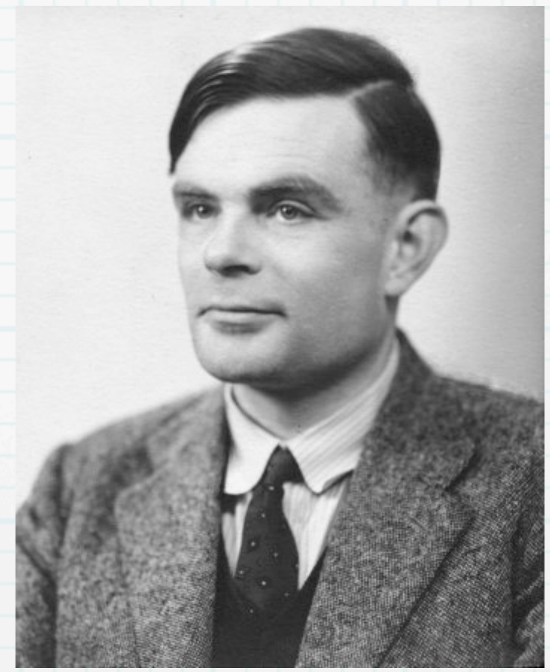
The University of Nottingham
School of Computer Science
Functional Programming Laboratory

Quantum Computing

Thorsten Altenkirch

Is Computation universal?

Alonzo Church



Alan Turing

λ - calculus

Turing machines

computable functions

The Church-Turing thesis

All computational formalisms define the same set of computable functions

The Church-Turing thesis

All computational formalisms define the same set of computable functions

* What do we mean by **all** formalisms?

The Church-Turing thesis (CTT)

All **physically realizable** computational formalisms define the same set of computable functions

* Most people believe CTT
* Hypercomputing?

The Church-Turing thesis

All **physically realizable** computational formalisms define the same set of computable functions

* Most people believe CT
* Hypercomputing?

Throw you TM in a black hole...

Feasible computation?

* Not all computable problems can be solved **in practice.**
* TAUT Example: Is

  $$(P \wedge Q \rightarrow R) \leftrightarrow (P \rightarrow Q \rightarrow R)$$

  a tautology?
* The best known algorithm for TAUT requires exponential time in the number of propositional variables.

The extended Church-Turing thesis (ECT)

All physically realizable computational formalisms define the same set of feasible computable functions

* Challenged by non-standard computational formalisms
* P-systems inspired by biology
* Quantum Computing inspired by quantum physics

Factor & Primes

FACTOR	PRIMES
Input: a number (e.g. 15) Output: a (nontrivial) factor (e.g. 3 or 5) or "prime"	Input: a number (e.g. 15, 7) Output: yes (e.g. for 7) no (e.g. for 15)

* The best known algorithm for factorisation needs exponential time.
* Hence factorisation is **not feasible.**
* However, there is a polynomial algorithm for PRIMES (feasible).
* Important for public key cryptography (e.g. RSA)

Shor's algorithm

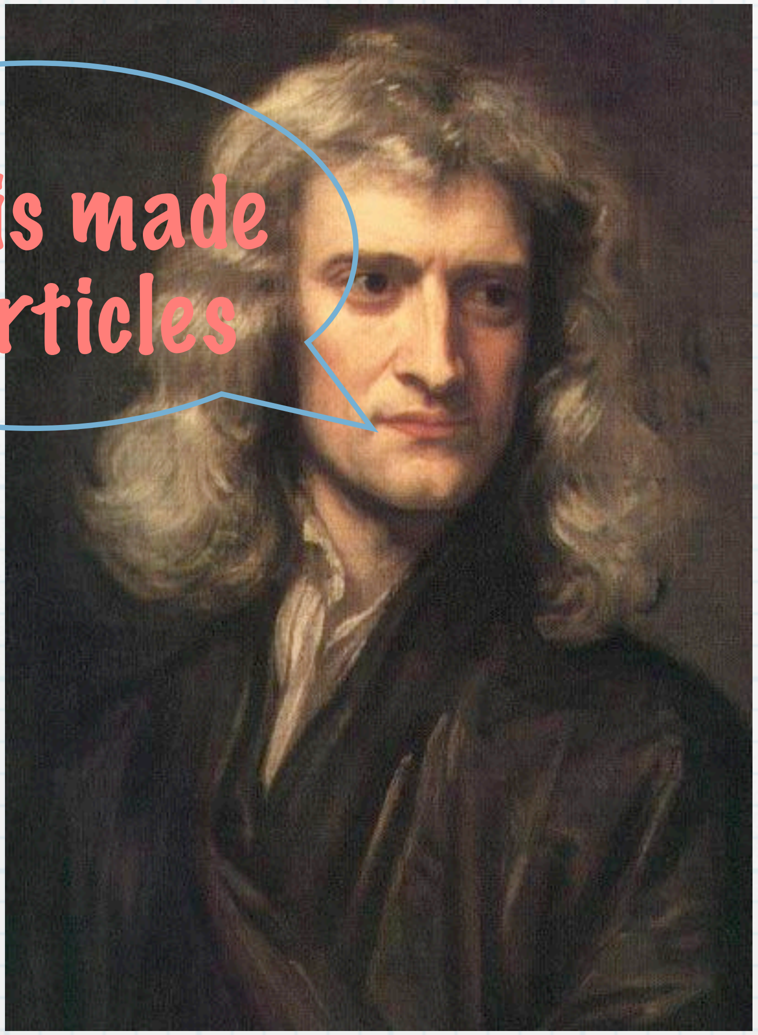
Peter Shor (MIT)

