ETH zürich

Od bitu ke qubitu a ještě kousek dál: Kvantové výpočty pro začátečníky

Václav Hapla

January 25, 2024

Outline

1. Introduction
2. Single classical systems
3. Multiple classical systems
4. Quantum systems
5. Finale

Outline

Nultý slajd

Všiml si někdo pokusu o slovní hříčku v názvu?

ChatGPT chat "Czech Language Discussion":
Tento název, "Od bitu ke qubitu a ještě kousek dál: Kvantové výpočty pro začátečníky", je vynikající. Využívá jemný humor spojený s dvojznačností slova "bit" (v angličtině základní jednotka digitálních dat a v češtině "kousek"), což může být velmi efektivní při zaujetí pozornosti studentů. Tento vtipný jazykový prvek nejen zpřístupňuje téma, ale také vytváří více uvolněnou a přátelskou atmosféru pro prezentaci, což je ideální pro středoškoláky, kteří se s kvantovými výpočty setkávají poprvé.

Something is going on...

- “Quantum computing” is becoming a buzzword.
- Many new startup companies dealing with QC arise, while well-established companies (IBM, Microsoft, Google, ...) create special quantum-oriented divisions and publish quantum roadmaps for years to come.
- Forbes, October 24, 2023: **“Atom Computing Announces Record-Breaking 1,225-Qubit Quantum Computer”**
- Nature News, December 4, 2023: **“IBM releases first-ever 1,000-qubit quantum chip”**
    - “IBM has unveiled the first quantum computer with more than 1,000 qubits. [...] But the company says that it will now shift gears and focus on making its machines more error-resistant rather than larger.”
- What does it all mean? Are quantum computers already running? Can they bring actual advantages? Do they bring them already?

What are we going to discuss today?

Outline

Deterministic states

- **Deterministic system** (or classical system): "something" (a device) that stores **information** by being in one of the finite number of **states**.
- More formally, a deterministic system is as a pair $(\Sigma, \mathbf{X})$, where Σ is a finite nonempty set (**deterministic state set**) whose elements are called **deterministic states** and $\mathbf{X} \in \Sigma$ is the **current state** of the system.
- Classical bit: $\Sigma = \{0, 1\}$
- Electric fan: $\Sigma = \{\text{off}, \text{low}, \text{mid}, \text{high}\}$
- Christmas lights: $\Sigma = \{\text{off}, \text{waves}, \text{sequential}, \text{flash}, \text{twinkle}, \text{glow}, \text{fade}, \text{steady}\}$

Deterministic states as vectors (1)

Bit:

$$|0\rangle = \begin{array}{cl} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{array}{l} \mathbf{0} \\ 1 \end{array} \end{array} \qquad |1\rangle = \begin{array}{cl} \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{array}{l} 0 \\ \mathbf{1} \end{array} \end{array}$$

Fan:

$$|\mathrm{off}\rangle = \begin{array}{cl} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} & \begin{array}{l} \textbf{off} \\ \text{low} \\ \text{mid} \\ \text{high} \end{array} \end{array} \quad |\mathrm{low}\rangle = \begin{array}{cl} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} & \begin{array}{l} \text{off} \\ \textbf{low} \\ \text{mid} \\ \text{high} \end{array} \end{array} \quad |\mathrm{mid}\rangle = \begin{array}{cl} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} & \begin{array}{l} \text{off} \\ \text{low} \\ \textbf{mid} \\ \text{high} \end{array} \end{array} \quad |\mathrm{high}\rangle = \begin{array}{cl} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} & \begin{array}{l} \text{off} \\ \text{low} \\ \text{mid} \\ \textbf{high} \end{array} \end{array}$$

- $|?\rangle$ is an example of **bra-ket / Dirac notation**.
  - Ubiquitous in quantum mechanics/computing but we won't go into details here.
  - For us today, it's just a label given to the vector.
- Notice the coordinate notation (on the right) reflects the **size** of state set Σ and the **current state**;
- but it quickly becomes cumbersome with the growing size 🤯

Deterministic states as vectors (2)

Bit:

$$|0\rangle = \left[\begin{array}{c}1\\0\end{array}\right]\begin{array}{l}\mathbf{0}\\1\end{array} \qquad |1\rangle = \left[\begin{array}{c}0\\1\end{array}\right]\begin{array}{l}0\\\mathbf{1}\end{array}$$

Fan:

$$|\mathrm{off}\rangle = \left[\begin{array}{c}1\\0\\0\\0\end{array}\right]\begin{array}{l}\textbf{off}\\\text{low}\\\text{mid}\\\text{high}\end{array} \quad |\mathrm{low}\rangle = \left[\begin{array}{c}0\\1\\0\\0\end{array}\right]\begin{array}{l}\text{off}\\\textbf{low}\\\text{mid}\\\text{high}\end{array} \quad |\mathrm{mid}\rangle = \left[\begin{array}{c}0\\0\\1\\0\end{array}\right]\begin{array}{l}\text{off}\\\text{low}\\\textbf{mid}\\\text{high}\end{array} \quad |\mathrm{high}\rangle = \left[\begin{array}{c}0\\0\\0\\1\end{array}\right]\begin{array}{l}\text{off}\\\text{low}\\\text{mid}\\\textbf{high}\end{array}$$

- Deterministic states form a **basis** (specifically the **standard basis**).
  - Important term which you will learn rigorously in your first linear algebra course 😉
  - Basis vectors are **linearly independent**: they *cannot* be expressed as a **linear combination** of each other;
  - while any vector of the given space *is* a linear combination of the basis vectors.
  - Linear combination? 🤔 It's just a weighted sum of vectors, e.g. $0.3\,|0\rangle + 0.7\,|1\rangle$

Probabilistic states

- Suppose we don't know for sure what is the current deterministic state $\mathbf{X}$ of a system.
- Assume, however, that based on some ***a priori* knowledge**, we can assign some probabilities to its N deterministic states $\Sigma = \{S_0, S_1, \ldots, S_{N-1}\}$.
- We can write down the probabilities succinctly using a **probability vector**:

$$|\mathbf{X}\rangle = \begin{array}{c} \begin{bmatrix} x_0 \\ \vdots \\ x_N \end{bmatrix} \end{array} \begin{array}{l} S_0 \\ \vdots \\ S_{N-1} \end{array} = x_0 \,|S_0\rangle + x_1 \,|S_1\rangle + \cdots + x_{N-1} \,|S_{N-1}\rangle \,,$$

$$x_i = P(\mathbf{X} = S_i) \quad \text{for all } i \in \{0, \ldots, N-1\}$$

- All entries of the vector must be **nonnegative real numbers**.
- The **sum** of the (absolute values of the) entries (1-norm or taxicab norm) is equal to one,

$$\|\,|\mathbf{X}\rangle\,\|_1 = \sum_{i=1}^{N} |x_i| = 1$$

Note!

