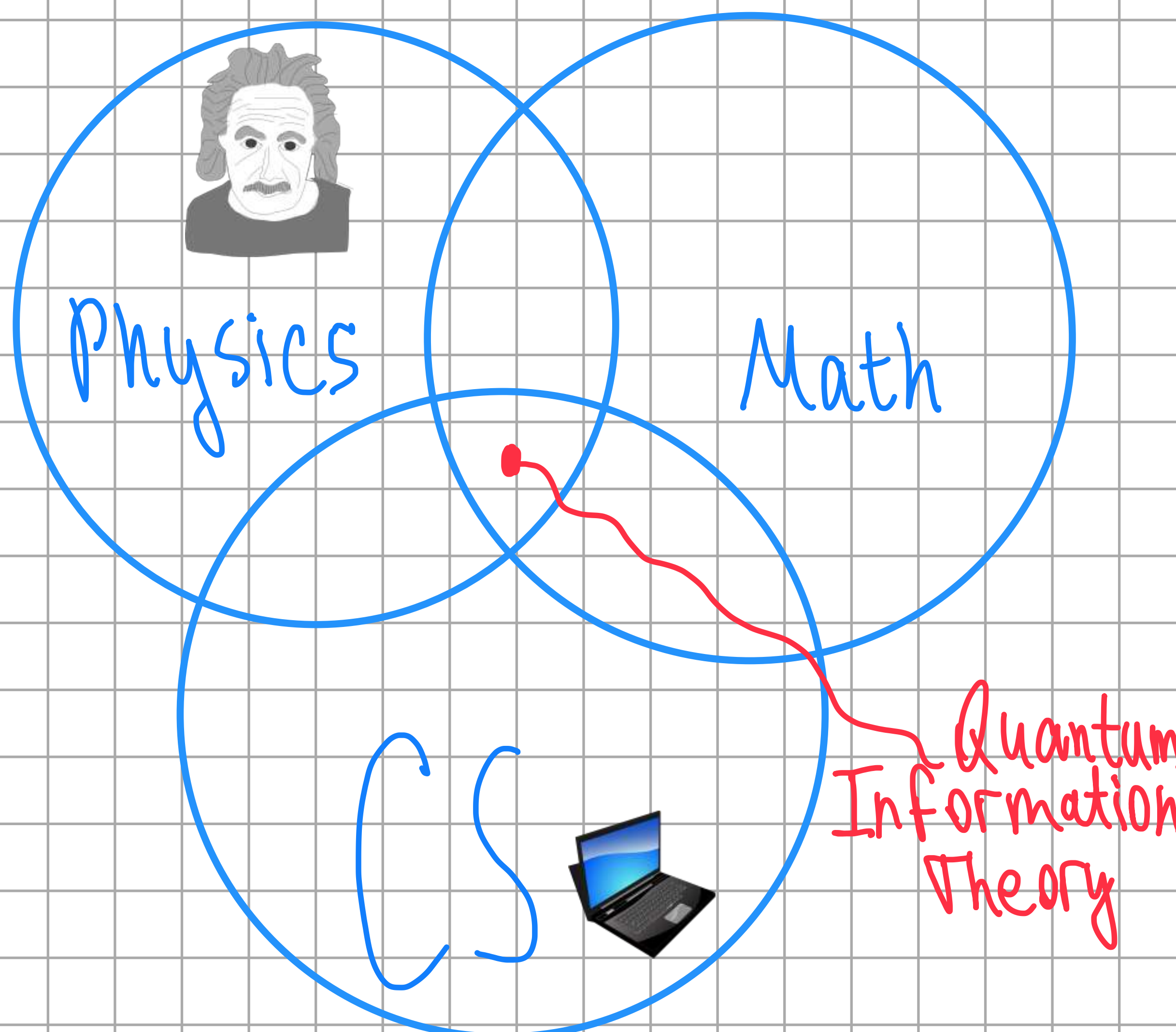
Lectures 1-5.



Boolean circuits.

Let $\mathbb{B} = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$.

Def-n. A **Boolean function** is a map

$$f: \mathbb{B}^n \longrightarrow \mathbb{B}$$

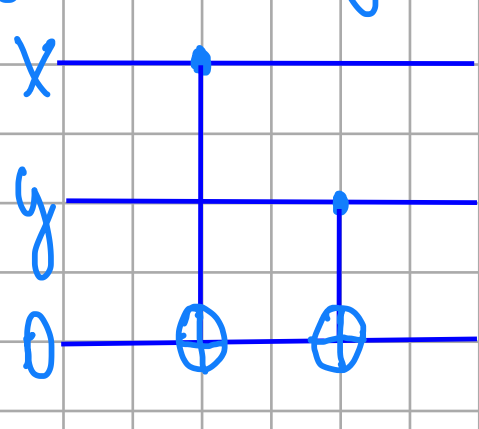
Let $\mathcal{A}$ be a fixed collection of Boolean functions. A circuit C over $\mathcal{A}$ is a sequence of applications of functions in $\mathcal{A}$ to input (and auxiliary) variables. The value of the last auxiliary variable is called the *result of the computation*.

Def-n. A circuit C with input variables $x_1, \ldots, x_n$ *computes* a Boolean function $F: \mathbb{B}^n \to \mathbb{B}$ if the result of computation coincides with the value of F on any collection of input values.

Examples.

