or $|x_-\rangle$. Both are qual superpositions

$$|x_+\rangle = \frac{1}{\sqrt{2}}|z_+\rangle + \frac{1}{\sqrt{2}}|z_-\rangle$$

$$|x_-\rangle = \frac{1}{\sqrt{2}}|z_+\rangle - \frac{1}{\sqrt{2}}|z_-\rangle$$

No matter if we obtain one measurement or the other in the Z measurement, the X-measurement either $|x_+\rangle$ or $|x_-\rangle$ with equal probability. This is also known as a **quantum jump**.



1.5 Quantum Key Distribution

We have seen that we can measure with certainty the same value in two consecutive measurements with the same basis. In other words, the interactions of a system with its environment become traceable. This traceability enables us to detect an eavesdropper in a **quantum cryptographic key agreement protocol**.

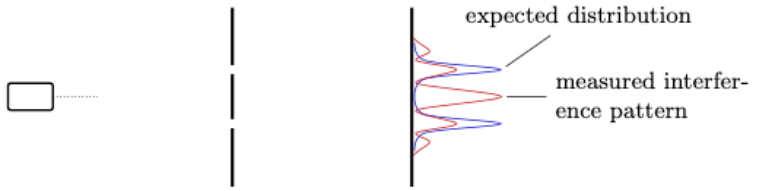
The key distribution starts with *Alice* using random measurements to encrypt the data. The encrypted photons are then sent to *Bob*, which also uses random measurements to try and decrypt the data. After this process has terminated, *Alice* sends the measurement basis she used to *Bob* on a public channel. *Bob* now takes the measurement basis and confronts it with his basis. The equal measurements are used as the **key**.

If an eavesdropper, say *Eve*, tries to intercept the message, she will need to

guess the measurements for each photon. If the measurement is wrong, the system is disturbed. This means that *Eve* has a probability of 1/4 to be wrong in each stage. Thus, there is an almost 100% probability of whether there was an eavesdropper.

1.6 The Double-Slit Experiment

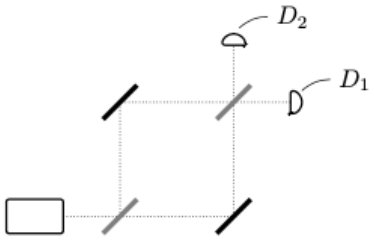
If one shines a light onto a double slit, an interference pattern appears on the screen behind the double slit.



If we were to measure the position of the photons on the screen (to the right of the image), an interference pattern would emerge. This means that single particles exhibit wave properties. However, the interference pattern disappears if we look at the particles' paths.

1.7 The Mach/Zehnder Interferometer

The Mach/Zehnder interferometer can be considered a variant of the double-slit experiment.



If one sends single photons into the interferometer, the interference will occur, and the photons will be detected with certainty in detector D_1.

In each **reflection**, the photon will pick up a phase shift of $\pi/2$. Let us label the state of the photon moving to the **right** as $|1\rangle$, and the state of the photon moving **up** as $|2\rangle$. Their effect on **fully-reflecting mirrors** will then be:

$$|1\rangle \mapsto i|2\rangle \qquad |2\rangle \mapsto i|1\rangle$$

While the effect on **semi-transparent mirrors** is:

$$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle) \qquad |2\rangle \mapsto \frac{1}{\sqrt{2}}(|2\rangle + i|1\rangle)$$

Since we have these linear mappings, we can now track the photon through the interferometer. Since the emitter sends it to its right, the photon will start with a state of $|1\rangle$ –. Then we will have the following when hitting the **first semi-transparent mirror**:

$$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle)$$

Now, the photon encounters a **fully-reflective mirror**, thus we need to apply the mappings to both $|1\rangle$ and $|2\rangle$ of the previous mapping:

$$\frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle) \mapsto \frac{1}{\sqrt{2}}(i|2\rangle + i \cdot i|1\rangle) \mapsto \frac{1}{\sqrt{2}}(i|2\rangle - |1\rangle)$$

Finally, the photon will again encounter a **semi-transparent mirror**. Thus, we will need to apply the mappings to both $|1\rangle$ and $|2\rangle$ again.

$$\begin{aligned}
\frac{1}{\sqrt{2}}(i|2\rangle - |1\rangle) &\mapsto \frac{1}{\sqrt{2}}\left(i\frac{1}{\sqrt{2}}(|2\rangle + i|1\rangle) - \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle)\right) \\
&\mapsto \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(i|2\rangle + i \cdot i|1\rangle) - \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle)\right) \\
&\mapsto \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(i|2\rangle - |1\rangle) - \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle)\right) \\
&= -|1\rangle
\end{aligned}$$

The photon, which now has state $-|1\rangle$, will be measured with certainty by detector D1.

1.8 Quantum Bit

To transfer a bit into the quantum world, we associate 0 and 1 with two orthogonal vectors:

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

A general quantum state can now be written as a superposition:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{with } \alpha, \beta \in \mathbb{C};\ \text{and } |\alpha|^2 + |\beta|^2 = 1$$

Measuring $|\psi\rangle$ in the standard basis will yield:

- 0 – With a probability of $|\alpha|^2$
- 1 – With a probability of $|\beta|^2$

1.8.1 Hadamard Gate

Quantum circuits are composed of quantum gates which are **unitary maps**. The most important gate is the Hadamard gate. Which can be formalized as follows:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Which maps to the following superpositions:

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

Applying the Hadamard gate again will yield the standard basis vectors again.

1.8.2 Square Root of NOT

Another interesting gate is the following:

$$F = \frac{1}{\sqrt{2i}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

When we apply this gate twice, we will obtain:

$$F \cdot F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

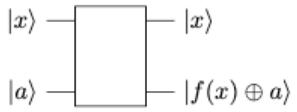
In classical mechanics, no gate yields the not-gate this way. The gate F has thus been called the "square root of NOT".