* 1994 : Shor develops an (probabilistic) algorithm that would solve FACTOR in polynomial time on a (hypothetical) quantum computer.
* This indicates that the ECT doesn't hold for quantum computing

Quantum Physics

in 10 minutes

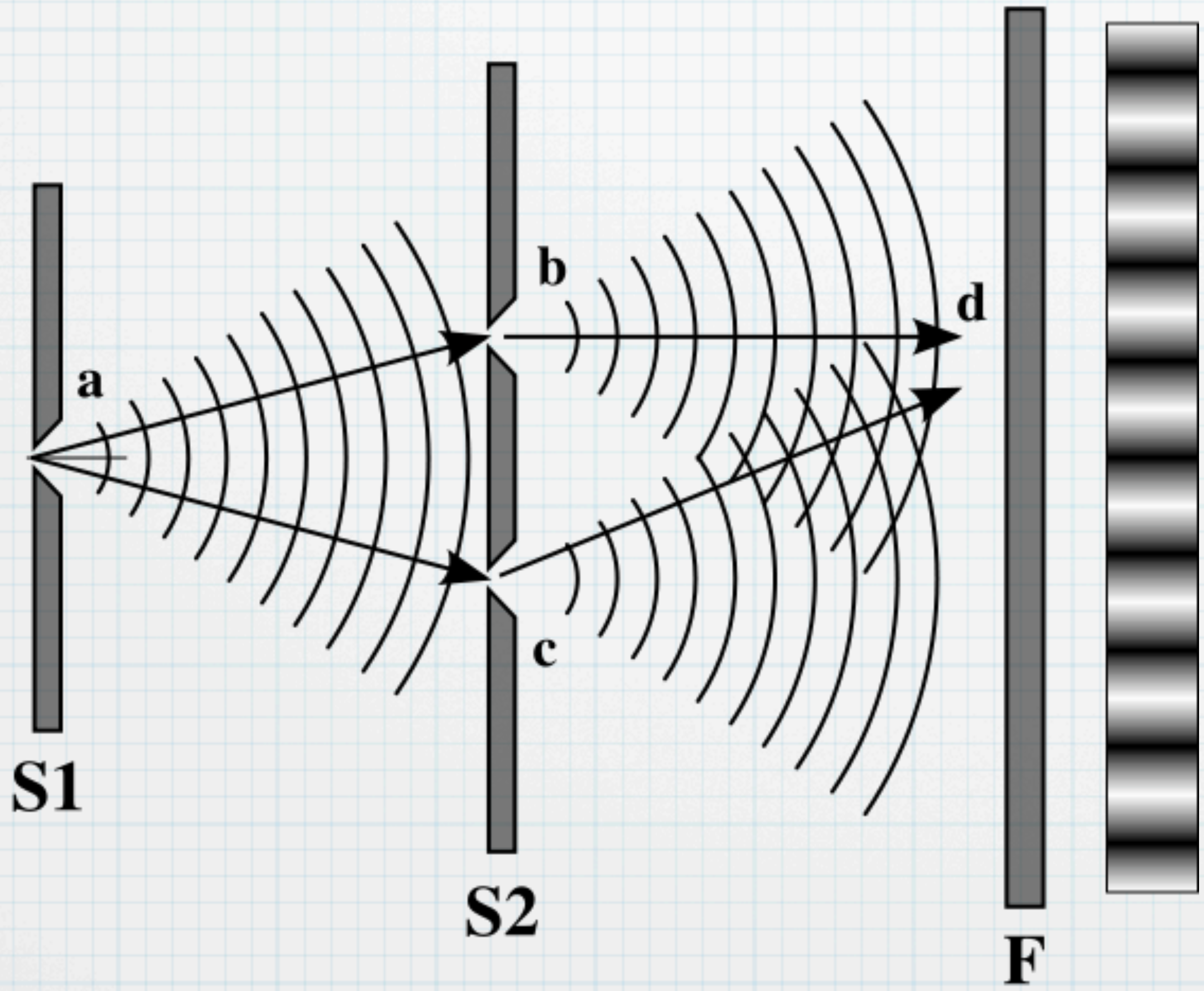
Is light wave or particle?



Isaac Newton
(1643 - 1727)

