Introduction to Quantum Computing

Lecture 1

Stefan Kühn
DESY Summer Student Program, 31.07.2023

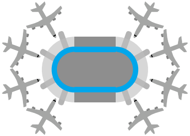
Motivation

Problems for which Quantum Computers might be advantageous

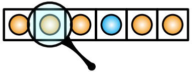
- Factoring

$$70747 = 263 \times 269$$

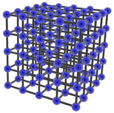
- Optimization problems



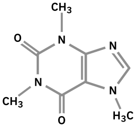
- Searching databases



- Quantum simulation
  - Lattice field theory

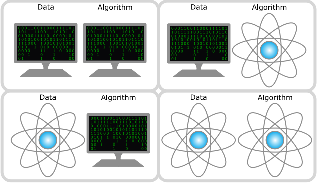


  - Quantum chemistry

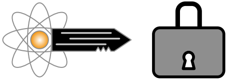


  - Material science
  - ...

- Machine learning



- Cryptography

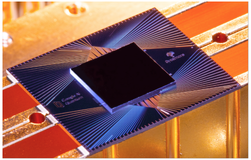


- ...

Motivation

On the verge of the NISQ era

- Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible

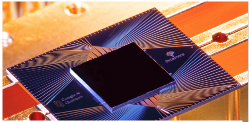


J. Preskill, Quantum 2, 79 (2018)

Motivation

On the verge of the NISQ era

- Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers



Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5
Received: 22 July 2019
Accepted: 20 September 2019
Published online: 23 October 2019

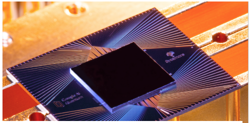
Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5*]

J. Preskill, Quantum 2, 79 (2018)
F. Arute et al., Nature 574, 5050 (2019)

Motivation

On the verge of the NISQ era

- Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers



Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-16
Received: 22 July 2019
Accepted: 20 September 2019
Published online: 23 October 2019

RESEARCH

QUANTUM COMPUTING

Quantum computational advantage using photons

Han-Sen Zhong[1,2]*, Hui Wang[1,2]*, Yu-Hao Deng[1,2]*, Ming-Cheng Chen[1,2]*, Li-Chao Peng[1,2], Yi-Han Luo[1,2], Jian Qin[1,2], Dian Wu[1,2], Xing Ding[1,2], Yi Hu[1,2], Peng Hu[3], Xiao-Yan Yang[3], Wei-Jun Zhang[3], Hao Li[3], Yuxuan Li[4], Xiao Jiang[1,2], Lin Gan[4], Guangwen Yang[4], Lixing You[3], Zhen Wang[3], Li Li[1,2], Nai-Le Liu[1,2], Chao-Yang Lu[1,2]†, Jian-Wei Pan[1,2]†

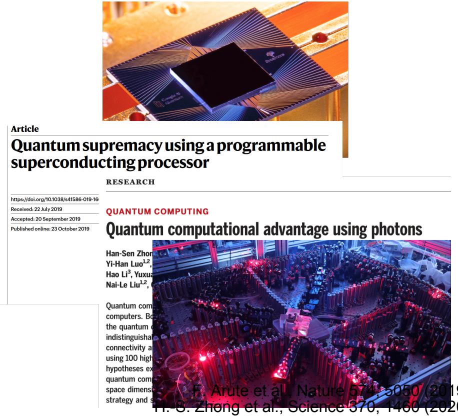
Quantum computers promise to perform certain tasks that are believed to be intractable to classical computers. Boson sampling is such a task and is considered a strong candidate to demonstrate the quantum computational advantage. We performed Gaussian boson sampling by sending 50 indistinguishable single-mode squeezed states into a 100-mode ultralow-loss interferometer with full connectivity and random matrix—the whole optical setup is phase-locked—and sampling the output using 100 high-efficiency single-photon detectors. The obtained samples were validated against plausible hypotheses exploiting thermal states, distinguishable photons, and uniform distribution. The photonic quantum computer, *Jiuzhang*, generates up to 76 output photon clicks, which yields an output state-space dimension of 10^{30} and a sampling rate that is faster than using the state-of-the-art simulation strategy and supercomputers by a factor of ~10^{14}.

F. Arute et al., Nature 574, 5050 (2019)
H.-S. Zhong et al., Science 370, 1460 (2020)

Motivation

On the verge of the NISQ era

- Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers


Article
Quantum supremacy using a programmable superconducting processor
Received: 22 July 2019
Accepted: 20 September 2019
Published online: 23 October 2019

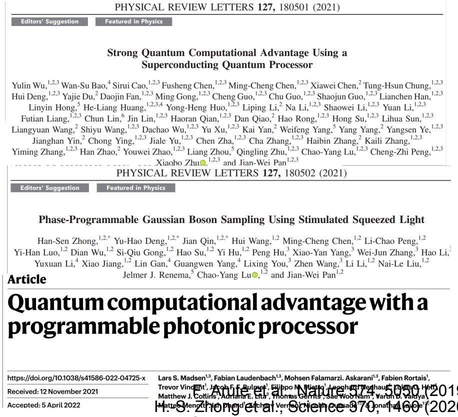
RESEARCH
QUANTUM COMPUTING
Quantum computational advantage using photons

F. Arute et al., Nature 574, 5050 (2019)
H.-S. Zhong et al., Science 370, 1460 (2020)

Motivation

On the verge of the NISQ era

- Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers


PHYSICAL REVIEW LETTERS **127,** 180501 (2021)

Editors' Suggestion | Featured in Physics

Strong Quantum Computational Advantage Using a Superconducting Quantum Processor

Yulin Wu,[1,2,3] Wan-Su Bao,[4] Sirui Cao,[1,2,3] Fusheng Chen,[1,2,3] Ming-Cheng Chen,[1,2,3] Xiawei Chen,[2] Tung-Hsun Chung,[1,2,3] Hui Deng,[1,2,3] Yajie Du,[2] Daojin Fan,[1,2,3] Ming Gong,[1,2,3] Cheng Guo,[1,2,3] Chu Guo,[1,2,3] Shaojun Guo,[1,2,3] Lianchen Han,[1,2,3] Linyin Hong,[5] He-Liang Huang,[1,2,3,4] Yong-Heng Huo,[1,2,3] Liping Li,[2] Na Li,[1,2,3] Shaowei Li,[1,2,3] Yuan Li,[1,2,3] Futian Liang,[1,2,3] Chun Lin,[6] Jin Lin,[1,2,3] Haoran Qian,[1,2,3] Dan Qiao,[2] Hao Rong,[1,2,3] Hong Su,[1,2,3] Lihua Sun,[1,2,3] Liangyuan Wang,[2] Shiyu Wang,[1,2,3] Dachao Wu,[1,2,3] Yu Xu,[1,2,3] Kai Yan,[2] Weifeng Yang,[5] Yang Yang,[2] Yangsen Ye,[1,2,3] Jianghan Yin,[2] Chong Ying,[1,2,3] Jiale Yu,[1,2,3] Chen Zha,[1,2,3] Cha Zhang,[1,2,3] Haibin Zhang,[2] Kaili Zhang,[1,2,3] Yiming Zhang,[1,2,3] Han Zhao,[2] Youwei Zhao,[1,2,3] Liang Zhou,[5] Qingling Zhu,[1,2,3] Chao-Yang Lu,[1,2,3] Cheng-Zhi Peng,[1,2,3] Xiaobo Zhu,[1,2,3] and Jian-Wei Pan[1,2,3]

PHYSICAL REVIEW LETTERS **127,** 180502 (2021)

Editors' Suggestion | Featured in Physics

Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light

Han-Sen Zhong,[1,2,*] Yu-Hao Deng,[1,2,*] Jian Qin,[1,2,*] Hui Wang,[1,2] Ming-Cheng Chen,[1,2] Li-Chao Peng,[1,2] Yi-Han Luo,[1,2] Dian Wu,[1,2] Si-Qiu Gong,[1,2] Hao Su,[1,2] Yi Hu,[1,2] Peng Hu,[3] Xiao-Yan Yang,[3] Wei-Jun Zhang,[3] Hao Li,[3] Yuxuan Li,[4] Xiao Jiang,[1,2] Lin Gan,[4] Guangwen Yang,[4] Lixing You,[3] Zhen Wang,[3] Li Li,[1,2] Nai-Le Liu,[1,2] Jelmer J. Renema,[5] Chao-Yang Lu,[1,2] and Jian-Wei Pan[1,2]