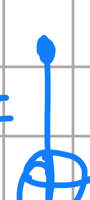
① $F: \mathbb{B}^2 \to \mathbb{B}$, $F(x,y) = x \oplus y$ (XOR)

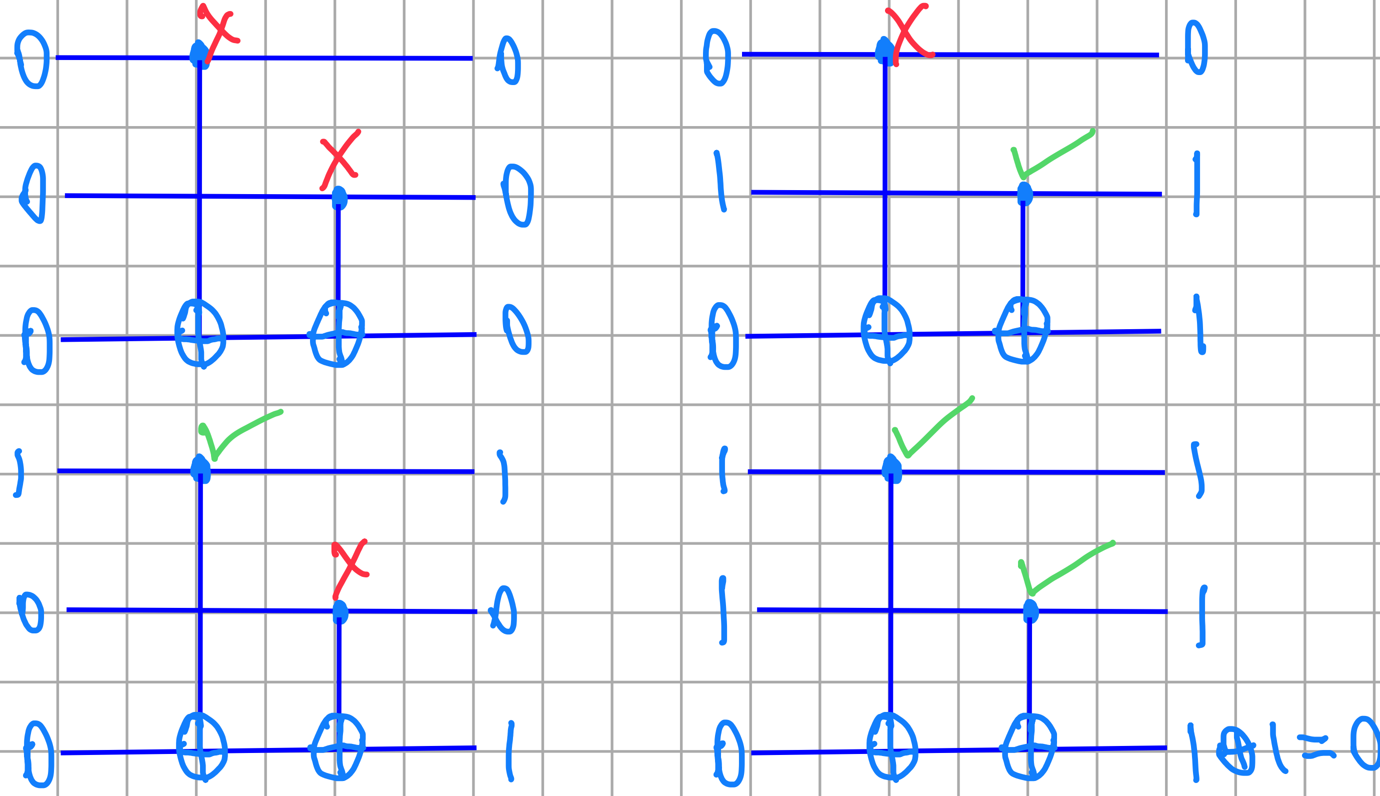
x/y	0	1
0	0	1
1	1	0



Circuit computing F

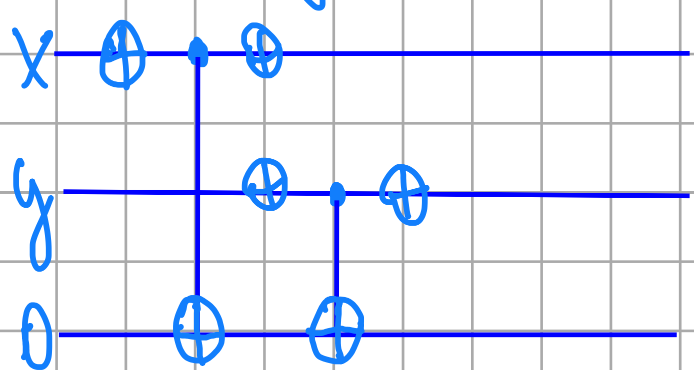
$NOT = \oplus : \mathbb{B} \to \mathbb{B}$, $0 \mapsto 1$, $1 \mapsto 0$

CNOT =  $: \mathbb{B}^2 \to \mathbb{B}^2$ $(0,0) \mapsto (0,0)$, $(0,1) \mapsto (0,1)$, $(1,0) \leftrightarrow (1,1)$



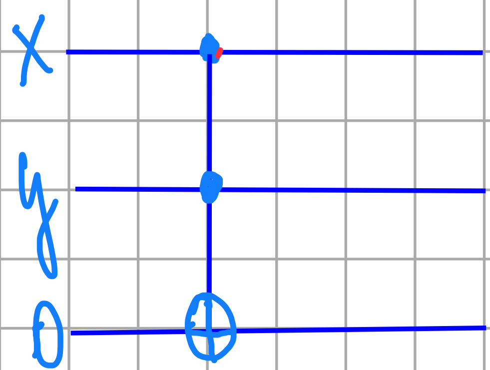
<u>Remark:</u> the circuit computing F is not unique.