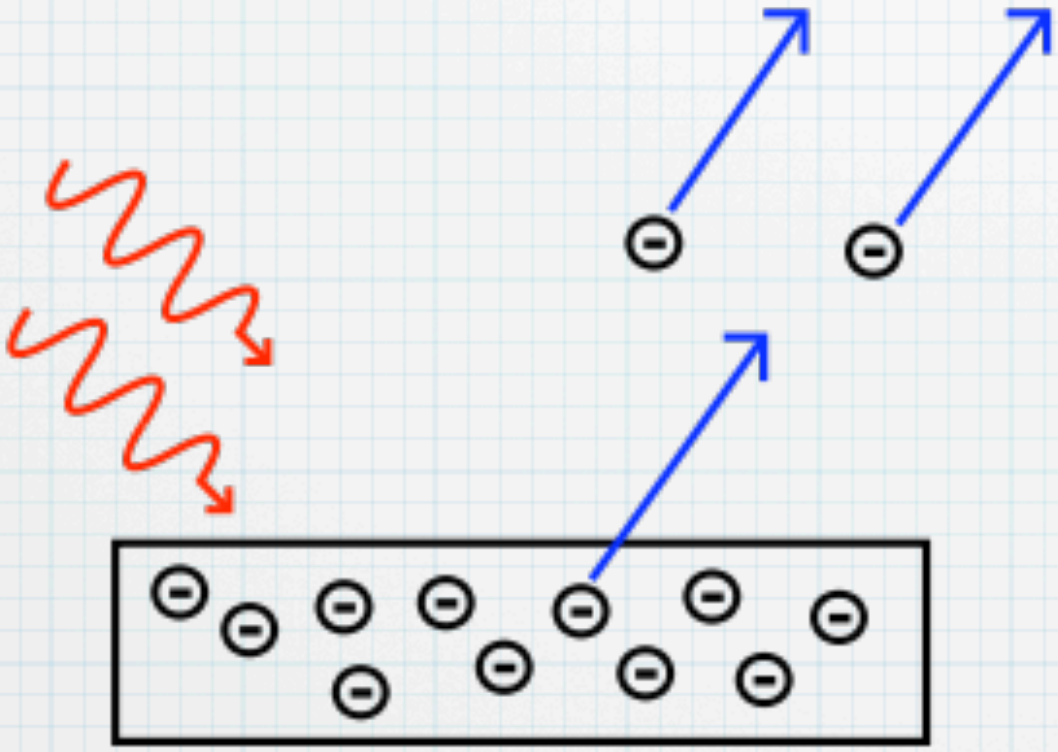
Christiaan Huygens
(1629 -1695)

Young's double slit experiment



* In 1801 Thomas Young performed the double slit experiment
* It produces an interference pattern
* Light is a wave!

The photoelectric effect



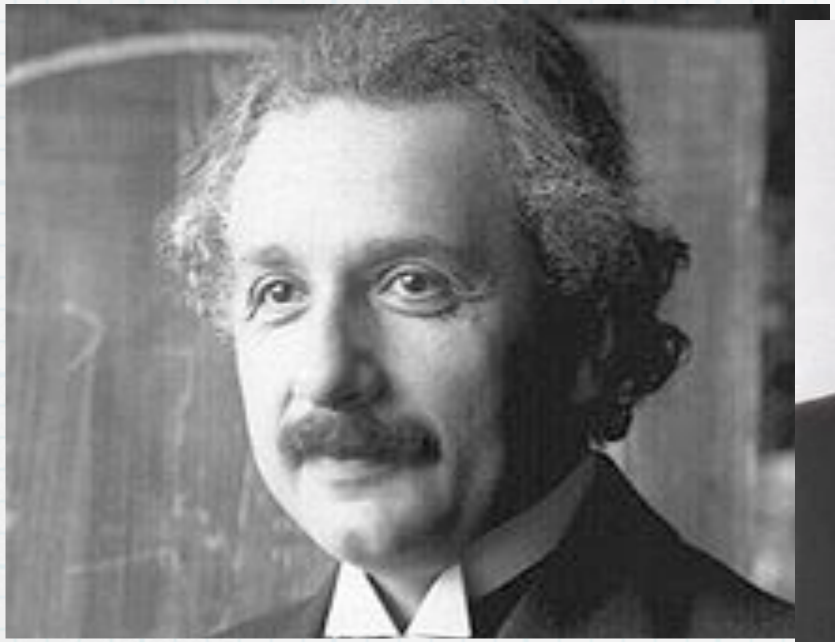
* Photons can dislocate electrons in certain materials
* The energy of the electrons only depends on the frequency of the light
* Not on intensity!
* Below a certain intensity no electrons can dislocated.
* Conclusion: light consists of particles (photons).

