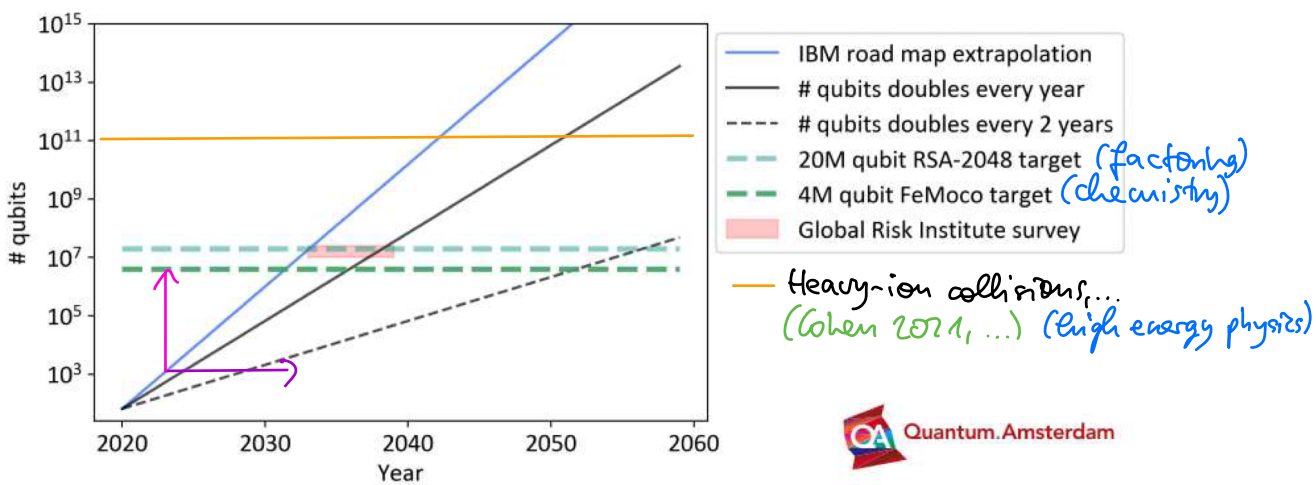
Quantum Computing (QC)

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: Noisy Intermediate-Scale Quantum era
- Rough sketch of the future:

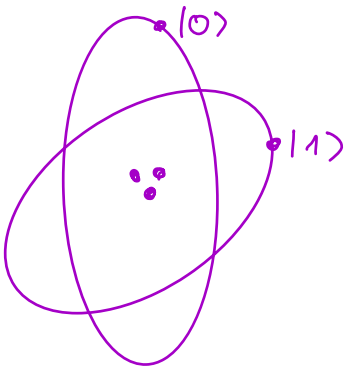


- Biggest challenge: quantum error correction (QEC) (see Thu.)
  - ⇒ need $O(10^3 - 10^4)$ qubits to encode one QECed qubit
  - ⇒ still many years away from useful QC applications

1.2 Basics of QC

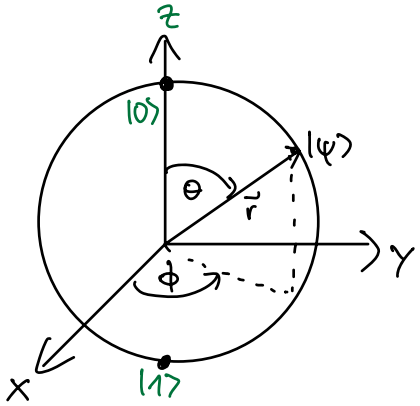
1.2.1 Qubits

- 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



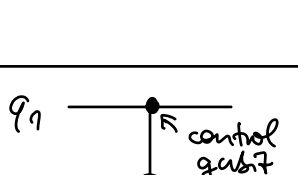
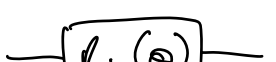
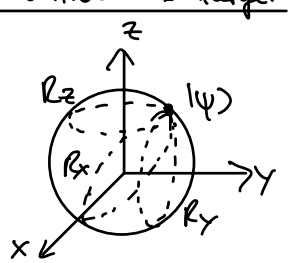
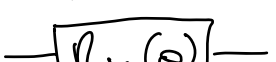
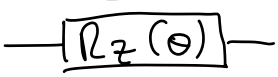
e.g. levels in atom