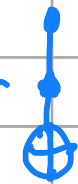
<u>Exercise:</u> check that the circuit below computes $x \oplus y$ as well.



② $G(x,y) = x \cdot y$

x/y	0	1
0	0	0
1	0	1



CCNOT =  : $\mathbb{B}^3 \to \mathbb{B}^3$,

$(x,y,z) \to (x,y,z)$ if $(x,y) \neq (1,1)$

$(1,1,0) \leftrightarrow (1,1,1)$.

Circuit computing G.

<u>Def-n.</u> A collection of functions $\mathcal{A}$ is called a <u>complete basis</u> if for any Boolean function F there exists a circuit over $\mathcal{A}$ that computes F.

<u>Example/Theorem.</u> $\mathcal{A} = \{AND, OR, NOT\}$ is a complete basis.

AND ($\wedge$) : $\mathbb{B}^2 \to \mathbb{B}$ (same as G above).

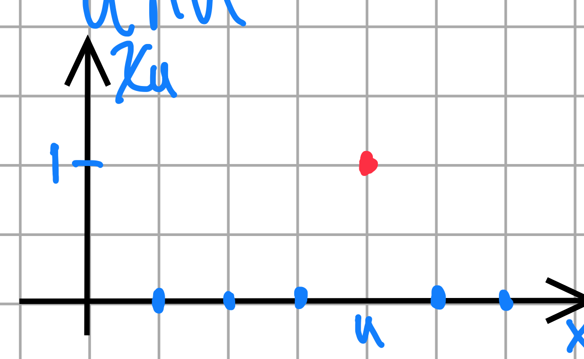
OR ($\vee$) : $\mathbb{B}^2 \to \mathbb{B}$

$$x \vee y = \begin{cases} 1, & (x,y) \neq (0,0) \\ 0, & (x,y) = (0,0) \end{cases}$$

NOT ($\neg$) : $\mathbb{B} \to \mathbb{B}$, $\neg x := 1 - x$.

<u>Proof.</u> Let $u = (u_1, u_2, \dots, u_n) \in \mathbb{B}^n$ and

$$\chi_u(x) = \begin{cases} 1, & u = x \\ 0, & u \neq x \end{cases}$$



Strategy.

Step 1. Realize χ_u for every $u \in \mathbb{B}^n$ as a 'composition' of AND, OR and 'NOT operators.

Step 2. Realize any f-n $f: \mathbb{B}^n \to \mathbb{B}$ as a 'composition' of χ_u's, AND, OR, NOT operators.

The execution of Step 1 in general case is one of the HW exercises. We give an example.

$$\chi_{11\ldots1} = x_1 \wedge x_2 \wedge \ldots \wedge x_n, \quad \chi_{00\ldots0} = \neg x_1 \wedge \neg x_2 \wedge \ldots \wedge \neg x_n$$

The second step is straightforward: f is a 'union' (OR) of the characteristic functions of the elements on which it attains 1 ('True').

Example. $f: \mathbb{B}^3 \to \mathbb{B}$.

$$f(100) = f(011) = f(000) = 1$$

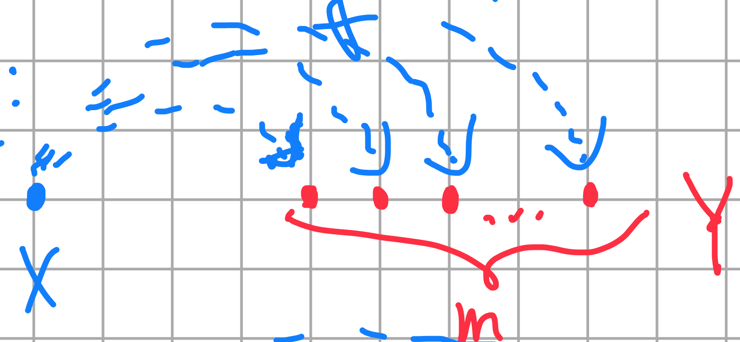
$$f(x) = 0, \quad x \notin \{100, 011, 000\}.$$

$$f = \chi_{100} \vee \chi_{011} \vee \chi_{000}.$$

Let X and Y be finite sets with $|X|=n$ and $|Y|=m$.

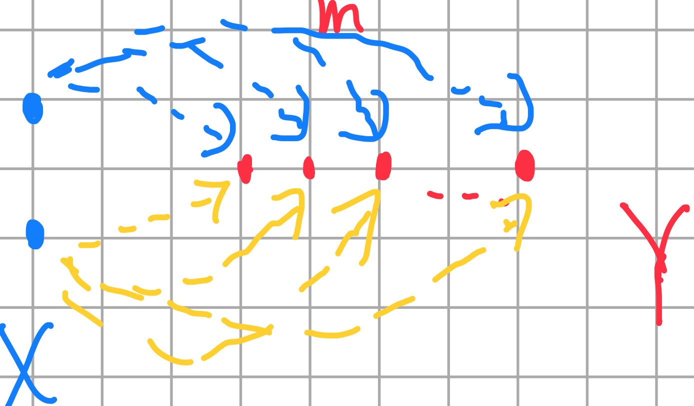
<u>Q.:</u> how many different maps $X \to Y$ are there?

<u>$n=1$:</u>



m maps

<u>$n=2$:</u>

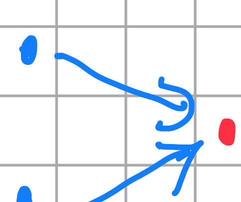


m^2 maps (pairs of arrows)

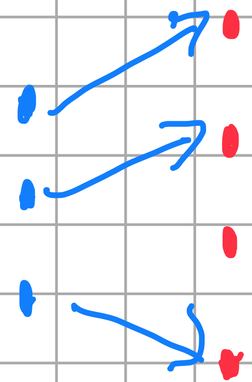
Similarly, in general case there are m^n maps. In particular, there are n^n distinct maps from X to itself.

