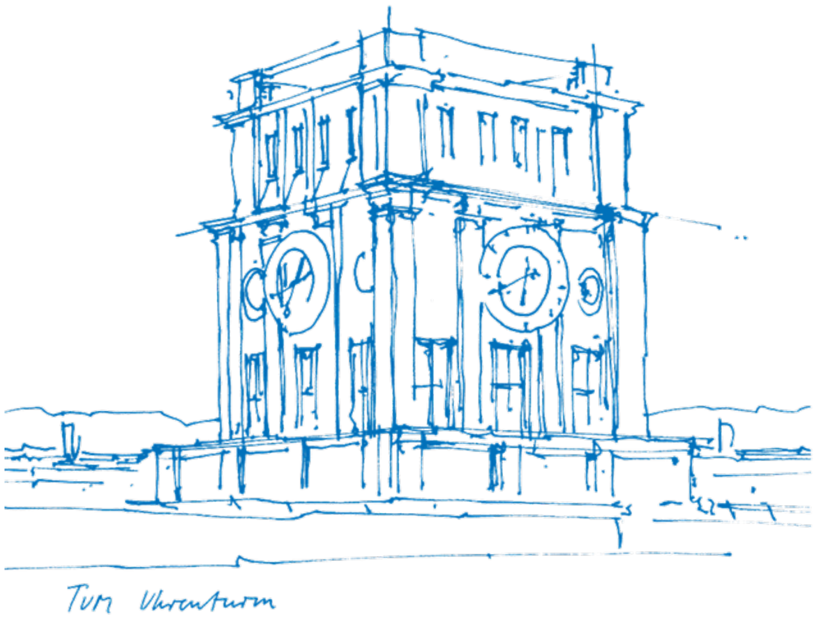
Introduction to Quantum Computing (IN2381)

Prof. Dr. Christian B. Mendl
Technische Universität München
Department of Informatics 5

November 2, 2020



Course organization

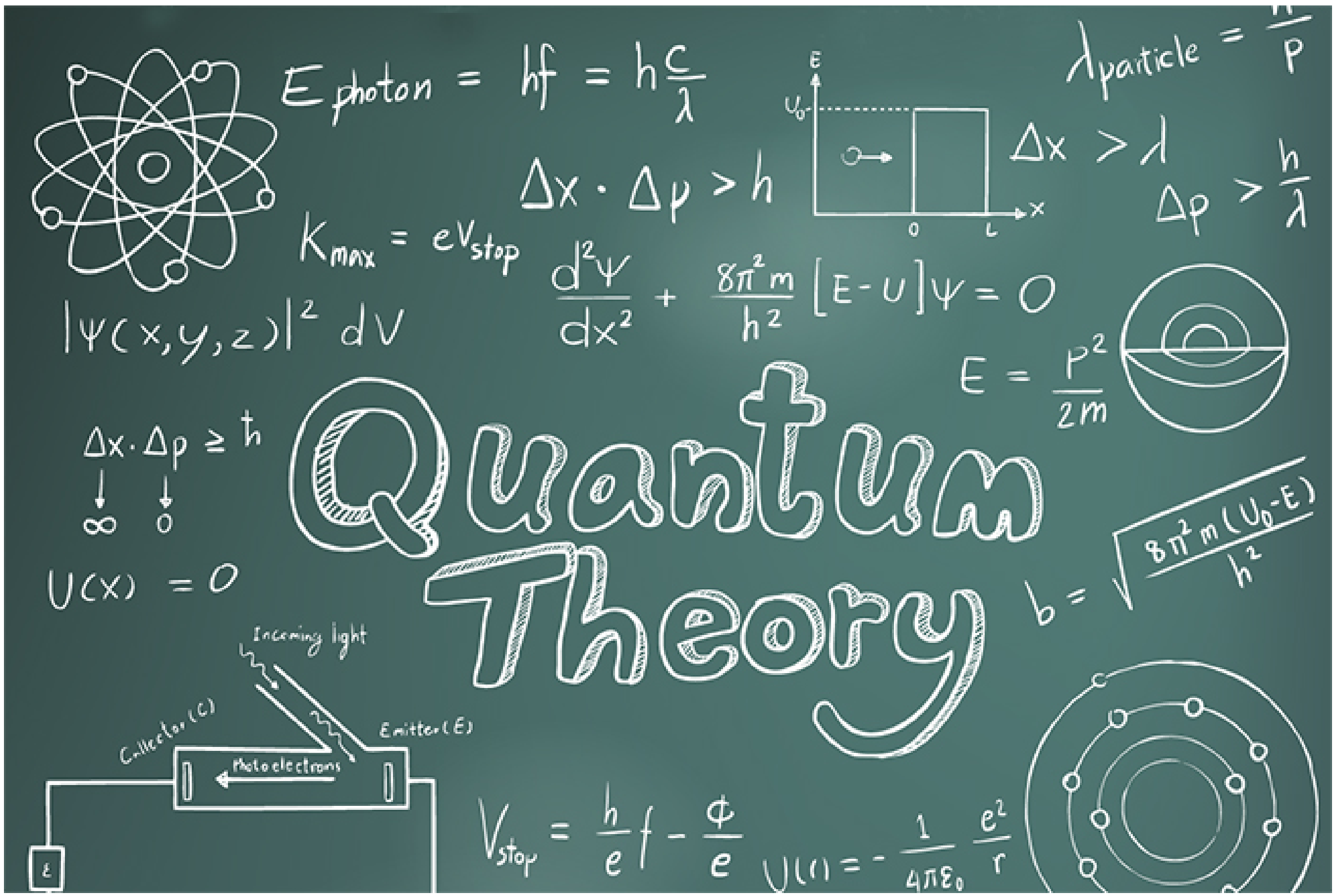
- People:

Prof. Dr. Christian B. Mendl	lecture
M.Sc. Irene López Gutiérrez	tutorial
M.Sc. Keefe Huang	tutorial

- Moodle: https://www.moodle.tum.de/course/view.php?id=57976
- Course will be offered using online video lectures, both an on-campus and a recorded tutorial, a script, the Nielsen and Chuang textbook, homework exercises and online exchange (see Moodle)
- Topics:
  - Introduction to quantum mechanics
  - Bell inequalities
  - Quantum circuits and algorithms
  - Quantum error correction
- Final exam: planned as on-campus written exam
- Grade bonus: 1 "*Notenstufe*" (+0.3 or +0.4) for 60% of appropriately solved ("sinnvoll bearbeitete") homework exercises (excluding failed exams and better than 1.0)
- Groups of up to 3 people allowed to hand in homework solutions (via Moodle)
  (please only hand in one solution for the whole group)

Quantum mechanics

Fundamental physical theory describing behavior of atoms, electrons and other elementary particles
(But: general relativity not taken into account $\rightsquigarrow$ area of active research)



Source: http://timesslate.com/2019/06/21/machine-assimilation-reveals-mysteries-of-quantum-physics/

Quantum theory and computing: a short history (1)

– 1900 Max Planck: energy quantization, invented as mathematical tool to describe black body radiation:

$$E = nh\nu, \quad n \in \mathbb{N},\ h\text{: Planck's constant},\ \nu\text{: frequency}$$

Quantum theory and computing: a short history (1)

– 1900 Max Planck: energy quantization, invented as mathematical tool to describe black body radiation:

$$E = nh\nu, \quad n \in \mathbb{N}, \; h\text{: Planck's constant}, \; \nu\text{: frequency}$$

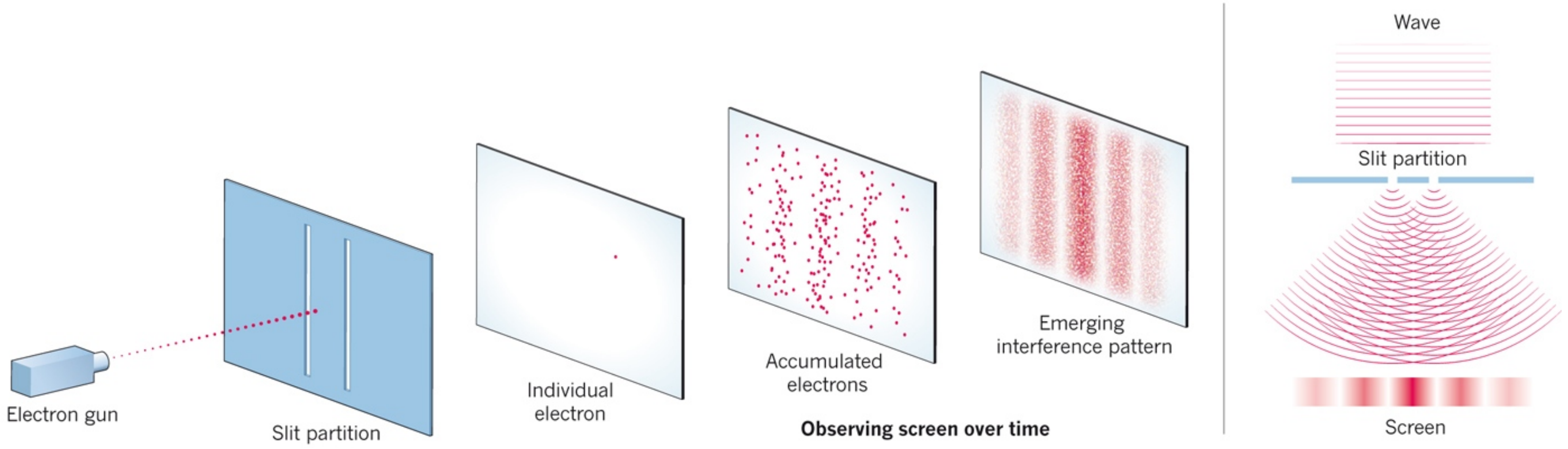
– 1905 Albert Einstein: explanation of the photoelectric effect by describing light as composed of discrete quanta (photons)

Quantum theory and computing: a short history (1)

- 1900 Max Planck: energy quantization, invented as mathematical tool to describe black body radiation:
$$E = nh\nu, \quad n \in \mathbb{N},\ h\text{: Planck's constant},\ \nu\text{: frequency}$$
- 1905 Albert Einstein: explanation of the photoelectric effect by describing light as composed of discrete quanta (photons)
- 1913 Niels Bohr: Bohr model of atoms: electrons in discrete energy states, Rydberg formula for spectral emission wavelengths of hydrogen

