Lecture 1: From Classical to Quantum Computing

Outline

- Brief history of quantum computing.
- Computational problems and efficiency of algorithms.
- Classical circuits and their matrix representation.
- The qubit and its mathematical description.

Intended Learning Outcomes

- Remembering the relationship between physics and computing and what is the current state of quantum computing.
- Analysing the efficiency of algorithms.
- Applying the matrix representation of classical gates.
- Creating new gates using the tensor product.
- Understanding the mathematical description of a qubit.

Why this matters

- Quantum computing allows computations impossible with a classical computer.
  - Deepens understanding of nature and of computational complexity.
  - Technological applications to healthcare, materials design, finance, etc. Several governments and tech companies heavily investing, industry grew by 30% from 2024 to 2025 and expected to continue growing [1]
- Notion of efficiency heart of understanding quantum advantage.
- Mathematical formalism based on linear algebra over complex numbers. Central to quantum theory and other branches of natural sciences and engineering, e.g. machine learning, optimisation.

[1] https://quantumconsortium.org/publications/stateofthequantumindustry2025/

1 A Brief History of Quantum Computing

- Computational devices are physical. Physics determine computational models and their efficiency.
- Classical computers follow classical physics, can be simulated by billiard balls:

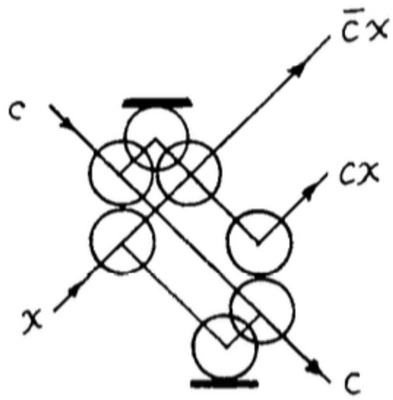


Figure 1: A switch gate realised by billiard balls with perfectly elastic collisions. The presence or absence of a ball corresponds to a bit being 1 or 0. From Fredkin & Toffoli, “Conservative logic” (1982).

- Quantum computers follow quantum physics.

INTERNATIONAL YEAR OF
Quantum Science
and Technology

Figure 2: 2025 is UNESCO Year of Quantum

- 2025: anniversary discovery of quantum mechanics by W. Heisenberg in 1925.

(a) Werner Heisenberg

(b) Erwin Schrödinger

Figure 3: The foundation fathers of quantum mechanics.

- Quantum mechanics explains phenomena that classical mechanics cannot
  - Example: Mach-Zender interferometer.

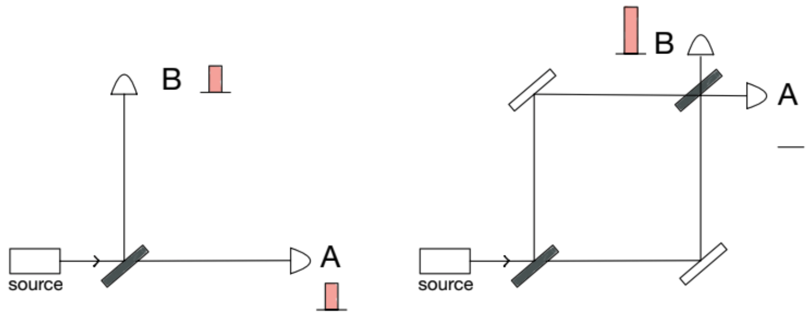


Figure 4: A source of light (photons) hits a beam-splitter (half silvered mirror). Left: measure photon at either A or B. Right: add mirrors and another beam-splitter, measure a photon only at B.

  - If photon classical particle, explain left experiment since photon goes through or turns left. However, cannot explain right experiment.
  - Solution: associate one amplitude per path ϕ_1, ϕ_2. Destructive interference at A and constructive at B.
- Quantum mechanics most accurate physical theory. The electromagnetic fine-structure constant α agrees with experiments within part in a billion.
- P.A.M. Dirac in 1929: "The fundamental laws [...] completely known, [...] difficulty [...] equations that are too complex to be solved."
  - n quantum particles each with k configurations described by k^n amplitudes.
- 1980's: R. Feynman and Y. Main conceived a quantum mechanical computer to simulate nature

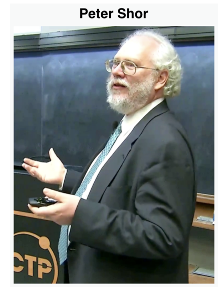
  Nature isn't classical, dammit!

(a) Yuri Manin

(b) Richard Feynman

- 1985: D. Deutsch proposes to use quantum computers for other problems than physics simulation.

- 1994: P. Shor finds an algorithm to factor integers exponentially faster than any known classical algorithm. 1995: P. Shor introduces quantum error correction



- ... A lot of work on building a quantum computer ...

- 2011: First commercial quantum computer by D-Wave. Not universal.

- Today:

  - Gate-based quantum computers with hundreds noisy qubits.
  - They can already do computations intractable for classical computers, however commercial applications not yet demonstrated.