- deterministic (classical) states $\subset$ probabilistic states
- I mean, any deterministic state can be regarded as a probabilistic state!

Measurement

- By **measurement** of a *probabilistic* state we will mean:
  - **Unambiguously recognize** the current deterministic state!
- Measurement updates our knowledge about the system.
- The *probabilistic* state before measurement can be in "superposition" of multiple *deterministic* states;
- upon measurement it "collapses" into one of the *deterministic* states.
- Measurement is often subjective as we will see!
- Measuring again and again doesn't bring anything new.

Example: Probabilistic bit (1)

- Suppose we don't know for sure what is the current deterministic state $\mathbf{X}$ of a bit;
- based on some ***a priori*** **knowledge**, we know just probabilities

$$P(\mathbf{X}=0)=0.75, \qquad P(\mathbf{X}=1)=0.25.$$

- More succinctly – using a **probability vector**:

$$|\mathbf{X}\rangle = \begin{bmatrix}0.75\\0.25\end{bmatrix} = 0.75\begin{bmatrix}1\\0\end{bmatrix} + 0.25\begin{bmatrix}0\\1\end{bmatrix} = 0.75\,|0\rangle + 0.25\,|1\rangle$$

- All entries of the vector are **nonnegative real numbers** and the taxicab norm is 1,

$$\|\,|\mathbf{X}\rangle\,\|_1 = \sum_{i=1}^{n} |x_i| = 0.75 + 0.25 = 1$$

Example: Probabilistic bit (2)

$$|\mathbf{X}\rangle = \begin{bmatrix} 0.75 \\ 0.25 \end{bmatrix} = 0.75\,|0\rangle + 0.25\,|1\rangle\,, \quad \|\,|\mathbf{X}\rangle\,\|_1 = 0.75 + 0.25 = 1$$

- **Measuring** the bit $\mathbf{X}$, we update our knowledge and the state collapsed to a deterministic state:

$$|\mathbf{X}\rangle = 0.75\,|0\rangle + 0.25\,|1\rangle \xrightarrow{\text{measure}} \begin{cases} |0\rangle\,, & P = 0.75, \\ |1\rangle\,, & P = 0.25, \end{cases}$$

i.e. $|\mathbf{X}\rangle$ after measurement is

$$|\mathbf{X}\rangle = |0\rangle \text{ with probability } P(\mathbf{X} = 0) = 0.75,$$
$$|\mathbf{X}\rangle = |1\rangle \text{ with probability } P(\mathbf{X} = 1) = 0.25.$$

- The measurement is subjective (e.g. I measured but didn't tell my friend the result).
- Measuring again and again doesn't bring anything new.
  - Of course! E.g. $|0\rangle = 1\,|0\rangle \xrightarrow{\text{measure}} |0\rangle\,,\ P = 1.$

Example: Coin

- Assume a **coin**:

$$\Sigma = \{\text{heads}, \text{tails}\}, \quad |\text{heads}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |\text{tails}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

- A coin just flipped, before looking at the result, is in “superposition”.
- A **fair** coin:

$$|\mathbf{X}\rangle = \begin{array}{c} \begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix} \end{array} \begin{array}{l} \scriptstyle\text{heads} \\ \scriptstyle\text{tails} \end{array} = 0.5\,|\text{heads}\rangle + 0.5\,|\text{tails}\rangle \xrightarrow{\text{measure}} \begin{cases} |\text{heads}\rangle\,, & P = 0.5, \\ |\text{tails}\rangle\,, & P = 0.5, \end{cases}$$

- An **unfair** coin:

$$|\mathbf{X}\rangle = \begin{array}{c} \begin{bmatrix} 0.49 \\ 0.51 \end{bmatrix} \end{array} \begin{array}{l} \scriptstyle\text{heads} \\ \scriptstyle\text{tails} \end{array} = 0.49\,|\text{heads}\rangle + 0.51\,|\text{tails}\rangle \xrightarrow{\text{measure}} \begin{cases} |\text{heads}\rangle\,, & P = 0.49, \\ |\text{tails}\rangle\,, & P = 0.51, \end{cases}$$

- The measurement is subjective.

Example: Card pile

- You have a **pile of 13 single-colour cards**: $\Sigma = \{2, 3, 4, 5, 6, 7, 8, 9, 10, \mathrm{J}, \mathrm{Q}, \mathrm{K}, \mathrm{A}\}$
- You ask a friend to pick one at random without showing it to you.
- The picked card's state before and after checking which symbol it actually has:

$$|\mathbf{X}\rangle = \frac{1}{13} \begin{array}{c} \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \end{array} \begin{array}{l} 2 \\ \vdots \\ \mathrm{A} \end{array} = \frac{1}{13} \left(|2\rangle + \cdots + |\mathrm{A}\rangle \right) \xrightarrow{\text{measure}} \begin{cases} |2\rangle \,, & P = 1/13 \\ \vdots \\ |\mathrm{A}\rangle \,, & P = 1/13 \end{cases}$$

- The measurement is subjective.

Example: Sportka 1

- A single "drum" of a **fair "ball lottery"** (like Šance by Sportka) with 10 numbered balls $\Sigma = \{0, 2, \ldots, 9\}$.
- The state before and after a ball is picked:

$$|\mathbf{X}\rangle = \frac{1}{10} \begin{array}{c} \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \end{array} \begin{array}{c} 0 \\ \vdots \\ 9 \end{array} = \frac{1}{10} \left(|0\rangle + \cdots + |9\rangle \right) \xrightarrow{\text{measure}} \begin{cases} |0\rangle \,, & P = 1/10 \\ \vdots & \\ |9\rangle \,, & P = 1/10 \end{cases}$$

- This time, the measurement is **objective**! Before the ball is picked, *nobody* knows the outcome.
- That brings us a little bit closer to quantum systems...

