Quantum computation: lecture 1

- General introduction
- Classical circuits - Post's theorem
- Reversible gates
- Linear algebra in Dirac's notation

Introduction : Chronology

80's: - **Feynman** : idea that using quantum properties of matter at a microscopic level could help compute more efficiently

- **Bennett, Wiesner, Deutsch** : quantum circuits

90's: - quantum algorithms (Deutsch-Josza, Simon, Bernstein-Vazirani, Shor, Grover)

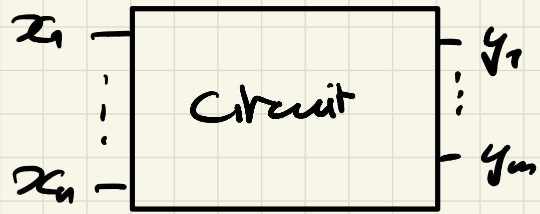
2000's: realization of quantum computers ...

Classical circuits

Let $f : \{0,1\}^n \to \{0,1\}^m$ be a Boolean function.

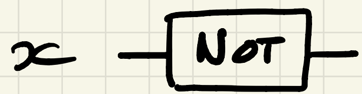
$$(x_1 .. x_n) \mapsto (y_1 .. y_m) = f(x_1 .. x_n)$$

Does there exist a classical circuit computing in an automated manner the value of f for every input $(x_1 .. x_n)$?



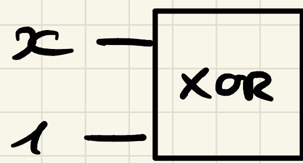
Examples of simple circuits (= elementary gates) and associated Boolean functions

a) **NOT gate:**



$$f(x) = \bar{x} = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } \bar{x} = 1 \end{cases}$$

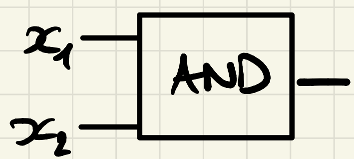
(equivalent to:



$$f(x) = x \oplus 1 = \bar{x}$$

)

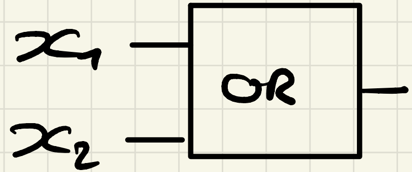
b) **AND gate:**



$$f(x_1, x_2) = x_1 \wedge x_2$$

$= 1$ iff $x_1 = 1$ and $x_2 = 1$

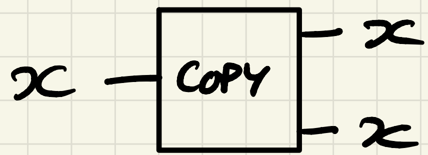
c) __OR gate:__



$$f(x_1, x_2) = x_1 \vee x_2$$
$$= 1 \text{ iff } x_1 = 1 \text{ or } x_2 = 1$$

__NB__: this is the __non-exclusive__ OR

d) __COPY gate__:

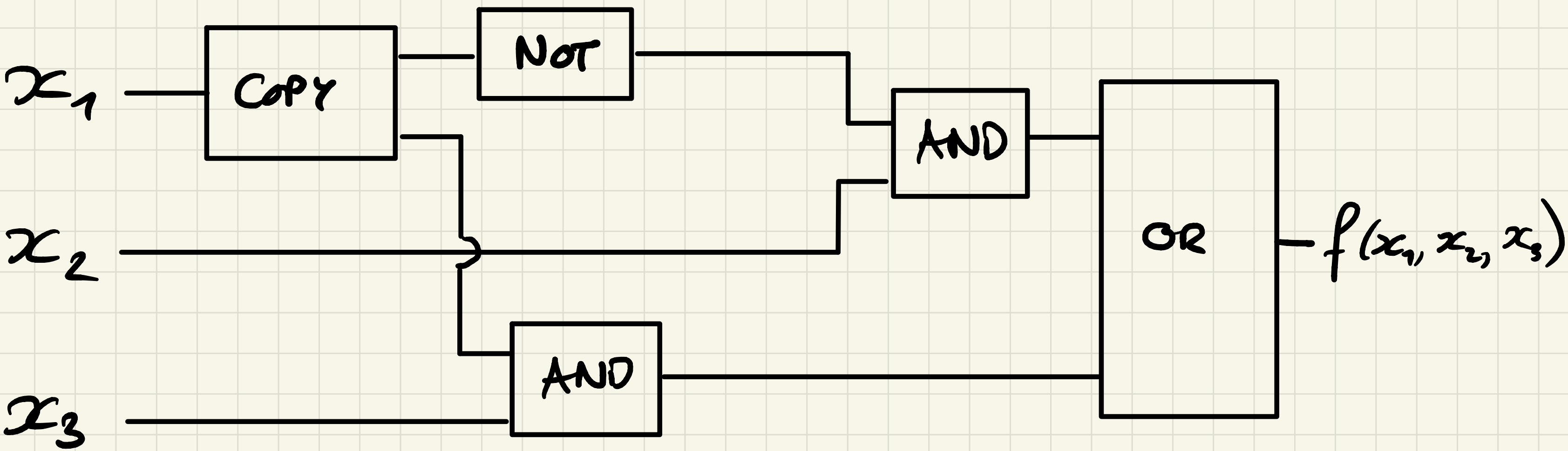


$$f(x) = (x, x)$$

__NB__: not really a gate, as it can be realized physically by joining two wires together

Example of a circuit for

$$f(x_1, x_2, x_3) = (\overline{x_1} \wedge x_2) \vee (x_1 \wedge x_3)$$



Formal definition of a Boolean circuit

A Boolean circuit is a directed, acyclic graph (DAG) with n-qubits input and m-qubits output, whose vertices are logic gates and edges are wires.

Theorem (Emil Post, 1921)

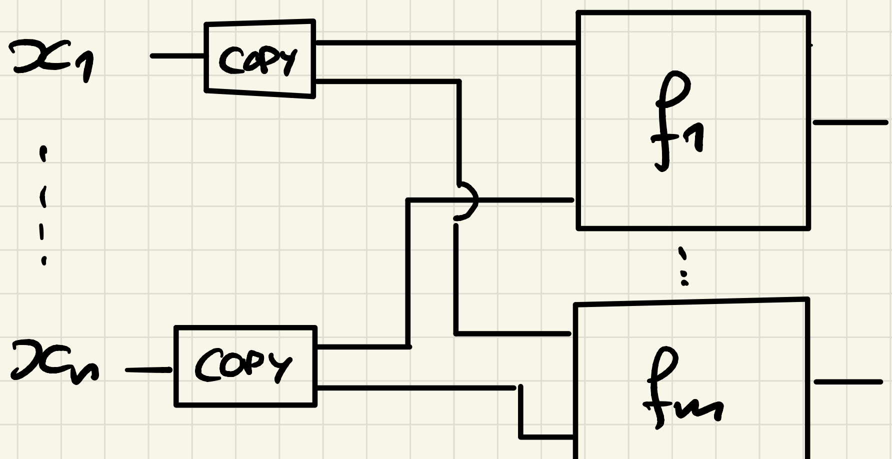
Every Boolean function f can be realized by a Boolean circuit made only of the elementary gates AND, OR, NOT and COPY.

This theorem therefore implies that this set of 4 gates is *universal*.

Proof

Let $f : \{0,1\}^n \longrightarrow \{0,1\}^m$ be a Boolean function

1) $f = (f_1, \dots, f_m)$ in general, but the theorem needs only to be proven for $m=1$ because:



2) Consider those vectors $a^{(1)} \ldots a^{(k)} \in \{0,1\}^n$

such that $\begin{cases} f(a^{(j)}) = 1 & \forall 1 \leq j \leq k \\ f(b) = 0 & \forall b \neq a^{(1)} \ldots a^{(k)} \end{cases}$

and define $C_a(x) = \begin{cases} 1 & \text{if } \overbrace{x = a}^{\text{vectors!}} \\ 0 & \text{otherwise} \end{cases}$

Then $f(x) = C_{a^{(1)}}(x) \vee \ldots \vee C_{a^{(k)}}(x)$

OR's

3) Observe now that for $a \in \{0,1\}^n$:

$$C_a(x) = \phi_{a_1}(x_1) \wedge \dots \wedge \phi_{a_n}(x_n)$$

AND's

where $\phi_{a_j}(x_j) = 1_{\{x_j = a_j\}} = \begin{cases} x_j & \text{if } a_j = 1 \\ \overline{x_j} & \text{if } a_j = 0 \end{cases}$