Quantum theory and computing: a short history (1)

- 1900 Max Planck: energy quantization, invented as mathematical tool to describe black body radiation:
$$E = nh\nu, \quad n \in \mathbb{N},\ h\text{: Planck's constant},\ \nu\text{: frequency}$$
- 1905 Albert Einstein: explanation of the photoelectric effect by describing light as composed of discrete quanta (photons)
- 1913 Niels Bohr: Bohr model of atoms: electrons in discrete energy states, Rydberg formula for spectral emission wavelengths of hydrogen
- 1924 Louis de Broglie: wave–particle duality of matter



Quantum theory and computing: a short history (2)

– 1925 Erwin Schrödinger: Schrödinger equation for the wave function Ψ of a quantum-mechanical system:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t} |\Psi(t)\rangle = \hat{H} |\Psi(t)\rangle$$

Quantum theory and computing: a short history (2)

– 1925 Erwin Schrödinger: Schrödinger equation for the wave function Ψ of a quantum-mechanical system:

$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\Psi(t)\rangle = \hat{H}|\Psi(t)\rangle$$

– 1927 Werner Heisenberg: uncertainty principle

Quantum theory and computing: a short history (2)

– 1925 Erwin Schrödinger: Schrödinger equation for the wave function Ψ of a quantum-mechanical system:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t} |\Psi(t)\rangle = \hat{H} |\Psi(t)\rangle$$

– 1927 Werner Heisenberg: uncertainty principle

– 1927 Niels Bohr and Werner Heisenberg: Copenhagen interpretation of quantum mechanics

Quantum theory and computing: a short history (2)

- 1925 Erwin Schrödinger: Schrödinger equation for the wave function Ψ of a quantum-mechanical system:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t} |\Psi(t)\rangle = \hat{H} |\Psi(t)\rangle$$

- 1927 Werner Heisenberg: uncertainty principle
- 1927 Niels Bohr and Werner Heisenberg: Copenhagen interpretation of quantum mechanics
- 1928 Paul Dirac: Dirac equation, combines special relativity and quantum mechanics; first prediction of antimatter

Quantum theory and computing: a short history (2)

– 1925 Erwin Schrödinger: Schrödinger equation for the wave function Ψ of a quantum-mechanical system:

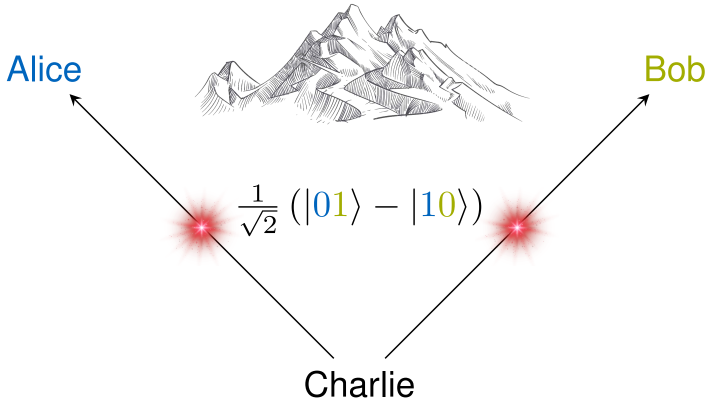
$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\Psi(t)\rangle = \hat{H}|\Psi(t)\rangle$$

– 1927 Werner Heisenberg: uncertainty principle

– 1927 Niels Bohr and Werner Heisenberg: Copenhagen interpretation of quantum mechanics

– 1928 Paul Dirac: Dirac equation, combines special relativity and quantum mechanics; first prediction of antimatter

– 1935 Einstein, Podolsky, Rosen: EPR paradox: “spooky action at a distance” due to quantum entanglement ($\rightsquigarrow$ Bell’s inequality)



Quantum theory and computing: a short history (3)

– 1948 Claude Shannon: “A Mathematical Theory of Communication”: foundation of information theory

Quantum theory and computing: a short history (3)

- 1948 Claude Shannon: “A Mathematical Theory of Communication”: foundation of information theory
- 1961 Rolf Landauer: Landauer’s principle: logically irreversible manipulation of information is necessarily dissipative

Quantum theory and computing: a short history (3)

- 1948 Claude Shannon: “A Mathematical Theory of Communication”: foundation of information theory
- 1961 Rolf Landauer: Landauer’s principle: logically irreversible manipulation of information is necessarily dissipative
- 1964 John Bell: Bell’s inequality: “local realism” violates predictions by quantum mechanics (later experiments agree with quantum mechanics)

Quantum theory and computing: a short history (3)

- 1948 Claude Shannon: “A Mathematical Theory of Communication”: foundation of information theory
- 1961 Rolf Landauer: Landauer’s principle: logically irreversible manipulation of information is necessarily dissipative
- 1964 John Bell: Bell’s inequality: “local realism” violates predictions by quantum mechanics (later experiments agree with quantum mechanics)
- 1982 Richard Feynman: idea of a universal quantum computer

Quantum theory and computing: a short history (3)

– 1948 Claude Shannon: “A Mathematical Theory of Communication”: foundation of information theory