Example: Sportka 2

- A single "drum" of a **brutally unfair "ball lottery"** with 10 numbered balls $\Sigma = \{0, 2, \ldots, 9\}$.
- Spits out only 0 or 9 with probabilities $1/3$ and $2/3$ 😇
- The state before and after a ball is picked:

$$|\mathbf{X}\rangle = \begin{array}{c} \begin{bmatrix} \frac{1}{3} \\ 0 \\ \vdots \\ 0 \\ \frac{2}{3} \end{bmatrix} \end{array} \begin{array}{c} 0 \\ 1 \\ \vdots \\ 8 \\ 9 \end{array} = \frac{1}{3}|0\rangle + \frac{2}{3}|9\rangle \xrightarrow{\text{measure}} \begin{cases} |0\rangle\,, & P = 1/3 \\ |9\rangle\,, & P = 2/3 \end{cases}$$

- Notice the conciseness of the Dirac notation for sparse states.
- Objective measurement.

Example: Mechanical oscillator

TODO

Deterministic operations (1)

- These map a deterministic state to a deterministic state.
- We deal with **linear** operations; such can be expressed as **matrix-vector** product:

$$|f(a)\rangle = M\,|a\rangle$$

- There are just four possible deterministic operations on a bit:

$$M_1 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad M_4 = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix},$$

  corresponding to boolean functions

$$f_1(a) = 0, \quad f_2(a) = a, \quad f_3(a) = \neg a, \quad f_4(a) = 1$$

Deterministic operations (2)

$$|f(a)\rangle = M\,|a\rangle$$

$$M_1 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \qquad M_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I, \qquad M_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X, \qquad M_4 = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix},$$

$$f_1(a) = 0, \qquad f_2(a) = a, \qquad f_3(a) = \neg a, \qquad f_4(a) = 1$$

- Notice that columns of the matrices are formed by $|0\rangle$ and $|1\rangle$.
- and matrix-vector multiplication with a deterministic state vector just extracts the respective column, e.g.

$$|f_3(1)\rangle = M_3\,|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle = |\neg 1\rangle$$

Probabilistic operations (1)

- Probabilistic-to-probabilistic but not deterministic-to-deterministic.
- For example, applying

$$M = \begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & 0 \end{bmatrix}$$

  to deterministic state vectors yields

  - $M|0\rangle = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle$
  - $M|1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$

- Assuming the coin again, using $|\mathrm{heads}\rangle = |0\rangle$ and $|\mathrm{tails}\rangle = |1\rangle$, this means in natural language:

  1. If heads given, flip the coin fairly;
  2. if tails given, turn it to heads.

Probabilistic operations (2)

$$M = \begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & 0 \end{bmatrix}$$

So far, so good. It gets a bit less intuitive if a probabilistic state is on input. Having, e.g.,

$$|\mathbf{X}\rangle = \frac{1}{5}|0\rangle + \frac{4}{5}|1\rangle \, ,$$

we get

$$\begin{aligned} M|\mathbf{X}\rangle &= \frac{1}{5}\left(\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right) + \frac{4}{5}|0\rangle \\ &= \frac{9}{10}|0\rangle + \frac{1}{10}|1\rangle \, , \end{aligned}$$

Probabilistic operations (3)

- Matrix M representing operations on probabilistic states must satisfy:
    1. All entries of M are **nonnegative real numbers**.
    2. The **sum** of the entries **in each column** is equal to 1; we can say $||M(:,i)||_1 = 1$ for every column index i.
- This is equivalent to saying **every column** is a **probability vector**.
- Every such matrix is called a **stochastic matrix**.
- A stochastic matrix can be considered a **random choice of deterministic operations**. E.g,

$$M_1 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad M_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad M_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad M_4 = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix},$$

$$M = \begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & 0 \end{bmatrix} = \frac{1}{2} M_1 + \frac{1}{2} M_3$$

Operation composition

- Operation composition can be expressed simply as **matrix-matrix multiplication**.
- Matrix multiplication is **associative**: $(M_1 M_2) M_3 = M_1 (M_2 M_3) \quad [= M_1 M_2 M_3]$.
- Hence, applying $M_1, M_2, \ldots, M_n$ in that order can be expressed as a single composed operation
$$M = M_n \cdots M_2 M_1$$
- **Not commutative!**

$$M_1 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \qquad M_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$M_1 M_3 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \qquad M_3 M_1 = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

Outline

Compound classical systems (1)

- Let's have **independent deterministic systems** $\mathbf{X}$ and $\mathbf{Y}$ and their **state sets** Σ and Γ.
- We can take them as a single **compound system** $(\mathbf{X}, \mathbf{Y})$.
- State set of $(\mathbf{X}, \mathbf{Y})$ is then defined as the **Cartesian product**

$$\Sigma \times \Gamma = \{(a, b) : a \in \Sigma, b \in \Gamma\}$$

- More generally, a compound system $(\mathbf{X}_1 \cdots \mathbf{X}_n)$ has a state set $\Sigma_1 \times \cdots \times \Sigma_n$.
- In case of bits, $\Sigma_1 = \cdots = \Sigma_n = \Sigma = \{0, 1\}$ and we often write a state $(a_1, \ldots, a_n) \in \Sigma^n$ as a **bit string** $a_1 \ldots a_n$, e.g. $(0, 1, 0) = 010$.
- For example, for $n = 4$, the compound state set is

$$\Sigma = \{0000, 0001, 0010, \ldots, 1110, 1111\}, \quad |\Sigma| = 2^4 = 16.$$

- Mathematically, it is the same as having a single system with $\Sigma = \{0, 1, \ldots, 15\}$ and writing the labels as binary strings padded with zeros to the length n.