Article

Quantum computational advantage with a programmable photonic processor

https://doi.org/10.1038/s41586-022-04725-x

Received: 12 November 2021

Accepted: 5 April 2022

Lars S. Madsen[1,3], Fabian Laudenbach[1,3], Mohsen Falamarzi. Askarani[1,3], Fabien Rortais[1], Trevor Vincent[1], Jacob F. F. Bulmer[1], Filippo M. Miatto[1], Leonhard Neuhaus[1], Lukas G. Helt[1], Matthew J. Collins[1], Adriana E. Lita[2], Thomas Gerrits[2], Sae Woo Nam[2], Varun D. Vaidya[1], Matteo Menotti[1], Ish Dhand[1], Zachary Vernon[1], Nicolás Quesada[1] & Jonathan Lavoie[1]

F. Arute et al., Nature 574, 5050 (2019)
H.-S. Zhong et al., Science 370, 1460 (2020)
Y. Wu et al., PRL **127**, 180501 (2021), Han-Sen Zhong et al., Phys. Rev. Lett. **127**, 180502 (2021), L. S. Madsen et al., Nature **606**, 75 (2022)

Motivation

On the verge of the NISQ era

- Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers
- Larger quantum devices in the near future
  - IBM: 1000 qubits by the end of 2023
  - Google: 10^6 qubits and error correction 2029

PHYSICAL REVIEW LETTERS **127**, 180501 (2021)

Editors' Suggestion | Featured in Physics

Strong Quantum Computational Advantage Using a Superconducting Quantum Processor

Yulin Wu,[1,2,3] Wan-Su Bao,[4] Sirui Cao,[1,2,3] Fusheng Chen,[1,2,3] Ming-Cheng Chen,[1,2,3] Xiawei Chen,[2] Tung-Hsun Chung,[1,2,3] Hui Deng,[1,2,3] Yajie Du,[2] Daojin Fan,[1,2,3] Ming Gong,[1,2,3] Cheng Guo,[1,2,3] Chu Guo,[1,2,3] Shaojun Guo,[1,2,3] Lianchen Han,[1,2,3] Linyin Hong,[5] He-Liang Huang,[1,2,3,4] Yong-Heng Huo,[1,2,3] Liping Li,[2] Na Li,[1,2,3] Shaowei Li,[1,2,3] Yuan Li,[1,2,3] Futian Liang,[1,2,3] Chun Lin,[6] Jin Lin,[1,2,3] Haoran Qian,[1,2,3] Dan Qiao,[2] Hao Rong,[1,2,3] Hong Su,[1,2,3] Lihua Sun,[1,2,3] Liangyuan Wang,[2] Shiyu Wang,[1,2,3] Dachao Wu,[1,2,3] Yu Xu,[1,2,3] Kai Yan,[2] Weifeng Yang,[5] Yang Yang,[2] Yangsen Ye,[1,2,3] Jianghan Yin,[2] Chong Ying,[1,2,3] Jiale Yu,[1,2,3] Chen Zha,[1,2,3] Cha Zhang,[1,2,3] Haibin Zhang,[2] Kaili Zhang,[1,2,3] Yiming Zhang,[1,2,3] Han Zhao,[2] Youwei Zhao,[1,2,3] Liang Zhou,[5] Qingling Zhu,[1,2,3] Chao-Yang Lu,[1,2,3] Cheng-Zhi Peng,[1,2,3] Xiaobo Zhu,[1,2,3] and Jian-Wei Pan[1,2,3]

PHYSICAL REVIEW LETTERS **127**, 180502 (2021)

Editors' Suggestion | Featured in Physics

Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light

Han-Sen Zhong,[1,2,*] Yu-Hao Deng,[1,2,*] Jian Qin,[1,2,*] Hui Wang,[1,2] Ming-Cheng Chen,[1,2] Li-Chao Peng,[1,2] Yi-Han Luo,[1,2] Dian Wu,[1,2] Si-Qiu Gong,[1,2] Hao Su,[1,2] Yi Hu,[1,2] Peng Hu,[3] Xiao-Yan Yang,[3] Wei-Jun Zhang,[3] Hao Li,[3] Yuxuan Li,[4] Xiao Jiang,[1,2] Lin Gan,[4] Guangwen Yang,[4] Lixing You,[3] Zhen Wang,[3] Li Li,[1,2] Nai-Le Liu,[1,2] Jelmer J. Renema,[5] Chao-Yang Lu,[1,2] and Jian-Wei Pan[1,2]

Article

Quantum computational advantage with a programmable photonic processor

https://doi.org/10.1038/s41586-022-04725-x
Received: 12 November 2021
Accepted: 5 April 2022

Lars S. Madsen[1,3], Fabian Laudenbach[1,3], Mohsen Falamarzi. Askarani[1,3], Fabien Rortais[1], Trevor Vincent[1], Jacob F. F. Bulmer[1], Filippo M. Miatto[1], Leonhard Neuhaus[1], Lukas G. Helt[1], Matthew J. Collins[1], Adriana E. Lita[2], Thomas Gerrits[2], Sae Woo Nam[2], Varun D. Vaidya[1], Matteo Menotti[1], Ish Dhand[1], Zachary Vernon[1], Nicolás Quesada[1] & Jonathan Lavoie[1]

F. Arute et al., Nature 574, 5050 (2019)
H.-S. Zhong et al., Science 370, 1460 (2020)
Y. Wu et al., PRL **127**, 180501 (2021), Han-Sen Zhong et al., Phys. Rev. Lett. **127**, 180502 (2021), L. S. Madsen et al., Nature **606**, 75 (2022)
`https://research.ibm.com/blog/ibm-quantum-roadmap`, `https://blog.google/technology/ai/unveiling-our-new-quantum-ai-campus/`

Outline

Motivation

Classical computing

The circuit model of Quantum Computing

Experimental realization of qubits

2.

Motivation

Classical computing

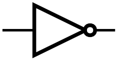
The circuit model of Quantum Computing

Experimental realization of qubits

Classical computing

Classical computing

- Classical bits take values in $\mathbb{Z}_2$, meaning 0 or 1
- Goal: compute Boolean functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$
- Logic gates

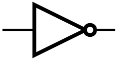


a	$\neg a$
0	1
1	0

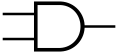
Classical computing

Classical computing

- Classical bits take values in $\mathbb{Z}_2$, meaning 0 or 1
- Goal: compute Boolean functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$
- Logic gates



a	$\neg a$
0	1
1	0

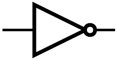


a	b	ab
0	0	0
0	1	0
1	0	0
1	1	1

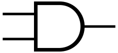
Classical computing

Classical computing

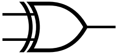
- Classical bits take values in $\mathbb{Z}_2$, meaning 0 or 1
- Goal: compute Boolean functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$
- Logic gates



a	$\neg a$
0	1
1	0



a	b	ab
0	0	0
0	1	0
1	0	0
1	1	1

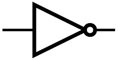


a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

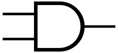
Classical computing

Classical computing

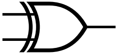
- Classical bits take values in $\mathbb{Z}_2$, meaning 0 or 1
- Goal: compute Boolean functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$
- Logic gates



a	$\neg a$
0	1
1	0



a	b	ab
0	0	0
0	1	0
1	0	0
1	1	1



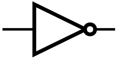
a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- **Universal** gate set: allows for expressing any Boolean function, e.g. $\{\text{NOT}, \text{AND}\}$ are universal

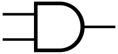
Classical computing

Classical computing

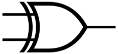
- Classical bits take values in $\mathbb{Z}_2$, meaning 0 or 1
- Goal: compute Boolean functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$
- Logic gates



a	$\neg a$
0	1
1	0

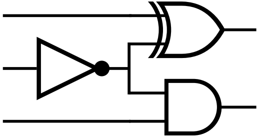


a	b	ab
0	0	0
0	1	0
1	0	0
1	1	1



a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

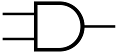
- **Universal** gate set: allows for expressing any Boolean function, e.g. $\{\mathrm{NOT}, \mathrm{AND}\}$ are universal
- We can arbitrarily copy bits