1.9 Deutsch's Algorithm

Given a function

$$f : \{0, 1\} \to \{0, 1\}$$

We want to find out whether f is constant and $f(0) \oplus f(1)$ is 0 or 1. We would have to query the function twice in classical mechanics to get both answers. But there is another way to find out. First, we must transform the black box into a **quantum black box**. Because of the unitarity of the quantum mechanical time evolution, the quantum box is **reversible**.



This means that, if a is 0, then x is mapped to $|f(x)\rangle$ on the ouput wire. Moreover, if a is 1, then x is mapped to $\overline{|f(x)\rangle}$ – which is the negation of $|f(x)\rangle$.

If we were to put a superposition on the input wire and set a to 0, we would obtain the following combined input:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle)$$

If:

$$|0\rangle \otimes |0\rangle \mapsto |0\rangle \oplus |f(0)\rangle \qquad |1\rangle \otimes |0\rangle \mapsto |1\rangle \oplus |f(1)\rangle$$

Then, by linearly combining the two we obtain:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle \oplus |f(0)\rangle + |1\rangle \oplus |f(1)\rangle$$

The resulting state is said to be **entangled**. This means that we cannot access information about $f(0)$ and $f(1)$ by merely measuring the output wire. However, if we also put a superposition on the second wire

$$|a\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Then we can expand the combined input as:

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ = \; & \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \end{aligned}$$

Applying the gate to each summand, we obtain:

$$\frac{1}{\sqrt{2}}\left(|0\rangle \otimes \left(|f(0)\rangle - \overline{|f(0)\rangle}\right) + |1\rangle \otimes \left(|f(1)\rangle - \overline{|f(1)\rangle}\right)\right)$$

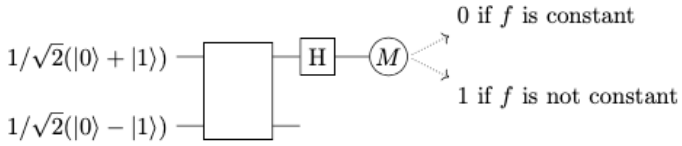
If $f(0) = f(1)$, then:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \left(|f(0)\rangle - \overline{|f(0)\rangle}\right)$$

Otherwise:

$$\pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \left(|f(0)\rangle - \overline{|f(0)\rangle}\right)$$

If we now measure the standard basis of the output – after having applied the Hadamard gate, this will yield:



This algorithm does not allow us to retrieve more information. It does not yield the values of $f(0)$ or $f(1)$. What it yields is the result of $f(0) \oplus f(1)$.

1.10 The Aspect/Gisin/Zelinger Experiments

Quantum information processing is more than the fact that "a pair of Qbits is just one Qbit plus another Qbit". A striking manifestation is that other qualities arise when two entangled Qbits are independently measured.

Imagine that – inside of a preparation center – pairs of Qbits (i.e., polarized photons) are generated and sent onto their respective paths to two parties – *Alice* and *Bob*. What is sent to both *Alice* and *Bob* are two parts of the equal superpositions of $|0\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$. If *Alice* and *Bob* both measure in the standard basis – i.e., $\{|0\rangle, |1\rangle\}$, then they always receive the same output: a **perfect correlation**.

1.10.1 Einstein/Podolsky/Rosen's Claim

These three scientists, in 1935, claimed that quantum theory was **incomplete** and that it must be augmented by some "hidden parameters" that determine the measurement outcomes of all alternative measurements entirely.

1.10.2 Bell's Claim

Bell gave *Alice* and *Bob* more freedom. Now they could do measurements on a standard basis and other orthogonal bases. Bell claimed that EPR (Einstein/Podolsky/Rosen) is in doubt. There exist quantum correlations that go beyond the explanatory power of shared classical information. To prove it, Bell used a **singlet** and made *Alice* and *Bob* make measurements on different bases.

Moreover, Bell discovered that measurement results are correlated; however, this correlation arises only upon measurement – and not before it. This is known as **Bell non-locality**.

2 Information is Physical

A computing device essentially transforms **electrical free energy** into **heat**. If we consider a Turing Machine, even for deterministic TMs, computations are not logically reversible.

2.1 Thermodynamics and Entropy

2.1.1 First Law

The first law of thermodynamics says that the total energy is constant in a closed system. Moreover, a perpetuum mobile of the first kind is impossible.

2.1.2 Second Law

The second law of thermodynamics says that in a closed system, entropy does not decrease. Moreover, a perpetuum mobile of the second kind is impossible.

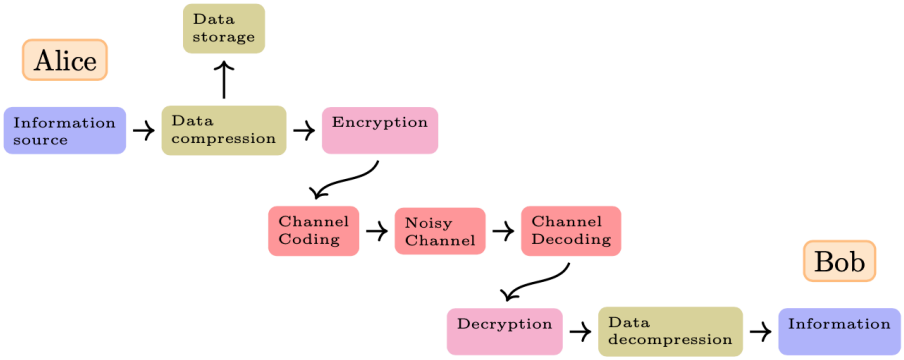
This law is **asymmetric in time**.

2.2 Information Theory

Information theory was developed in 1948 by Claude Shannon to determine the fundamental limits of signal-processing operations such as **data compression on reliable storage** and **communication**.

2.2.1 Standard Model of Communication

Information theory initially focused on communication. In the most common scenario, we have *Alice* and *Bob* sending information to one another.