<u>Q.:</u> how many invertible maps from X to X are there?

Two possible issues for a map to fail being invertible:

①  'glueing' points

(2)



'missing' points

There are $n! = 1\cdot 2\cdot \ldots \cdot n$ invertible maps from X to itself (same as permutations or rearrangements of elements).

<u>Remark.</u> $\lim\limits_{n\to\infty} \frac{n!}{n^n} = \lim\limits_{n\to\infty} \frac{1}{n} \cdot \lim\limits_{n\to\infty} \frac{n\cdot n\cdot\ldots\cdot n}{(n-1)\cdot(n-2)\cdot\ldots\cdot 2} = 0,$

implying that for $n \gg 0$ a randomly chosen map from X to X will very unlikely be invertible.

<u>Reversible Boolean circuits.</u>

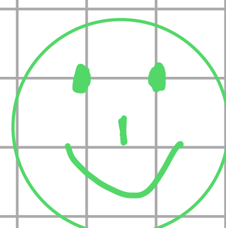
<u>Goal:</u> realize any Boolean map as a reversible circuit and find a (nice) complete basis.

<u>Remark:</u> most maps are not invertible. 

Let $f: \mathbb{B}^n \to \mathbb{B}^m$ be a map.

Consider the map $f_\oplus : \mathbb{B}^{n+m} \longrightarrow \mathbb{B}^{n+m}$ given by $f_\oplus(x,y) := (x, f(x)\oplus y)$, where $\mathbb{B}^{n+m} = \mathbb{B}^n \times \mathbb{B}^m$, $x \in \mathbb{B}^n$, $y \in \mathbb{B}^m$ and '$\oplus$' stands for coordinate-wise addition modulo 2, i.e. $(1,1,0,1) \oplus (0,1,1,1) = (1,0,1,0)$.

<u>Exercise.</u> Show that $f_\oplus$ is invertible for any f.



<u>Thm.</u> Negation (NOT) and CCNOT (Toffoli) operators form a complete basis for reversible circuits of type $f_\oplus$.

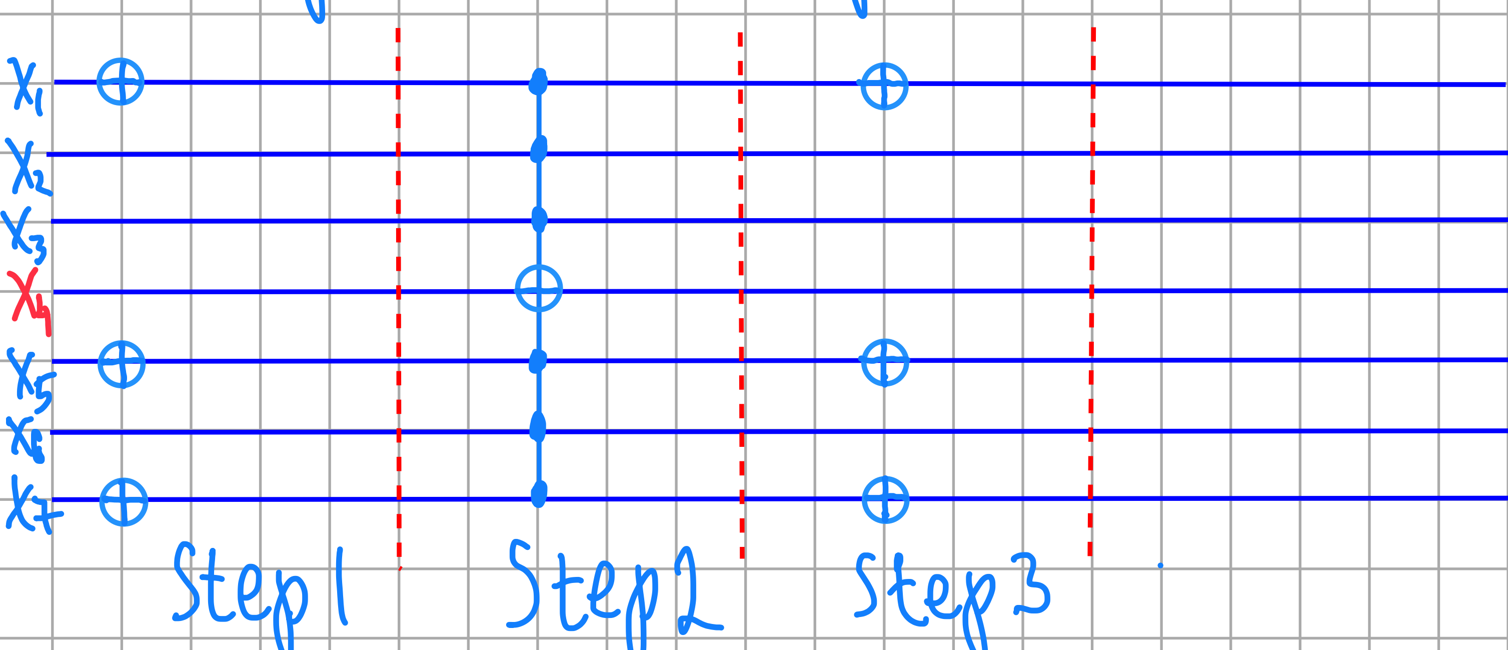
In order to prove this theorem, as well as construct circuits in general, it is helpful to use $\underbrace{CC\ldots C}_{k}NOT$ operators. These are maps from $\mathbb{B}^{k+1}$ to $\mathbb{B}^{k+1}$ with k bits being 'control bits' and the remaining one being changed to its negative provided all control bits are 1 ('True').