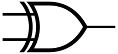
Classical computing

Irreversible vs. reversible gates

- Typically on uses a irreversible gate set, e.g. AND, XOR
- Can we make them reversible?



a	b	ab
0	0	0
0	1	0
1	0	0
1	1	1

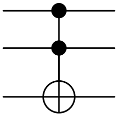


a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

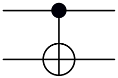
Classical computing

Irreversible vs. reversible gates

- Typically on uses a irreversible gate set, e.g. AND, XOR
- Can we make them reversible?



a	b	c	a	b	$c \oplus ab$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



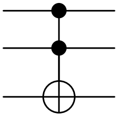
a	b	a	$a \oplus b$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$\Rightarrow$ It is possible to work with reversible gates

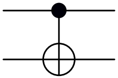
Classical computing

Irreversible vs. reversible gates

- Typically on uses a irreversible gate set, e.g. AND, XOR
- Can we make them reversible?



a	b	c	a	b	$c \oplus ab$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



a	b	a	$a \oplus b$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$\Rightarrow$ It is possible to work with reversible gates

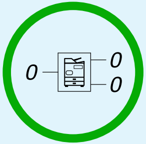
- Toffoli is universal

Classical computing

Classical vs. Quantum computing

Classical computing

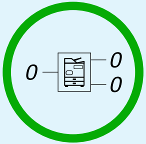
- Classical bits are 0 or 1
- Typically irreversible gate set, but reversible is possible
- We can arbitrarily copy bits



Classical computing

Classical vs. Quantum computing

Classical computing	Quantum computing
> Classical bits are 0 or 1 > Typically irreversible gate set, but reversible is possible > We can arbitrarily copy bits	> Quantum analog of bits? > Quantum logic gates? > Copying quantum information?



3.

Motivation

Classical computing

The circuit model of Quantum Computing

Experimental realization of qubits

Quantum bits

The circuit model of Quantum Computing

Quantum bit

- Qubit: two-dimensional quantum system
- Hilbert space $\mathcal{H}$ with basis $\{|0\rangle, |1\rangle\}$, called the **computational basis**
- Contrary to classical bits, it can be in a superposition

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

The circuit model of Quantum Computing

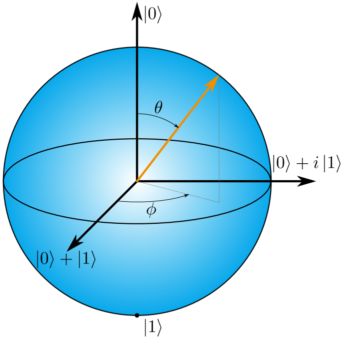
Quantum bit

- Qubit: two-dimensional quantum system
- Hilbert space $\mathcal{H}$ with basis $\{|0\rangle, |1\rangle\}$, called the **computational basis**
- Contrary to classical bits, it can be in a superposition

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

- Angles can be associated to a vector in spherical coordinates

$$\vec{r} = \begin{pmatrix} \sin(\theta)\cos(\phi) \\ \sin(\theta)\sin(\phi) \\ \cos(\theta) \end{pmatrix}$$



$\Rightarrow$ **Bloch-sphere** representation

The circuit model of Quantum Computing

Extracting information from quantum bits: projective measurements

- Consider the spectral decomposition of some observable

$$O = \sum_k o_k \, |o_k\rangle\langle o_k|$$

with eigenvalues o_k and orthogonal projectors $P_k = |o_k\rangle\langle o_k|$ onto the eigenspaces

- Measuring in the O basis: projecting the state onto one of the eigenspaces of O

The circuit model of Quantum Computing

Extracting information from quantum bits: projective measurements

- Consider the spectral decomposition of some observable

$$O = \sum_k o_k \left|o_k\right\rangle\left\langle o_k\right|$$

  with eigenvalues o_k and orthogonal projectors $P_k = \left|o_k\right\rangle\left\langle o_k\right|$ onto the eigenspaces
- Measuring in the O basis: projecting the state onto one of the eigenspaces of O
- Probability of measuring outcome k in state $\left|\psi\right\rangle = \sum_k c_k \left|o_k\right\rangle$

$$p_k = \left\langle\psi\right|P_k\left|\psi\right\rangle = \left|c_k\right|^2$$

- State of the system after measuring outcome k

$$\frac{c_k}{\sqrt{p_k}} \left|o_k\right\rangle$$

The circuit model of Quantum Computing

Extracting information from quantum bits: projective measurements

- Consider the spectral decomposition of some observable

$$O = \sum_k o_k \left|o_k\right\rangle\!\left\langle o_k\right|$$

with eigenvalues o_k and orthogonal projectors $P_k = \left|o_k\right\rangle\!\left\langle o_k\right|$ onto the eigenspaces

- Measuring in the O basis: projecting the state onto one of the eigenspaces of O
- Probability of measuring outcome k in state $\left|\psi\right\rangle = \sum_k c_k \left|o_k\right\rangle$

$$p_k = \left\langle\psi\middle|P_k\middle|\psi\right\rangle = \left|c_k\right|^2$$

- State of the system after measuring outcome k

$$\frac{c_k}{\sqrt{p_k}} \left|o_k\right\rangle$$

- In quantum computing we typically consider the computational basis or Z-basis $\{\left|0\right\rangle, \left|1\right\rangle\}$ for measurements

The circuit model of Quantum Computing

Multiple quantum bits

- n qubits: Hilbert space is the tensor product $\underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n \text{ times}}$
- Most general state in the computational basis

$$|\psi\rangle = \sum_{i_1,\ldots,i_n=0}^{1} c_{i_1\ldots i_n} |i_1\rangle \otimes \cdots \otimes |i_n\rangle$$

- In the following $\otimes$ often suppressed: $|0\rangle \otimes |0\rangle \rightarrow |0\rangle\,|0\rangle\,,\ |00\rangle$
- Shorthand notation for basis states: $|x\rangle$ where $x \in 0, \ldots, 2^n - 1$

The circuit model of Quantum Computing

Multiple quantum bits

- n qubits: Hilbert space is the tensor product $\underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n \text{ times}}$
- Most general state in the computational basis

$$|\psi\rangle = \sum_{i_1,\ldots,i_n=0}^{1} c_{i_1\ldots i_n} |i_1\rangle \otimes \cdots \otimes |i_n\rangle$$

- In the following $\otimes$ often suppressed: $|0\rangle \otimes |0\rangle \rightarrow |0\rangle |0\rangle \, , \ |00\rangle$
- Shorthand notation for basis states: $|x\rangle$ where $x \in 0, \ldots, 2^n - 1$
- Qubits can be **entangled**

The circuit model of Quantum Computing

Entanglement of bipartite systems

- Consider bipartite systems $\mathcal{H}_A \otimes \mathcal{H}_B$
- A **quantum state** that can be factored as a tensor product of states of its local constituents is called a **separable state** or **product state**

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$$

- Otherwise the state is **entangled**

The circuit model of Quantum Computing

Entanglement of bipartite systems

- Consider bipartite systems $\mathcal{H}_A \otimes \mathcal{H}_B$
- A **quantum state** that can be factored as a tensor product of states of its local constituents is called a **separable state** or **product state**

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$$

- Otherwise the state is **entangled**

Example

- $|\psi_1\rangle = |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$

The circuit model of Quantum Computing

Entanglement of bipartite systems

- Consider bipartite systems $\mathcal{H}_A \otimes \mathcal{H}_B$
- A **quantum state** that can be factored as a tensor product of states of its local constituents is called a **separable state** or **product state**

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$$

- Otherwise the state is **entangled**

Example

- $$\begin{aligned}|\psi_1\rangle &= |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \\ &= (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)\end{aligned}$$

$\Rightarrow$ Product state

- $|\Phi^+\rangle = |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$

The circuit model of Quantum Computing

Entanglement of bipartite systems

- Consider bipartite systems $\mathcal{H}_A \otimes \mathcal{H}_B$
- A **quantum state** that can be factored as a tensor product of states of its local constituents is called a **separable state** or **product state**

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$$

- Otherwise the state is **entangled**

Example

- $$\begin{aligned}|\psi_1\rangle &= |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \\ &= (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)\end{aligned}$$

$\Rightarrow$ Product state

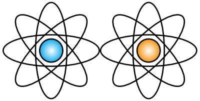
- $|\Phi^+\rangle = |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$