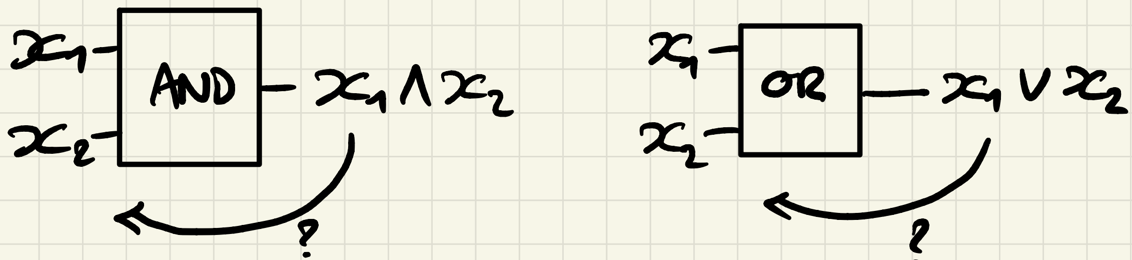
NOT

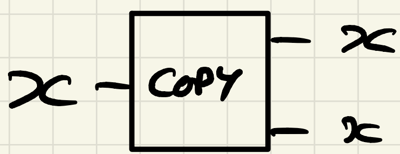
So the computation of $f(x_1 .. x_n)$ can be realized exclusively with COPY, OR, AND & NOT gates.

#

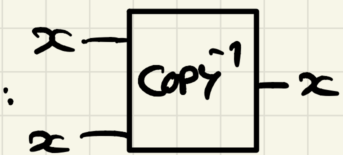
Irreversibility

The gates AND, OR & COPY are irreversible:





is logically reversible:



but its inverse deletes a bit: physically, it dissipates heat = irreversible process!

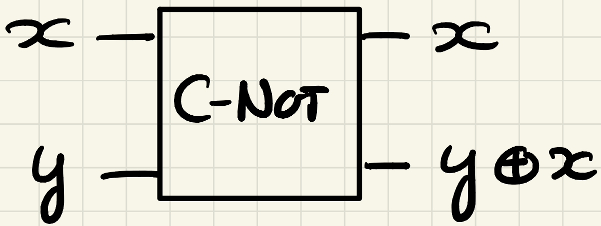
Reversible gates

In quantum circuits, irreversibles gates are forbidden. Fortunately, the previous gates can be emulated by reversible gates:

1) <u>NOT gate</u>: $x \;-\!\boxed{\text{NOT}}\!-\; f(x) = x \oplus 1 = \bar{x}$

is obviously reversible (apply it twice to recover the initial state)

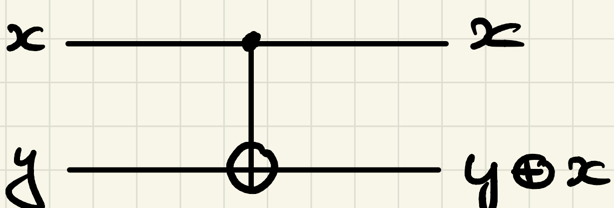
2) Controlled-NOT (C-NOT) gate



$$f(x,y) = (x, y \overset{\text{XOR}}{\oplus} x)$$

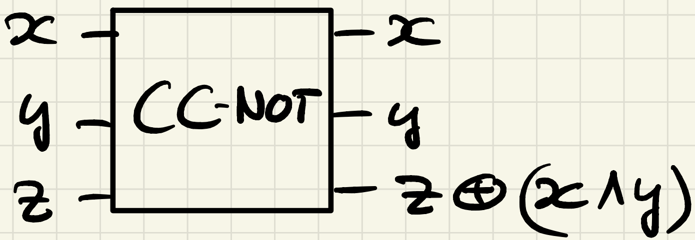
$$\begin{cases} f(0,y) = (0,y) \\ f(1,y) = (0, y \oplus 1) = (1, \bar{y}) \end{cases}$$

Equivalent symbol:



This gate is also reversible (again, apply it twice)