A model usually contains **compression** to reduce the size of the data representing specific information. **Encryption** is then used to minimize attacks upon information transfer. **Channel coding** is used to introduce redundancy to protect against errors during transmission. Finally, there are all of the counterparts of the previous steps.

2.2.2 The Game of 20 Questions

If we imagine that *Bob* can retrieve a secret by *Alice* just by using 20 yes/no questions.

Since *Bob* from 20 questions can receive 20 answers – 20 bits, this means that he will be able to distinguish between 2^20 different questions.

Assuming that *Alice* chooses an element $x \in X$. *Bob* now wants to determine which element *Alice* has chosen. To do so, one could divide the set X into

subsets of equal size and ask in which one the chosen element was. The number of questions now is:

$$\#Q = \lceil \log_2 |X| \rceil$$

This consideration motivated Hartley's formula for the **entropy of a uniform random variable X** over X (the elements), with

$$P_x(x) = \frac{1}{|X|}$$

And the formula is:

$$H(X) = \log_2 |X|$$

Where the first X is the random variable. Now, **uncertainty becomes a function of a random variable**. *Bob*'s prior knowledge about *Alice*'s choice can be formally described by a pdf (probability density function). For a general random variable, the measure of uncertainty – i.e., the **entropy**, should correspond to the expectation value of the number of yes/no questions to find an element $x \in X$ using an optimal strategy and combining asymptotically many realizations of the random variable X.

2.3 Entropy

The entropy of a random variable X over X, with distribution:

$$P_X(x) = p_x$$

Is given by:

$$H(X) = E[-(\log_2 P_X(x)] = -\sum_{x \in X} p_x \log_2 p_x$$

In the case of a uniform distribution, the **entropy** of a random variable is equal to the size of its range. The **entropy of a macrostate** is the logarithm of the number of microstates that correspond to it.

The **microstate** of a physical system specifies the position and momentum of each of the molecules. The **macrostate** of a physical system is a set of microstates.

In the example above, the probability of going from the state on the left to the state on the right is:

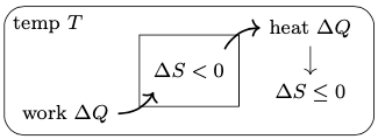
$$2^{-N}$$

Where N is the **number of particles**. Moreover, the entropy difference is:

$$\Delta S = -Nk \ln 2$$

Where N is the **number of particles** and k is the **Boltzmann's constant**. We can say that the right-to-left transition is **probable**, and allows for **gaining work**.

The left-to-right transition can be enforced. For instance, this can be done by pushing a piston. Although in this case, the gas will cease to be in a closed system.



In this case, the amount of entropy in the gas decreases. To compress this gas, we will have to use a certain amount of **free energy**. This energy will then be dissipated into the environment as **heat**.

The minimal investment in terms of free energy to enforce that entropy decreases is:

$$\Delta Q \geq \Delta S \cdot T$$

2.4 Bit Analogy

If we interpret the molecule in the canister as storing one bit – a 0 if it is on the left and a 1 if it is on the right, forcing the molecule to the left would correspond to erasing that bit.

The price for erasing that bit is:

$$kT \ln 2$$

This, together with the claim that it's irrelevant by what physical system the bit is stored, is called **Landauer's Principle**.

2.5 Landauer's Principle

Erasing a bit requires

$$kT \ln 2 \quad (\approx 3 \times 10^{-21} J \text{ at room tempterature})$$

Of free energy. This energy must, in the process, be dissipated into the environment.

2.6 The Converse of Landauer's Principle

The inverse process of erasure, which is **randomization**, allows for the gain of free energy. For example, the amount of environmental heat energy that can be

transformed into work is $kTN \ln 2$ – in the case of an *all-0-string* of length N. Another example is the string of the first N digits of the decimal expansion of π, which is $kTN \log 10$.

The previously defined examples offer the possibility of a logically reversible computation between the given string (for example, the first N decimal digits of π) and the *all-0-string* of the same length.

2.7 Bennett's Solution to Maxwell's Demon

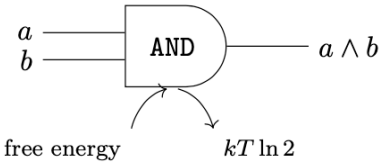
The demon must erase all the information accumulated in its brain during the sorting procedure. The necessary heat dissipation will exactly compensate for the entropy decrease. The demon must have an internal state depending on its observations and guiding its actions.

This does not violate the second law of thermodynamics, as the demon will generate heat whenever it resets its internal memory to a known state. This will result in an entropy decrease and the emission of heat.

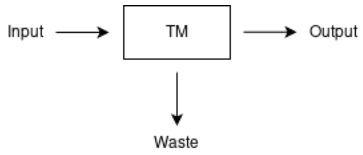
2.8 Reversible Computing

If in the course of computation, information is lost about *which branch the computation came from*, then the free energy $kT \ln 2$ must be invested. This free energy will then be dissipated through the environment. This means that **loss of information** implies **loss of free energy**.

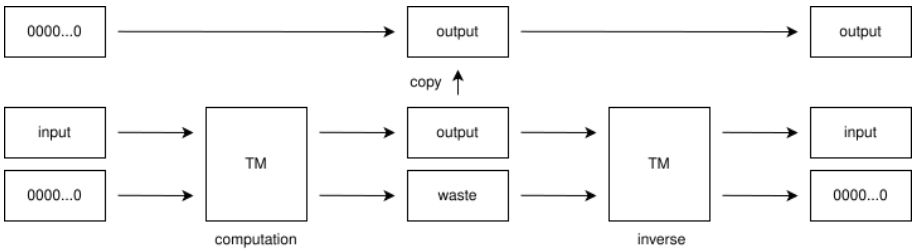
If we consider a classical gate, such as the one below



It is logically irreversible since the output does not allow for a complete reconstruction of the input. A way to make a computation logically reversible would be to use a **history tape** to a Turing Machine for storing the entire path of the computation. This solution, though, is not sustainable. This is because the original state of the history tape is lost and replaced by the waste piled up.