$\Rightarrow$ Entangled state (Bell state)

The circuit model of Quantum Computing

Entanglement of bipartite systems

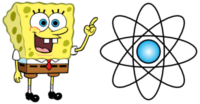
- Entangled states **cannot be described** by the individual **states of the constituent systems**
- Consider the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

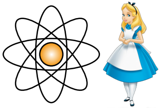


The circuit model of Quantum Computing

Entanglement of bipartite systems

- Entangled states **cannot be described** by the individual **states of the constituent systems**
- Consider the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

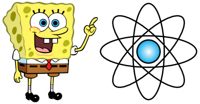


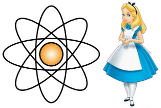


The circuit model of Quantum Computing

Entanglement of bipartite systems

- Entangled states **cannot be described** by the individual **states of the constituent systems**
- Consider the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$





- Bob can measure his qubit

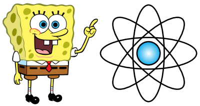
$$p_{\text{Bob}}(0) = 1/2,$$
$$p_{\text{Bob}}(1) = 1/2,$$

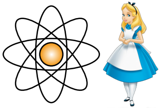
$\Rightarrow$ Bob does not obtain information about the state, his outcomes are random

The circuit model of Quantum Computing

Entanglement of bipartite systems

- Entangled states **cannot be described** by the individual **states of the constituent systems**
- Consider the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$





- Bob can measure his qubit

$$
\begin{aligned}
p_{\text{Bob}}(0) &= 1/2, \qquad & |\psi\rangle &= |00\rangle\,, \\
p_{\text{Bob}}(1) &= 1/2, \qquad & |\psi\rangle &= |11\rangle\,,
\end{aligned}
$$

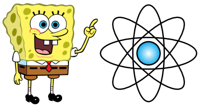
$\Rightarrow$ Bob does not obtain information about the state, his outcomes are random

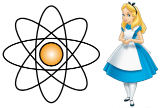
The circuit model of Quantum Computing

Entanglement of bipartite systems

> Entangled states **cannot be described** by the individual **states of the constituent systems**

> Consider the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$





> Bob can measure his qubit

$$
\begin{aligned}
p_{\text{Bob}}(0) &= 1/2, & |\psi\rangle &= |00\rangle\,, & p_{\text{Alice}}(0) &= 1\\
p_{\text{Bob}}(1) &= 1/2, & |\psi\rangle &= |11\rangle\,, & p_{\text{Alice}}(1) &= 1
\end{aligned}
$$

$\Rightarrow$ Bob does not obtain information about the state, his outcomes are random

> If Alice measures after Bob she obtains the same result as Bob with certainty

$\Rightarrow$ Perfect **correlation** between the measurement outcomes

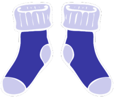
The circuit model of Quantum Computing

Entanglement of bipartite systems

- Let us consider the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right)$

$\Rightarrow$ The measurement outcomes are perfectly correlated

- Are these correlations any special?



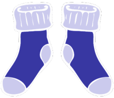
The circuit model of Quantum Computing

Entanglement of bipartite systems

- Let us consider the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right)$

$\Rightarrow$ The measurement outcomes are perfectly correlated

- Are these correlations any special?



- Outcome is correlated no matter which basis we choose

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \quad \Rightarrow \quad \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle\right)$$

- These type of correlations **do not have a classical counterpart**

How to characterize entanglement?

The circuit model of Quantum Computing

Mixed states and density operators

- So far we have considered **pure states** $|\psi\rangle \in \mathcal{H}$
- Assume the system can be various states $|\psi_i\rangle$ with probability p_i
- The ensemble of pure states $\{p_i, |\psi_i\rangle\}$ is called a **mixed state**

The circuit model of Quantum Computing

Mixed states and density operators

- So far we have considered **pure states** $|\psi\rangle \in \mathcal{H}$
- Assume the system can be various states $|\psi_i\rangle$ with probability p_i
- The ensemble of pure states $\{p_i, |\psi_i\rangle\}$ is called a **mixed state**
- Mixed states are described by the **density operator**

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \,, \qquad \sum_i p_i = 1$$

- Properties of the density operator
  1. self-adjoint: $\rho^\dagger = \rho$
  2. positive semidefinite (eigenvalues are real and non-negative)
  3. tr$(\rho) = 1$
  4. tr$(\rho^2) \leq 1$ with equality iff ρ describes a pure state ($p_k = 1$, $p_i = 0 \; \forall i \neq k$)

The circuit model of Quantum Computing

Mixed states and density operators

Example 1

- Consider the pure state

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

- Corresponding density operator

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

$\Rightarrow$ $\rho^2 = \rho$, pure state

The circuit model of Quantum Computing

Mixed states and density operators

Example 1

- Consider the pure state

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

- Corresponding density operator

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

$\Rightarrow$ $\rho^2 = \rho$, pure state

Example 2

- Consider the ensemble

$$p_0 = 1/2 \ |0\rangle \,, \quad p_1 = 1/2 \ |1\rangle$$

- Corresponding density operator

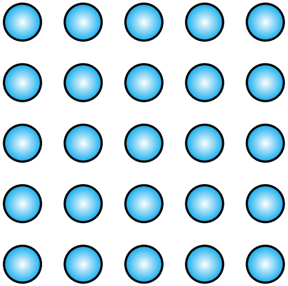
$$\rho = p_0 \, |0\rangle\langle 0| + p_1 \, |1\rangle\langle 1| = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

$\Rightarrow$ $\rho^2 = \frac{1}{2}\rho \neq \rho$, mixed state

The circuit model of Quantum Computing

Reduced density operator

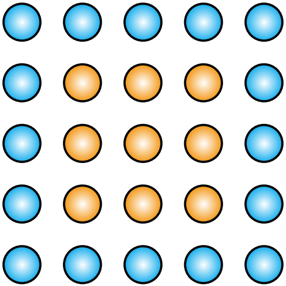
- Consider bipartite systems $\mathcal{H}_A \otimes \mathcal{H}_B$ described by ρ



The circuit model of Quantum Computing

Reduced density operator

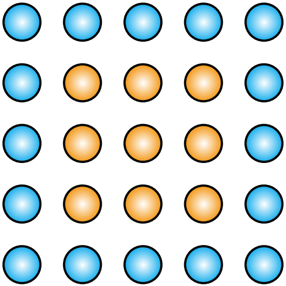
- Consider bipartite systems $\mathcal{H}_A \otimes \mathcal{H}_B$ described by ρ
- In practice we often have only sufficient knowledge of one subsystem (e.g. we know the lab system but not the environment)



The circuit model of Quantum Computing

Reduced density operator

- Consider bipartite systems $\mathcal{H}_A \otimes \mathcal{H}_B$ described by ρ
- In practice we often have only sufficient knowledge of one subsystem (e.g. we know the lab system but not the environment)
- Subsystem is described by the **reduced density operator** obtained by taking the **partial trace** with respect to one subsystem



$$\rho_B := \mathrm{tr}_A(\rho)$$

The circuit model of Quantum Computing

Reduced density operator

Example

- Consider the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right)$
- Corresponding density matrix

$$\rho = \frac{1}{2}\left|\Phi^+\right\rangle\left\langle\Phi^+\right| = \frac{1}{2}\Big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\Big)$$

- Taking the trace over the second system we obtain

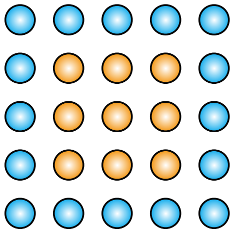
$$\rho_1 = \mathrm{tr}_2(\rho) = \frac{1}{2}\Big(|0\rangle\langle 0| + |1\rangle\langle 1|\Big)$$

$\Rightarrow$ The **first qubit** is in a **mixed state** although the **two-qubit state** is **pure**!

