Quantum Computing (QC)

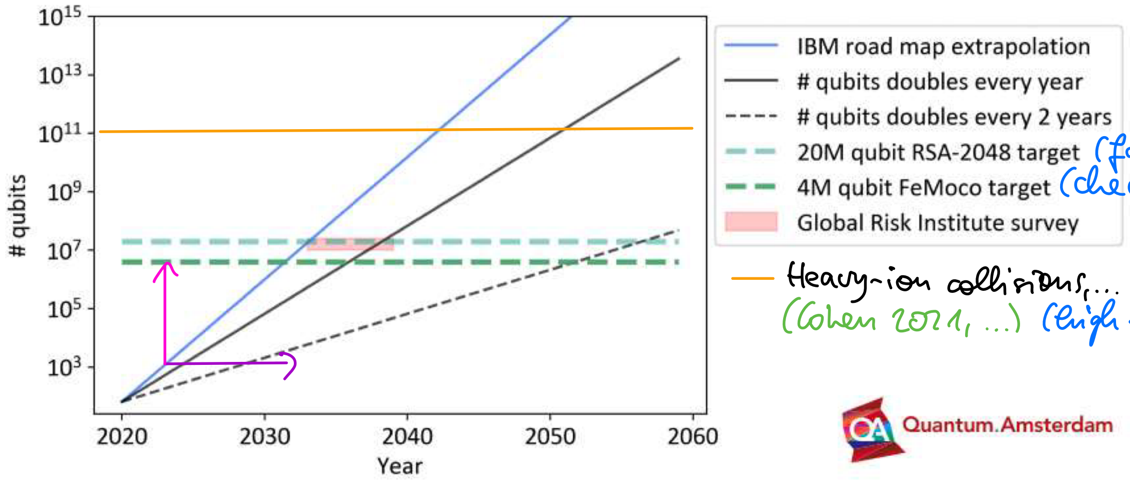
1 Introduction

1.1 Past, present, future of QC

- 1980-82: Concept of QC (Benioff, Feynman, Manin,...)
- 1985-93: First quantum algorithms (Deutsch, ...) (see Thu.)
- 1994: Quantum algorithm for factoring (Shor)

⋮

- 2019-...: "Quantum supremacy" (Arute et al., Zhong et al.,...)
  - ⇒ exponential speedup of artificial computations, e.g. quantum: 200s vs. classical: 10,000 y (Arute et al.)
  - ⇒ partially refuted: "Closing the quantum supremacy gap", classical: 2.5d (2019) → 304s (2021) (Yong et al.)
- State-of-the-art: **N**oisy **I**ntermediate-**S**cale **Q**uantum era
- Rough sketch of the future:



(factoring)

(chemistry)

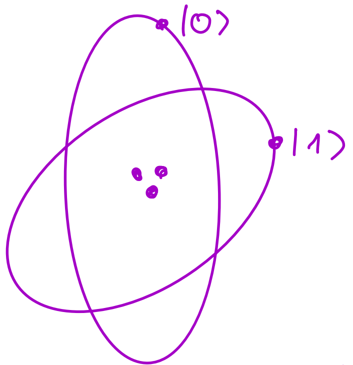
Heavy-ion collisions,...
(Cohen 2021, ...) (high energy physics)

- Biggest challenge: quantum error correction (QEC) (see Thu.)
  - ⇒ need $\mathcal{O}(10^3-10^4)$ qubits to encode one QECed qubit
  - ⇒ still many years away from useful QC applications