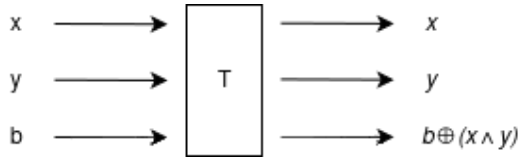
Bennett's idea was to eliminate the waste in an *orderly fashion*. This means that the waste was **uncomputed** instead of erased. Here the output of the computation is copied onto some extra bit positions, and then the computation is undone step by step in reverse order.



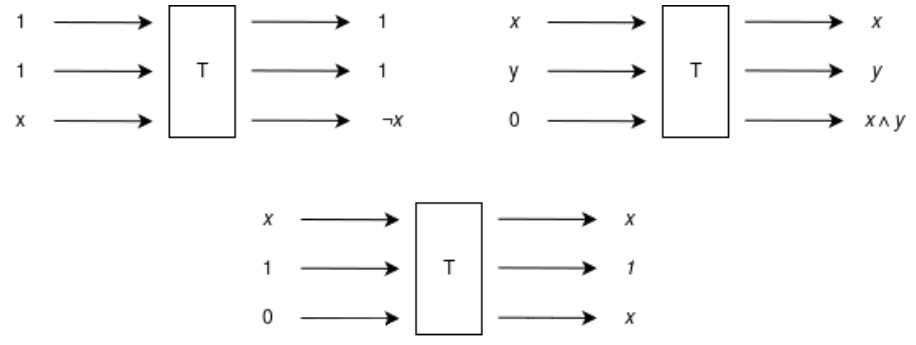
We have seen that any computation can now be made logically reversible. Furthermore, **Friedkin** and **Toffoli** demonstrated that every logically reversible computation could be carried out in a thermodynamically reversible way. This was shown with the elastic collision of balls onto a billiard table. Loss of information is impossible due to the time-reversal symmetry of the laws of classical mechanics.

2.9 Toffoli Gate

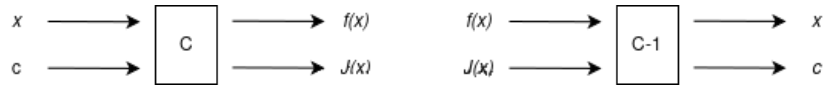
The Toffoli gate is a made-reversible **AND** gate. This is done by adding an output wire for each input wire. This makes sure that the output of the gate contains the input values of the gate. This is the schematic for the **Toffoli Gate**:



The Toffoli gate is **universal**. This means that any circuit can be translated into a Toffoli gate. This follows from the possibility to get – from one Toffoli gate each – the **NOT**, **AND**, and **FAN-OUT**.



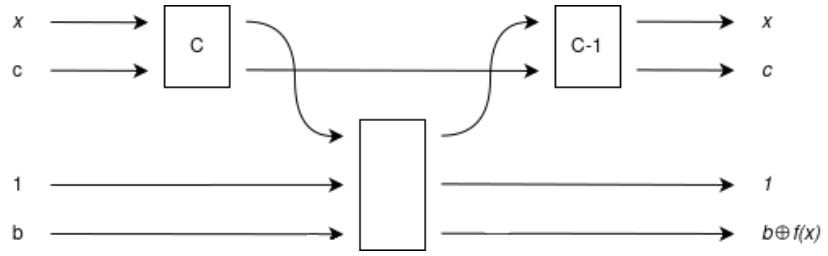
To remove the **junk** from a circuit, we can now use the following two gates:



Bennett's trick to uncompute the junk is the following:

1. Apply C
2. The output we want is copied using the Toffoli gate
3. Use C^{-1} to uncompute the junk

The following is the visual representation of such circuit:



From this, we can conclude that the best reversible circuit is half as efficient as its irreversible counterpart.

3 Key Experiments and Postulates of Quantum Physics

The **UV catastrophe of black body radiation** and the **photoelectric effect** lead to the development of quantum physiscs.

3.1 Black-Body Radiation

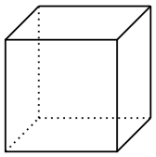
3.1.1 Classical Mechanics

In classical statistical mechanics, the **law of equipartition** expresses the idea that, in thermal equilibrium, energy is usually shared over all possible corresponding microstates. If we assume the head to be transferred by electromagnetic waves, the equipartition law leads to problematic consequences.

Let's imagine the following, we have a **cubic vacuum** with side length l. This vacuum has the following properties:

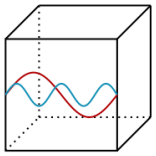
- It absorbs and emits all radiation frequencies

- It is in thermodynamic equilibrium with its environment, in a heat bath of temperature T



The thermal electromagnetic radiation within this body can be thought of as **standing waves** within the body. Generally, a **standing wave** is a superposition of three standing waves, each corresponding to one spacial direction. Thus, a wave can be described by a three-dimensional vector of positive integers

$$\overrightarrow{n} = (n_1, n_2, n_3) \in (\mathbb{N}_{>0})^3$$

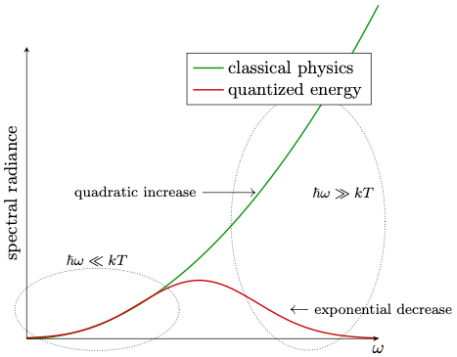


If we consider a shell of radius $|\overrightarrow{n}|$, then the number of waves scales with the scaling of the shell. This means that the number of waves also becomes $|\overrightarrow{n}|^2$. Likewise, the energy density scales with the square of the frequency

$$\omega = c\pi\frac{|\overrightarrow{n}|}{l}$$

This growth in energy is referred to as **ultraviolet catastrophe**. This is absurd since, for instance, if we take a classroom at room temperature, everyone in it would drop dead immediately due to the intensity of the X-rays.