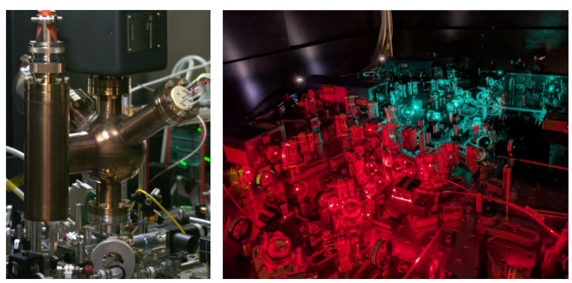


Figure 6: Left: Vacuum chamber housing ion trap chip. Right: Optics preparing visible lasers that drive transitions between energy levels. Source.

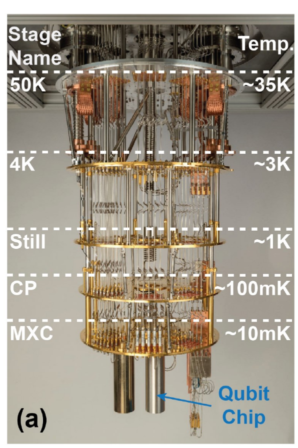


Figure 7: A quantum computer based on superconducting qubits require a fridge to cool down the system.

- Current **challenges**
  - Implement quantum error correction
  - Discover novel quantum algorithms
  - Ethics and regulations
    * Quantum computers can discover better drugs to cure disease and more sustainable materials.
    * They can also break RSA cryptosystems, threatening security of communication.
    * Quantum algorithms have dual use and can be used for nefarious purposes, e.g. weapons.
    * Quantum computing dev concentrated in a few countries, how can everyone benefit from quantum technologies?

2 Motivating Examples

- **Computational problem**: compute function from n to m bits.
- General: integral approximation and bitwise representation $x = \sum_{i=0}^{n-1} x_i 2^i, x_i \in \{0, 1\}$.
  - **Integer factoring**: find prime factors of the integer x.
    * Example: $x = 15$, return $y =$.
    * Classical hardness underlies security of public-key cryptography behind internet transaction.
    * Shor's algorithm can solve this problem efficiently.
  - **3SAT problem**: is there a p-bit string z that satisfies all clauses $C_i(z)$? C_i is the logical OR of 3 variables or their negation.
    * Example: $p = 4$: $C_1(z) = z_1 \vee z_2 \vee z_3$, $C_2(z) = \neg z_2 \vee \neg z_3 \vee z_4$
      Answer:
    * Central problem in computational complexity, one of the hardest problems.
    * We do not believe quantum computers can solve this efficiently.

3 Efficiency of Algorithms

- Efficiency of algorithm to compute function depends on 1) computational model (classical vs quantum), 2) resource.
- Focus on **worst case runtime**
- Asymptotic complexity: growth with input size n, avoid manufacture hardware details.
- **big-O notation**: f is $\mathcal{O}(g(n))$ if there exists n_0 and $C \geq 0$ such that for $n \geq n_0$, $|f(n)| \leq C|g(n)|$.

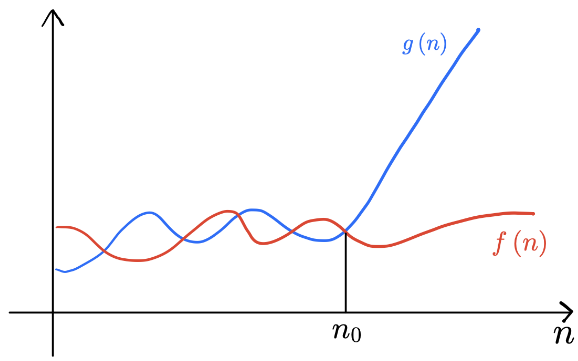


Figure 8: $f(n)$ being $\mathcal{O}(g(n))$ means that after some n_0, $f(n)$ is upper bounded by $Cg(n)$.

- Efficient if runtime is $\mathcal{O}(p(n))$ with $p(n)$ **polynomial** of n.
- If no polynomial algorithm, problem is hard. Note: if $n > 265$, then 2^n is greater than atoms in the universe!

4 Classical Circuits

- Mathematical model of classical computer.
- **wires** (carry bits) and **gates** (transform bits).

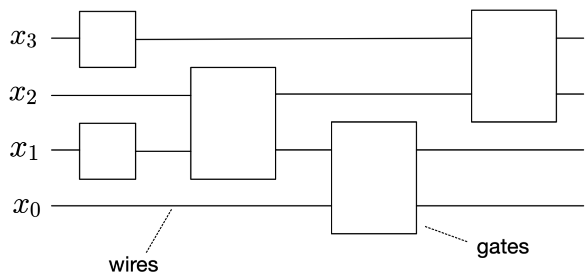


Figure 9: A classical circuit with $n = 4$ input bits x_0, x_1, x_2, x_3 and $m = 4$ outputs. Note that we label the bits from 0 to $n-1$ and from bottom to top.

