Classical Computing and Classical Information

The Bit

The fundamental unit of information is the bit. The term bit was introduced by Claude Shannon in 1948. It was a contraction of "binary information digit". A bit is the smallest nontrivial unit of information.

A bit b has two possible states. Generally, this is represented as

$$b \in \{0, 1\} \simeq \{\text{True},\ \text{False}\} \simeq \mathbb{Z}/2\mathbb{Z}$$

Sometimes thinking of a bit as true/false is helpful.

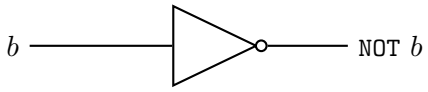
Importantly, we can have a list of several bits. A string s (of length n) is an ordered tuple of n-bits. This is expressed as a cartesian product

$$s \in \{0, 1\}^n \simeq (\mathbb{Z}/2\mathbb{Z})^n$$

Logic Gates and Bit Operations

We can perform operations on bits. We will express these as logic gates. If you've done propositional logic in a philosphy or math class, this is the same system just with different notation.

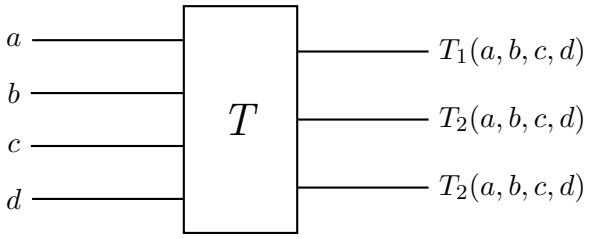
We start with the unary gates. These take one bit as input and return one bit. Here is a `NOT` gate:



It takes 0 to 1 and 1 to 0. It can be defined by the truth table:

0	1
1	0

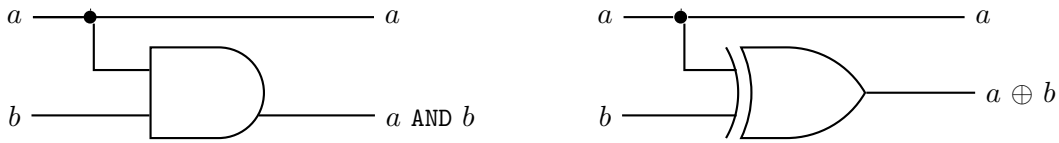
There are in fact 4 unary gates, one for each of the 4 truth tables. Writing them out is a good exercise. Importantly More generally, the logic of any circuit is nothing more or less than a truth table. Here is an arbitary circuit:



In this case $T : \{0,1\}^4 \to \{0,1\}^3$ takes as input 4 bits and returns 3 bits. I use the variable T to emphasize that could be thought of as a truth table.

There are two-bit gates `AND` and `XOR`. The fancy symbol here $\oplus$ means `XOR`. It gets a special symbol because it has the special property of being linear.

I should mention that you can build any arbitrary circuit using `AND` and `NOT`. Here are two examples, `Controlled AND` and `Controlled XOR`



The second one, `Controlled XOR` is *reversible*. If we apply it twice, we get the identity. Such gates are classically important because they don't add entropy and thus generate less heat.

Quantum Computing and Quantum Information

The Qubit

Background: Just as the bit is the fundamental unit of information, the qubit is the fundamental unit of quantum information. It represents the state of a 2 state quantum mechanical system (the simplest nontrivial quantum system)

A classical bit is either 0 or 1. A qubit is a pair of complex numbers

$$(\alpha, \beta) \in \mathbb{C}^2$$

satisfying the condition

$$|\alpha|^2 + |\beta|^2 = 1$$

Importantly, $\mathbb{C}^2$ is a 2-dimensional vector space and so it has a basis. There is o

$$\left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$$

which we will call $|0\rangle$ and $|1\rangle$, using the physics notation.

Why does it live in $\mathbb{C}^2$? That's what the physicists tell me.
This does raise an issue though. $\mathbb{C}^2$ is a continuous vector space. This means that we couldn't even write down the state of a qubit in a finite number of classical bits.