- 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 unitary matrices
  - ⇒ 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)
  - ⇒ $|\psi\rangle \xrightarrow{NOT} |\psi'\rangle = X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
  - ⇒ unitary: $X^+X = XX = 1$
- Common gates:

Name	Circuit rep.	Matrix rep.	Acting on qubit
X		$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\|0\rangle \to \|1\rangle$, $\|1\rangle \to \|0\rangle$
Y		$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\|0\rangle \to -i\|1\rangle$, $\|1\rangle \to i\|0\rangle$
Z		$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\|0\rangle \to \|0\rangle$, $\|1\rangle \to -\|1\rangle$
Hadamard ⇒ superposition		$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\|0\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $\|1\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
CNOT ⇒ entanglement		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ X	$\|00\rangle \to \|00\rangle$ $\|01\rangle \to \|01\rangle$ $\|10\rangle \to \|11\rangle$ $\|11\rangle \to \|10\rangle$ ↑ unchanged = "control" ← changes iff control is in state $\|1\rangle$ = "target"
$R_x(\theta)$		$\exp\left(-i\frac{\theta}{2}X\right)$	
$R_y(\theta)$		$\exp\left(-i\frac{\theta}{2}Y\right)$	
$R_z(\theta)$		$\exp\left(-i\frac{\theta}{2}Z\right)$	

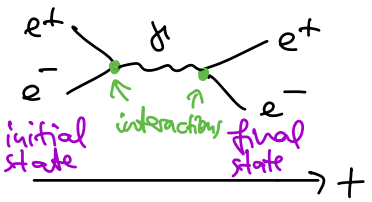
⇒ rotation

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

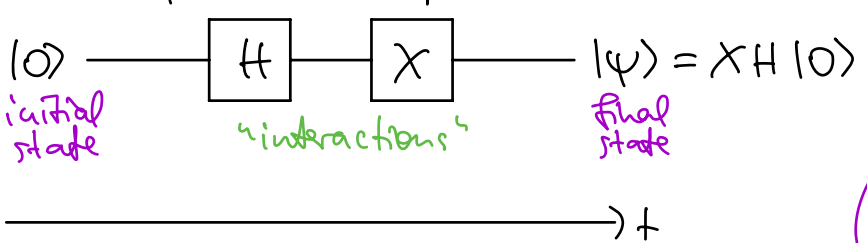
- Remark: N-qubit gates act on N qubits
  ⇒ N qubits can be in superposition of 2^N basis states
  ⇒ QC efficiently encodes exponentially large Hilbert space

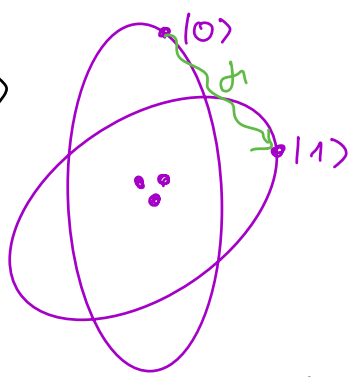
1.2.3 Quantum circuits

- 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:



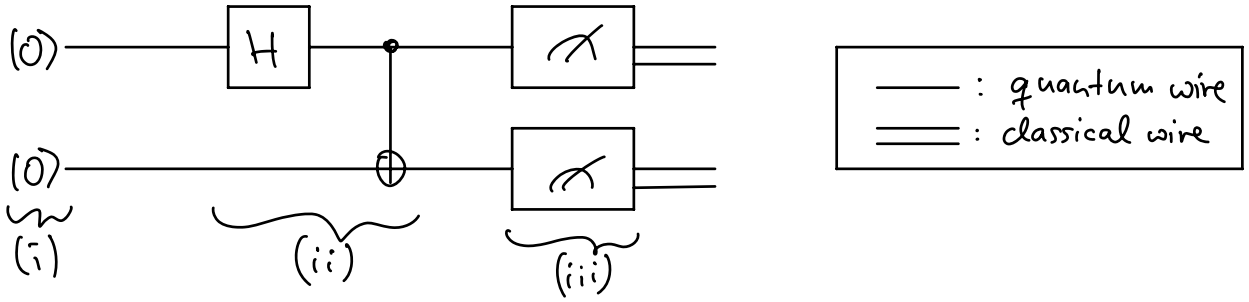
⇒ one-qubit example:





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: $|00\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

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

(iii) $-\boxed{\nearrow}=$: projective measurement in computational basis

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

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

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

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

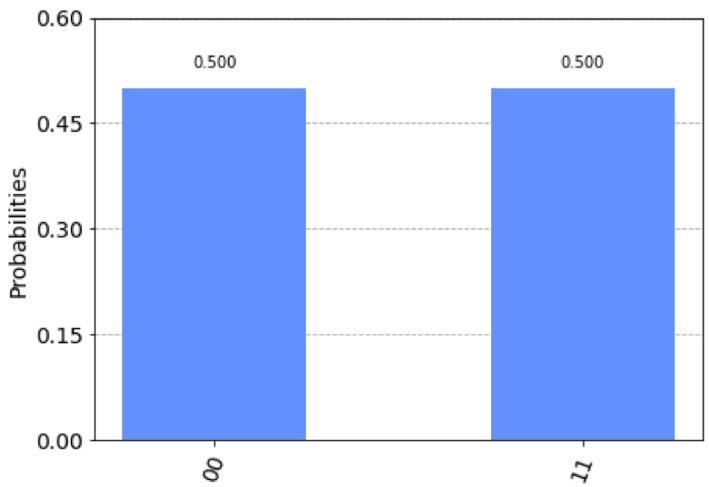
$\Rightarrow$ Bell state: if we measure one qubit, we know state of the other qubit

$\Rightarrow$ Entanglement: key ingredient of quantum parallelism (see Thu.)

2 Quantum errors

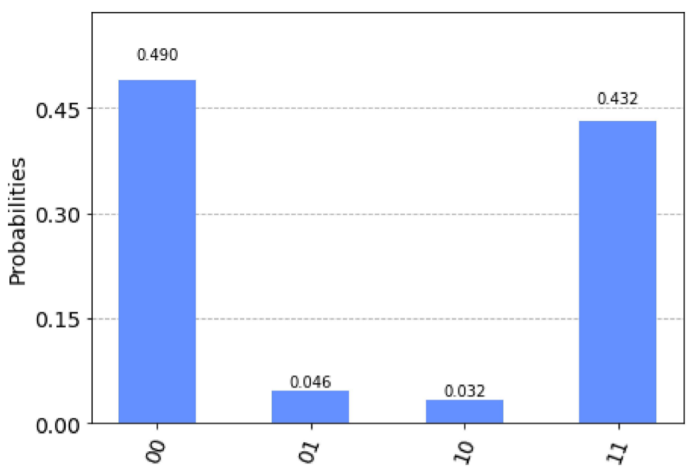
2.1 Example: Bell state

- classical simulation of noise-free QC:



(see "Quantum Programming Tutorial 1: Bell State" by "Full-Stack Quantum Computation" website)

- Quantum simulation, e.g. on IBM-Q's "Melbourne" device



⇒ $\Theta(10^{-2})$ errors, but old data (2020, see website above)

⇒ current typical error rates: $\Theta(10^{-3})$ (Acharya et al. 2408.13687)