– 1961 Rolf Landauer: Landauer’s principle: logically irreversible manipulation of information is necessarily dissipative

– 1964 John Bell: Bell’s inequality: “local realism” violates predictions by quantum mechanics (later experiments agree with quantum mechanics)

– 1982 Richard Feynman: idea of a universal quantum computer

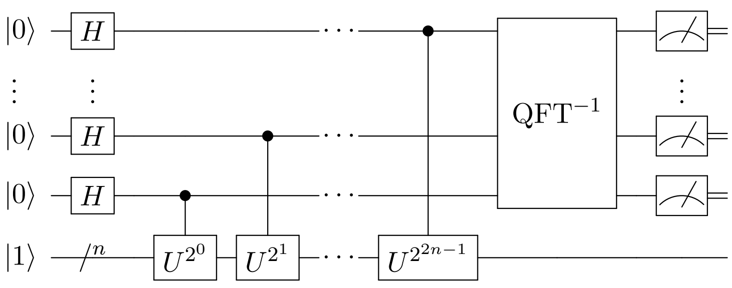
– 1985 David Deutsch: precursor of Deutsch-Jozsa algorithm: exponentially faster than any possible deterministic classical algorithm

Quantum theory and computing: a short history (3)

- 1948 Claude Shannon: “A Mathematical Theory of Communication”: foundation of information theory
- 1961 Rolf Landauer: Landauer’s principle: logically irreversible manipulation of information is necessarily dissipative
- 1964 John Bell: Bell’s inequality: “local realism” violates predictions by quantum mechanics (later experiments agree with quantum mechanics)
- 1982 Richard Feynman: idea of a universal quantum computer
- 1985 David Deutsch: precursor of Deutsch-Jozsa algorithm: exponentially faster than any possible deterministic classical algorithm
- 1993 Bernstein und Vazirani: foundations of quantum complexity theory

Quantum theory and computing: a short history (3)

- 1948 Claude Shannon: “A Mathematical Theory of Communication”: foundation of information theory
- 1961 Rolf Landauer: Landauer’s principle: logically irreversible manipulation of information is necessarily dissipative
- 1964 John Bell: Bell’s inequality: “local realism” violates predictions by quantum mechanics (later experiments agree with quantum mechanics)
- 1982 Richard Feynman: idea of a universal quantum computer
- 1985 David Deutsch: precursor of Deutsch-Jozsa algorithm: exponentially faster than any possible deterministic classical algorithm
- 1993 Bernstein und Vazirani: foundations of quantum complexity theory
- 1994 Peter Shor: Shor’s algorithm for integer factorization ($\rightsquigarrow$ highly relevant for public-key cryptography)



Quantum theory and computing: a short history (4)

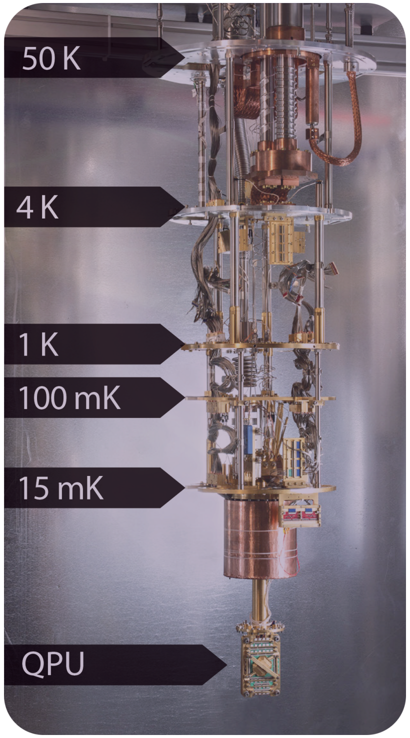
– 1998 2-qubit nuclear spin resonance quantum system

Quantum theory and computing: a short history (4)

- 1998 2-qubit nuclear spin resonance quantum system
- 2009 Research group of John Martinis: “Josephson-junction superconducting qubit”

Quantum theory and computing: a short history (4)

- 1998 2-qubit nuclear spin resonance quantum system
- 2009 Research group of John Martinis: “Josephson-junction superconducting qubit”
- 2015 DWAVE “quantum annealing” system (2048 qubits)



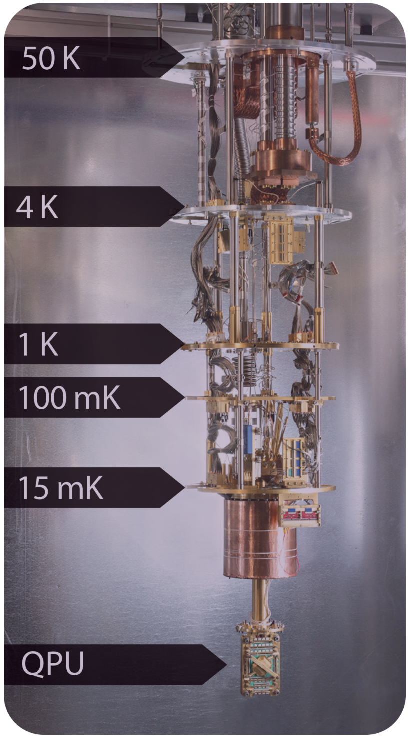
Quantum theory and computing: a short history (4)