- Gate with k inputs/outputs is function $g : \{0,1\}^k \to \{0,1\}^k$.
- **Reversible** if there exists g^{-1} such that $g(g^{-1}(x)) = x$ for all x.
- We can implement any function $f : \{0,1\}^k \to \{0,1\}^\ell$ reversibly. $R_f : \{0,1\}^{k+\ell} \to \{0,1\}^{k+\ell}$

$$R_f : (x, y) \mapsto (x, y \oplus f(x)) \,.$$

  by taking $y = 0$. Bitwise XOR:

$$x_{n-1} \cdots x_1 x_0 \oplus y_{n-1} \cdots y_1 y_0 = z_{n-1} \cdots z_1 z_0 \,, \quad z_i = x_i \oplus y_i$$
$$0 \oplus 0 = 1 \oplus 1 = 0 \,, \quad 0 \oplus 1 = 1 \oplus 0 = 1 \,.$$

- Inverse of R_f is R_f: check

$$(R_f)^2 : (x, y) \mapsto R_f(x, y \oplus f(x)) = (x, y \oplus f(x) \oplus f(x)) = (x, y)$$

thats identity!

- Reversible gates important in quantum computing.
- Runtime algorithm is number **elementary gates**.
  - Elementary means acting on constant number of inputs/outputs. Which set irrelevant for asymptotic complexity.
  - Efficient: polynomial gates.
  - Universal gates: implement any functions. E.g. AND and XOR.

5 Matrix Representation of Classical Gates

5.1 Single Bit Gates

5.1.1 Dirac notation

→ Says on which position the „1" stands, zero-based

- Bit: $x \in \{0, 1\}$. Represent as a two-dimensional one-hot vector:

$$0 \mapsto |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad 1 \mapsto |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- $|v\rangle$: "ket", Dirac notation. Analogous to $\vec{v}$.
- Name from bracket or inner product or scalar product. Define "bra"

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

and their scalar products denoted as $\langle x|y\rangle$ $\quad \langle\ \rangle \sim [\text{braket}]$

$$\langle 0|0\rangle = 1$$

$$\langle 0|1\rangle = 0$$

$$\langle 1|0\rangle = 0 \qquad \sim \oplus$$

$$\langle 1|1\rangle = 1$$

- $|0\rangle, |1\rangle$ for an orthonormal basis of $\mathbb{R}^2$. → jsou na sebe kolmé: $\langle 0|1\rangle = \langle 1|0\rangle = 0$
jsou normální: $\langle 1|1\rangle = \langle 0|0\rangle = 1$
- $|x\rangle\langle y|$ are matrices:

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad |1\rangle\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

- Compatible with matrix multiplication.
$\langle x|y\rangle$: 1×2 by $2 \times 1 \to 1 \times 1$ scalar
$|x\rangle\langle y|$: 2×1 by $1 \times 2 \to 2 \times 2$ matrix.
- Also, note:

$$(|x\rangle\langle y|)\,|z\rangle = \langle y|z\rangle\,|x\rangle$$

↪ linearity of scal. product.

- Resolution of unity:

$$|0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$$

- Matrix elements:

$$M = \begin{pmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \end{pmatrix}$$

the matrix element $M_{xy} = \langle x| M |y\rangle$. For example,

$$\langle 0| M |1\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \cdot 0 \end{pmatrix} \cdot \begin{pmatrix} M_{01} \\ M_{11} \end{pmatrix}$$

$$= M_{01}$$

- still not knowing what this notation is for...

- can be extended two any dimension instead of just 2.

linearity

$M|0\rangle = |0\rangle(\langle 0| + \langle 1|)|0\rangle$

$\langle 0|0\rangle + \langle 1|0\rangle$

$1 + 0$

5.1.2 Gates

- Four possible Boolean functions from bit x to bit y:

x	y
0	0
1	0

$M = |0\rangle(\langle 0| + \langle 1|)$,

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

pos. $\quad (1\ 1)$

x	y
0	1
1	1

$M = |1\rangle(\langle 0| + \langle 1|)$

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

$M = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$

x	y
0	1
1	0

$M = |0\rangle\langle 1| + |1\rangle\langle 0| = X$,

$(|0\rangle\langle 1| + |1\rangle\langle 0|)|0\rangle = (|0\rangle\langle 1|)|0\rangle + (|1\rangle\langle 0|)|0\rangle = |1\rangle$

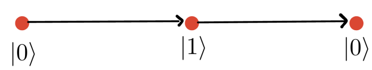
$M = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$

x	y
0	0
1	1

$M = |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbf{1}_2$

inversion

- Interpret M as deterministic dynamical system: $|x\rangle^{t+1} = M|x\rangle^t$, e.g. $M = X$



t	0	1	2
$\lvert x\rangle^t$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$

Figure 10

- Reversible functions: X (NOT gate), $\mathbf{1}_2$. Dynamics can be time reversed

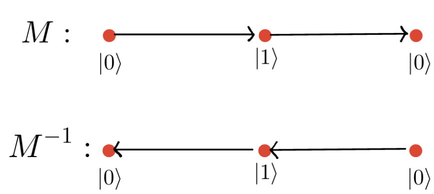


Figure 11

$X^2 = (|0\rangle\langle 1| + |1\rangle\langle 0|) \cdot (|0\rangle\langle 1| + |1\rangle\langle 0|)$

$= |0\rangle\underbrace{\langle 1|0\rangle}_{0}\langle 1| + |1\rangle\underbrace{\langle 0|0\rangle}_{1}\langle 1| + |0\rangle\underbrace{\langle 1|1\rangle}_{1}\langle 0| + |1\rangle\underbrace{\langle 0|1\rangle}_{0}\langle 0|$