1.2 Basics of QC

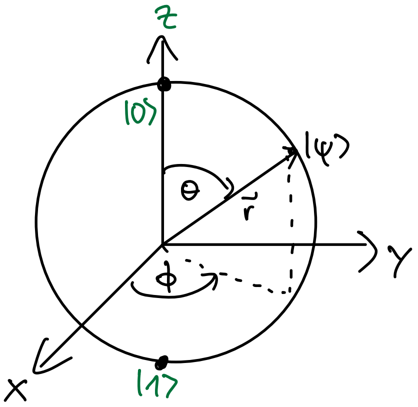
1.2.1 Qubits

- Classical computer: bit takes values 0 or 1
- Quantum computer: qubit is 2-dim. quantum state:
  - ⇒ $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ ⇒ superposition
  - ⇒ basis states: $|0\rangle = \begin{pmatrix}1\\ 0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\ 1\end{pmatrix}$ ⇒ "computational basis" = "z basis"
  - ⇒ coefficients: $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$
  - ⇒ infinitely many possible states



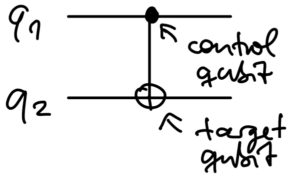
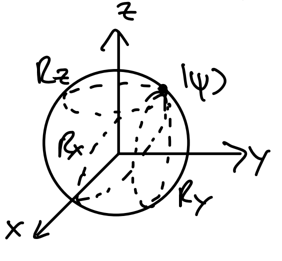
e.g. levels in atom

- Bloch sphere representation:
  - ⇒ $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$
  - ⇒ Bloch vector: $\vec{r} = \begin{pmatrix}\sin\theta\cos\phi\\ \sin\theta\sin\phi\\ \cos\theta\end{pmatrix}$



1.2.2 Quantum gates

- Classical gates: e.g. NOT $\quad 0 \xrightarrow{NOT} 1$, $1 \xrightarrow{NOT} 0$
- Quantum gates: represented by <u>unitary</u> matrices
  $\Rightarrow$ e.g. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{NOT} |\psi'\rangle = \alpha|1\rangle + \beta|0\rangle$
- Matrix representation: e.g. $NOT \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X$ (Pauli σ_x)
  $\Rightarrow |\psi\rangle \xrightarrow{NOT} |\psi'\rangle = X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
  $\Rightarrow$ unitary: $X^+X = XX = 1$
- Common gates:

Name	Circuit rep.	Matrix rep.	Acting on qubit
X	$-\boxed{X}-$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\|0\rangle \to \|1\rangle, \|1\rangle \to \|0\rangle$
Y	$-\boxed{Y}-$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\|0\rangle \to -i\|1\rangle, \|1\rangle \to i\|0\rangle$
Z	$-\boxed{Z}-$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\|0\rangle \to \|0\rangle, \|1\rangle \to -\|1\rangle$
Hadamard $\Rightarrow$ superposition	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\|0\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $\|1\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
CNOT $\Rightarrow$ entanglement		$\begin{pmatrix} \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} & 0 \\ 0 & \underbrace{\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}}_{X} \end{pmatrix}$	$\|00\rangle \to \|00\rangle$ $\|01\rangle \to \|01\rangle$ $\|10\rangle \to \|11\rangle$ $\|11\rangle \to \|10\rangle$ unchanged = "control" changes iff control is in state $\|1\rangle$ = "target"
$R_X(\theta)$	$-\boxed{R_X(\theta)}-$	$\exp\left(-i\frac{\theta}{2}X\right)$	
$R_Y(\theta)$	$-\boxed{R_Y(\theta)}-$	$\exp\left(-i\frac{\theta}{2}Y\right)$	
$R_Z(\theta)$	$-\boxed{R_Z(\theta)}-$	$\exp\left(-i\frac{\theta}{2}Z\right)$	

⇒ rotation

⇒ crucial for physics & chemistry applications (see Fri.)