For lower frequencies of waves, the quadratic dependence of the spectral radiance on the frequency matches experimental findings – the **Rayleigh-Jeans Law**. In the case of higher frequencies, the spectral radiance exponentially decreases again.



3.1.2 Quantum Mechanics

Max Plank discovered that the probability of emission and absorption of the cube would exponentially decrease at higher frequencies. He assumed that the radiation energy to be absorbed and emitted multiplies $\hbar\omega$, where $\hbar = 1.054 \times 10^{-34} Nms$. The probability of emission or absorption decreases exponentially in

$$\frac{\hbar\omega}{kT}$$

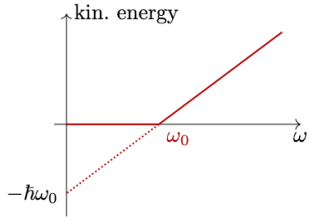
In particular, the probability falls off exponentially for higher frequencies.

3.2 Photoelectric Effect

3.2.1 Classical Mechanics

By examining the emission of electrons from a metal surface if a light is shone onto it, the expectation was that the velocity of the emitted electrons faster depends on the intensity of the light but is independent of the frequency of the light – i.e., its color.

However, from experimental findings, Hertz found out that the intensity of the light merely changed the number of electrons. By increasing the frequency of the light, the velocity of the electrons increased. Below a specific frequency ω_0, there were no emitted electrons, whatever the intensity or the duration of shining the light onto the surface.



3.2.2 Quantum Mechanics

Alber Einstein explained the behavior observed by Plank. Einstein regarded light as a quantized packet of a certain frequency-dependent energy. Light comes in packets of $\hbar\omega$ energy. If the frequency is lower than ω_0, then the energy lies below the energy $W = \hbar\omega_0$ needed to remove the electrons from the metal. Thus, the kinetic energy of the electron becomes

$$E_{kin} = \hbar\omega - W$$

This shows the fundamental dualism in quantum mechanics, the **wave-particle dualism**.

3.3 Wave-Particle Dualism

We now examine the wave-particle dualism by using the example of a plane wave:

$$\psi(\overrightarrow{x}, t) = C \cdot e^{i(\overrightarrow{k} \cdot \overrightarrow{x} - \omega t)}$$

Where $\overrightarrow{k}$ is the **wave vector** – which is perpendicular to the wavefront. The relation between the wavelength and the wave vector is:

$$\lambda = \frac{2\pi}{|\overrightarrow{k}|}$$

The **period** of the wave – i.e., the time that elapses between the passage of two wavefronts – is:

$$\Delta t = \frac{2\pi}{\omega}$$

The **phase velocity** – i.e., the velocity of the wavefront – is:

$$v = \frac{\omega}{|\overrightarrow{k}|}$$

If we examine the partial derivative of the plane wave, we obtain:

$$\frac{\partial}{\partial t}\psi(\overrightarrow{x}, t) = -\frac{\hbar^2}{2m}\Delta\psi$$

Which directly corresponds to the **Shrödinger equation of a free particle**.

$$i\hbar\frac{\partial}{\partial t}\psi = -\frac{\hbar^2}{2m}\Delta\psi$$

3.3.1 Schrödinger's Equation

The Schödinger equation of a free particle has two fundamental properties:

- **It is linear**
  Any linear combination of solution of the Schrödinger equation

  $$\psi(\overrightarrow{x}, t) = \alpha\psi(\overrightarrow{x}, t) + \beta\psi(\overrightarrow{x}, t) \qquad \forall\alpha, \beta \in \mathbb{C}$$

  Will again yield a solution.

- **It preserves the inner product**
  This means that a solution can be written as

  $$\psi(\overrightarrow{x}, t) = U(t)\psi(\overrightarrow{x}, 0)$$

  Thus, the **time evolution operator** is unitary. This also implies that the **time evolution in quantum mechanics is reversible**.

3.4 Postulates of Quantum Theory

The postulates of quantum mechanics form the axiomatic basis of the theory.

3.4.1 The State

In quantum mechanics, a system (e.g. an electron, a photon, or an atom) is assigned a **normalized state vector** in a complex Hilbert space:

$$\psi(\overrightarrow{x}, t) \in H \qquad \text{with } ||\psi|| = 1$$

3.4.2 The Time Evolution

The time evolution of a quantum state is governed by the **Schrödinger equation**:

$$\frac{\hbar}{i}\frac{\partial \psi}{\partial t} = H\psi$$

3.4.3 The Observables

In quantum mechanics, measurable entities correspond to observables. These are Hermitian operators A with $A^\dagger = A$. More generally, **any Hermitian operator is an observable**.

The **spectral theorem** for finite-dimensional linear operators states that an operator A has a spectral decomposition with real eigenvalues if and only if the operator is Hermitian. Thus, an observable – which is Hermitian by definition – has a corresponding spectral decomposition.

From the spectral decomposition, we obtain the weighted sum over all possible results of the measurement corresponding to A.

3.4.4 Joint Systems and Composition

Any linear combination in any of the subspaces corresponds to a linear combination in the joint space. This is an essential characteristic of the **tensor product**. Given two Hilbert spaces H_A and H_B, the joint system has a state-space that is isomorphic to the tensor product of the Hilbert spaces – $H_A \otimes H_B$.

If the systems are in **pure states** $\psi_A \in H_A$ and $\psi_B \in H_B$, then the joint state becomes:

$$\psi_A \otimes \psi_B \in H_A \otimes H_B$$

However, any superposition of such product states is also a state in the joint Hilber space, and such superpositions may not have a representation as a product. Such states are said to be **entangled**.