$= |1\rangle\langle 1| + |0\rangle\langle 0|$

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

This is actually quite cool notation

5.2 States of two bits

- 4 states of 2: $|x_1 x_0\rangle, x_0, x_1 \in \{0,1\}$: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, four-dimensional one-hot vector:

$$|00\rangle \equiv |0\rangle_2 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle \equiv |1\rangle_2 = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle \equiv |2\rangle_2 = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle \equiv |3\rangle_2 = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

- Label right to left, 1 in the position integer associated with bit string:

$$|x_1 x_0\rangle \equiv \left|2^1 x_1 + 2^0 x_0\right\rangle_2$$

↳ bit repr. of this int.

- **Tensor product**

↗ just one long noodle

$$|\psi\rangle = \begin{pmatrix}\psi_1\\ \psi_2\end{pmatrix}, |\phi\rangle = \begin{pmatrix}\phi_1\\ \phi_2\end{pmatrix}, \quad |\psi\rangle \otimes |\phi\rangle = \begin{pmatrix}\boxed{\psi_1}|\phi\rangle\\ \boxed{\psi_2}|\phi\rangle\end{pmatrix} = \begin{pmatrix}\psi_1\phi_1\\ \psi_1\phi_2\\ \psi_2\phi_1\\ \psi_2\phi_2\end{pmatrix}$$

finish as an exercise

- Check $|x_1 x_0\rangle = |x_1\rangle \otimes |x_0\rangle$

$\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |00\rangle$ ✓

$$|0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\cdot 1\\ 1\cdot 0\\ 0\cdot 1\\ 0\cdot 0\end{pmatrix}, \quad |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\cdot 0\\ 1\cdot 1\\ 0\cdot 0\\ 0\cdot 1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = |01\rangle$$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\cdot 1\\ 0\cdot 0\\ 1\cdot 1\\ 1\cdot 0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |10\rangle, \quad |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\cdot 0\\ 0\cdot 1\\ 1\cdot 0\\ 1\cdot 1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = |11\rangle$$

- Summary: with $x = 2^1 x_1 + 2^0 x_0$ – sometimes omit $\otimes$ since no ambiguity

$$|x_1 x_0\rangle \equiv |x_1\rangle \otimes |x_0\rangle \equiv |x_1\rangle |x_0\rangle \equiv |x\rangle_2$$

- Inner product $|\psi_1\rangle \otimes |\phi_1\rangle$ with $|\psi_2\rangle \otimes |\phi_2\rangle$ (proof, see exercises)

$\langle \psi_2 \phi_2 | \psi_1 \phi_1 \rangle$

$$(\langle\psi_2| \otimes \langle\phi_2|)(|\psi_1\rangle \otimes |\phi_1\rangle) = \langle\psi_2|\psi_1\rangle \langle\phi_2|\phi_1\rangle = \langle 0|1\rangle \cdot \langle 1|0\rangle = 0 \cdot 0$$

- Example

$$(\langle 0| \otimes \langle 1|)(|1\rangle \otimes |0\rangle) = \begin{pmatrix}0 & 1 & 0 & 0\end{pmatrix} \cdot \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = 0$$

check home

5.3 Transformations of two bits

- Functions 2 to 2 bits as $2^2 \times 2^2$ matrices. Example: Dirac and matrix notation.

x_1	x_0	y_1	y_0
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

$M =$ $|00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11| =$

$M|00\rangle = |00\rangle \cdot \underbrace{\langle 00|00\rangle}_{1} + |10\rangle \underbrace{\langle 01|00\rangle}_{0} + |01\rangle \cdot \underbrace{\langle 10|00\rangle}_{0} + |11\rangle \cdot \underbrace{\langle 11|00\rangle}_{0}$

= everything goes to 0

– we can do the rest at home

$(|x\rangle\langle y|)|z\rangle = |x\rangle$

- SWAP gate

$$S_{01}|x\rangle|y\rangle = |y\rangle|x\rangle$$

Note $S_{01} = S_{10}$.

- CNOT (Controlled-NOT) C_{ij}. Not symmetric: i control, j target. Target flips if control is 1:

bit num: 1. 0.

$C_{10}|1\rangle|y\rangle = |1\rangle|\underbrace{y \oplus 1}_{\bar{y}}\rangle$

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle , \quad C_{01}|x\rangle|y\rangle = |x \oplus y\rangle|y\rangle ,$$

Recall $\oplus =$ XOR: $0 \oplus 0 = 0, 0 \oplus 1 = 1 \oplus 0 = 1, 1 \oplus 1 = 0$.