– 1998 2-qubit nuclear spin resonance quantum system

– 2009 Research group of John Martinis: “Josephson-junction superconducting qubit”

– 2015 DWAVE “quantum annealing” system (2048 qubits)

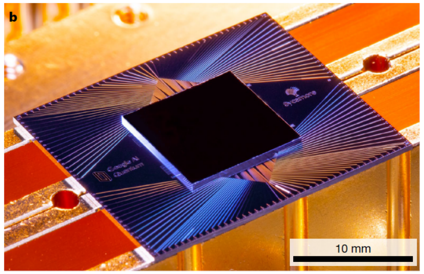
– 2016 IBM quantum computer with 50 qubits

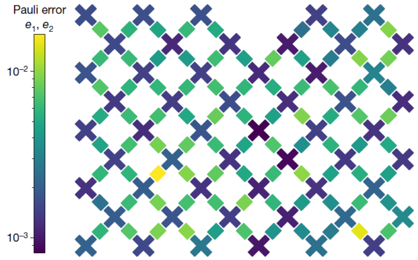


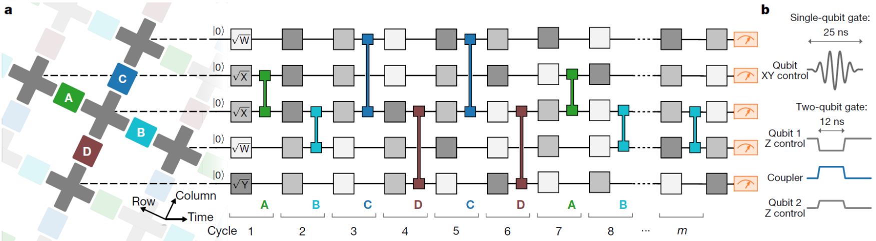
Quantum theory and computing: a short history (4)

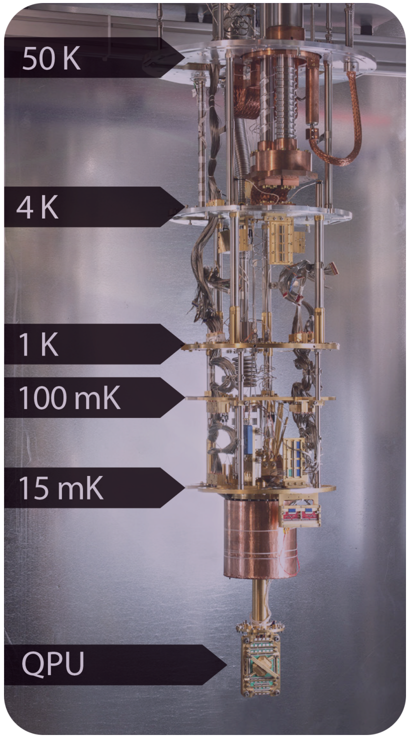
– 1998 2-qubit nuclear spin resonance quantum system
– 2009 Research group of John Martinis: “Josephson-junction superconducting qubit”
– 2015 DWAVE “quantum annealing” system (2048 qubits)

– 2016 IBM quantum computer with 50 qubits
– 2019 Google / Martinis group: “quantum supremacy”, Sycamore processor (53 qubits)





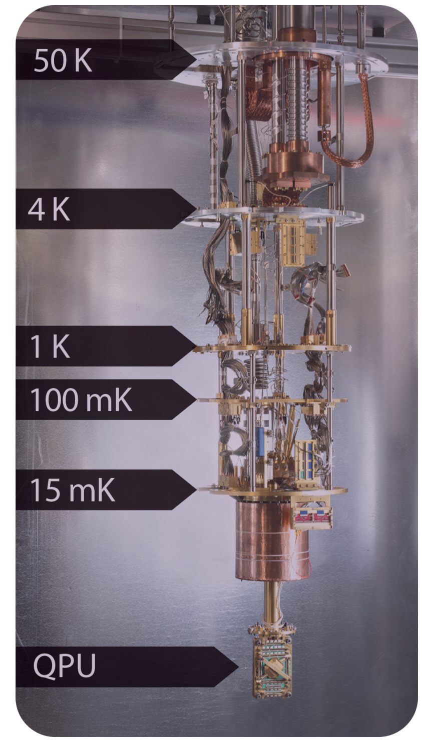




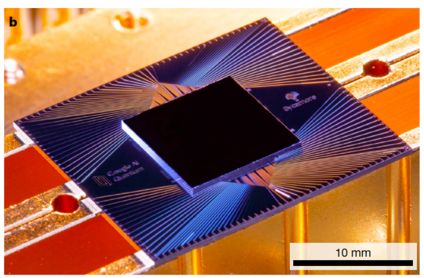
F. Arute, . . . , H. Neven, J. M. Martinis. *Quantum supremacy using a programmable superconducting processor.* Nature 574, 505 (2019)

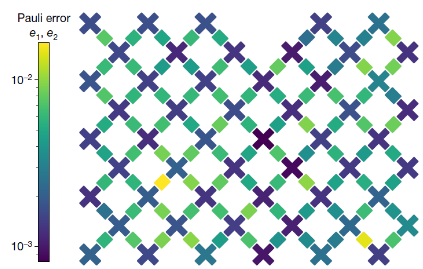
Quantum theory and computing: a short history (4)