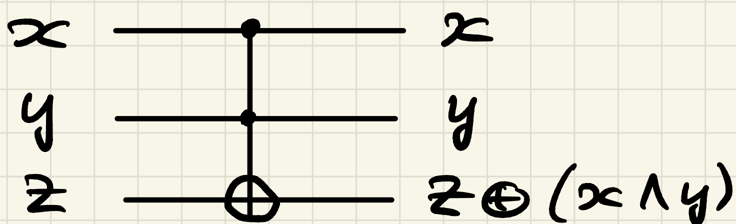
3) Toffoli gate (or CC-NOT gate)



$$f(x,y,z) = (x,\, y,\, z \oplus (x \wedge y))$$

$$\begin{cases} f(x,y,z) = (x,y,z) & \text{as long as } x=0 \text{ or } y=0 \\ f(1,1,z) = (x,\, y,\, z \oplus 1) = (x,\, y,\, \overline{z}) & \end{cases}$$

Equivalent symbol:

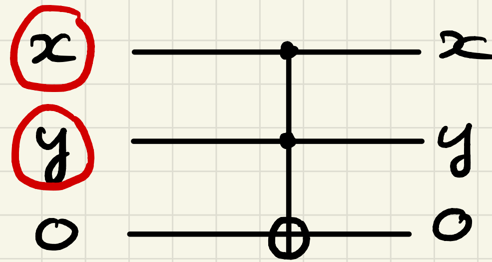


Again a reversible gate (apply it twice)

All previously seen gates can be retrieved from these 3 reversible gates: (use red input/output)

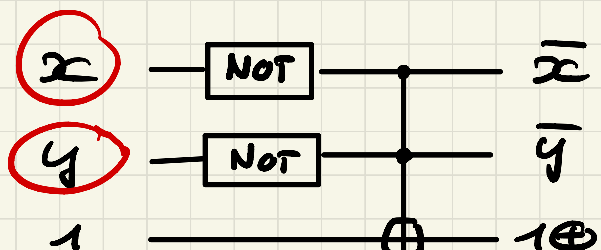
1) NOT : obviously...

2) AND :



$0 \oplus (x \wedge y) = x \wedge y$

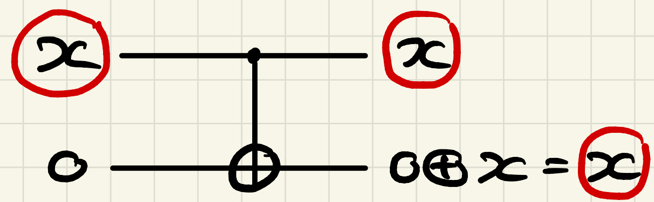
3) OR :



De Morgan's law

$1 \oplus (\bar{x} \wedge \bar{y}) = \overline{\bar{x} \wedge \bar{y}} = x \vee y$

4) COPY :



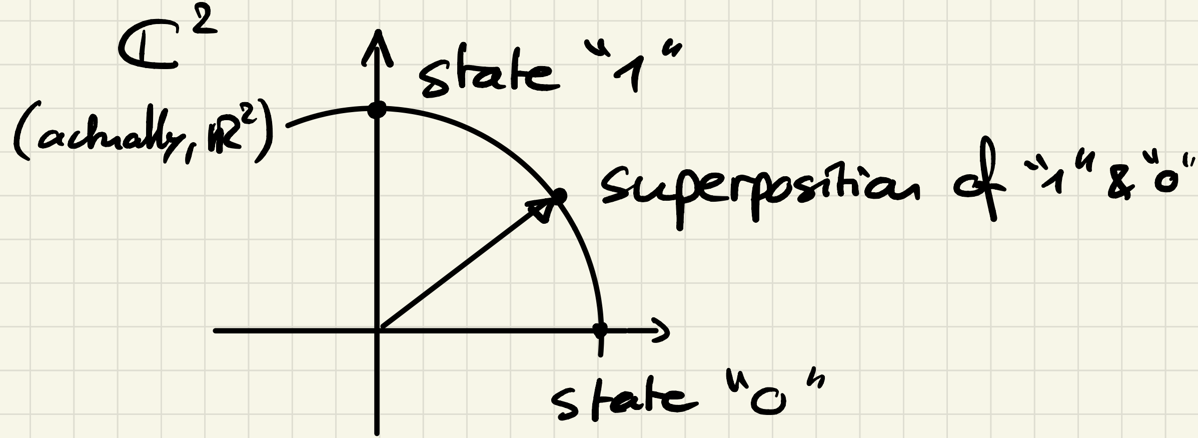
So the set of 3 gates NOT, C-NOT, CC-NOT is also universal, according to Post's thm.