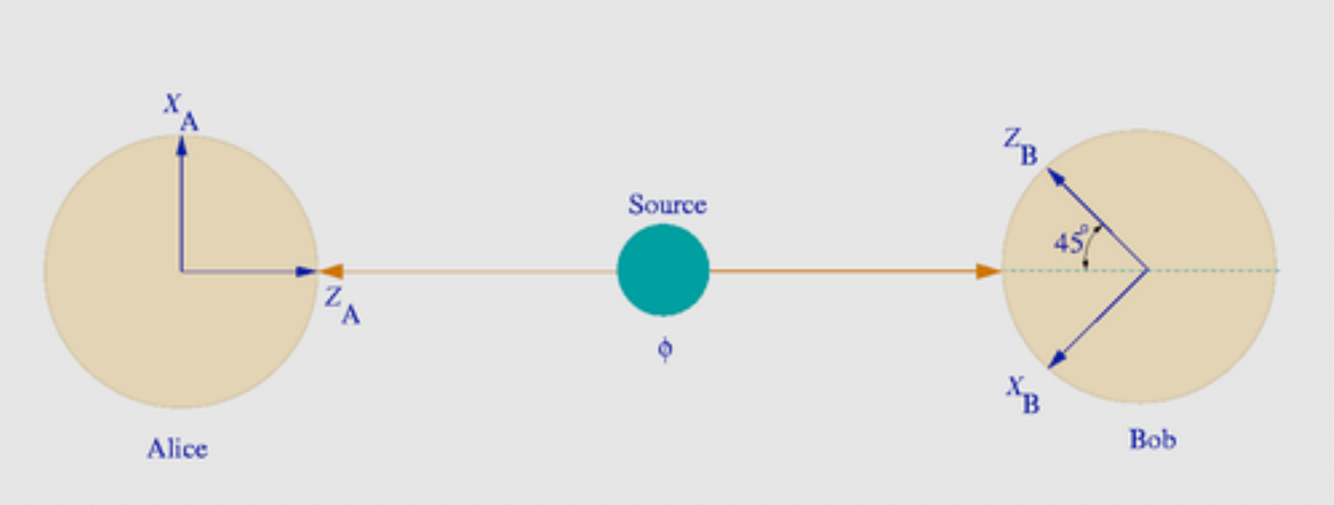
Wave particle duality

* Electrons also behave this way.
* Copenhagen interpretation
* Particles are probability waves
* Amplitude corresponds to the probability that we observe the particle.

Niels Bohr
(1885 - 1962)

Einstein-Podelsky-Rosen paradox (EPR)





* Thought experiment about non-locality
* Two particles with opposite spin are produced.
* They are measured far apart.
* According to QM we always measure both particle if we measure one.
* EPR argue that there have to be hidden variables

Bell inequality

* Local variables or non-locality?
* Is there an experiment to show who is right?
* Bell showed that there are experiments which refute hidden-variable theory
* An intuitive account of Bell's theorem has been given by Mermin

Mermin's thought experiment

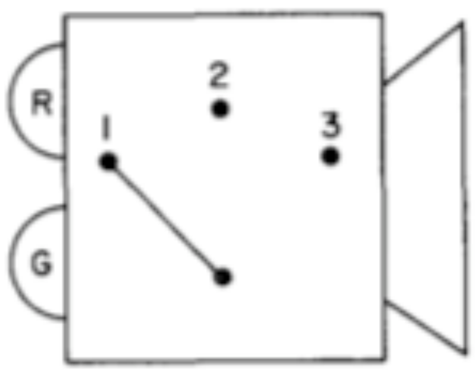
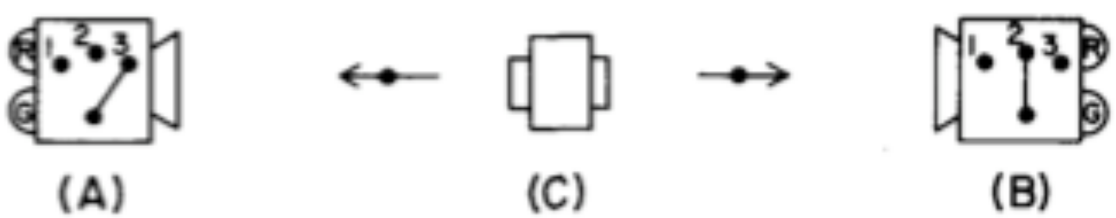
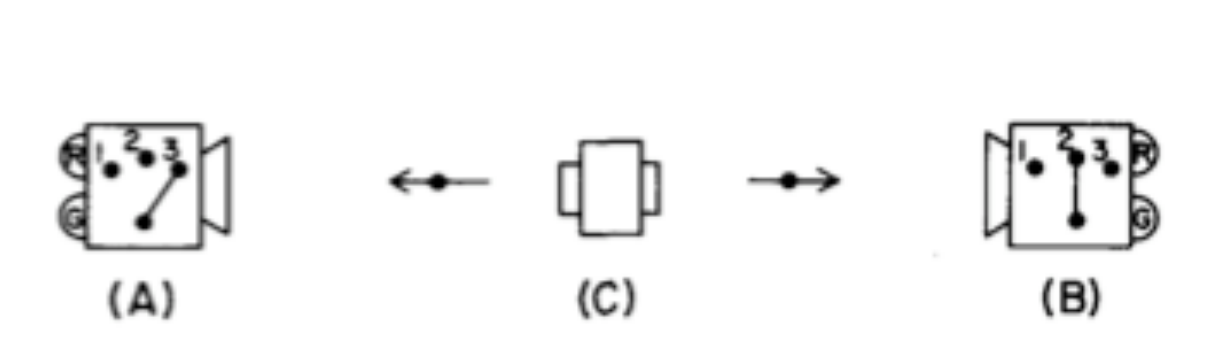


Fig. 1. Detector. Particles enter on the right. The red (R) and green (G) lights are on the left. The switch is set to position 1.



* Each time we press the button on C both detectors show a red or green light.
* If both detectors have the same settings (1,2,3) the same light goes on.
* If the detectors have different settings the same light goes on in 1/4 of the cases.

“The conundrum of the device”



* Each particle has to carry the information which light to flash for each setting (3 bits).
* Both particles have the same instruction set.
* Assume the instruction set is RRG.
* If we measure different bits, the same light goes on in at least 1/3 of all cases.
* The same is true for all other instruction sets.
* This is incompatible with the observation that same light went on only in 1/4 of all cases!

Non-locality rules !

* Mermin's experiment cannot explain by hidden variables.