3.4.5 Astraction and Simplification

If we assume the Hilbert space to be finite-dimensional, then this Hilbert space is isomorphic to an n dimensional complex vector space $H \cong \mathbb{C}^n$. With this assumption, the states can be expressed by coordinates with respect to some fixed basis.

For $\varphi \in H \cong \mathbb{C}^n$, we call the corresponding vector **ket** of φ, and represent it as:

$$|\varphi\rangle = \begin{bmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \\ \varphi_n \end{bmatrix}$$

Similarly, a **bra** is the conjugate transpose of a **ket**.

$$\langle\varphi| = |\varphi\rangle^\dagger = \begin{bmatrix} \overline{\varphi}_1 & \overline{\varphi}_2 & \cdots & \overline{\varphi}_n \end{bmatrix}$$

Now, we can write the inner product as:

$$(\varphi, \psi) = \begin{bmatrix} \overline{\varphi}_1 & \overline{\varphi}_2 & \cdots & \overline{\varphi}_n \end{bmatrix} \begin{bmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \\ \varphi_n \end{bmatrix} = \langle\varphi|\psi\rangle \in \mathbb{C}$$

This is known as **Dirac's Bra-ket notation**. This notation is useful in expressing Hamiltonian observables. For example, the effect of an observable A on a vector ψ, can be expressed as:

$$|A\psi\rangle = \sum_i \lambda_i |P_{\varphi_i}\psi\rangle = \sum_i \lambda_i |\varphi_i\rangle\langle\varphi_i||\psi\rangle = \sum_i \lambda_i |\varphi_i\rangle\langle\varphi_i|$$

Where $|\varphi_i\rangle\langle\varphi_i|$ is the common way to represent a **projector**. A linear operator on a finite-dimensional vector space can be represented with a fixed basis as a matrix. In Dirac's notation, we can abbreviate the basis vector to their indices ($|\varphi_i\rangle =: |i\rangle$), this reads as:

$$A = \sum_{k,l} \langle k|A|l\rangle |k\rangle\langle l|$$

Where $\langle k|A|l\rangle$ is the **matrix entry** of the k-th row and the l-th column. A property of the bra-ket notation is that:

$$\sum_i |i\rangle\langle i| = \mathbb{1}$$

3.4.6 The Trace

The trace is an important linear map $End(\mathcal{H}) \to \mathbb{C}$ defined as the sum over the diagonal elements of the matrix corresponding a linear operator $A \in End(\mathcal{H})$.

$$Tr(A) := \sum_k \langle k|A|k\rangle$$

3.4.7 Density Matrix

A density matrix represents a statistical mixture of states. This matrix is defined as ρ and is a positive trance-one operator. So ρ is both Hermitian and all its eigenvalues are positive and sum to one.

$$\rho = \sum_i \lambda_i |\varphi_i\rangle\langle\varphi_i|$$

$$\sum_i \lambda_i = 1$$

The eigenvalues can be regarded as probabilities for the system to be in the state of the corresponding eigenvector.

3.4.8 The Time Evolution

The time evolution of density matrices derives from the unitary propagator

$$U(t) = e^{iHt/\hbar}$$

To be:

$$\rho(t) = U(t)\rho(0)U^\dagger(t)$$

3.4.9 The Probability

The probability of obtaining the result λ_i when measuring an observable A is:

$$P(\lambda_i) = Tr(|\varphi_i\rangle\langle\varphi_i|\rho)$$

Where φ_i is the **eigenvector** corresponding to the eigenvalue λ_i of A.

3.4.10 Pure States

The density matrices with no uncertainties – which are those with eigenvalues corresponding to a deterministic probability distribution – are the **projectors** on $\mathcal{H}$.

3.4.11 Separability and Entanglement

States of a joint system $H_A \otimes H_B$ that can be written as a product

$$\psi = \varphi_A \otimes \varphi_B$$

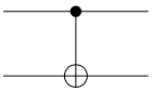
are called **separable**. On the other hand, states that are not separable are called **entangled**. Let's consider the entangled **singlet** state:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

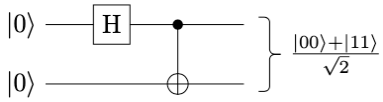
This state is a **superposition** of pure states, thus a pure state itself. On the contrary, density matrices are convex combinations of **projectors** – unless we are dealing with the special case of a pure density matrix.

3.5 CNOT Gate

The CNOT gate can be seen as a made-reversible XOR. The schematics for such a gate is:



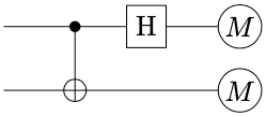
The CNOT can generate **entanglement**:



This combination between the Hadamard gate (which puts the input in superposition) and the CNOT (which, combined with the Hadamard, generates an entangled state) is a change of basis between the standard basis and the **Bell basis**. The Bell basis is the following:

$$\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$$

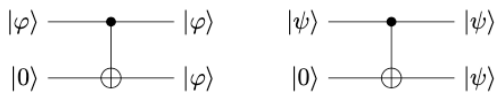
In particular, the following is a **Bell measurement**:



3.6 Cloning, Pseudo-Cloning, and Pseudo-Measurements

To copy classical bits, we can use the CNOT gate. If the source is 0, then the CNOT gate does the following:

In the case of CNOT gates with $|0\rangle$ as a source, we can see that it also allows for **cloning** quantum information.



Only **parallel** and **orthogonal** states can be cloned by the CNOT. The cloning operation is not unitary, hence not allowed by quantum theory. This is known as the **no-cloning theorem**. The CNOT does not clone quantum states; it generates superpositions. This is why the action of the CNOT is sometimes referred to as **pseudo-cloning**.

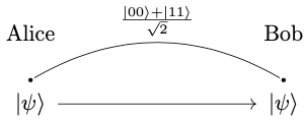
The CNOT can also be seen as a **pseudo-measurement** since there is no outcome. Moreover, because it is reversible, the CNOT is an **involution** – i.e., a self inverse.