The circuit model of Quantum Computing

Implications for quantum computing

- Unlike in classical computing in general **we cannot simply discard a subset of qubits**
  - Discarding a subset of qubits corrsponds to taking the partial trace over them
  - If there is entanglement between the two sets of qubits, this leads to a mixed state for the subsystem
- For the same reasons we need to **keep the qubits well isolated from the environment**



The circuit model of Quantum Computing

Entanglement bipartite systems: pure states

- Consider a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ in a pure state

$$|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \quad \rho = |\psi\rangle\langle\psi|$$

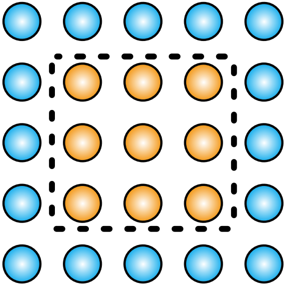
- Reduced density matrix describing B

$$\rho_B = \mathrm{tr}_A(\rho)$$

- von **Neumann entropy** for the reduced density operator

$$S = -\mathrm{tr}(\rho_B \log_2 \rho_B)$$

- The von Neumann entropy is zero iff $|\psi\rangle$ is a product state



The circuit model of Quantum Computing

Entanglement bipartite systems: pure states

Example

- We have already computed the reduced density operator for the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right)$

$$\rho_1 = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

- von Neumann entropy for ρ_1

$$S(\rho_1) = -\mathrm{tr}(\rho_1 \log_2 \rho_1) = -\left(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}\right) = 1$$

The circuit model of Quantum Computing

Entanglement bipartite systems: mixed states

- Consider a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ in a mixed state ρ
- A mixed state is called separable if and only if

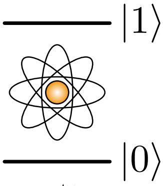
$$\rho = \sum_i w_i \rho_i^A \otimes \rho_i^B$$

- Otherwise the state is called entangled

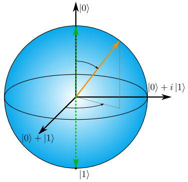
The circuit model of Quantum Computing

Summary qubits

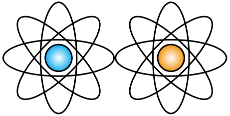
> A qubit is a **two-level quantum system**



> Qubits can be in **superposition**



> Multi-qubit systems can exhibit **entanglement**



Quantum gates

The circuit model of Quantum Computing

Quantum gates

- Quantum mechanics is reversible, $|\psi\rangle$ undergoes unitary evolution under some (time-dependent) Hamiltonian $H(t)$

$$|\psi(t)\rangle = T\,\text{exp}\left(-i\int_0^t ds\, H(s)\right)|\psi_0\rangle$$

- **Quantum gates** are represented by **unitary matrices**

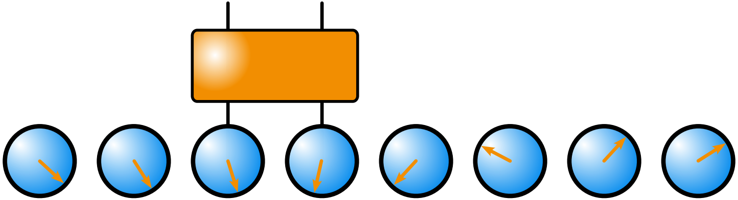
The circuit model of Quantum Computing

Quantum gates

- Quantum mechanics is reversible, $|\psi\rangle$ undergoes unitary evolution under some (time-dependent) Hamiltonian $H(t)$

$$|\psi(t)\rangle = T\,\text{exp}\left(-i\int_0^t ds\, H(s)\right)|\psi_0\rangle$$

- **Quantum gates** are represented by **unitary matrices**
- Typically gates only act on a few qubits in a nontrivial way



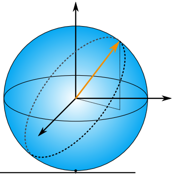
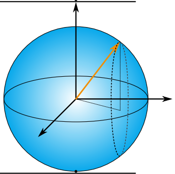
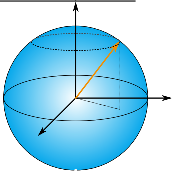
The circuit model of Quantum Computing

Common single-qubit quantum gates

Hadamard	$-\boxed{H}-$	$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$	$\vert 0\rangle \rightarrow \frac{1}{\sqrt{2}}(\vert 0\rangle + \vert 1\rangle)$ $\vert 1\rangle \rightarrow \frac{1}{\sqrt{2}}(\vert 0\rangle - \vert 1\rangle)$
X	$-\boxed{X}-$	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\vert 0\rangle \rightarrow \vert 1\rangle$ $\vert 1\rangle \rightarrow \vert 0\rangle$
Y	$-\boxed{Y}-$	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\vert 0\rangle \rightarrow -i\vert 1\rangle$ $\vert 1\rangle \rightarrow i\vert 0\rangle$
Z	$-\boxed{Z}-$	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\vert 0\rangle \rightarrow \vert 0\rangle$ $\vert 1\rangle \rightarrow -\vert 1\rangle$

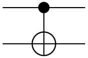
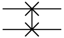
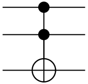
The circuit model of Quantum Computing

Common single-qubit rotations

$R_x(\theta)$	$-\boxed{R_x(\theta)}-$	$R_x(\theta) = \exp\left(-i\frac{\theta}{2}X\right)$	
$R_y(\theta)$	$-\boxed{R_y(\theta)}-$	$R_y(\theta) = \exp\left(-i\frac{\theta}{2}Y\right)$	
$R_z(\theta)$	$-\boxed{R_z(\theta)}-$	$R_z(\theta) = \exp\left(-i\frac{\theta}{2}Z\right)$	

The circuit model of Quantum Computing

Common multi-qubit quantum gates

CNOT		$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	$\vert 00\rangle \to \vert 00\rangle$ $\vert 01\rangle \to \vert 01\rangle$ $\vert 10\rangle \to \vert 11\rangle$ $\vert 11\rangle \to \vert 10\rangle$
SWAP gate		$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\vert 00\rangle \to \vert 00\rangle$ $\vert 01\rangle \to \vert 10\rangle$ $\vert 10\rangle \to \vert 01\rangle$ $\vert 11\rangle \to \vert 11\rangle$
Toffoli gate		$\begin{pmatrix} \mathbb{1}_{6\times 6} & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	CCNOT

The circuit model of Quantum Computing

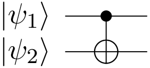
Quantum gates

> The reversible classical gates can be implemented on a quantum computer
$\Rightarrow$ We can replicate classical computation

> The Hadamard gate can **create superpositions** out of a single basis state

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

> The CNOT gate can **create entanglement**

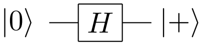


$$|\psi_1\rangle \otimes |\psi_2\rangle \to |\phi_{12}\rangle \neq |\phi_1\rangle \otimes |\phi_2\rangle$$

The circuit model of Quantum Computing

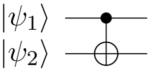
Quantum gates

- The reversible classical gates can be implemented on a quantum computer
  $\Rightarrow$ We can replicate classical computation
- The Hadamard gate can **create superpositions** out of a single basis state



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

- The CNOT gate can **create entanglement**



$$|\psi_1\rangle \otimes |\psi_2\rangle \rightarrow |\phi_{12}\rangle \neq |\phi_1\rangle \otimes |\phi_2\rangle$$

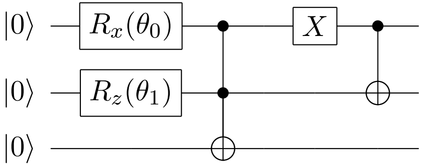
- Since quantum mechanics is linear, we can apply gates to superpositions of basis states

$$\text{CNOT}\big(\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\big) = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|11\rangle + \delta\,|10\rangle$$

The circuit model of Quantum Computing

Quantum gates

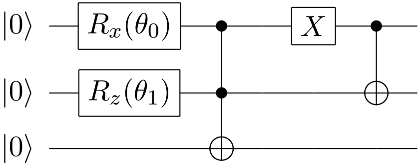
> Combining multiple gates we can build **quantum circuits**



The circuit model of Quantum Computing

Quantum gates

- Combining multiple gates we can build **quantum circuits**

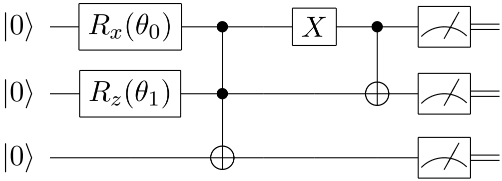


- **Depth** of a circuit: maximum length of a directed path from the input to the output

The circuit model of Quantum Computing

Quantum gates

> Combining multiple gates we can build **quantum circuits**



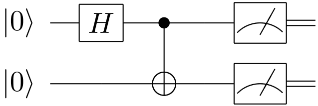
> **Depth** of a circuit: maximum length of a directed path from the input to the output