<u>Note</u> that actually, the NOT & C-NOT gates can themselves be retrieved from CC-NOT gates; but the reciprocal statement is wrong.

Linear algebra in Dirac's notation

The state of a quantum system is described by a unit vector in a Hilbert space $\mathcal{H}$ (on $\mathbb{C}$).
In this course, we will only consider the finite-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^N$ with $N = 2^n$ (n = number of qubits). In particular, the state of a single qubit is a unit vector in $\mathbb{C}^2$.

Illustration:



The whole idea of quantum computation is to work with qubits in these superposed states in order to perform simultaneous computations.

Dirac's notation

- "ket" : $|\varphi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} \in \mathbb{C}^N$ column vector

complex-conjugate

- "bra" : $\langle\varphi| = (\overline{\alpha_0}, \dots, \overline{\alpha_{N-1}})$ raw vector

- scalar product between $|\varphi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{pmatrix}$ & $|\psi\rangle = \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$:

$$\langle\varphi|\psi\rangle = \sum_{i=0}^{N-1} \overline{\alpha_i}\,\beta_i \quad , \quad \| |\varphi\rangle \| = \sqrt{\langle\varphi|\varphi\rangle}$$

"braket" norm

Properties:

- Positivity: $\langle \varphi | \varphi \rangle = \sum_{i=0}^{N-1} |\alpha_i|^2 \geq 0$
- Strict positivity: $\langle \varphi | \varphi \rangle = 0$ iff $|\varphi\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$
- Symmetry:

$$\langle \psi | \varphi \rangle = \sum_{i=0}^{N-1} \overline{\beta_i} \alpha_i = \overline{\sum_{i=0}^{N-1} \overline{\alpha_i} \beta_i} = \overline{\langle \varphi | \psi \rangle}$$

- Bilinearity:

$$\langle \varphi | \left(\alpha |\psi_1\rangle + \beta |\psi_2\rangle \right) = \sum_{i=0}^{N-1} \overline{\alpha_i} \left(\alpha \beta_{1i} + \beta \beta_{2i} \right) = \ldots$$

$$\ldots = \alpha \sum_{i=0}^{N-1} \overline{\alpha_i} \beta_{1i} + \beta \sum_{i=0}^{N-1} \overline{\alpha_i} \beta_{2i} = \alpha \langle \varphi | \psi_1 \rangle + \beta \langle \varphi | \psi_2 \rangle$$

Also:

$$(\alpha \langle \varphi_1 | + \beta \langle \varphi_2 |) | \psi \rangle = \sum_{i=0}^{N-1} \overline{(\alpha \alpha_{1i} + \beta \alpha_{2i})} \beta_i$$

$$= \overline{\alpha} \sum_{i=0}^{N-1} \overline{\alpha_{1i}} \beta_i + \overline{\beta} \sum_{i=0}^{N-1} \overline{\alpha_{2i}} \beta_i = \overline{\alpha} \langle \varphi_1 | \psi \rangle + \overline{\beta} \langle \varphi_2 | \psi \rangle$$

Computational basis of $\mathcal{H} = \mathbb{C}^N$ $(N = 2^n)$

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i^{\text{th}} \text{ position} = | x_1 x_2 \ldots x_n \rangle \qquad 0 \leq i \leq N-1$$

where $x_1 x_2 \ldots x_n$ = binary representation of i

Observe that $\langle x_1' \dots x_n' | x_1 \dots x_n \rangle = \delta_{x_1' x_1} \cdots \delta_{x_n' x_n}$

(i.e. $\{ |x_1 \dots x_n\rangle, x_1 \dots x_n \in \{0,1\} \}$ is an orthogonal basis)

Also, any $|\varphi\rangle \in \mathbb{C}^N$ can be written as

$$|\varphi\rangle = \sum_{x_1 \dots x_n \in \{0,1\}} \alpha_{x_1 \dots x_n} |x_1 \dots x_n\rangle$$

$$= \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \quad \left(\begin{matrix}\text{short-hand} \\ \text{notation}\end{matrix}\right)$$

& $\langle \varphi | \varphi \rangle = 1$ iff $\sum_{x_1 \dots x_n \in \{0,1\}} |\alpha_{x_1 \dots x_n}|^2 = 1$

(unit vector)