4 Quantum Communication

4.1 Teleportation

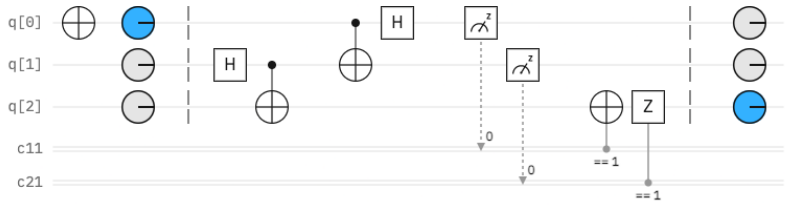
An object is said to be teleported from point A to point B if it is first at A and at the end at B. However, the object must have never been anywhere in between A and B. Moreover, the transfer does not have to be instantaneous – as this would contradict relativity.

Teleportation allows for carrying over the ability to transmit quantum information between two parties to a later point in time – when only a classical channel is available. A priori, sending an unknown quantum state over a classical channel is **impossible**. If, however, the parties additionally both share entanglement, then it **becomes possible**.



4.1.1 Circuit

The teleportation circuit is the following:



As we can see from the diagram above, the Qbit $|1\rangle$ at state `q[0]` – which represents $|\varphi\rangle$ (i.e., the Qbit that Alice needs to send to Bob) – has been teleported to `q[2]` – which represents Bob.

In the **first step** of the circuit – Hadamard + CNOT – an entangled pair of Qbits is created and given to Alice (`q[1]`) and Bob (`q[2]`). In the **second step** of the circuit – CNOT + Hadamard – we prepare for a Bell measurement, which is done in **step three**. The two measurements are saved to two classical registers – `c11` and `c21`. In **step four**, the final step, Bob now measures the bits sent by Alice. Bob, to read them, applies the transformation

$$X^{b_1} Z^{b_2}$$

Where X is a **X-pauli gate** (i.e., a negation), Z is a **Z-Pauli gate** (i.e., a conditional phase flip), b_1 is the **bit on the `c21` classical register** (sent to Bob by Alice), and b_2 is the **bit on the `c11` classical register**. The transformations will only occur if the classical bit is equal to 1 (as we can see in the circuit above).

4.1.2 Quantum Repeaters

The main application of teleportation are **quantum repeaters**, which allow something called **entanglement-swapping**. There exist some device-independent cryptographic protocols. For these protocols, no trust in manufacturers and no correctness of quantum theory are required.

The protocols are based on the parties sharing maximally entangled states. Such entanglement is complicated to establish over long distances. This is because the further the particles are transported, the more likely it is that they interact with the environment, thus losing their initial entanglement.

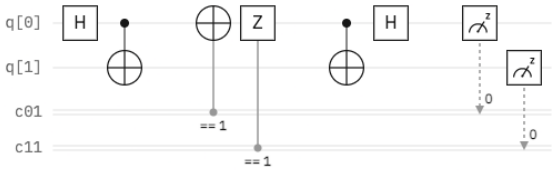
If Alice and Bob are too far away from each other, we can use Charlie – who is in between them – to establish a **singlet** with both Alice and Bob. A property of teleportation is that if part of the entangled state is sent, then this entanglement is preserved. Charlie acts as a **quantum repeater**.

In this cryptographic context, a downside of the **quantum repeater** is that the inner node – i.e., the repeater – must be trusted.

4.2 Superdense Coding

The scenario of superdense coding is the exact opposite of that of teleportation. In the case of teleportation, we use two classical bits to transport one Qbit. On the other hand, in the case of superdense coding, we transmit two bits using one Qbit.

The circuit is the following:



In the **first step** of the circuit – Hadamard + CNOT – an entangled pair of Qbits is created and given to Alice (`q[1]`) and Bob (`q[2]`). In the **second step** – X-Pauli + Z-Pauli – we encode the two classical bits. To encode these bits we use the following transformation:

$$X^{b_1} Z^{b_2}$$

Where b_1 and b_2 are the **classical bits**. This transformation is the same as the one done in the teleportation. We prepare for a Bell measurement in the **third step** of the circuit – CNOT + Hadamard. In **step four**, the final step, we perform the measurement – i.e., decoding the originally sent bits.

5 Simple Algorithms

5.1 n Qbits

The state space of systems of n Qbits is the n-fold tensor product of $\mathbb{C}^2$ with itself:

$$\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \equiv \mathbb{C}^{2^n}$$

A basis of the space is given by the classical basis characterized through the set of all **classical** n-bit strings:

$$\{|i\rangle \mid i \in \{0,1\}^n\}$$

The action of the n-fold, bitwise, **Hadamard transform** is:

$$H^{\otimes n}|i\rangle = \bigotimes_{l=1}^{n} \left(\frac{|0\rangle + (-1)^{i_1}|1\rangle}{\sqrt{2}} \right) = \frac{1}{2^{n/2}} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} |j\rangle$$

Where the product $i \cdot j$ is defined as:

$$i \cdot j := \bigotimes_{k=1}^{n} = i_k \wedge j_k$$

The product is always 0 if **one** of the two strings is the all-zero string 0. This means that the Hadamard applied to this vector has only plus signs. **This is the equal superposition of all classical states and will be the input for all quantum algorithms**. This is known as **quantum parallelism**. The state $|0\rangle$ also always has a positive sign.