> Extracting information: measurement of the qubits (usually in the computational basis)

The circuit model of Quantum Computing

Example: preparing a Bell state

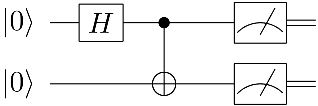
- Simple circuit preparing an entangled state (Bell state)



The circuit model of Quantum Computing

Example: preparing a Bell state

> Simple circuit preparing an entangled state (Bell state)



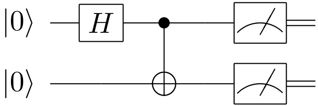
1 $|00\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle =$

$\frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$

The circuit model of Quantum Computing

Example: preparing a Bell state

- Simple circuit preparing an entangled state (Bell state)



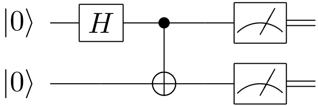
1 $$|00\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$$

2 $$\frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \rightarrow \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

The circuit model of Quantum Computing

Example: preparing a Bell state

- Simple circuit preparing an entangled state (Bell state)



1 $|00\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle =$

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

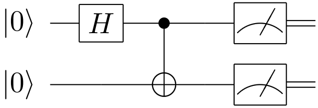
2 $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

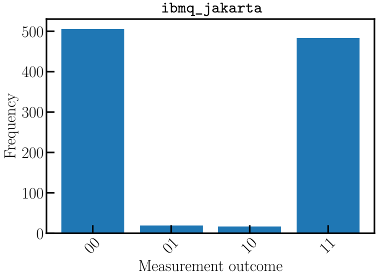
3 Measurement: $p(00) = 1/2$, $p(11) = 1/2$

The circuit model of Quantum Computing

Example: preparing a Bell state

- Simple circuit preparing an entangled state (Bell state)





1. $$|00\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

2. $$\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \to \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

3. Measurement: $p(00) = 1/2$, $p(11) = 1/2$

The circuit model of Quantum Computing

Universal gate set

A set of gates is **universal** if, by composing gates from it, one can express **any unitary transformation** on any number of qubits.

- Since the n-qubit unitaries form an uncountable infinite set $U(2^n)$, this requires an infinite number of gates
- Example: $\{\text{CNOT}, R_x(\theta), R_y(\theta), R_z(\theta)\}$, $\theta \in [0, 2\pi)$

The circuit model of Quantum Computing

Universal gate set

A set of gates is **universal** if, by composing gates from it, one can express **any unitary transformation** on any number of qubits.

- Since the n-qubit unitaries form an uncountable infinite set $U(2^n)$, this requires an infinite number of gates
- Example: $\{\text{CNOT}, R_x(\theta), R_y(\theta), R_z(\theta)\}$, $\theta \in [0, 2\pi)$

Approximate universal gate set

A set of gates is **universal** if, by composing gates from it, one can **approximate any unitary transformation** on any number of qubits to **any desired precision**.

- Examples: $\{\text{CNOT}, R_y(\pi/4), R_z(\pi/2)\}$, $\{\text{Toffoli}, H, R_z(\pi/2)\}$

The circuit model of Quantum Computing

Universal gate set

A set of gates is **universal** if, by composing gates from it, one can express **any unitary transformation** on any number of qubits.

- Since the n-qubit unitaries form an uncountable infinite set $U(2^n)$, this requires an infinite number of gates
- Example: $\{\text{CNOT}, R_x(\theta), R_y(\theta), R_z(\theta)\}$, $\theta \in [0, 2\pi)$

Approximate universal gate set

A set of gates is **universal** if, by composing gates from it, one can **approximate any unitary transformation** on any number of qubits to **any desired precision**.

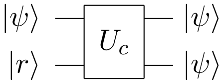
- Examples: $\{\text{CNOT}, R_y(\pi/4), R_z(\pi/2)\}$, $\{\text{Toffoli}, H, R_z(\pi/2)\}$
- Approximation can be done efficiently (Solovay-Kitaev theorem, $\mathcal{O}(\text{polylog}(1/\varepsilon))$)

Can we copy quantum states?

The circuit model of Quantum Computing

Can we copy quantum states?

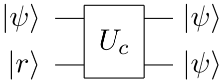
- Classically: we can arbitrarily copy bits
- Quantum version: we want a unitary U_c which allows for



The circuit model of Quantum Computing

Can we copy quantum states?

- Classically: we can arbitrarily copy bits
- Quantum version: we want a unitary U_c which allows for



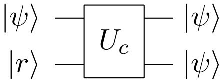
- In particular we have have to be able to copy basis states

$$U_c\,|0\rangle \otimes |r\rangle \rightarrow |0\rangle \otimes |0\rangle$$
$$U_c\,|1\rangle \otimes |r\rangle \rightarrow |1\rangle \otimes |1\rangle$$

The circuit model of Quantum Computing

Can we copy quantum states?

- Classically: we can arbitrarily copy bits
- Quantum version: we want a unitary U_c which allows for



- In particular we have have to be able to copy basis states

$$U_c |0\rangle \otimes |r\rangle \rightarrow |0\rangle \otimes |0\rangle$$
$$U_c |1\rangle \otimes |r\rangle \rightarrow |1\rangle \otimes |1\rangle$$

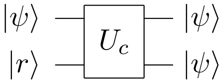
- Since $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$

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

The circuit model of Quantum Computing

Can we copy quantum states?

- Classically: we can arbitrarily copy bits
- Quantum version: we want a unitary U_c which allows for



- In particular we have have to be able to copy basis states

$$U_c\,|0\rangle \otimes |r\rangle \to |0\rangle \otimes |0\rangle$$
$$U_c\,|1\rangle \otimes |r\rangle \to |1\rangle \otimes |1\rangle$$

- Since $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

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

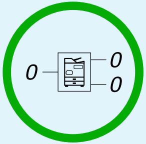
No cloning theorem

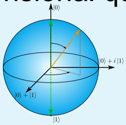
A quantum state cannot be copied with perfect fidelity.

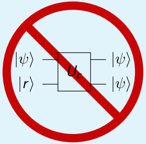
The circuit model of Quantum Computing

Summary: Classical vs. Quantum Computing

Classical computing	Quantum computing
> Classical bits are 0 or 1 > Typically irreversible gate set, but reversible is possible > We can arbitrarily copy bits	> Qubit: two-dimensional quantum system ⇒ Can be in superposition > Unitary evolution, reversible > No cloning theorem







The circuit model of Quantum Computing

Why is quantum computing more powerful?

- The Hilbert space of n qubits is the tensor product $\underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n \text{ times}}$

  $\Rightarrow$ Dimension 2^n, **number of basis states grows exponentially**

The circuit model of Quantum Computing

Why is quantum computing more powerful?

- The Hilbert space of n qubits is the tensor product $\underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n \text{ times}}$

  $\Rightarrow$ Dimension 2^n, **number of basis states grows exponentially**
- We can build **superpositions** of basis states and apply unitary gates to them

$$|0\rangle + |1\rangle \quad \text{—}\boxed{U}\text{—} \quad U|0\rangle + U|1\rangle$$

$\Rightarrow$ **“Quantum parallelism”**

The circuit model of Quantum Computing

Why is quantum computing more powerful?

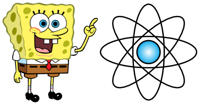
- The Hilbert space of n qubits is the tensor product $\underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n \text{ times}}$

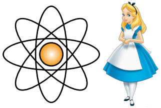
  $\Rightarrow$ Dimension 2^n, **number of basis states grows exponentially**
- We can build **superpositions** of basis states and apply unitary gates to them

$$|0\rangle + |1\rangle \; — \boxed{U} — \quad U|0\rangle + U|1\rangle$$

$\Rightarrow$ **“Quantum parallelism”**

- Multiple **qubits can be entangled**





$\Rightarrow$ Correlations that have no classical analog

4.