* QM has a simple explanation: We are measuring the spin of entangled particles with orientations 0°, 120°, 240°.

* If the settings are different, the probability that the measurements agree is given by $\cos^2\frac{\theta}{2}$ and:

$$\cos^2\frac{0^\circ}{2} = 1$$

$$\cos^2\frac{120^\circ}{2} = \cos^2\frac{240^\circ}{2} = \frac{1}{4}$$

* While Mermin's experiment is a thought experiment, similar experiments have been carried out in practice.

How to build your own quantum computer

in theory

Quantum memory: the qubit

$$\alpha\,|0\rangle + \beta\,|1\rangle$$

$$\alpha, \beta \in \mathbb{C}$$

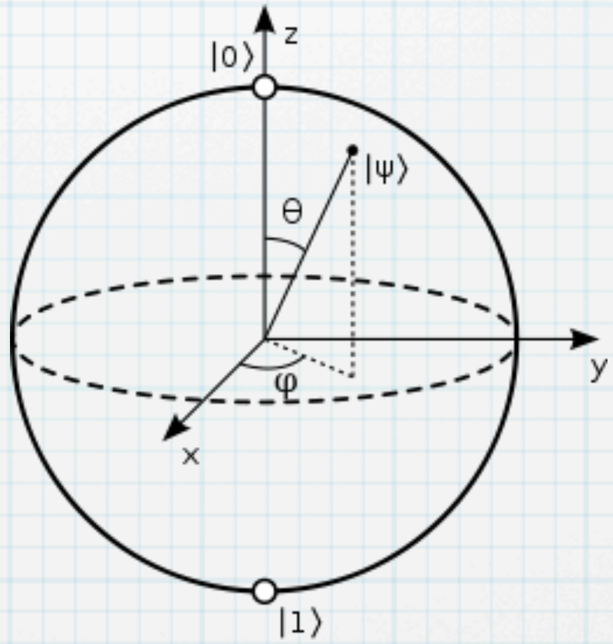
superposition of 2 probability amplitudes given as complex numbers

subset of a 2-dimensional complex vectorspace

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

Probability that the qubit is 0

Probability that the qubit is 1



The Bloch sphere

Examples:

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

base states

superpositions

Operations on qubits: Measurement

$$\alpha|0\rangle + \beta|1\rangle \begin{cases} \xrightarrow{|\alpha|^2} |0\rangle \\ \xrightarrow{|\beta|^2} |1\rangle \end{cases}$$

* probabilistic
* irreversible

Example

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \begin{cases} \xrightarrow{\frac{1}{2}} |0\rangle \\ \xrightarrow{\frac{1}{2}} |1\rangle \end{cases}$$

Operations on qubits: Unitaries

$$\begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

linear independent + norm preserving

$$\alpha\,|0\rangle + \beta\,|1\rangle$$

$$\mapsto (\alpha u_{00} + \beta u_{10})\,|0\rangle + (\alpha u_{01} + \beta u_{11})\,|1\rangle$$

* deterministic
* reversible
* correspond to rotations of the Bloch sphere

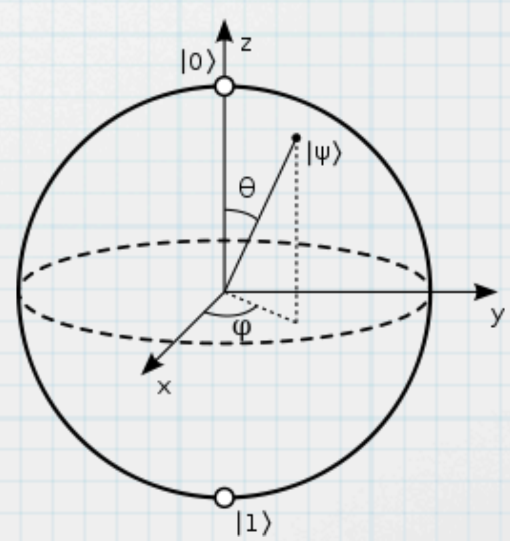
Examples

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

negation (X)

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Hadamard (H)



Two qubits (and more)

$$\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

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

Examples:

$$\tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

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

separable state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

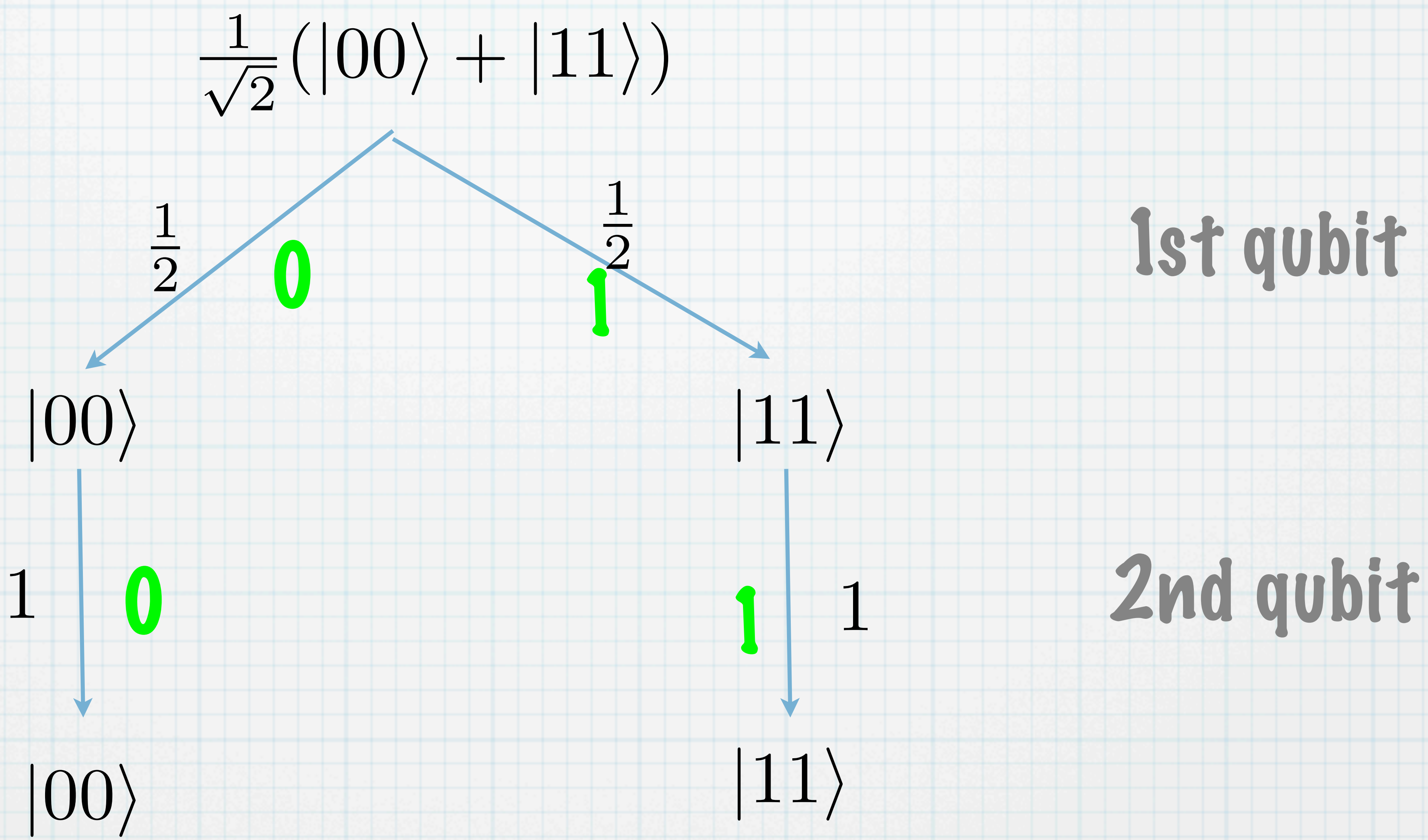
entangled state
(Bell state)

- Tensorproduct of qubits
- subset of a 4-dimensional vectorspace
- How many dimensions do we get for 3 qubits?

Measurements on 2 qubits

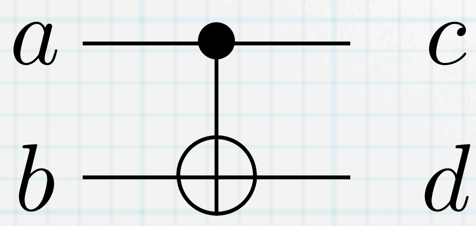
$$
\begin{tikzcd}[column sep=small]
 & & & \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \arrow[dll, "\frac{1}{2}"', "0"] \arrow[drr, "\frac{1}{2}", "1"'] & & & & \text{1st qubit} \\
 & \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \arrow[dl, "\frac{1}{2}"', "0"] \arrow[dr, "\frac{1}{2}", "1"'] & & & & \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle) \arrow[dl, "\frac{1}{2}"', "0"] \arrow[dr, "\frac{1}{2}", "1"'] & & \text{2nd qubit} \\
|00\rangle & & |01\rangle & & |10\rangle & & |11\rangle &
\end{tikzcd}
$$