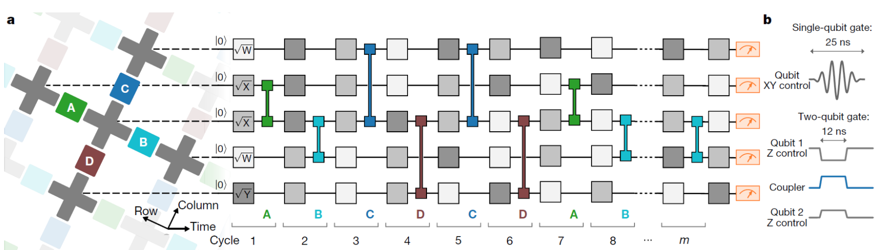
– 1998 2-qubit nuclear spin resonance quantum system
– 2009 Research group of John Martinis: “Josephson-junction superconducting qubit”
– 2015 DWAVE “quantum annealing” system (2048 qubits)



– 2016 IBM quantum computer with 50 qubits
– 2019 Google / Martinis group: “quantum supremacy”, Sycamore processor (53 qubits)



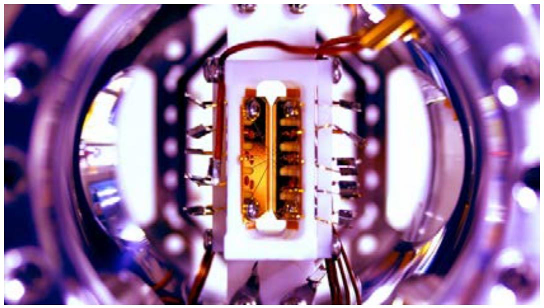




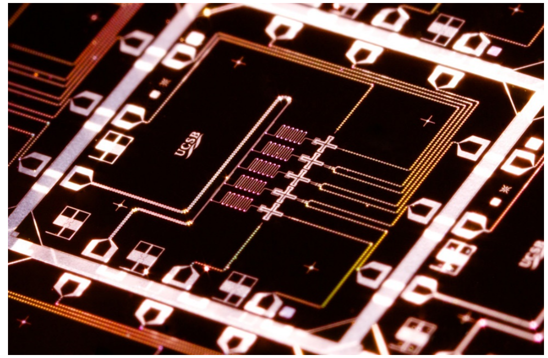
F. Arute, . . . , H. Neven, J. M. Martinis. *Quantum supremacy using a programmable superconducting processor.* Nature 574, 505 (2019)

– 2020 Alpine Quantum Technologies (aqt.eu): ion-trap QC, qubit loss detection and correction

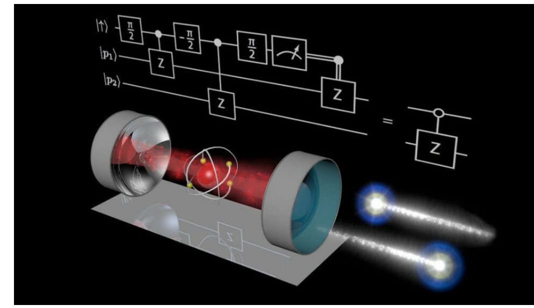
Various approaches for physical realizations