- Dirac and matrix notation:

$$C_{10}|00\rangle = |00\rangle$$
$$C_{10}|01\rangle = |0\rangle \otimes |1 \otimes 0\rangle = |01\rangle$$
$$C_{10}|10\rangle = |1\rangle \otimes |0 \otimes 1\rangle = |11\rangle$$
$$C_{10}|11\rangle = |1\rangle \otimes |1 \otimes 1\rangle = |10\rangle$$

$\rightarrow$

00	00
01	01
10	11
11	10

$|\text{output}\rangle\langle\text{input}|$

$= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$

$$\Rightarrow C_{10} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle \cdot \langle 11| .$$

- Reversible:

$$C_{10}^2|x\rangle|y\rangle =$$

$C_{10}^2 = 1_4$

$$M = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

$$M|01\rangle = |00\rangle\underbrace{\langle 00|01\rangle}_{0} + |01\rangle\underbrace{\langle 10|01\rangle}_{0} + |10\rangle\underbrace{\langle 01|01\rangle}_{1} + |11\rangle\underbrace{\langle 11|01\rangle}_{0} = |10\rangle$$

$$M|10\rangle = |00\rangle\underbrace{\langle 00|10\rangle}_{0} + |01\rangle\underbrace{\langle 10|10\rangle}_{1} + |10\rangle\underbrace{\langle 01|10\rangle}_{0} + |11\rangle\underbrace{\langle 11|10\rangle}_{0} = |01\rangle$$

$$M|11\rangle = |00\rangle\underbrace{\langle 00|11\rangle}_{0} + |01\rangle\underbrace{\langle 10|11\rangle}_{0} + |10\rangle\underbrace{\langle 01|11\rangle}_{0} + |11\rangle\underbrace{\langle 11|11\rangle}_{1} = |11\rangle$$

Controlled – NOT $\qquad C_{ij}$: i = control, j = target

$$C_{10}|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus x\rangle$$

$$C_{01}|x\rangle \otimes |y\rangle = |x \oplus y\rangle \otimes |y\rangle$$

– indices counted from right

- Reversible transformation 2 bits is $A \otimes B$ where A, B are reversible 1 bit gates, i.e. $A, B \in \{\mathbf{1}_2, X\}$.
- Tensor product matrices

$$A \otimes B \, |\psi\rangle \otimes |\phi\rangle = A\,|\psi\rangle \otimes B\,|\phi\rangle$$

first apply matrix
then apply a tensor product

- $A \otimes B$ is $MN \times MN$ matrix:

$$A \otimes B = \begin{pmatrix} A_{00}B & \dots & A_{0,N-1}B \\ \vdots & \ddots & \vdots \\ A_{N-1,0}B & \dots & A_{N-1,N-1}B \end{pmatrix}$$

→ going block by block

- In our case:

$$X \otimes \mathbf{1}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\mathbf{1}_2 \otimes X =$$

$$X \otimes X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

→ transpose matrix

- Note

$$C_{10} = |0\rangle\langle 0| \otimes \mathbf{1}_2 + |1\rangle\langle 1| \otimes X\,,$$
$$C_{01} = \mathbf{1}_2 \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|\,.$$

$M = C_{10}$

Check:

$$|0\rangle\langle 0| \otimes \mathbf{1}_2 + |1\rangle\langle 1| \otimes X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \left(\begin{array}{cc|cc} 1 & 0 & & \\ 0 & 1 & & \\ \hline & & & \\ & & & \end{array}\right) + \left(\begin{array}{cc|cc} & & & \\ & & & \\ \hline & & 0 & 1 \\ & & 1 & 0 \end{array}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$M|10\rangle = M|11\rangle$

5.4 States of n bits

- n bits, 2^n bit strings:

one-hot vector

$$|x_{n-1} \cdots x_0\rangle = |x_{n-1}\rangle \otimes \cdots \otimes |x_0\rangle \equiv \underline{|x\rangle_n} \; , \quad x = \sum_{j=0}^{n-1} 2^j x_j \; ,$$

$\{|x\rangle_n\}_{x=0}^{N-1}$ orthonormal basis of $\mathbb{R}^N$, $N = 2^n$.

- n-fold tensor product recursively using (output has length MN)

$$|\psi\rangle = \begin{pmatrix} \psi_0 \\ \vdots \\ \psi_{N-1} \end{pmatrix} , |\phi\rangle = \begin{pmatrix} \phi_0 \\ \vdots \\ \phi_{M-1} \end{pmatrix} , \quad |\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \psi_0 \, |\phi\rangle \\ \psi_1 \, |\phi\rangle \\ \vdots \\ \psi_{N-1} \, |\phi\rangle \end{pmatrix}$$

- Example: $n = 3$

$$|110\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \\ \hline 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \hline 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |6\rangle_3 \; .$$

again on position 6 (zero-based)

implicitly doing $\otimes$ instead of multiplying into matrices

- Notation

$$|x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle \equiv |x_2\rangle \, |x_1\rangle \, |x_0\rangle \equiv |x_2 x_1 x_0\rangle$$

5.5 Transformations of n bits

- Functions of n bits are represented by $2^n \times 2^n$ matrices. Reversible: permutations.
- SWAP 1-st and 3-rd bits

$$S_{31} |x_3\rangle |x_2\rangle |x_1\rangle |x_0\rangle = |x_1\rangle |x_2\rangle |x_3\rangle |x_0\rangle$$

- CNOT C_{ij} (recall: i control, j target)

control target

$$C_{20} \underset{2.}{|x_3\rangle |x_2\rangle} \underset{0.}{|x_1\rangle |x_0\rangle} = |x_3\rangle |x_2\rangle |x_1\rangle |x_0 \oplus x_2\rangle$$