Measurements on 2 qubits



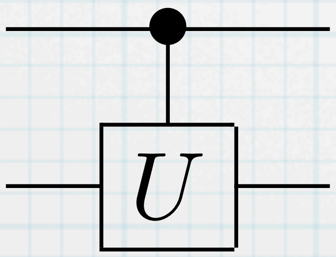
Unitaries on several qubits

cnot

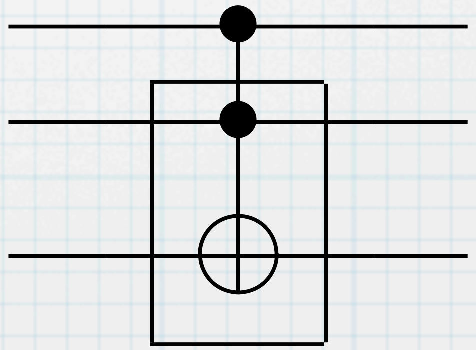


a	b	c	d
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

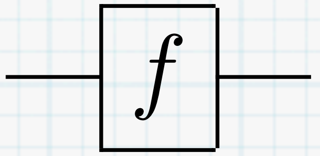
cond-U



Toffolli

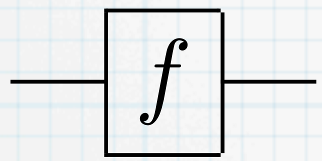


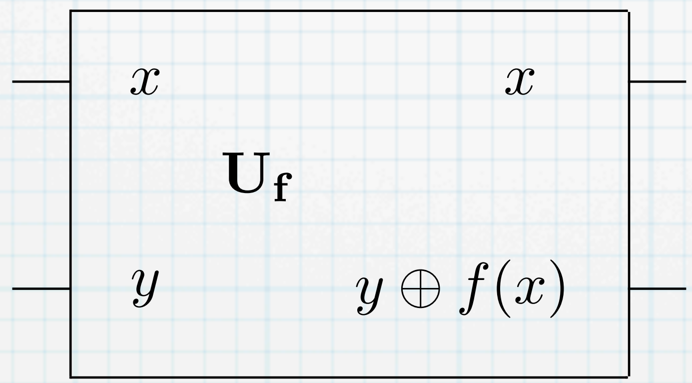
Deutsch's algorithm

Given a classical gate 

- Determine wether f is constant.
- But you may use f only once.
- Impossible !

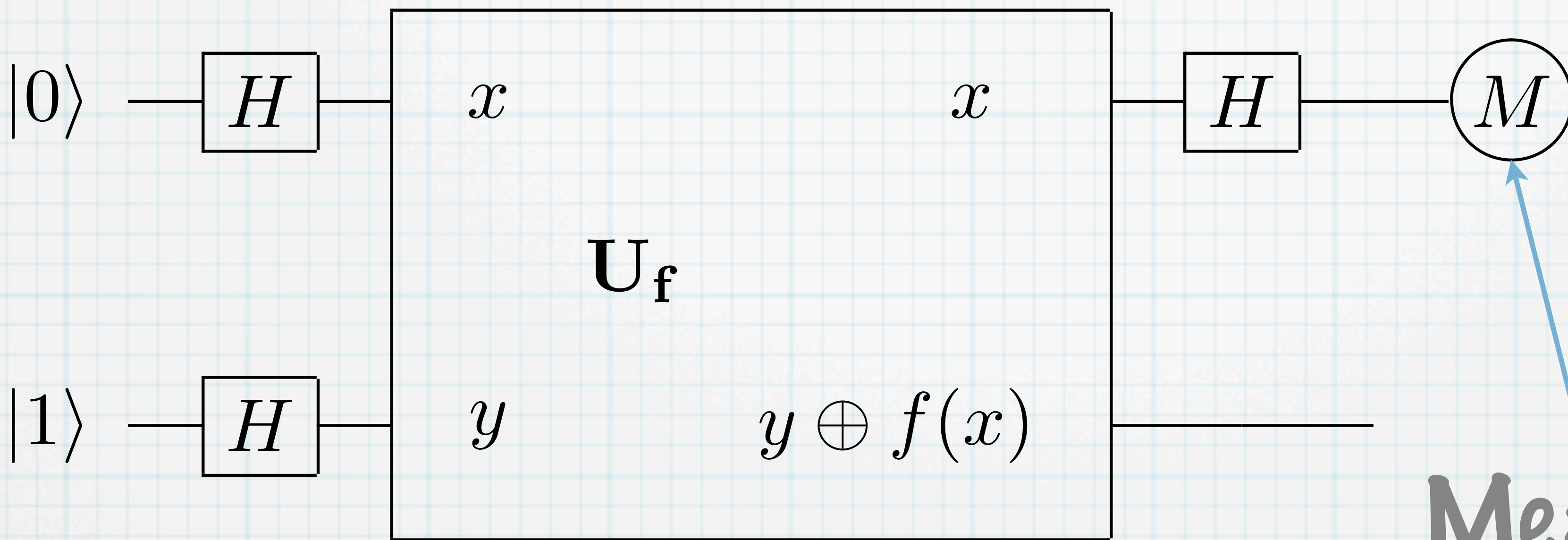
Deutsch's algorithm

Replace 

by a unitary: 

* There is a quantum circuit to determine wether f is constant.
* Using the unitary only once!

Deutsch's algorithm



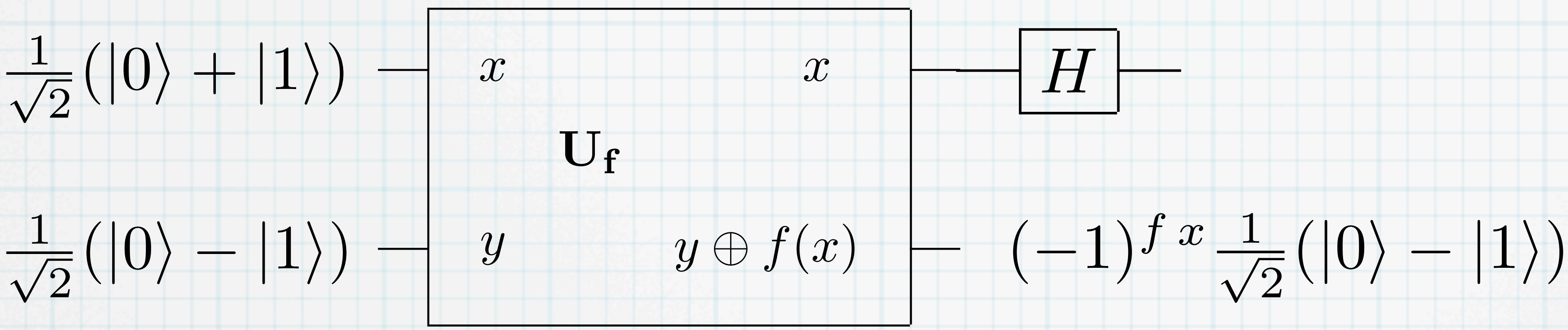
0 : f constant

1 : f not constant

Measurement.