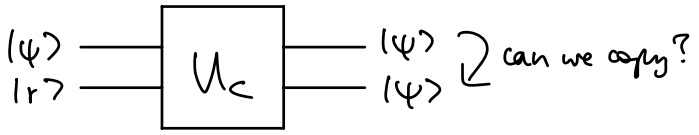
2.2 Quantum error correction (QEC)

- Classically: can copy arbitrary bits

⇒ simple error correction

⇒ e.g. repetition code

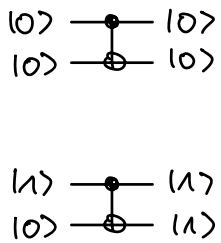
- Quantum version?



- Aim: find U_C to copy arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- First: copy basis states ✓

$U_C|0\rangle \otimes |r\rangle \longrightarrow |0\rangle \otimes |0\rangle$ for $|r\rangle = |0\rangle$

$U_C|1\rangle \otimes |r\rangle \longrightarrow |1\rangle \otimes |1\rangle$ for $|r\rangle = |0\rangle$



- Next: try to copy arbitrary state ↯

$$
\begin{aligned}
U_C|\psi\rangle \otimes |r\rangle &= U_C(\alpha|0\rangle + \beta|1\rangle) \otimes |r\rangle \\
&= U_C(\alpha|0\rangle \otimes |r\rangle + \beta|1\rangle \otimes |r\rangle) \\
&= \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle \\
&\neq |\psi\rangle \otimes |\psi\rangle
\end{aligned}
$$

- A quantum state cannot be copied with perfect fidelity
  ⇒ "no-cloning theorem" (proof: Wootters, Zurek, Nature 299, 802 (1982))
  ⇒ no simple QEC!
- QEC requires
  (i) additional qubits
  (ii) noise below certain threshold
- Many QEC "codes": Shor's code, GKP code, ...

⇒ example: surface code requires
(i) $\mathcal{O}(10^4)$ additional qubits per logical qubit
(ii) for physical error rate of $p \lesssim 10^{-5}$
(see e.g. Campbell et al., 1612.07330)

- Near-future "compromise": quantum error mitigation
  ⇒ example: zero-noise extrapolation for Schwinger model

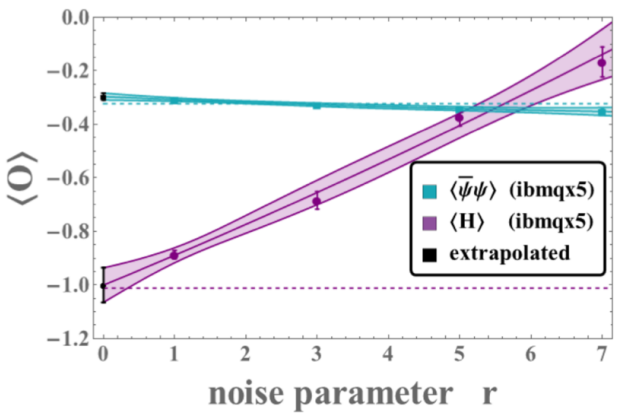


FIG. 2. The $H^{\tilde{\Lambda}=3}_{\mathbf{k}=\mathbf{0},+}$ ground state energy and chiral condensate (purple, blue extrapolated to -1.000(65) and -0.296(13), respectively) expectation values as a function of r, the noise parameter. $r-1$ is the number of additional CNOT gates inserted at each location of a CNOT gate in the original VQE circuit. (1200 IBM allocation units and ~ 6.4 QPU·s)

(Klco et al., 1803.03326) (algorithm: see Fri.)