- Shortcut notation for 2×2 matrix A acting on the i-th vector of an n-fold tensor product:

$$A_i = \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes \cdots \otimes A \otimes \cdots \otimes \mathbf{1}_2 \, .$$

counting from right

- Example: $n = 3$

$$X_1 = \mathbb{1}_2 \otimes X \otimes \mathbb{1}_2 \quad , \quad X_1 |x_2\rangle |x_1\rangle |x_0\rangle = \mathbb{1}_2 |x_2\rangle \cdot X|x_1\rangle \cdot \mathbb{1}_2 |x_0\rangle = |x_2\rangle |\bar{x}_1\rangle |x_0\rangle$$

- Operators on different bits commute: $A_i B_j = B_j A_i$ if $i \neq j$. Example, $n = 6$:

$$A_3 B_1 = \mathbf{1}_2 \otimes \mathbf{1}_2 \otimes A \otimes \mathbf{1}_2 \otimes B \otimes \mathbf{1}_2 = B_1 A_3$$

- Similarly, A_{ij} the 4×4 matrix on the i and j bits, e.g. S_{ij} and C_{ij} above.

$$\underbrace{(\mathbb{1}_2 \otimes \mathbb{1}_2 \otimes A \otimes \mathbb{1}_2 \otimes \mathbb{1}_2 \otimes \mathbb{1}_2)}_{A_3} \cdot \underbrace{(\mathbb{1}_2 \otimes \mathbb{1}_2 \otimes \mathbb{1}_2 \otimes \mathbb{1}_2 \otimes B \otimes \mathbb{1}_2)}_{B_1}$$

$$X_1 = \mathbb{1}_2 \otimes X \otimes \mathbb{1}_2$$

$$X_1 |x_1\rangle |x_2\rangle |x_3\rangle = (\mathbb{1}_2 \otimes X \otimes \mathbb{1}_2) \cdot (|x_1\rangle |x_2\rangle |x_3\rangle) = \mathbb{1}_2 |x_1\rangle \otimes X \cdot |x_2\rangle \otimes \mathbb{1}_2 |x_3\rangle$$

$$= |x_1\rangle |\bar{x}_2\rangle |x_3\rangle$$

Summary

- A computational problem is modelled mathematically as computing a function from n to m bits, e.g. the problem of factoring integers or finding a satisfying assignment to a Boolean formula.
- The efficiency of an algorithm depends on the computational model used to run it. An algorithm is efficient if its runtime grows as $\mathcal{O}(p(n))$ where $p(n)$ is a polynomial of the input size of the problem n.
- A classical circuit is a model of a classical computer that has wires and gates.
- We can associate one-hot vectors to bit strings and matrices to gates. The states and gates of many bits are described by the tensor product.
- Important reversible classical gates are the NOT gate (also called the X gate), the CNOT gate, and the SWAP gate.

6 Manipulating single qubits

6.1 Qubit

6.1.1 Complex numbers

- Imaginary number i, $i^2 = -1$, define complex number $c = a + ib$, $a, b \in \mathbb{R}$. $\mathbb{C}$ set complex numbers, $a = \mathrm{Re}(c)$ real part, $b = \mathrm{Im}(c)$ imaginary part.

- Usual addition, product rules: example:

$$(1+i)(2-3i) = 5 - i$$

- $\bar{c} = a - ib$ complex conjugate, $|c|^2 = c\bar{c} = a^2 + b^2$ modulus squared. example:

$$\overline{1+i} = 1 - i$$
$$|1+i|^2 = 2 \qquad c = 1 + 1i \Rightarrow 1^2 + 1^2 = 2$$

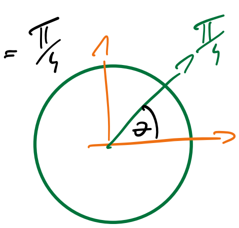
|c| is the size of the vector, θ defines the direction

- Polar representation: with $\rho = |c|$, Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$

$$c = \rho(\cos(\theta) + i\sin(\theta)) = \underbrace{\rho}_{\text{modulus}}\underbrace{\mathrm{e}^{i\theta}}_{\text{angle}} \longrightarrow \text{proven with Taylor expansion}$$

example

$$c = 1 + i = \sqrt{2} \cdot (\cos\theta + i\sin\theta) \qquad \theta \text{ s.t. } \begin{array}{l} \sqrt{2}\cos\theta = 1 \\ \sqrt{2}\sin\theta = 1 \end{array} \rightarrow \theta = \pi/4$$



- Product, division in polar representation

$$c_1 c_2 = \rho_1\rho_2 \mathrm{e}^{i(\theta_1+\theta_2)}\,, \quad c_1/c_2 = \rho_1/\rho_2 \mathrm{e}^{i(\theta_1-\theta_2)}\,.$$

- Complex vectors:

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} \in \mathbb{C}^2\,, \qquad \text{e.g. } |\psi\rangle = \begin{pmatrix} 1+i \\ 2-i \end{pmatrix} \in \mathbb{C}^2$$
$$\langle\psi| = (1-i,\ 2+i) \in \mathbb{C}^2$$

bra is transpose complex conjugate, also use adjoint symbol $|\psi\rangle^\dagger = \langle\psi|$

$$\langle\psi| = \begin{pmatrix} \overline{\psi_1} & \overline{\psi_2} \end{pmatrix}$$