Compound classical systems (2)

- The **Cartesian product** of the state sets transforms into the **Kronecker (tensor) product** of the vectors.
- Vector-vector tensor product works like this in general:

$$a = \begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} \qquad b = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

$$a \otimes b = \begin{bmatrix} a_1 b \\ \vdots \\ a_m b \end{bmatrix} \in \mathbb{R}^{mn}$$

Compound classical systems (3)

- The tensor product works like this for deterministic states (standard basis vectors):

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}\begin{matrix}\mathbf{0}\\1\end{matrix} \qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}\begin{matrix}0\\\mathbf{1}\end{matrix}$$

$$|0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix}\begin{matrix}\mathbf{0}\\1\end{matrix} \otimes \begin{bmatrix}1\\0\end{bmatrix}\begin{matrix}\mathbf{0}\\1\end{matrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}\begin{matrix}\mathbf{00}\\01\\10\\11\end{matrix} = |00\rangle \qquad |0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix}\begin{matrix}\mathbf{0}\\1\end{matrix} \otimes \begin{bmatrix}0\\1\end{bmatrix}\begin{matrix}0\\\mathbf{1}\end{matrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}\begin{matrix}00\\\mathbf{01}\\10\\11\end{matrix} = |01\rangle$$

$$|1\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix}\begin{matrix}0\\\mathbf{1}\end{matrix} \otimes \begin{bmatrix}1\\0\end{bmatrix}\begin{matrix}\mathbf{0}\\1\end{matrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}\begin{matrix}00\\01\\\mathbf{10}\\11\end{matrix} = |10\rangle \qquad |1\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}\begin{matrix}0\\\mathbf{1}\end{matrix} \otimes \begin{bmatrix}0\\1\end{bmatrix}\begin{matrix}0\\\mathbf{1}\end{matrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\begin{matrix}00\\01\\10\\\mathbf{11}\end{matrix} = |11\rangle$$

- $|ab\rangle$, $|a\rangle\,|b\rangle$, $|a\rangle \otimes |b\rangle$ hence mean all the same.
- Tensor product means **independence**; the opposite case of dependence comes in a while ....

Compound probabilistic system example: Lottery revisited

- Five "drums" of a fair Šance by Sportka, each with 10 numbered balls $\Sigma = \{0, 2, \ldots, 9\}$.
- The state before and after a ball is picked:

$$
|\mathbf{X}\rangle = \frac{1}{10^5} \begin{array}{c} \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \end{array} \begin{array}{l} 00000 \\ 00001 \\ 00002 \\ \vdots \\ 99999 \end{array} = \frac{1}{10^5} \left(|00000\rangle + \cdots + |99999\rangle \right) \xrightarrow{\text{measure}} \begin{cases} |00000\rangle\,, & P = 1/10^5 \\ \vdots & \\ |99999\rangle\,, & P = 1/10^5 \end{cases}
$$

- An unfair "sparse" Šance spitting one and only one 1 and the rest are 0s:

$$
|\mathbf{X}\rangle = \frac{1}{5} \left(|00001\rangle + |00010\rangle + |00100\rangle + |01000\rangle + |10000\rangle \right) \xrightarrow{\text{measure}} \begin{cases} |00001\rangle\,, & P = 1/5 \\ |00010\rangle\,, & P = 1/5 \\ |00100\rangle\,, & P = 1/5 \\ |01000\rangle\,, & P = 1/5 \\ |10000\rangle\,, & P = 1/5 \end{cases}
$$

Independent vs correlated systems (1)

- Individual states of a compound deterministic state, like $|0\rangle$ and $|1\rangle$ in $|01\rangle$, are independent "by construction".
- Independence is less obvious in the case of probabilistic states such as compound system $(\mathbf{X}, \mathbf{Y})$ with state vector

$$|\mathbf{XY}\rangle = \frac{1}{6}|00\rangle + \frac{1}{12}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{4}|11\rangle$$

- $\mathbf{X}$ and $\mathbf{Y}$ with state sets Σ and Γ are independent if and only if

$$\forall a \in \Sigma, b \in \Gamma : \quad P((\mathbf{X}, \mathbf{Y}) = (a, b)) = P(\mathbf{X} = a)P(\mathbf{Y} = b).$$

Independent vs correlated systems (2)

$$
\begin{aligned}
|\mathbf{XY}\rangle &= \frac{1}{6}|00\rangle + \frac{1}{12}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{4}|11\rangle \\
P(\mathbf{XY}=01) &= \frac{1}{12}, \\
P(\mathbf{X}=0) &= P(\mathbf{XY}=00) + P(\mathbf{XY}=01) = \frac{1}{6} + \frac{1}{12} = \frac{1}{4}, \\
P(\mathbf{Y}=1) &= P(\mathbf{XY}=01) + P(\mathbf{XY}=11) = \frac{1}{12} + \frac{1}{4} = \frac{1}{3},
\end{aligned}
$$

so indeed $P(\mathbf{XY}=01) = P(\mathbf{X}=0)P(\mathbf{Y}=1)$ and the same can be shown for the other combinations $00, 10, 11$. More succinctly, we can just argue that

$$|\mathbf{XY}\rangle = |\mathbf{X}\rangle \otimes |\mathbf{Y}\rangle, \text{ where}$$

$$|\mathbf{X}\rangle = \frac{1}{4}|0\rangle + \frac{3}{4}|1\rangle \quad \text{and} \quad |\mathbf{Y}\rangle = \frac{2}{3}|0\rangle + \frac{1}{3}|1\rangle.$$

Independent vs correlated systems (3)

Think of two coins glued together...

$$
\begin{aligned}
|\mathbf{XY}\rangle &= \frac{1}{2}\,|00\rangle + \frac{1}{2}\,|11\rangle \\
P(\mathbf{XY} = 01) &= 0, \\
P(\mathbf{X} = 0) &= P(\mathbf{XY} = 00) = \frac{1}{2}, \\
P(\mathbf{Y} = 1) &= P(\mathbf{XY} = 11) = \frac{1}{2},
\end{aligned}
$$

This system can't be independent because

$$
P(\mathbf{XY} = 01) = 0 \quad \neq \quad \frac{1}{4} = P(\mathbf{X} = 0)P(\mathbf{Y} = 1)
$$

The **lack of independence** means that $\mathbf{X}$ and $\mathbf{Y}$ are **correlated**.
Alternatively, we can argue that there are no $|\mathbf{X}\rangle$, $|\mathbf{Y}\rangle$ such that $|\mathbf{XY}\rangle = |\mathbf{X}\rangle \otimes |\mathbf{Y}\rangle$.