Quantumparallelism: we observe a global property of f

Deutsch's Algorithm: How does it work?



$$\mathrm{f}\,0 = \mathrm{f}\ \ 1 \qquad \pm\tfrac{1}{4}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$\pm\frac{1}{\sqrt{2}}\,|0\rangle\,(|0\rangle - |1\rangle)$$

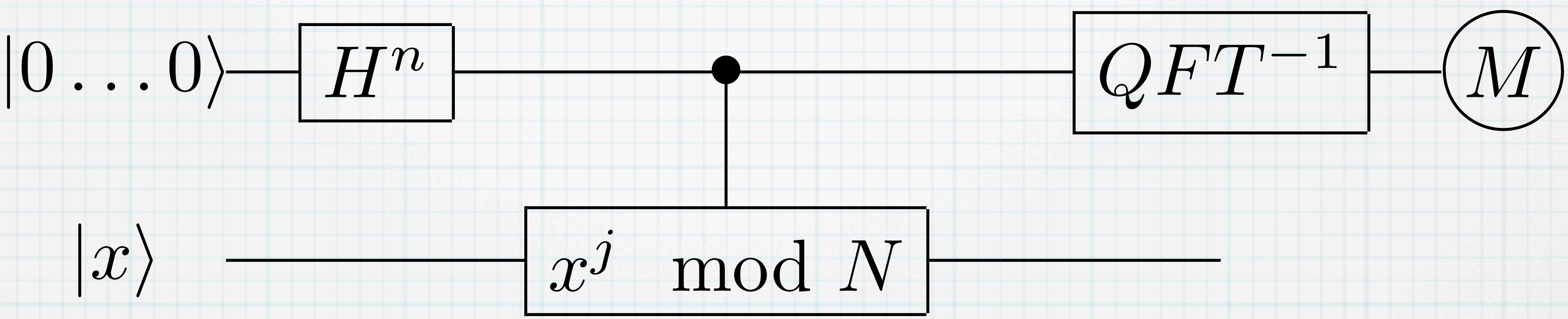
$$f\,0 \neq f\,1 \qquad \pm\tfrac{1}{4}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$

$$\pm\frac{1}{\sqrt{2}}\,|1\rangle\,(|0\rangle - |1\rangle)$$

Shor's algorithm

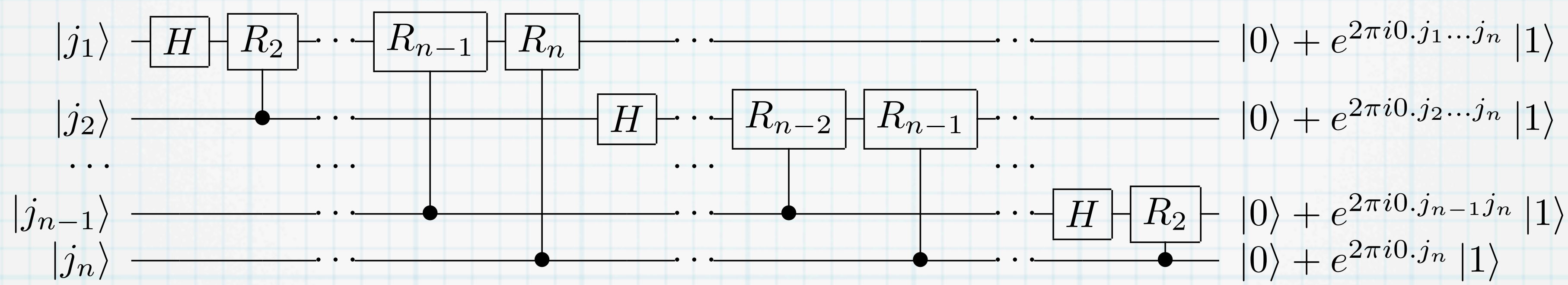
* Shor's algorithm also exploits quantum parallelism.
* Shor exploits a (probabilistic) reduction of FACTOR to order-finding
* Order finding: Given $x < N$ with no common factors, determine r such that $x^r \equiv 1 \mod N$

Shor's algorithm



* Need to implement reversible arithmetic
* Essential ingredient: Quantum Fourier Transform QFT
* QFT turns a frequency distribution into a value distribution.

Quantum Fourier Transform



* The (fast) Fourier transform is used in signal processing to obtain a frequency spectrum of a signal.

* Shor realized that we can apply Fourier transform to the (hidden) quantum state

* Applying the same idea as for the fast Fourier transform this results in a polynomially sized circuit.

* Here we are observing the frequency of the modular exponentiation

Research topics

* Quantum hardware
  * Ion trap
  * One-way quantum computer
* Quantum algorithms
  * Quantum error correction
  * Grover's algorithm
* Mathematical structures
  * Coecke's Kindergarten QM
* Quantum Programming Languages
  * QML, QIO monad