VIP Property. The $\underbrace{C\ldots C}_{k}NOT$ operator allows to permute a single bit in an expression without altering any other elements:

$\forall\, a = a_1\ldots a_i\ldots a_{k+1} \in \mathbb{B}^{k+1}$, let $f_{\hat{a},i} : \mathbb{B}^{k+1} \longrightarrow \mathbb{B}^{k+1}$ be given by

$$f_{\hat{a},i}(X) = \begin{cases} a_1\ldots 1-a_i\ldots a_{k+1}, & X = a \\ a, & X = a_1\ldots 1-a_i\ldots a_{k+1} \\ X, & X \neq a_1\ldots a_i\ldots a_{k+1} \text{ or } a_1\ldots 1-a_i\ldots a_{k+1}. \end{cases}$$

Example. Let $a = 0111010$ and $i = 4$. The following circuit computes $f_{\hat{a},i}(X)$.



Step 1. Map $a_1\ldots a_{i-1}\,\cancel{X}\,a_{i+1}\ldots a_{k+1}$ to $1\ldots1\,\cancel{X}\,1\ldots1$ via applying NOTs to the 0 bits.

Step 2. Apply $\underset{x_1}{C}\ldots\underset{x_{k+1}}{C}\underset{x_i}{NOT}$ to permute $1\ldots101\ldots1$ and

$1\ldots 1\,1\,1\ldots 1.$

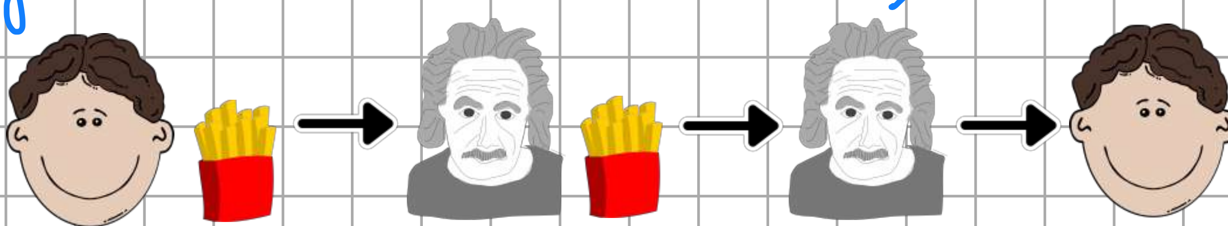
<u>Step 3.</u> 'Undo Step 1' via putting the 'artificially' created 1 bits back to their initial 0 value.

Informal slogan: flip — change — flip back.

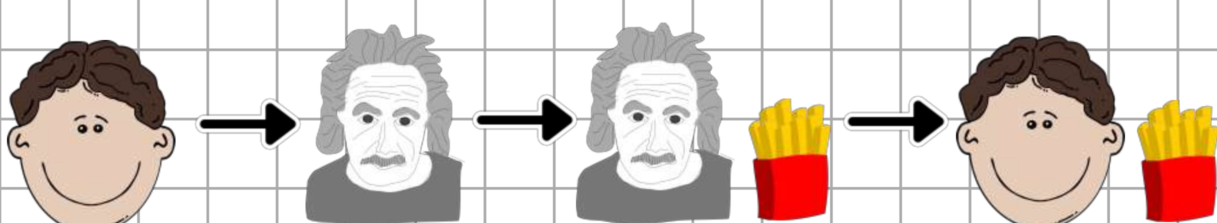
<u>Exercise.</u> Build up and solve a word problem corresponding to the pictures below using the algorithm above:

'one and only'

general person



'with or without'



Back to the proof of the theorem.

Let $f:\mathbb{B}^n \to \mathbb{B}^m$ be a Boolean map. Our goal is to construct a circuit that computes $f_\oplus:\mathbb{B}^{n+m} \to \mathbb{B}^{n+m}$.

First we present a circuit comprised of NOT and $\underbrace{C\ldots C}_{k}NOT$ operators with $k \le n$ and then show that $\underbrace{C\ldots C}_{k}NOT$ is a composition of NOTs and CCNOTs.

For each $x \in \mathbb{B}^n$ do the following.

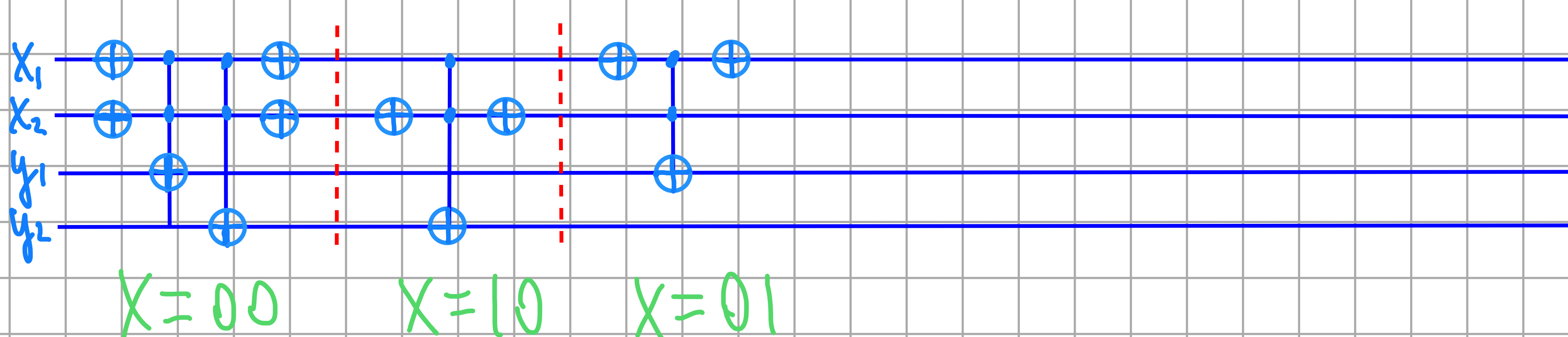
<u>Step 1.</u> 'Isolate' x (map it to $\underbrace{11\ldots1}_{n}$ using NOTs);