Motivation

Classical computing

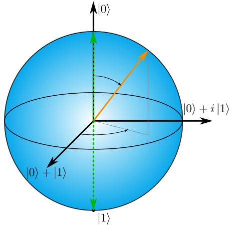
The circuit model of Quantum Computing

Experimental realization of qubits

Experimental realization of qubits

Di Vincenzo's criteria

- Criteria for a physical system to be a qubit
  1. System needs to have well defined qubits and has to be scalable
  2. Qubits can be prepared in a pure state
  3. Decoherence time has to be longer than the one for a single operation
  4. It has to be possible to implement an (approximate) universal set of gates
  5. Each qubit can be measured individually



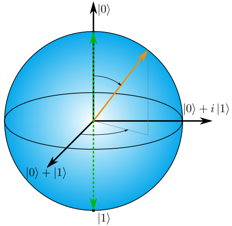
D. P. DiVincenzo, Fortschritte der Physik 48, 771 (2000)

Experimental realization of qubits

Di Vincenzo’s criteria

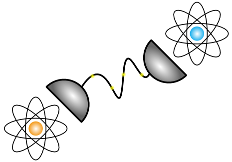
> Criteria for a physical system to be a qubit

1. System needs to have well defined qubits and has to be scalable
2. Qubits can be prepared in a pure state
3. Decoherence time has to be longer than the one for a single operation
4. It has to be possible to implement an (approximate) universal set of gates
5. Each qubit can be measured individually



> Requirements for communication

1. Possibility to interconvert stationary and flying qubits
2. Faithful transmission flying qubits between specified locations



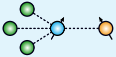
D. P. DiVincenzo, Fortschritte der Physik 48, 771 (2000)

Experimental realization of qubits

Neutral atoms

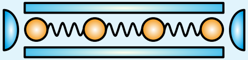
- Cold atoms in an optical lattices
- Manipulation via laser/microwave pulses

Nuclear spins



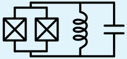
- Nuclear spins of a molecule as qubits
- Manipulation via NMR techniques

Trapped ions



- Manipulation via lasers and phonon mode
- System with few degrees of freedom

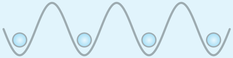
Superconducting circuits



- Manipulation via microwave pulses
- Used in most commercially available quantum computers

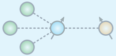
Experimental realization of qubits

Neutral atoms



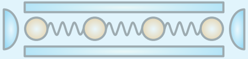
- Cold atoms in an optical lattices
- Manipulation via laser/microwave pulses

Nuclear spins



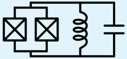
- Nuclear spins of a molecule as qubits
- Manipulation via NMR techniques

Trapped ions



- Manipulation via lasers and phonon mode
- System with few degrees of freedom

Superconducting circuits

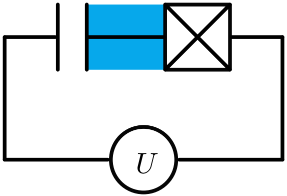


- Manipulation via microwave pulses
- Used in most commercially available quantum computers

Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Circuit



- Josephson junction and capacitor connected to voltage
- Hamiltonian

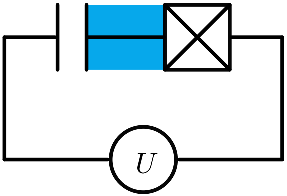
$$H = E_c(n - n_g)^2 - E_J \cos(\phi)$$

M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Circuit



- Josephson junction and capacitor connected to voltage
- Hamiltonian

$$H = E_c(n - n_g)^2 - E_J \cos(\phi)$$

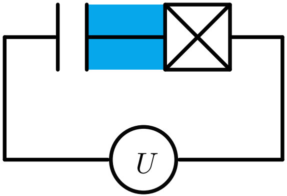
- Constant E_c depends on the capacities in the circuit
- Constants E_J and n_g can be tuned via the magnetic field and the voltage

M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Circuit



- Josephson junction and capacitor connected to voltage
- Hamiltonian

$$H = E_c(n - n_g)^2 - E_J \cos(\phi)$$

- Constant E_c depends on the capacities in the circuit
- Constants E_J and n_g can be tuned via the magnetic field and the voltage
- Number of Cooper pairs n and phase ϕ are conjugate variables: $[n, \phi] = i$
- In the eigenbasis of n we thus have

$$n\,|n\rangle = n\,|n\rangle\,, \quad \exp(i\phi)\,|n\rangle = |n+1\rangle$$

- $E_J \cos(\phi) = \frac{1}{2} E_J \left(\exp(i\phi) + \exp(-i\phi)\right)$

M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

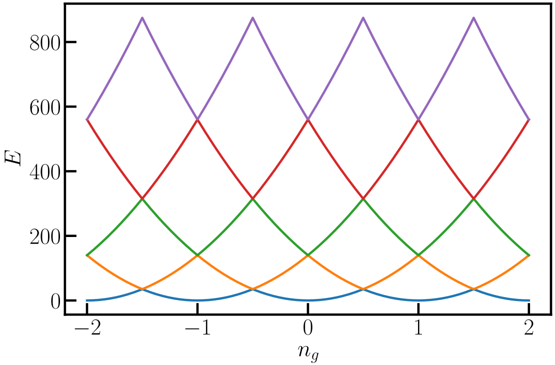
Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Hamiltonian

$$W = (n - n_g)^2 - \frac{E_J}{E_c}\,\text{cos}(\phi)$$

- For $E_J/E_c = 0$: harmonic potential
- $n = 0$: lowest two levels are not well separated from others
- $n_g = 1/2$: lowest two levels are degenerate



M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

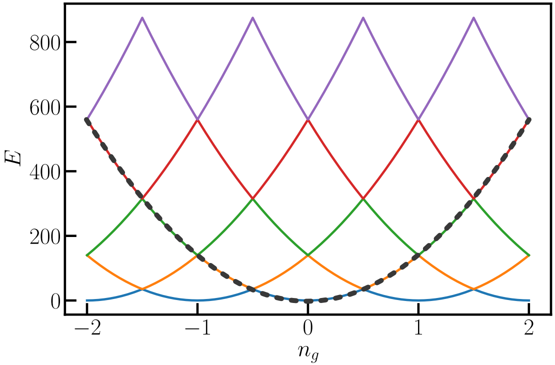
Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Hamiltonian

$$W = (n - n_g)^2 - \frac{E_J}{E_c}\cos(\phi)$$

- For $E_J/E_c = 0$: harmonic potential
- $n = 0$: lowest two levels are not well separated from others
- $n_g = 1/2$: lowest two levels are degenerate



M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

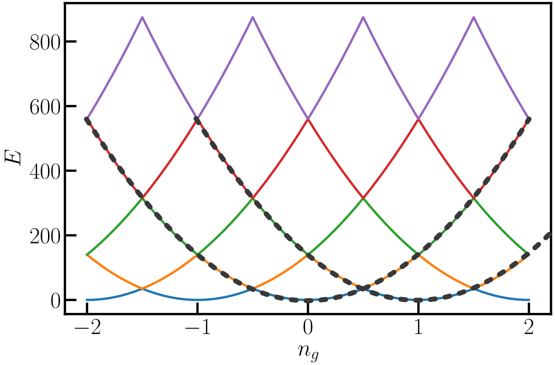
Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Hamiltonian

$$W = (n - n_g)^2 - \frac{E_J}{E_c}\cos(\phi)$$

- For $E_J/E_c = 0$: harmonic potential
- $n = 0$: lowest two levels are not well separated from others
- $n_g = 1/2$: lowest two levels are degenerate



M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

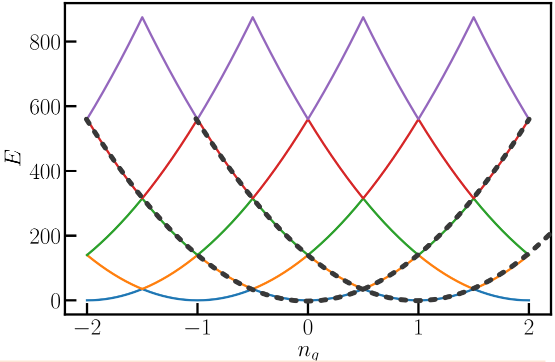
Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Hamiltonian

$$W = (n - n_g)^2 - \frac{E_J}{E_c}\cos(\phi)$$

- For $E_J/E_c = 0$: harmonic potential
- $n = 0$: lowest two levels are not well separated from others
- $n_g = 1/2$: lowest two levels are degenerate



$E_J/E_c = 0$ is not suitable to have a qubit.