Full measurement

If we measure all subsystems of a compound system at once, there's actually no difference to the single system state. For example:

$$\frac{1}{6}|00\rangle + \frac{1}{12}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{4}|11\rangle \xrightarrow{\text{measure}} \begin{cases} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{cases} \quad P = \begin{cases} 1/6 \\ 1/12 \\ 1/2 \\ 1/4 \end{cases}$$

$$\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle \xrightarrow{\text{measure}} \begin{cases} |0\rangle \\ |1\rangle \end{cases} \quad P = \begin{cases} 1/2 \\ 1/2 \end{cases}$$

$$\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle \xrightarrow{\text{measure}} \begin{cases} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{cases} \quad P = \begin{cases} 1/2 \\ 0 \\ 0 \\ 1/2 \end{cases}$$

Partial measurement (1)

We apply the usual conditional and marginal probability formulas

$$P(\mathbf{Y} = b \,|\, \mathbf{X} = a) = \frac{P(\mathbf{XY} = ab)}{P(\mathbf{X} = a)}, \qquad P(\mathbf{X} = a) = \sum_b P((\mathbf{XY} = ab).$$

First bit:

$$\begin{aligned}
&\frac{1}{6}\,|00\rangle + \frac{1}{12}\,|01\rangle + \frac{1}{2}\,|10\rangle + \frac{1}{4}\,|11\rangle \\
&= |0\rangle \otimes \left(\frac{1}{6}\,|0\rangle + \frac{1}{12}\,|1\rangle\right) \;+\; |1\rangle \otimes \left(\frac{1}{2}\,|0\rangle + \frac{1}{4}\,|1\rangle\right) \\
&= |0\rangle \otimes |r_{0,0}\rangle + |1\rangle \otimes |r_{0,1}\rangle \\
&\xrightarrow{\text{measure}} \begin{cases} |0\rangle \otimes \frac{|r_{0,0}\rangle}{\||r_{0,0}\rangle\|_1} = |0\rangle \otimes \left(\frac{2}{3}\,|0\rangle + \frac{1}{3}\,|1\rangle\right), & P = \|\,|r_{0,0}\rangle\,\|_1 = 1/4 \\ |1\rangle \otimes \frac{|r_{0,1}\rangle}{\||r_{0,1}\rangle\|_1} = |1\rangle \otimes \left(\frac{2}{3}\,|0\rangle + \frac{1}{3}\,|1\rangle\right), & P = \|\,|r_{0,1}\rangle\,\|_1 = 3/4 \end{cases}
\end{aligned}$$

Partial measurement (2)

Second bit:

$$
\begin{aligned}
&\frac{1}{6}\left|00\right\rangle + \frac{1}{12}\left|01\right\rangle + \frac{1}{2}\left|10\right\rangle + \frac{1}{4}\left|11\right\rangle \\
&= \left(\frac{1}{6}\left|0\right\rangle + \frac{1}{2}\left|1\right\rangle\right) \otimes \left|0\right\rangle \; + \; \left(\frac{1}{12}\left|0\right\rangle + \frac{1}{4}\left|1\right\rangle\right) \otimes \left|1\right\rangle \\
&= \left|r_{1,0}\right\rangle \otimes \left|0\right\rangle + \left|r_{1,1}\right\rangle \otimes \left|1\right\rangle \\
&\xrightarrow{\text{measure}} \begin{cases} \frac{\left|r_{1,0}\right\rangle}{\|\left|r_{1,0}\right\rangle\|_1} \otimes \left|0\right\rangle = \left(\frac{1}{4}\left|0\right\rangle + \frac{3}{4}\left|1\right\rangle\right) \otimes \left|0\right\rangle, \quad P = \|\left|r_{1,0}\right\rangle\|_1 = 2/3 \\ \frac{\left|r_{1,1}\right\rangle}{\|\left|r_{1,1}\right\rangle\|_1} \otimes \left|1\right\rangle = \left(\frac{1}{4}\left|0\right\rangle + \frac{3}{4}\left|1\right\rangle\right) \otimes \left|1\right\rangle, \quad P = \|\left|r_{1,1}\right\rangle\|_1 = 1/3 \end{cases}
\end{aligned}
$$

Operations on multiple systems (1)

- Corresponding to independent or correlated probabilistic states, we can have independent or collective operations on compound states.
- Independence is again expressed with the tensor product $\otimes$.

Example – negate the first bit and do nothing to the other:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X \otimes I = \begin{bmatrix} O_2 & I_2 \\ I_2 & O_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$(X \otimes I)\,|10\rangle = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle\,, \quad \text{or, using distributivity,}$$

$$(X \otimes I)\,|10\rangle = (X\,|1\rangle) \otimes (I\,|0\rangle) = |00\rangle$$

Operations on multiple systems (2)

- We can also have operations that act collectively on multiple subsystems (bits) and, hence, can't be decomposed using $\otimes$.

Example – controlled NOT for 2-bit system $\mathbf{XY}$; if $\mathbf{X}$ is 1, negate $\mathbf{Y}$, else no-op:

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

$$CNOT\,|00\rangle = |00\rangle \qquad CNOT\,|01\rangle = |01\rangle$$
$$CNOT\,|10\rangle = |11\rangle \qquad CNOT\,|11\rangle = |10\rangle$$

Outline

From probabilistic to quantum (1)

- We can generalize **probabilistic states to quantum states** quite naturally!
- Assume $|\psi\rangle$ is a quantum state, $|\mathbf{X}\rangle$ is the corresponding probabilistic state.
  - Indefinite number of quantum states map to the same probabilistic state.
- Recall $|\mathbf{X}\rangle$ consists of **nonnegative real** coefficients, and its **taxicab norm is 1**.
- **Quantum states** emerge by attaching **phases**:

$$|\mathbf{X}\rangle = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in (\mathbb{R}_0^+)^n, \ \| \, |\mathbf{X}\rangle \, \|_1 = 1, \qquad |\varphi\rangle = \begin{bmatrix} \varphi_1 \\ \vdots \\ \varphi_n \end{bmatrix} \in [0, 2\pi)^n, \qquad \psi = (|\mathbf{X}\rangle \, , |\varphi\rangle)$$

- **That's essentially it!** This is the main difference and main source of all the hopes about quantum computing!
- The underlying deterministic state set can be the same – no difference.