<u>Step 1'.</u> If the j^{th} bit of $f(x)$ is 1, apply $\underbrace{CC\ldots C}_{n}\underset{\uparrow\, n+j}{NOT}$

<u>Step 2.</u> ~~X~~ (apply NOTs to the same bits as in Step 1.)

<u>Example.</u> Consider the function $F: \mathbb{B}^2 \to \mathbb{B}^2$ given by

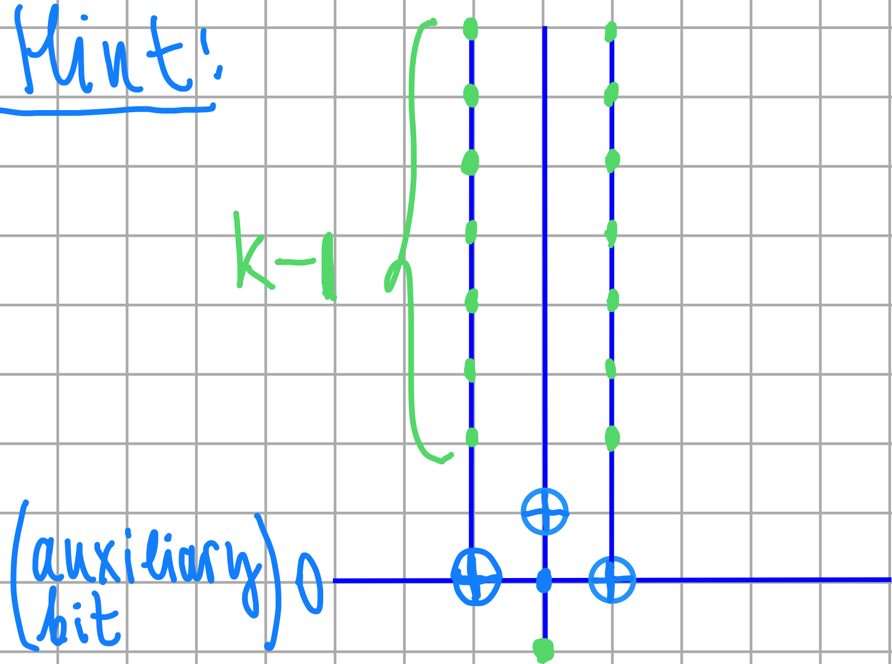
$$F(0,0)=(1,1),\ F(1,0)=(0,1),\ F(0,1)=(1,0),\ F(1,1)=(0,0)$$



<u>Remark</u>: as $F(11)=00$, no action is required for that element.

It remains to construct $\underbrace{C\ldots C}_{k}NOT$ as a circuit over $\{NOT, CCNOT\}$. This can be done by induction on k and is left as an exercise.

<u>Hint:</u>



• - control bits

Physics.

Classical	Quantum
• large objects	• particles
• position and momentum (velocity) of an object is known precisely	• the simultaneous knowledge of position and momentum is bounded by Heisenberg's inequality: $\underbrace{\Delta x \cdot \Delta p}_{\text{standard deviations (error margins) of the values of position and momentum.}} \geq \frac{\hbar}{2}$

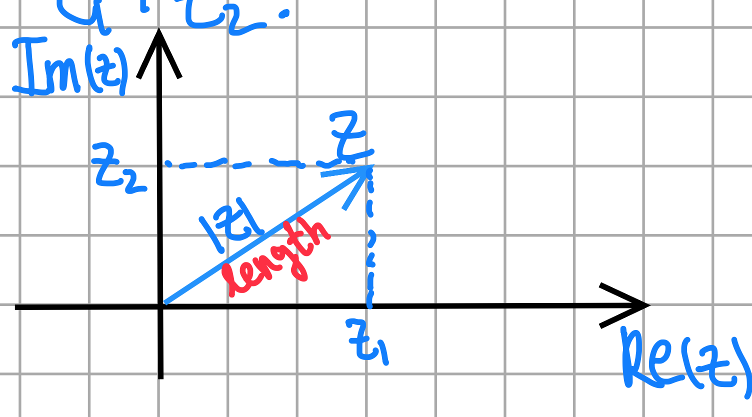
- the evolution with time is governed by solutions of Euler-Lagrange (or Hamilton) differential eq-ns.

- the system evolves according to sol-ns of Shrödinger's eq-n: $i\hbar \frac{d\Psi(\mathbf{x},t)}{dt} = H\cdot\Psi(x,t)$, $i=\sqrt{-1}$, $H=K+U$ Hamiltonian (energy). Sol-n $\Psi(\mathbf{x},t)$ is called a <u>wave f-n</u>, it gives probabilistic locations of a system of particles at time t.

A bit has two possible states: 0 and 1.

A qubit (quantum bit) can be in any <u>superposition</u> of these two states: $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $\alpha,\beta\in\mathbb{C}$ and $|\alpha|^2+|\beta|^2=1$ called <u>amplitudes</u>.