3 Quantum algorithms

3.1 Deutsch algorithm

- Simple algorithm that demonstrates concept of quantum parallelism ⇒ inspiration for Shor's algorithm
- Goal: Given a black-box function $f: \{0,1\} \to \{0,1\}$, find out if $f(0) = f(1)$ ⇒ constant (1€ → 1€)

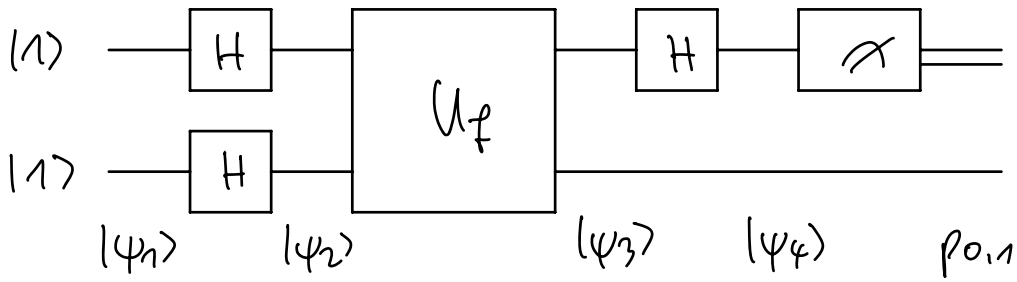
or $f(0) \neq f(1)$ ⇒ balanced (1€ → ☺)

- Generalization: $f: \{0,1\}^n \to \{0,1\}$ ⇒ "Deutsch-Jozsa"

3.1.1 Quantum circuit

- Define unitary gate: $U_f |x,y\rangle \equiv |x, y \oplus f(x)\rangle$,
  where $|x,y\rangle \equiv |x\rangle \otimes |y\rangle \equiv |xy\rangle$ and $\underbrace{1 \oplus 1}_{\text{addition modulo 2}} = 0$

  ⇒ U_f is black box function called "quantum oracle"



- $|\psi_1\rangle = |1\rangle \otimes |1\rangle$
- $|\psi_2\rangle = (H \otimes H)\,|\psi_1\rangle$
  $= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
  $= \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle + |1\rangle \otimes |1\rangle)$

  ⇒ superposition
- $|\psi_3\rangle = U_f\,|\psi_2\rangle$
  $= \frac{1}{2}\big(|0\rangle \otimes |f(0)\rangle - |1\rangle \otimes |f(1)\rangle$
  $- |0\rangle \otimes |1 \oplus f(0)\rangle + |1\rangle \otimes |1 \oplus f(1)\rangle\big)$

- Two cases:

	$f(0)=f(1)$	$f(0)=1\oplus f(1)\neq f(1)$
$\lvert\psi_3\rangle$	$\frac{1}{\sqrt{2}}(\lvert 0\rangle-\lvert 1\rangle)$ $\otimes\frac{1}{\sqrt{2}}(\lvert f(0)\rangle-\lvert 1\oplus f(0)\rangle)$	$\frac{1}{\sqrt{2}}(\lvert 0\rangle+\lvert 1\rangle)$ $\otimes\frac{1}{\sqrt{2}}(\lvert f(0)\rangle-\lvert 1\oplus f(0)\rangle)$
$\lvert\psi_4\rangle$	$\lvert 1\rangle$ $\otimes\dots$	$\lvert 0\rangle$ $\otimes\dots$
p_0	0	1
p_1	1	0

3.1.2 Quantum parallism

- with a single measurement of the first qubit in the state $\lvert\psi_4\rangle$, we find out if 1€ → 1€ or 1€ → 🙂
- 1 instead of 2 function calls, only 1 application of U_f
  ⇒ "quantum parallelism"
- Note: quantum parallelism alone yields no advantage
  ⇒ interference: $H(\lvert 0\rangle\mp\lvert 1\rangle)=\frac{1}{\sqrt{2}}[(\lvert 0\rangle+\lvert 1\rangle)\mp(\lvert 0\rangle-\lvert 1\rangle)]$
- without interference: QC can enable parallel computation but either no useful output or sequential measurement