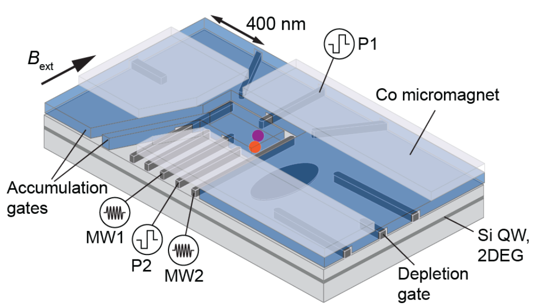
ion traps



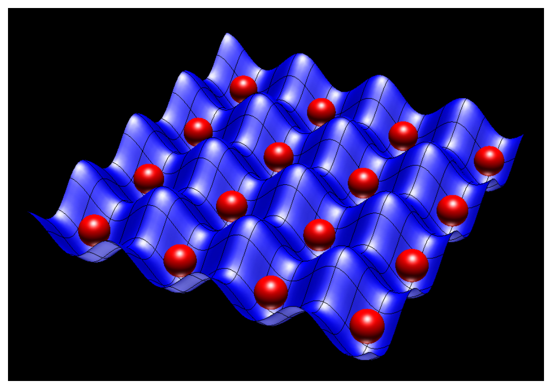
superconducting qubits



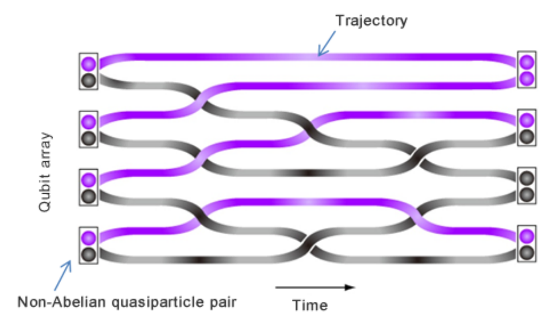
photons



quantum dots



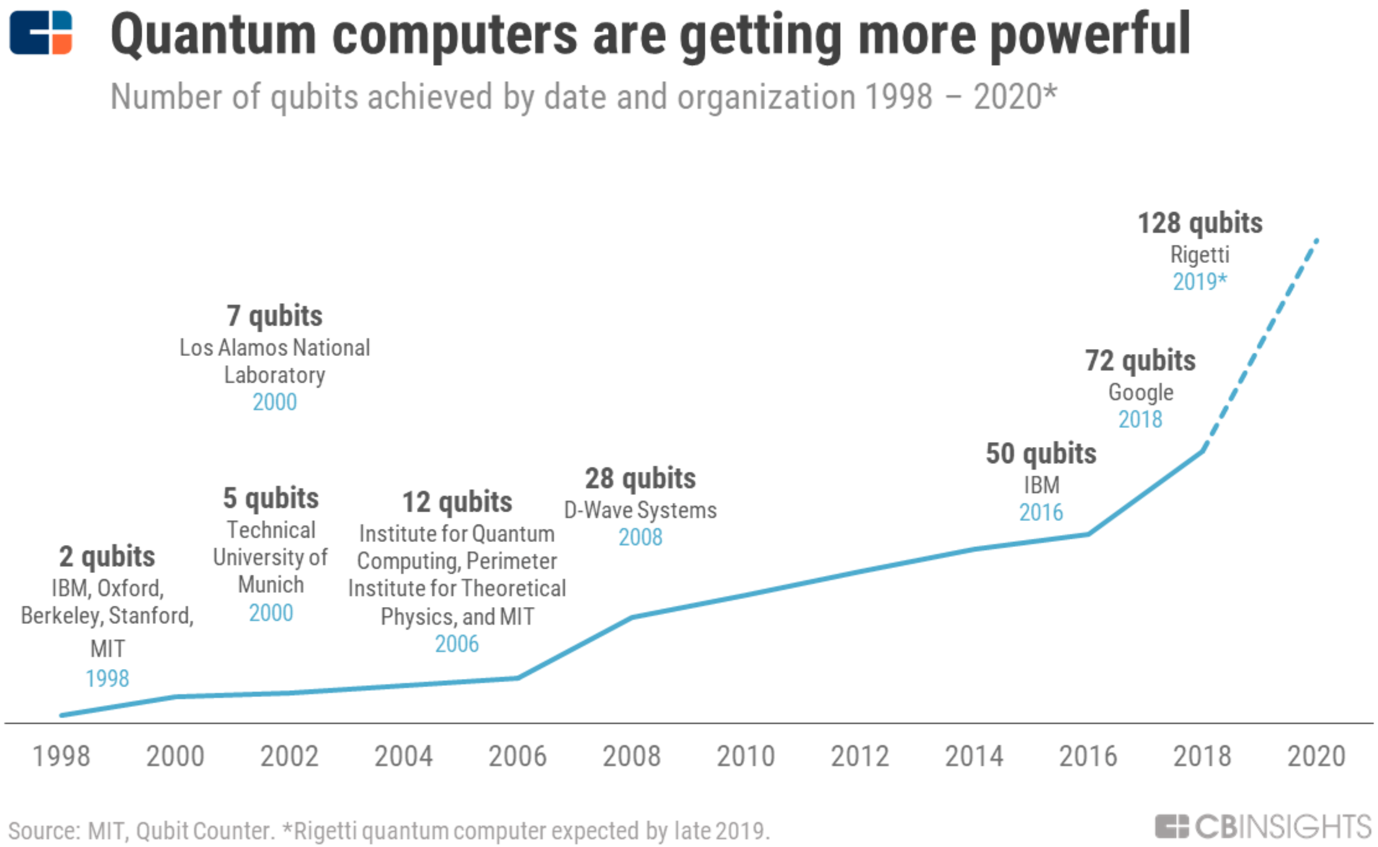
optical lattices



topological

Several hardware platforms thinkable due to “universality” of quantum mechanics, current cloud-accessible devices based on superconducting qubits or ion-traps

Number of qubits



Source: https://www.cbinsights.com/research/report/quantum-computing/

"Qubit quality", gate fidelity, decoherence time, . . . relevant as well

Shor's algorithm for integer factorization

$$15 = 3 \cdot 5$$

Peter Shor

Peter Shor (1994)

Quantum algorithm, polynomial w.r.t. number of bits

$\rightsquigarrow$ thread to RSA cryptosystem?

Idea: reduce factoring to order-finding:

given co-prime integers x, N, compute smallest integer $\mathbf{r} \geq 1$ such that

$$x^{\mathbf{r}} = 1 \mod N$$

In case $\mathbf{r}$ is even: find factor of N via

$$x^{\mathbf{r}} - 1 = \left(x^{\mathbf{r}/2} - 1\right)\left(x^{\mathbf{r}/2} + 1\right)$$

Solve order-finding by *quantum phase estimation*

But: not feasible on current quantum hardware: length of circuit, qubit number, low noise tolerance ...