? just as in lin. alg., the transpose is transposing the complex sign as well

Inner product

$$\langle\phi|\psi\rangle = \overline{\phi_1}\psi_1 + \overline{\phi_2}\psi_2\,.$$

Norm squared

$$\|\,|\psi\rangle\,\|^2 = \langle\psi|\psi\rangle = \overline{\psi_1}\psi_1 + \overline{\psi_2}\psi_2 = |\psi_1|^2 + |\psi_2|^2 \geq 0$$

? we need this to be positive number, therefore we need the complex transpositions

Similar for N-dimensional vectors $\mathbb{C}^N$

Qubit can be seen as a coin-flip. However, we have many assignments for $\alpha, \beta \in \mathbb{C}$

6.1.2 Qubit

$Prob(0) = |\alpha|^2$

$Prob(1) = |\beta|^2$

qubit $\in \mathbb{C}^2$

- Quantum state of a qubit is superposition of $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1\,.$$

- α, β called amplitudes. Interpret as probability in 0: $|\langle 0|\psi\rangle|^2 = |\alpha|^2$, probability in 1: $|\langle 1|\psi\rangle|^2 = |\beta|^2$. Note: normalisation

$$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$$

→ this makes it probability

thanks to this

- Global phase does not change the probability: $|\psi\rangle \equiv \mathrm{e}^{i\varphi}\,|\psi\rangle$.

→ $|\alpha|^2 = \alpha\bar{\alpha}$

$\beta = \alpha \cdot e^{i\varphi}$

$|\beta|^2 = \beta\bar{\beta} = \alpha \cdot \cancel{e^{i\varphi}} \cdot \bar{\alpha}\, \cancel{e^{-i\varphi}}$

$= \alpha\bar{\alpha}$

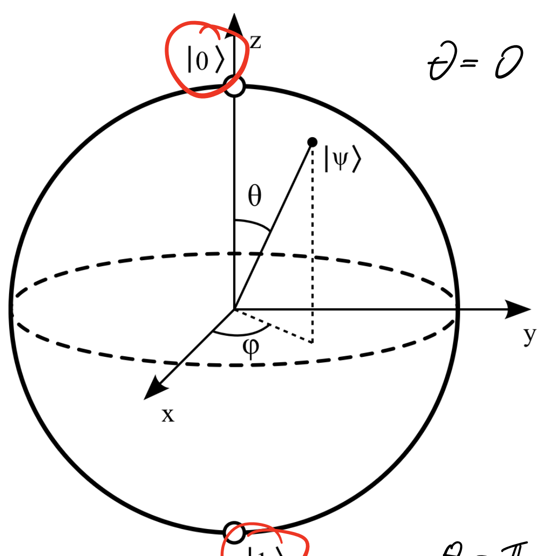
$\alpha \to \alpha \cdot e^{-i\gamma}$

$\beta \to \beta \cdot e^{-i\gamma}$

- Degrees of freedom: $\alpha = p\mathrm{e}^{i\gamma}, \beta = q\mathrm{e}^{i\varphi}$.
  - $p^2 + q^2 = 1 \Rightarrow p = \cos\left(\frac{\theta}{2}\right), q = \sin\left(\frac{\theta}{2}\right), \theta \in [0, \pi]$.
  - Global phase: $\alpha = p, \beta = q\mathrm{e}^{i(\varphi-\gamma)}$
  - Two angles: Bloch sphere

letters ran out

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\,, \quad \theta \in [0, \pi], \varphi \in [0, 2\pi)\,.$$



$\theta = 0\,,\ \cos 0 = 1\,,\ \sin 0 = 1$

$\theta = \pi\,,\ \cos\frac{\pi}{2} = 0\,,\ \sin\frac{\pi}{2} = 1$

Figure 12: Bloch sphere

How we represent qubit in reality?

- superconducting circuit

⋮

- One of the questions is to find physical implementation of a qubit.

6.2 Transformations of a qubit

- Adjoint matrix A as transpose complex conjugate:
  - $A^\dagger = \overline{A^T}$.
  - If $|\phi\rangle = A|\psi\rangle$, $\langle\phi| = \langle\psi| A^\dagger$.
  - $(AB)^\dagger = B^\dagger A^\dagger$.
- General linear transform $|\phi\rangle = U|\psi\rangle$, needs to preserve normalization:

$$\langle\phi|\phi\rangle = \langle\psi| U^\dagger U |\psi\rangle = \langle\psi|\psi\rangle = 1\,,$$

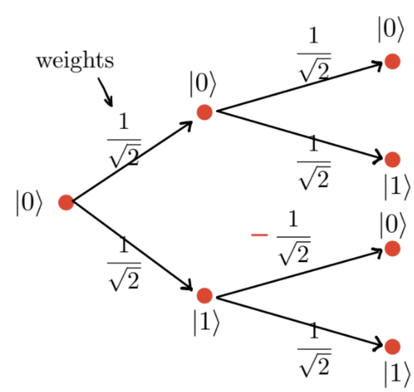
transformation of qubit is again a gate

$U^\dagger U = \mathbf{1}$: **unitary**.