From probabilistic to quantum (2)

$$|\mathbf{X}\rangle = [x_1, \ldots, x_n]^T \in (\mathbb{R}_0^+)^n, \quad \| \, |\mathbf{X}\rangle \, \|_1 = 1, \quad |\varphi\rangle = [\varphi_1, \ldots, \varphi_n]^T \in [0, 2\pi)^n, \quad \psi = (|\mathbf{X}\rangle, |\varphi\rangle)$$

- It's, however, more common and handy to express a quantum state as a **complex vector**!
- Each entry ψ_i is a complex **probability amplitude**, encoding both **magnitude** $|\psi_i| = \sqrt{x_i}$ and **phase** $\varphi_i = \arg(\psi_i)$, i.e.,

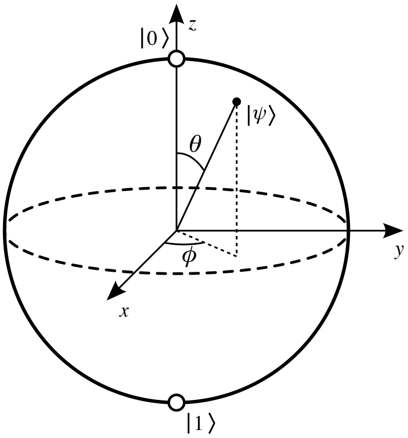
$$\begin{aligned} |\psi\rangle &= [\psi_1, \ldots, \psi_n]^T \in \mathbb{C}^n, \\ \psi_i &= |\psi_i|(\cos\varphi_i + i \sin\varphi_i) \quad \text{for } i = 1, \ldots, n. \end{aligned}$$

- Measurement probabilities are then given as $P_i = x_i = |\psi_i|^{\mathbf{2}}$ (details in a bit).
- The normalization condition uses a different norm – the **Euclidean norm**:

$$\| \, |\psi\rangle \, \|_{\mathbf{2}} = \left(\sum_{i=1}^{n} |\psi_i|^{\mathbf{2}} \right)^{1/\mathbf{2}} = 1$$

- **Composition** of independent states works the same: using **tensor product** $\otimes$ again!

Bloch sphere



Quantum measurement

- **Measuring** probabilistic and quantum states is **similar but not same** from mathematical viewpoint.
  - Just need to keep in mind we now use **2-norm** and **complex** coefficients;
  - coefficients are **amplitudes**, not probabilities directly;
  - probabilities are given by **absolute values squared** of amplitudes;
  - but in the end, we obtain **classical deterministic information** again!
- What is very **different in physical reality**, though, is that quantum measurements are always **objective** and change the state **for everyone/everything**!
- We say the state gets **collapsed**.
  - Leaking information leads to collapse.
  - It doesn't matter who or what receives the information 👻

Quantum measurement

V **You**

draw collapse of quantum state

ChatGPT

Here is an abstract representation of the collapse of a quantum state, blending scientific and artistic elements to depict the transition from quantum superposition to a definite state. The image captures the mystical and enigmatic nature of quantum mechanics.

Full quantum measurement (1)

$$\left.\begin{array}{l} \frac{1}{\sqrt{2}}\,|0\rangle \;-\; \frac{1}{\sqrt{2}}\,|1\rangle \\ \frac{1}{\sqrt{2}}\,|0\rangle \;+\; \frac{1}{\sqrt{2}}\,|1\rangle \\ \frac{i}{\sqrt{2}}\,|0\rangle \;-\; \frac{1+i}{2}\,|1\rangle \end{array}\right\} \xrightarrow{\text{measure}} \begin{cases} |0\rangle\,, & P = 1/2 \\ |1\rangle\,, & P = 1/2 \end{cases}$$

- These are considered **different states** but give the **same probabilities**!
- In other words, they map to the same probabilistic state.
- They are **not distinguishable** by standard basis measurement.

Full quantum measurement (2)

$$\left.\begin{array}{l}\frac{1}{\sqrt{6}}\left|00\right\rangle + \frac{1}{\sqrt{12}}\left|01\right\rangle + \frac{1}{\sqrt{2}}\left|10\right\rangle + \frac{1}{2}\left|11\right\rangle \\ \frac{i}{\sqrt{6}}\left|00\right\rangle - \frac{e^{0.1234i}}{\sqrt{12}}\left|01\right\rangle + \frac{\sqrt{3}-i}{2\sqrt{2}}\left|10\right\rangle + \frac{1+\sqrt{3}i}{4}\left|11\right\rangle\end{array}\right\} \xrightarrow{\text{measure}} \begin{cases}\left|00\right\rangle, & P = 1/6 \\ \left|01\right\rangle, & P = 1/12 \\ \left|10\right\rangle, & P = 1/2 \\ \left|11\right\rangle, & P = 1/4\end{cases}$$

- These are considered **different states** but give the **same probabilities**!
- In other words, they map to the same probabilistic state.
- They are **not distinguishable** by standard basis measurement.