5.2 The Secret Mask

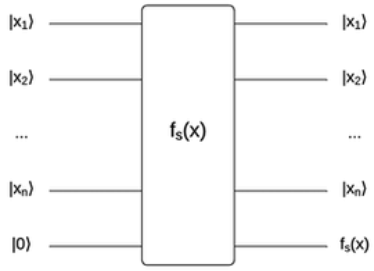
Let $s \in \{0,1\}^n$. Then f_s is the function from n bits to 1 bit:

$$f_s := s \cdot x = \bigotimes_{i=1}^{n} (s_i \wedge x_i)$$

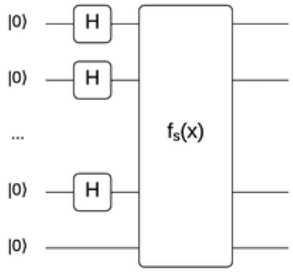
To find out s, one must make exactly n queries. This algorithm is **optimal**, and only one bit of information per query is learned. The above function is for classical circuits; this cannot be directly translated to a quantum circuit. This is because classical circuits are **non-reversible**. Thus we need another function $\tilde{f}_s$, that is reversible:

$$\tilde{f}_s(x, b) = (x, b \oplus f_s(x))$$

This reversible function can now be represented as a reversible quantum circuit:



It can be queried with the equal superpositions of classical inputs. This can be obtained by applying an Hadamard gate to each input wire – except the last one.

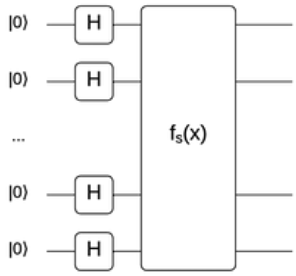


The joint input of the output wires is now:

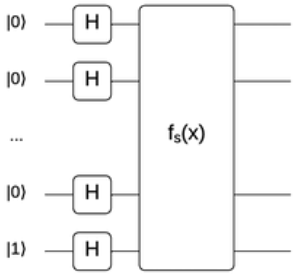
$$\frac{1}{2^{n/2}} \sum_j (|j\rangle \otimes |f_s(j)\rangle)$$

This is **quantum parallelism**. This means that a single execution of the circuit allows for generating a state containing the function value for all inputs simultaneously. Though, such parallelism alone is not very helpful.

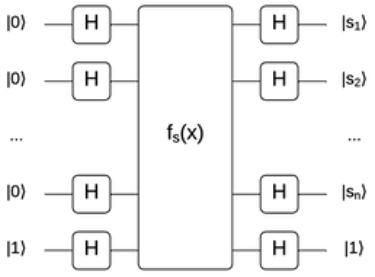
To improve the circuit, let's add a Hadamard to the last wire:



Now the circuit acts as the identity and thus cannot be of any help. For this reason we flip the last state from $|0\rangle$ to $|1\rangle$. By doing so, the addition of the mapping becomes a subtraction, which is not commutative. The circuit becomes:



For the given function, the sign factor equals to $(-1)^{j \cdot s}$, and all the n Qbits are in the state $H^{\otimes n}|s\rangle$. Thus, if we apply H again, this will yield $|s\rangle$ on the first n Qbits.



The initial problem can be solved with one single call to the above quantum circuit. This algorithm combines the following two tricks:

1. **Quantum Parallelism**
2. **Phase Kick-back**
   When the state input on the result wire is $H|1\rangle$, then the function's output is encoded in a phase factor of the state of the input wires.

5.3 Deutsch/Josza Algorithm

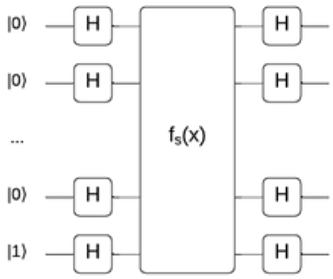
Let

$$f \ : \ \{0,1\}^n \rightarrow \{0,1\}$$

Together with the promise that f is either **constant** – i.e., $f \equiv 0$ or $f \equiv 1$, or **balanced** – i.e., $|\{x|f(x) = 0\}| = |\{x|f(x) = 1\}| = 2^{n-1}$ The circuit needs to decide whether f is **constant** or **balanced**. Given a classical circuit, the number of calls would be in the order of:

$$\frac{2^n}{2} + 1$$

In the case of the quantum circuit, we would need only 1 call. The quantum circuit is the following:



The state after the first Hadamard gate is:

$$\frac{1}{2^{n/2}} \sum_j |j\rangle \otimes H|1\rangle$$

The state, after the f-gate, then becomes:

$$\frac{1}{2^{n/2}} \sum_j (-1)^{f(j)} |j\rangle \otimes H|1\rangle$$

The final n-fold Hadamard gate is applied to this state. The probability amplitude of only the output state $|000\ldots0\rangle$ is equal to:

- 0 - if f is **balanced**

- 1 - if $f \equiv 0$ – i.e., **constant**
- -1 - if $f \equiv 1$ – i.e., **constant**

This means that the output is **always** measured when f is **constant**, but **never** when the function is **balanced**.

6 Glossary

6.1 Magnetic Dipole Moment

The magnetic dipole moment is a vector that represents the strength and orientation of a magnet or other object that produces a magnetic field (e.g., an electron).

6.2 Singlet

A singlet is a maximally-entangled state. However, this one has nicer transformation properties differently from other maximally-entangled states. For instance, a singlet written with respect to a general basis has the same form as the standard basis.

6.3 Hilbert Spaces

The Hilbert spaces are the state spaces of quantum-mechanical systems. Quantum informatics happens in finite-dimensional Hilbert spaces – while, in general, they can be infinite-dimensional.

For a given dimension, there exists **exactly one** Hilbert space.

6.4 Hermitian Operator

A linear operator is said to be self-adjoint or Hermitian if and only if

$$A^\dagger = A$$

6.5 Unitary Operator

A linear operator is said to be unitary if and only if

$$U \cdot U^\dagger = 1$$

6.6 Superposition

Any convex combination of state vectors:

$$\alpha\psi_1 + \beta\psi_2 \in H \qquad \alpha, \beta \in \mathbb{C} \text{ with } |\alpha|^2 + |\beta|^2 = 1$$

Is again a vector associated with a state of the system. Correspondingly, this linear structure of the state space gives rise to the interference effects and, generally, the wave characteristics of quantum mechanics.