<u>Remark.</u> Recall that for $z=z_1+z_2\cdot i$ with $z_1,z_2\in\mathbb{R}$, we have $|z|^2=z_1^2+z_2^2$:



The possible pairs of amplitudes (α, β) form a 3-dimensional unit sphere in $\mathbb{C}^2 \simeq \mathbb{R}^4$:

$$S^3 = \{ v \in \mathbb{R}^4 \mid |v| = \sqrt{\alpha_1^2 + \alpha_2^2 + \beta_1^2 + \beta_2^2} = 1 \}.$$

The physical meaning of amplitudes is the following. Let $P(\Psi = |0\rangle)$ and $P(\Psi = |1\rangle)$ be the probabilities of observing Ψ in basic state $|0\rangle$ and $|1\rangle$.

Then $P(\Psi = |0\rangle) = |\alpha|^2$ and $P(\Psi = |1\rangle) = |\beta|^2$.

Let $\lambda \in \mathbb{C}$ with $|\lambda| = 1$ and $\Psi_\lambda := \lambda \Psi$, then

$P(\Psi_\lambda = |0\rangle) = |\lambda \cdot \alpha|^2 = |\alpha|^2 = P(\Psi = |0\rangle)$ and

$P(\Psi_\lambda = |1\rangle) = |\lambda \beta|^2 = |\beta|^2 = P(\Psi = |1\rangle)$,

implying that we can't distinguish between Ψ and Ψ_λ ('probability-wise').

Notice that $\{ \lambda \in \mathbb{C} \mid |\lambda| = 1 \} = \{ (\lambda_1, \lambda_2) \in \mathbb{R}^2 \mid \lambda_1^2 + \lambda_2^2 = 1 \} \simeq S^1$, the unit circle.

It follows that the qubits (up to redundancy described above) can be identified with the quotient space S^3 / S^1.

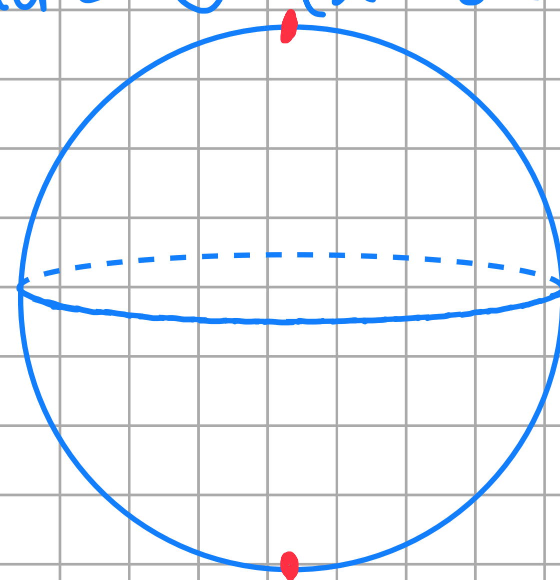
Exercise. Show that S^3/S^1 can be identified with the 2-dimensional sphere S^2 (see the bonus problem).

Mathematicians:

Riemann sphere ($\mathbb{CP}^1$)

Physicists:

Bloch sphere



- states of bit
- states of qubit

We need to work with multiple qubits, i.e. an analogue of $\mathbb{B}^n = \{0,1\}^n$.

Recall that the states of a bit gave a basis for the states of a qubit. In order to obtain a generalization to n bits and qubits, we need to 'build' a $2^n = |\mathbb{B}^n|$-dimensional vector space out of n copies of $\mathbb{C}^2$.

Tensor products.

Let $V = \mathrm{span}(e_1, e_2, \dots, e_n)$ and $W = (f_1, f_2, \dots, f_m)$ be two vector spaces of dimension n and m. Here is a canonical way to construct the 'product' vector space of V and W:

$$V \otimes W := \operatorname{span}\underbrace{(e_i \otimes f_j)}_{\text{basis}}{}_{\substack{i \in \{1,\dots,n\} \\ j \in \{1,\dots,m\}}}.$$

Properties:

1. $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w \quad \forall v_1, v_2 \in V, \ \forall w \in W.$
2. $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2 \quad \forall v \in V, \ \forall w_1, w_2 \in W.$
3. $\lambda v \otimes w = v \otimes \lambda w = \lambda (v \otimes w) \quad \forall v \in V, \ \forall w \in W, \ \forall \lambda \in \mathbb{C}.$

Recall that the state of a qubit $|\psi\rangle \in \mathbb{C}^2$ is a vector of norm 1. So is a state vector $|\Psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ in a system of n qubits. More generally, any state vector in any system of particles in quantum mechanics is of norm 1. This is due to the 'amplitude-probability' correspondence and the total probability (sum of probabilities that the vector flips to concrete basic state after measurement) is equal to 1.

The set of unit vectors (of norm 1) is closed under tensor product:

$\forall v \in V, w \in W$ with $|v| = |w| = 1 \rightsquigarrow |v \otimes w| = 1$

Example. Let $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\eta\rangle = \beta_0|0\rangle + \beta_1|1\rangle \in \mathbb{C}^2$ be state vectors of qubits. Then $||\psi\rangle| = |\alpha_0|^2 + |\alpha_1|^2 = 1$ and $||\eta\rangle| = |\beta_0|^2 + |\beta_1|^2 = 1$. We compute

$|\psi\rangle \otimes |\eta\rangle = \alpha_0\beta_0|0\rangle \otimes |0\rangle + \alpha_0\beta_1|0\rangle \otimes |1\rangle + \alpha_1\beta_0|1\rangle \otimes |0\rangle + \alpha_1\beta_1|1\rangle \otimes |1\rangle$ and $|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 + |\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2 = (|\alpha_0|^2 + |\alpha_1|^2)(|\beta_0|^2 + |\beta_1|^2) = 1$, giving $||\psi\rangle \otimes |\eta\rangle| = 1$.