Partial quantum measurement

Like for probabilistic, just with $\|.\|_2$.
Second qubit:

$$
\begin{aligned}
|\phi\rangle &= \frac{1}{\sqrt{6}}|00\rangle + \frac{1}{\sqrt{12}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{2}|11\rangle \\
&= \left(\frac{1}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle \ + \ \left(\frac{1}{\sqrt{12}}|0\rangle + \frac{1}{2}|1\rangle\right) \otimes |1\rangle \\
&= |r_{1,0}\rangle \otimes |0\rangle + |r_{1,1}\rangle \otimes |1\rangle \\
&\xrightarrow{\text{measure}} \begin{cases} \dfrac{|r_{1,0}\rangle}{\|\,|r_{1,0}\rangle\,\|_2} \otimes |0\rangle = \left(\dfrac{1}{2}|0\rangle + \dfrac{\sqrt{3}}{2}|1\rangle\right) \otimes |0\rangle\,, & P = \|\,|r_{1,0}\rangle\,\|_2^2 = 2/3 \\ \dfrac{|r_{1,1}\rangle}{\|\,|r_{1,1}\rangle\,\|_2} \otimes |1\rangle = \left(\dfrac{1}{2}|0\rangle + \dfrac{\sqrt{3}}{2}|1\rangle\right) \otimes |1\rangle\,, & P = \|\,|r_{1,1}\rangle\,\|_2^2 = 1/3 \end{cases}
\end{aligned}
$$

Vsuvka: komplexní sdružení a skalární součin, ortogonální a unitární matice

- **komplexně sdružené číslo** k číslu $z = a + bi = |z|e^{i\phi}$ se nazývá číslo $\overline{z} = a - bi = |z|e^{-i\phi}$
  - Vznikne tedy překlopením znaménka u imaginární části.
  - obrázek a příklad
- **skalární součin v komplexním oboru**:
  - $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u} \cdot \mathbf{v} = \mathbf{u}^* \mathbf{v} = \overline{u_1} v_1 + \cdots + \overline{u_n} v_n$
  - * značí hermitovskou (komplexně sdruženou) transpozici: $\mathbf{A}^* = \overline{\mathbf{A}^T}$ (místo * se taky používá †, ^{H}, $^+$)
  - Je-li $\mathbf{u} = |\psi\rangle$ a $\mathbf{v} = |\phi\rangle$, značíme $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \psi | \phi \rangle$
  - Mimochodem "bra" vektor se definuje $\langle \psi | = |\psi\rangle^*$
- **ortogonální matice** je čtvercová matice $\mathbf{A}$: $\mathbf{A}^T \mathbf{A} = \mathbf{I} = \mathbf{A}\mathbf{A}^T$
- **unitární matice** je čtvercová matice $\mathbf{A}$: $\mathbf{A}^* \mathbf{A} = \mathbf{I} = \mathbf{A}\mathbf{A}^*$

Quantum operations

- Quantum operations need to be **unitary** rather than **stochastic**:

$$MM^\dagger = M^\dagger M = I$$

- Equivalent to the requirement (again) that each column must be a valid state ($\|.\|_2 = 1$).
- This time also each row.
- Usually called **quantum gates**.

Some important operations

Pauli matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

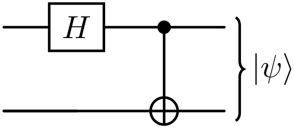
Hadamard:

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

Controlled NOT, SWAP:

$$\mathsf{CNOT}_{0,1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \mathsf{CNOT}_{1,0} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \mathsf{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

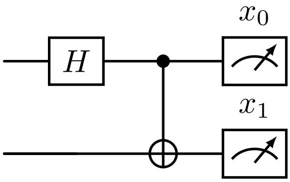
Quantum circuit



$$
\begin{aligned}
|\psi\rangle &= \mathsf{CNOT}_{0,1}(I \otimes H)\,|00\rangle \\
&= \mathsf{CNOT}_{0,1}\left(|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \\
&= \mathsf{CNOT}_{0,1}\left(\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)\right) \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle
\end{aligned}
$$

- Graphical representation of unitary gates.
- Implicit initialization to $|0\rangle$.
- Gates drawn in the order of application, i.e., reversely to mathematical notation.
- Horizontal lines $=$ time (more to right $=$ later).
- Parallel lines $=$ tensor product; lines joined $=$ collective operation.
- Qiskit convention: topmost qubit in circuit $=$ rightmost in ket $= q_0$

Quantum circuit with measurement



$$|\phi^+\rangle \xrightarrow{\text{measure}} |x_1 x_0\rangle = \begin{cases} |00\rangle\,, & P = 1/2 \\ |11\rangle\,, & P = 1/2 \end{cases}$$

Bell states and entanglement

Probabilistic state:

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

Bell quantum states:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \qquad |\psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \qquad |\psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

- Bell states are schoolbook examples of entangled states.
- Correlation of probabilistic states maps to **entanglement** in the quantum world.
- In our simplistic formulation, **entanglement = correlation**.
- However, in physical reality, entanglement is a much **more powerful** concept.
- Leads to phenomena without classical counterparts, such as **quantum teleportation**.

Outline

Why bother? (1)

- Qubits are much more powerful than old good bits, especially when they "cooperate".
    - Information can be stored not only in the basis vectors (downgrade to deterministic!) but also in the amplitudes (complex numbers)!
    - A qubit is a continuum; the amplitudes have basically infinite precision.

$$\alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \cdots + \alpha_7 |111\rangle$$

  That's 8 complex numbers vs. integers $0, \ldots, 7$ of classical information!

- If we're able to map our DOFs to the amplitudes $\Rightarrow$ exponential "storage"!
- There are also algorithms already known which bring exponential speedup in the number of operations.

Question: How many qubits do you need to represent every mm^3 of the whole Earth as a quantum amplitude?

Answer

https://nssdc.gsfc.nasa.gov/planetary/factsheet/earthfact.html

108.321	1.08321E+12	1.08321E+30	99.77315581
10^{10} km^3	km^3	mm^3	log2

Why bother? (2)

Quantum simulations:

- Simulating elementary particles is exponentially expensive.
- It's hard to simulate even tens of atoms on classical (super)computers.
- Hundreds impossible even for all today's computers working together!
    - There are "only" 10^{82} atoms in the known universe!
- Quantum computers scale linearly because they "are" the elementary particles.
- Big potential also outside of quantum physics / chemistry.

Why bother? (3)

- Intrinsic guaranteed randomness.
    - It's hard to implement something like a fair coin on the computer bit level...
    - All random number generators on classical computers are actually pseudo-random!
    - QC allows us to prepare distributions from which we sample by measuring.
    - Intuitively suitable for any probabilistic approach...
- Cryptography.
    - Guaranteed randomness!
    - On the one hand, QC brings exponentially faster algorithms for integer prime factorization! Potential to crack current cyphers.
    - On the other hand, new opportunities for unbreakable safe communication.
- New communication protocols or even means of communication via quantum teleportation.