M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

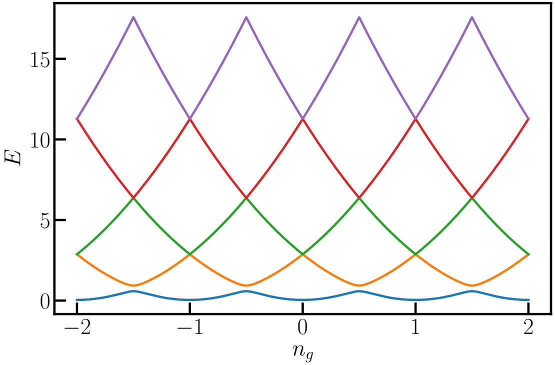
Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Hamiltonian

$$W = (n - n_g)^2 - \frac{E_J}{E_c} \cos(\phi)$$

- For $E_J/E_c \ll 1$: level splitting due to nonlinearity of the Josephson junction
- n has a fairly concrete value
- For $n_g = 1/2$ levels are well separated from the ones above



M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

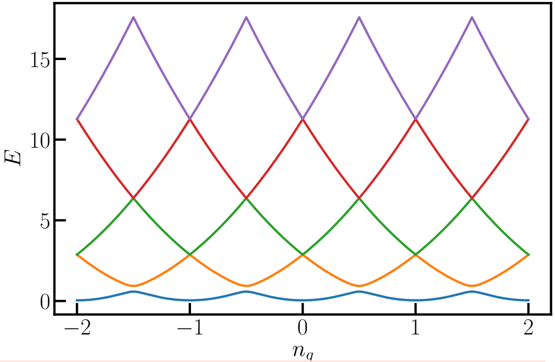
Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Hamiltonian

$$W = (n - n_g)^2 - \frac{E_J}{E_c} \cos(\phi)$$

- For $E_J/E_c \ll 1$: level splitting due to nonlinearity of the Josephson junction
- n has a fairly concrete value
- For $n_g = 1/2$ levels are well separated from the ones above



$E_J/E_c \ll 1$ is a charge qubit.

M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

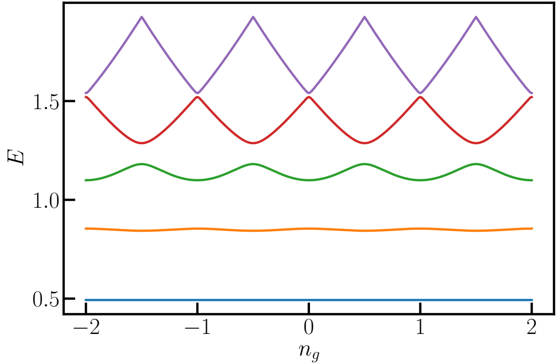
Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Hamiltonian

$$W = (n - n_g)^2 - \frac{E_J}{E_c} \cos(\phi)$$

- For intermediate E_J/E_c lowest levels fairly flat
- Less sensitivity to charge noise but less separation to higher levels



M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

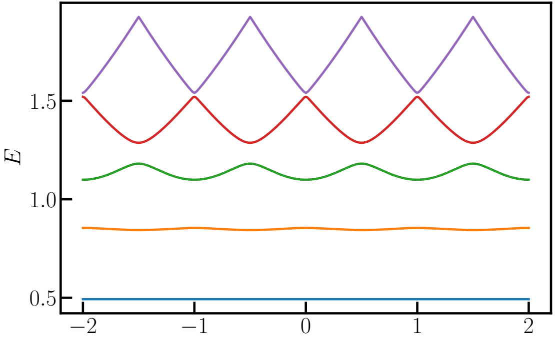
Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

- Hamiltonian

$$W = (n - n_g)^2 - \frac{E_J}{E_c}\cos(\phi)$$

- For intermediate E_J/E_c lowest levels fairly flat
- Less sensitivity to charge noise but less separation to higher levels



This regime is a transmon qubit.

M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

> Hamiltonian

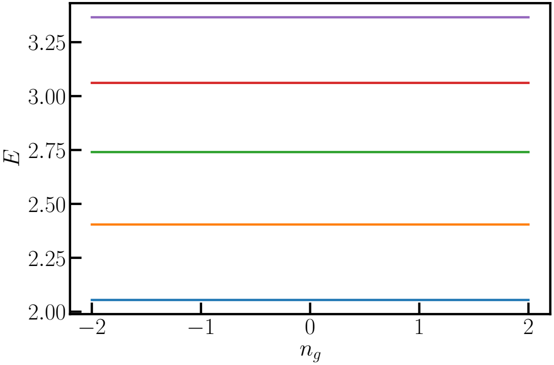
$$W = (n - n_g)^2 - \frac{E_J}{E_c} \cos(\phi)$$

> $E_J/E_c \gg 1$: $\cos(\phi)$ dominates

> Expanding around $\phi = 0$

$$\cos(\phi) \approx 1 - \tfrac{1}{2}\phi^2$$

> Harmonic oscillator in ϕ independent of n_g



M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

Experimental realization of qubits

A simple superconducting qubit: the Cooper pair box

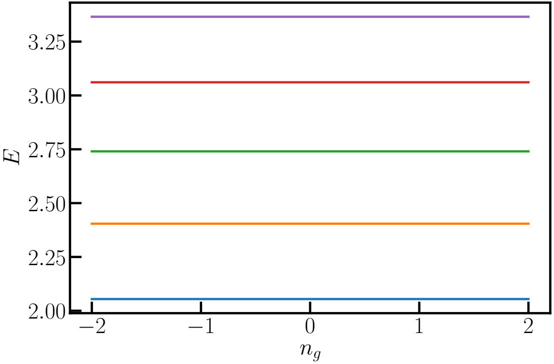
- Hamiltonian

$$W = (n - n_g)^2 - \frac{E_J}{E_c}\,\text{cos}(\phi)$$

- $E_J/E_c \gg 1$: $\text{cos}(\phi)$ dominates
- Expanding around $\phi = 0$

$$\text{cos}(\phi) \approx 1 - \tfrac{1}{2}\phi^2$$

- Harmonic oscillator in ϕ independent of n_g



Evenly spaced energy levels, not to have a qubit.

M. H. Devoret, A. Wallraff, J. M. Martinis, arXiv:cond-mat/0411174 (2004)

Experimental realization of qubits

Superconducting qubits

- Applying gates: couple the qubit to a microwave cavity
- Jaynes-Cummings Hamiltonian

$$\mathcal{H} = \underbrace{\boxed{\hbar\omega a^\dagger a}}_{\text{cavity}} + \underbrace{\boxed{\hbar\frac{\Omega}{2}Z}}_{\text{qubit}} + \underbrace{\boxed{\hbar g(a^\dagger\sigma^- + a\sigma^+)}}_{\text{coupling between qubit and cavity}}$$

  $a^\dagger$: creation operator for microwave photons

  $\sigma^\pm = \frac{1}{2}(X \pm iY)$

  ω: microwave frequency

  Ω: frequency of the qubit

  g: coupling strength

- In practice more elaborate designs

J. M. Chow et al., Nature Comm. 5 4015 (2014)

Experimental realization of qubits

Superconducting qubits

- Applying gates: couple the qubit to a microwave cavity
- Jaynes-Cummings Hamiltonian

$$\mathcal{H} = \underbrace{\boxed{\hbar\omega a^\dagger a}}_{\text{cavity}} + \underbrace{\boxed{\hbar\frac{\Omega}{2}Z}}_{\text{qubit}} + \underbrace{\boxed{\hbar g(a^\dagger\sigma^- + a\sigma^+)}}_{\text{coupling between qubit and cavity}}$$

$a^\dagger$: creation operator for microwave photons

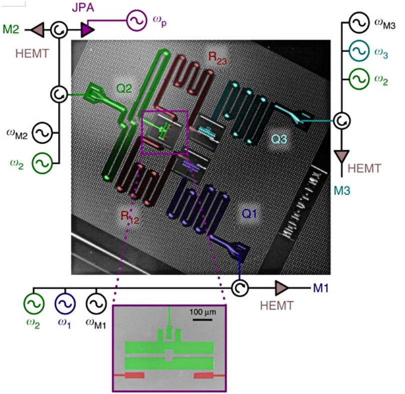
$\sigma^\pm = \frac{1}{2}(X \pm iY)$

ω: microwave frequency

Ω: frequency of the qubit

g: coupling strength

- In practice more elaborate designs



J. M. Chow et al., Nature Comm. 5 4015 (2014)

Thank you for your attention!

Questions?