- $U^{-1} = U^\dagger$, reversible

$$|\psi\rangle \to |\phi\rangle = U|\psi\rangle$$
$$|\psi\rangle = U^\dagger|\phi\rangle \leftarrow |\phi\rangle$$

- Discrete quantum dynamics $|\psi\rangle^{t+1} = U|\psi\rangle^t$. Example: $U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$



t	0	1	2
$\|\psi\rangle^t$	$\|0\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|1\rangle$
$\|\langle 0\|\psi\rangle^t\|^2$	1	$\frac{1}{2}$	0

$\Rightarrow \alpha = \beta = \frac{1}{\sqrt{2}}$

deterministic states

Figure 13

- Negative signs: destructive interference, deterministic outcome from randomised operation. Impossible with classical probabilities!

do at home

6.3 Single qubit gates

- Classical reversible gates are unitary

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{1}_2 = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

  Example

$$X|\psi\rangle = X(\alpha|0\rangle + \beta|1\rangle) =$$

- X is called the x Pauli matrix. Other important unitary gates:
  - The y and x Pauli matrices

$$Y = iXZ = -i|0\rangle\langle 1| + i|1\rangle\langle 0| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$
$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

  - Hadamard gate

$$H = \frac{1}{\sqrt{2}}(X+Z) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Relations
  - $XZ = -ZX$:

$$XZ = (|0\rangle\langle 1| + |1\rangle\langle 0|)(|0\rangle\langle 0| - |1\rangle\langle 1|) = |1\rangle\langle 0| - |0\rangle\langle 1|,$$
$$ZX = (|0\rangle\langle 0| - |1\rangle\langle 1|)(|0\rangle\langle 1| + |1\rangle\langle 0|) = |0\rangle\langle 1| - |1\rangle\langle 0|$$

  - $H^2 = \mathbf{1}_2$:

$$H^2 = \frac{1}{2}(X+Z)(X+Z) = \frac{1}{2}(X^2 + ZX + ZX + Z^2) = \mathbf{1}_2.$$

  - $HXH = Z$

$$HXH = \frac{1}{2}(X+Z)X(X+Z) = \frac{1}{2}(\mathbf{1}_2 + ZX)(X+Z)$$
$$= \frac{1}{2}(X + Z + Z + ZXZ) = Z.$$

  - $HZH = X$. This follows from the previous property and $H^2 = \mathbf{1}_2$.

- Measurement gate, irreversible: projects and returns readout bit (Born rule)

$$\alpha|0\rangle + \beta|1\rangle \to |x\rangle = \begin{cases} |0\rangle & \text{prob } |\alpha|^2 \\ |1\rangle & \text{prob } |\beta|^2 \end{cases}.$$

  Only way to get classical information from a qubit. Samples from binary random variable $p = (p_0, p_1)$ with

$$p_0 = |\alpha|^2, \quad p_1 = |\beta|^2 = 1 - |\alpha|^2.$$

6.4 Circuit diagrams for a single qubit

- **wire**: qubit, **gates**: transformations (unitary and measurement)

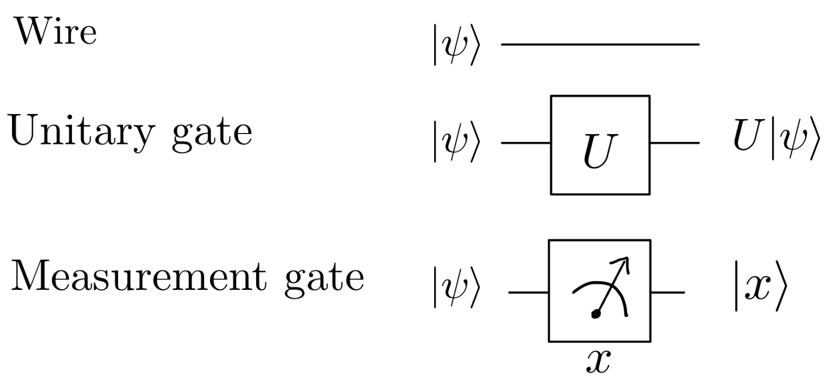


Figure 14

- Concatenation

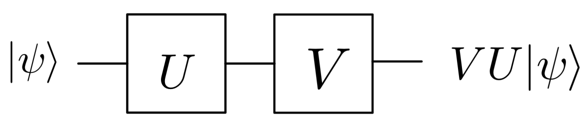


Figure 15

- Compute the probability of measuring $x = 0$

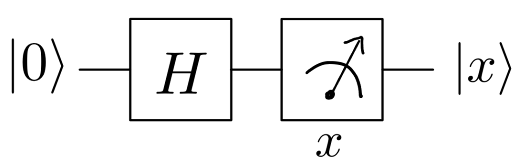


Figure 16

$$|0\rangle \mapsto H\,|0\rangle =$$

probability measuring 0 is

Summary

- Qubit superposition of classical bit strings, normalised complex vector.
- Quantum circuits give a convenient way to describe quantum a sequence of quantum gates.
- The most important unitary single qubit gates are the Pauli matrices and the Hadamard gate.
- Measurement gates are irreversible. Born rule dictates the outcome of a measurement.