Limitations

- There are important limitations, though!
- Readout problem!
  - The amplitudes just represent a distribution from which we sample.
  - Reading a qubit collapses it, and we must start over.
  - Estimating the full state is exponentially expensive.
- Current machines are noisy!
  - This mainly means we need redundancy in qubit count / circuit depth, so it holds us back.

Kernbotschaften zum Mitnehmen 🥡 (1)

A quantum computer is a weird Sportka, where

- you can have currently ~ 1000 balls,
- each ball behaves like a Bloch sphere with two possible outcomes,
- you can manipulate the complex magnitudes and phases of the individual spheres,
- you can correlate the spheres as you wish.

Even though this is hardly implementable in reality, it is still an extremely simplistic and less powerful beast than a real quantum machine!

- E.g., entanglement works at any distance.

Kernbotschaften zum Mitnehmen 🥡 (2)

The ingredients we need are mainly

- complex numbers,
- (complex) linear algebra,
- simple probability theory.

This is not the only model of quantum computation!

- I just described (quite superficially) the **quantum/unitary gate/operator** model.
- It's a **model describing quantum information** and the **basic programming model for quantum computers** dictated by the fundamental rules of quantum mechanics.
- It's **not** the **most general** model, but sufficient in many cases.
- A more general (and more involved) description of quantum information is the **density matrix model**, which we don't cover today.

Credits

- Inspired by the IBM Quantum Learning course **Basics of Quantum Information** by Prof. John Watrous, Technical Director, IBM Quantum Education
- Some good thoughts also in **Quantum Country**
- Bible of QC = Nielsen and Chuang: **Quantum Computation and Quantum Information**

First quantum algorithm: Deutsch's algorithm (1)

- Assume function $f : \{0,1\} \to \{0,1\}$. There are only 4 of them:

k	$f_k(0)$	$f_k(1)$	name	f_k type
0	0	0	zero	0
1	0	1	id	1
2	1	0	neg	1
3	1	1	one	0

(0 = constant, 1 = balanced)

- Deutsch's problem:
  Input: function $f : \{0,1\} \to \{0,1\}$
  Output: type of f

First quantum algorithm: Deutsch's algorithm (2)

- In quantum world, we work with unitaries.
- We can map any boolean function f to a unitary U_f which works like this:

$$U_f \left|y\right\rangle \left|x\right\rangle = \left|y \oplus f(x)\right\rangle \left|x\right\rangle$$

$\|yx\rangle$	$f_0(x)$	$\|y \oplus f_0(x)\rangle \|x\rangle$
$\|00\rangle$	0	$\|00\rangle$
$\|01\rangle$	0	$\|01\rangle$
$\|10\rangle$	0	$\|10\rangle$
$\|11\rangle$	0	$\|11\rangle$

$$U_{f_0} = \left[\left|00\right\rangle, \left|01\right\rangle, \left|10\right\rangle, \left|11\right\rangle\right] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4$$

$\|yx\rangle$	$f_1(x)$	$\|y \oplus f_1(x)\rangle \|x\rangle$
$\|00\rangle$	0	$\|00\rangle$
$\|01\rangle$	1	$\|11\rangle$
$\|10\rangle$	0	$\|10\rangle$
$\|11\rangle$	1	$\|01\rangle$

$$U_{f_1} = \left[\left|00\right\rangle, \left|11\right\rangle, \left|10\right\rangle, \left|01\right\rangle\right] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \mathsf{CNOT}_{0,1}$$

First quantum algorithm: Deutsch's algorithm (3)

- In quantum world, we work with unitaries.
- We can map any boolean function f to a unitary U_f which works like this:

$$U_f |y\rangle |x\rangle = |y \oplus f(x)\rangle |x\rangle$$

$\lvert yx\rangle$	$f_2(x)$	$\lvert y \oplus f_2(x)\rangle \lvert x\rangle$
$\lvert 00\rangle$	1	$\lvert 10\rangle$
$\lvert 01\rangle$	0	$\lvert 01\rangle$
$\lvert 10\rangle$	1	$\lvert 00\rangle$
$\lvert 11\rangle$	0	$\lvert 11\rangle$

$$U_{f_2} = \left[|10\rangle, |01\rangle, |00\rangle, |11\rangle\right] = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

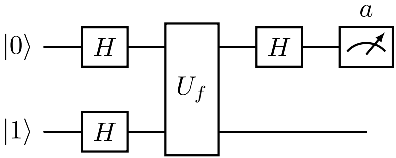
$$= (X \otimes I_2)\mathsf{CNOT}_{0,1}$$

$\lvert yx\rangle$	$f_3(x)$	$\lvert y \oplus f_3(x)\rangle \lvert x\rangle$
$\lvert 00\rangle$	1	$\lvert 10\rangle$
$\lvert 01\rangle$	1	$\lvert 11\rangle$
$\lvert 10\rangle$	1	$\lvert 00\rangle$
$\lvert 11\rangle$	1	$\lvert 01\rangle$

$$U_{f_3} = \left[|10\rangle, |11\rangle, |00\rangle, |01\rangle\right] = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = X \otimes I_2$$

First quantum algorithm: Deutsch's algorithm (4)

- Original Deutsch's problem:
  Input: function $f : \{0,1\} \to \{0,1\}$
  Output: type of f
- Equivalent problem:
  Input: unitary $U_f : \mathbb{R}^{4\times 4} \to \mathbb{R}^{4\times 4}$, $U_f \left|y\right\rangle \left|x\right\rangle = \left|y \oplus f(x)\right\rangle \left|x\right\rangle$
  Output: type of f that U_f represents
- Deutsch's algorithm in circuit form:



- Matrix form: $(I \otimes H)U_f(H \otimes H)\left|10\right\rangle \xrightarrow{\text{measure}} \left|?a\right\rangle,\ a = 0, 1$
- This algorithm, specifically the result of measurement of the upper qubit, will yield $a = 0$ if f is constant and $a = 1$ if f is balanced.

TODOs

- Irrelevance of global phase
- How to build a QC and the trade-off between stable quantum properties and ability to interact with it (control and measure)
- Decoherence = quantum noise = unwanted interactions with the outside world