- Remark: N-qubit gates act on N qubits

  ⇒ N qubits can be in superposition of 2^N basis states

  ⇒ QC efficiently encodes exponentially large Hilbert space

1.2.3 Quantum circuits

- Three stages of gate-based quantum computations:

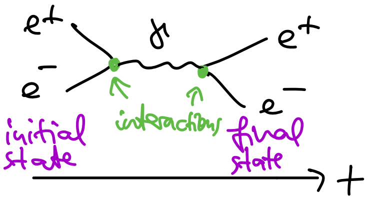
  (i) Initialization of all N qubits in $|0\rangle$ state

  (ii) Unitary transformations = quantum gates

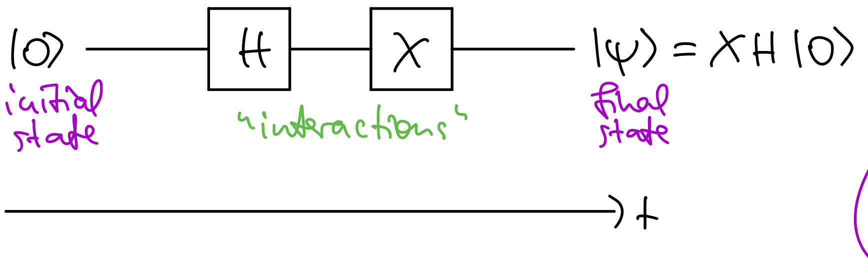
  (iii) Measurement of all or some qubits

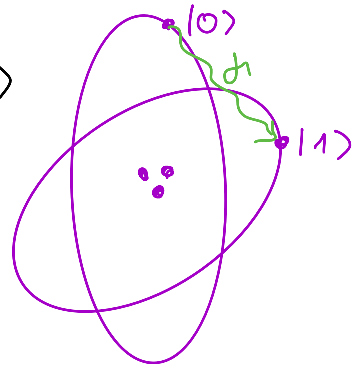
- Quantum circuit diagram:

  ⇒ useful tool to visualize quantum computations, like Feynman diagrams:



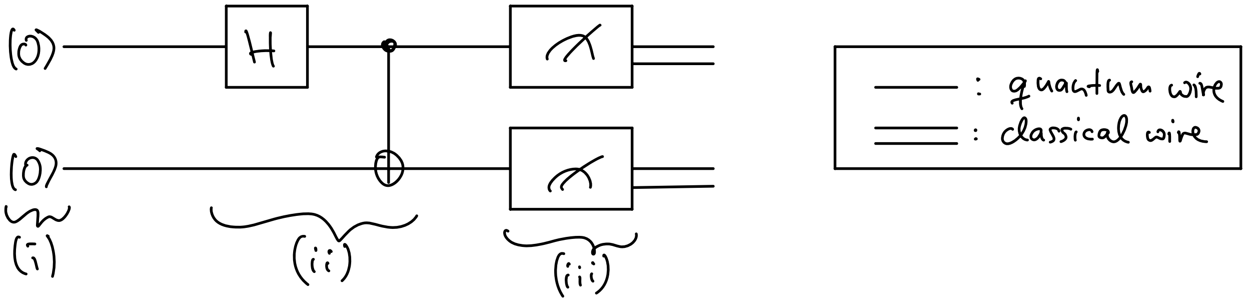
⇒ one-qubit example:





e.g. levels in atom
manipulate them by
e.g. laser light

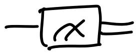
- Two-qubit example with measurement:



(i) tensor product: $|0\rangle \otimes |0\rangle \equiv |00\rangle$

(ii) matrix product: $|00\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$

$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \equiv |\psi\rangle$$

(iii)  : projective measurement in computational basis

=> probability $p_{0,1}$ of measuring $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in state $|0\rangle, |1\rangle$: $p_0 \equiv \langle\psi|M_0|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = |\alpha|^2$

$$p_1 \equiv \langle\psi|M_1|\psi\rangle = \langle\psi|1\rangle\langle 1|\psi\rangle = |\beta|^2$$

=> $M_{0,1}$: measurement operators = orthogonal projectors

=> Example: $p_{00} \equiv p(|00\rangle) = \frac{1}{2}$, $p_{11} \equiv p(|11\rangle) = \frac{1}{2}$

=> Bell state : if we measure one qubit, we know state of the other qubit

=> Entanglement: key ingredient of quantum parallelism (see Thu.)