Hermitian inner product.

A map $\langle \cdot | \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n \longrightarrow \mathbb{C}$ satisfying

- $\langle v_1 + v_2 | w \rangle = \langle v_1 | w \rangle + \langle v_2 | w \rangle \quad \forall v_1, v_2, w \in \mathbb{C}^n$,
- $\langle v | w_1 + w_2 \rangle = \langle v | w_1 \rangle + \langle v | w_2 \rangle \quad \forall v, w_1, w_2 \in \mathbb{C}^n$,
- $\langle \lambda v | w \rangle = \langle v | \bar{\lambda} w \rangle = \bar{\lambda} \langle v | w \rangle \quad \forall v, w \in \mathbb{C}^n, \forall \lambda \in \mathbb{C}$,

Example. Let $\mathbb{C}^n = \mathbb{C}\langle e_1, \dots, e_n \rangle$ and define the inner product on the basis via

$$\langle e_i | e_j \rangle = \delta_{ij} := \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

There is a unique way to continue $\langle \cdot | \cdot \rangle$ to all pairs $(v, w) \in \mathbb{C}^n \times \mathbb{C}^n$ so that $\langle \cdot | \cdot \rangle$ satisfies the required properties:

$$\langle v|w\rangle = \sum_{i=1}^{n} \overline{v_i} w_i, \text{ where } v = \sum_{i=1}^{n} v_i e_i,\ w = \sum_{i=1}^{n} w_i e_i.$$

Def-n. Let $(\mathbb{C}^n, \langle\cdot|\cdot\rangle)$ be a complex vector space with a hermitian inner product. A linear operator $U: \mathbb{C}^n \circlearrowleft$ is called <u>unitary</u> provided it preserves the inner product:

$$\langle Uv|Uw\rangle = \langle v|w\rangle \quad \forall v,w \in \mathbb{C}^n.$$

Let $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{n1} & \dots & & a_{nn} \end{pmatrix}$ be a linear map $\mathbb{C}^n \circlearrowleft$ written in the basis $e_1, \dots, e_n$. This means $A \cdot e_i = A \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{array}{l} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \end{array} = a_{1i} e_1 + a_{2i} e_2 + \dots + a_{ni} e_n$, hence,

$$\langle Ae_i|e_j\rangle = \langle \sum_{s=1}^{n} a_{si} e_s | e_j\rangle = \langle a_{ji} e_j | e_j\rangle = \overline{a_{ji}}$$

$$\langle e_i|A^{+} e_j\rangle = \langle e_i | \sum_{s=1}^{n} \overline{a_{js}} e_s\rangle = \langle e_i | \overline{a_{ji}} e_i\rangle = \overline{a_{ji}},$$

here $A^{+} = \overline{A}^{t} = \begin{pmatrix} \overline{a_{11}} & \overline{a_{21}} & \dots & \overline{a_{n1}} \\ \overline{a_{12}} & \overline{a_{22}} & & \vdots \\ \vdots & \vdots & \ddots & \\ \overline{a_{1n}} & \overline{a_{2n}} & \dots & \overline{a_{nn}} \end{pmatrix}$ is the hermitian conjugate of A.

The calculation above implies (think it over ☺) that

$$\forall v,w \in \mathbb{C}^n: \langle Av|w\rangle = \langle v|A^{+}w\rangle \Leftrightarrow \langle v|Aw\rangle = \langle A^{+}v|w\rangle.$$

<u>Observation:</u> $A^{++} = A$ (as $(\overline{\overline{A}^{t}})^{t} = A$ and $\overline{\overline{\lambda}} = \lambda \ \forall \lambda \in \mathbb{C}$).

Let $U: (\mathbb{C}^n, \langle\cdot|\cdot\rangle) \circlearrowleft$ be a unitary operator, then

$$\langle Uv|Uw\rangle = \langle U^{+}Uv|w\rangle = \langle v|w\rangle \quad \forall v,w \in \mathbb{C}^n.$$

Therefore, $U^{+}U = Id = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ is the identity matrix.

In turn, $U^{+}U = Id$ and $\det(U^{+}) = \overline{\det U}$ implies $|\det U| = 1$.

- $U^{-1} = U^{+}$
- U is diagonalizable: there is a basis $(v_1, \dots, v_n) \subset \mathbb{C}^n$ in which U acts as a diagonal matrix $\begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}$, moreover, each eigenvalue λ_i has norm 1, i.e. $|\lambda_i| = 1$.

<u>Remark.</u> The analogous statement for linear operators over $\mathbb{R}$ is not true. For instance, rotation by angle φ in $\mathbb{R}^2$ has no eigenvectors if $\varphi \neq k\pi$, $k \in \mathbb{Z}$.

<u>Q.:</u> Why unitary operators?

<u>Answer:</u> the states of a quantum system are represented by unit vectors ($|\psi\rangle = \sum_{i=1}^{n} \alpha_i |e_i\rangle$ with $\sum_{i=1}^{n} |\alpha_i|^2 = 1$). This is due to the fact that after a measurement $|\psi\rangle$ must clip to one of the basic states $|e_1\rangle$, $|e_2\rangle, \dots, |e_n\rangle$. The probability that $|\psi\rangle$ sticks to $|e_i\rangle$ is $P(|\psi\rangle = e_i) = |\alpha_i|^2$. It remains to notice that $\langle \psi | \psi \rangle = \sum_{i=1}^{n} |\alpha_i|^2 = 1$.