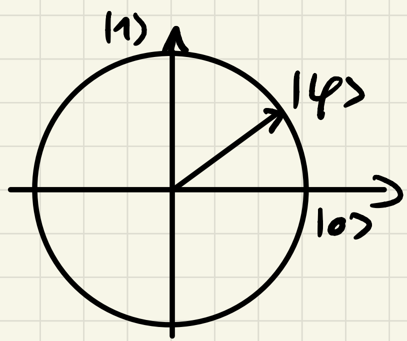
Examples:

- $\underline{n=1}$ $(\longleftrightarrow N=2)$

$$e_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad e_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$|\varphi\rangle = \alpha_0 e_0 + \alpha_1 e_1 = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

unit vector $\longleftrightarrow$ $|\alpha_0|^2 + |\alpha_1|^2 = 1$



(previously seen example)

- $\underline{n=2}$ $\quad (\leftrightarrow N = 2^2 = 4)$

$$e_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \underbrace{|00\rangle}_{\substack{\text{bin. rep.} \\ \text{of } i=0}} \qquad e_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \underbrace{|01\rangle}_{\substack{\text{bin. rep.} \\ \text{of } i=1}}$$

$$e_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \underbrace{|10\rangle}_{\substack{\text{bin. rep.} \\ \text{of } i=2}} \qquad e_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \underbrace{|11\rangle}_{\substack{\text{bin. rep.} \\ \text{of } i=3}}$$

$$|\varphi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Tensor product

Let $\mathcal{H}_1 = \mathbb{C}^{2^{n_1}}$ Hilbert space for n_1 qubits

$\mathcal{H}_2 = \mathbb{C}^{2^{n_2}}$ Hilbert space for n_2 qubits

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 = \mathbb{C}^{2^{n_1}} \otimes \mathbb{C}^{2^{n_2}} \underset{\text{(isomorphic)}}{\sim} \mathbb{C}^{2^{n_1+n_2}}$$

= vector space of dimension $2^{n_1+n_2}$ spanned by all basis elements $|x,y\rangle = \underset{\in \mathcal{H}_1}{|x\rangle} \otimes \underset{\in \mathcal{H}_2}{|y\rangle}$

$\forall |\varphi\rangle \in \mathcal{H}$, it holds that $|\varphi\rangle = \sum\limits_{\substack{0 \leq x \leq 2^{n_1}-1 \\ 0 \leq y \leq 2^{n_2}-1}} \alpha_{x,y} |x,y\rangle$

unit vector iff $\sum\limits_{x,y} |\alpha_{x,y}|^2 = 1$

Important remark

- Every element $|\varphi\rangle$ in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ can be written as a linear combination of the basis elements $|x, y\rangle$
- But <u>not</u> every element $|\varphi\rangle$ in $\mathcal{H}$ can be written in the product form $|\varphi_1\rangle \otimes |\varphi_2\rangle$ (those are called "product states")

Conjugation in $\mathcal{H}_1 \otimes \mathcal{H}_2$:

ket $|\varphi_1\rangle \otimes |\varphi_2\rangle \longrightarrow$ bra $\langle\varphi_1| \otimes \langle\varphi_2|$

⚠ the same order is kept!

Scalar product in $\mathcal{H}_1 \otimes \mathcal{H}_2$:

$$\left(\langle\varphi_1| \otimes \langle\varphi_2|\right)\left(|\psi_1\rangle \otimes |\psi_2\rangle\right) = \langle\varphi_1|\psi_1\rangle \cdot \langle\varphi_2|\psi_2\rangle$$

So $\langle x', y' | x, y\rangle = \langle x' | x\rangle \cdot \langle y' | y\rangle = \delta_{x'x} \cdot \delta_{y'y}$

Example: $\mathcal{H}_1 = \mathbb{C}^2$, $\mathcal{H}_2 = \mathbb{C}^2$, $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \sim \mathbb{C}^4$

$|\varphi_1\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \in \mathcal{H}_1$, $|\varphi_2\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle \in \mathcal{H}^2$

$$|\varphi_1\rangle \otimes |\varphi_2\rangle = \alpha_0\beta_0 |0,0\rangle + \alpha_0\beta_1 |0,1\rangle + \alpha_1\beta_0 |1,0\rangle + \alpha_1\beta_1 |1,1\rangle$$

(Note the specific form of a product state!)

$$|0,0\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = e_0$$

$$|0,1\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = e_1$$

binary representations!

$$|1,0\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = e_2$$

$$|1,1\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = e_3$$