P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring" (1994)
C. Gidney and M. Ekerå. "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits". arXiv:1905.09749

Shor's algorithm for integer factorization

$$231772171 = ?$$

Peter Shor

Peter Shor (1994)

Quantum algorithm, polynomial w.r.t. number of bits

$\rightsquigarrow$ thread to RSA cryptosystem?

Idea: reduce factoring to order-finding:

given co-prime integers x, N, compute smallest integer $r \geq 1$ such that

$$x^r = 1 \mod N$$

In case r is even: find factor of N via

$$x^r - 1 = \left(x^{r/2} - 1\right)\left(x^{r/2} + 1\right)$$

Solve order-finding by *quantum phase estimation*

But: not feasible on current quantum hardware: length of circuit, qubit number, low noise tolerance ...

P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring" (1994)

C. Gidney and M. Ekerå. "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits". arXiv:1905.09749

Shor's algorithm for integer factorization

$$231772171 = 11279 \cdot 20549$$

Peter Shor

Peter Shor (1994)

Quantum algorithm, polynomial w.r.t. number of bits

$\rightsquigarrow$ thread to RSA cryptosystem?

Idea: reduce factoring to order-finding:

given co-prime integers x, N, compute smallest integer $\mathbf{r} \geq 1$ such that

$$x^{\mathbf{r}} = 1 \mod N$$

In case $\mathbf{r}$ is even: find factor of N via

$$x^{\mathbf{r}} - 1 = \left(x^{\mathbf{r}/2} - 1\right)\left(x^{\mathbf{r}/2} + 1\right)$$

Solve order-finding by *quantum phase estimation*

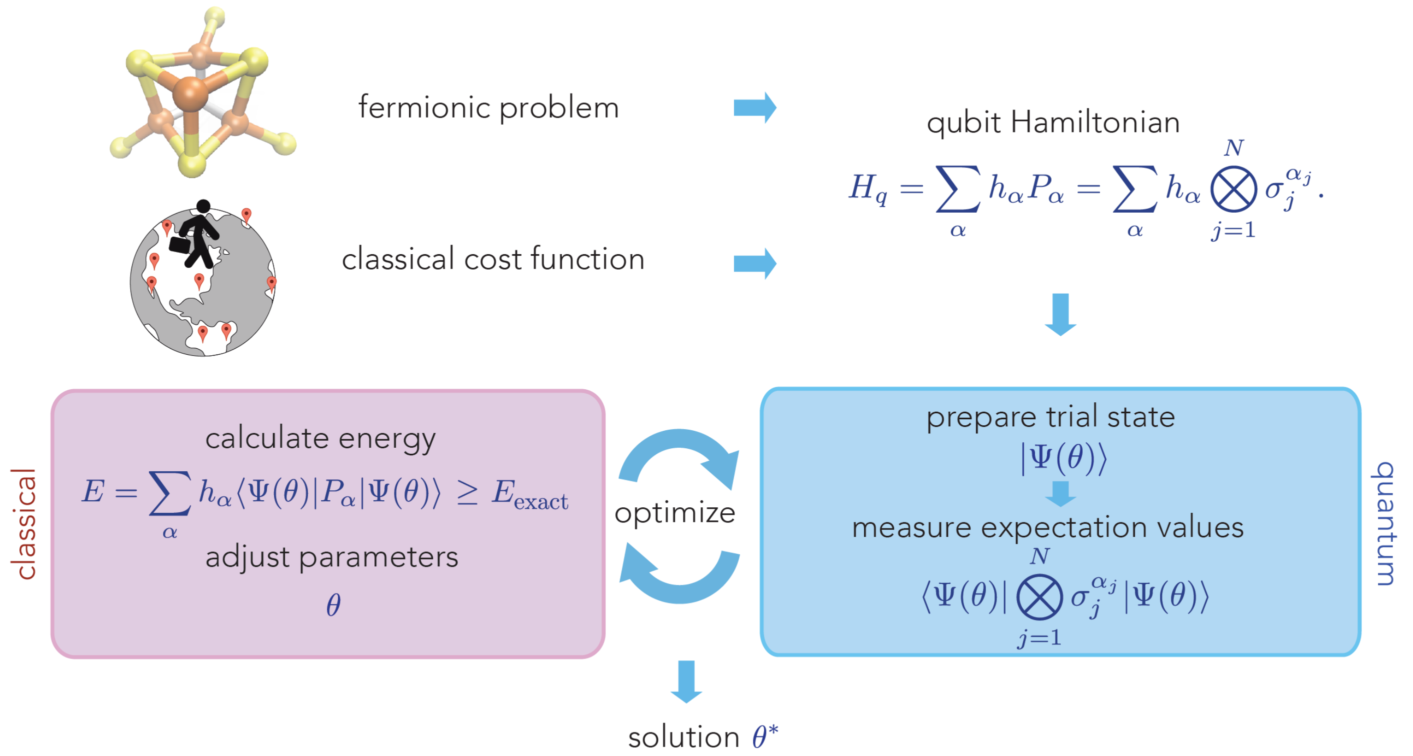
But: not feasible on current quantum hardware: length of circuit, qubit number, low noise tolerance ...

P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring" (1994)

C. Gidney and M. Ekerå. "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits". arXiv:1905.09749

Hybrid classical-quantum computing and QVE

QVE: quantum variational eigensolver

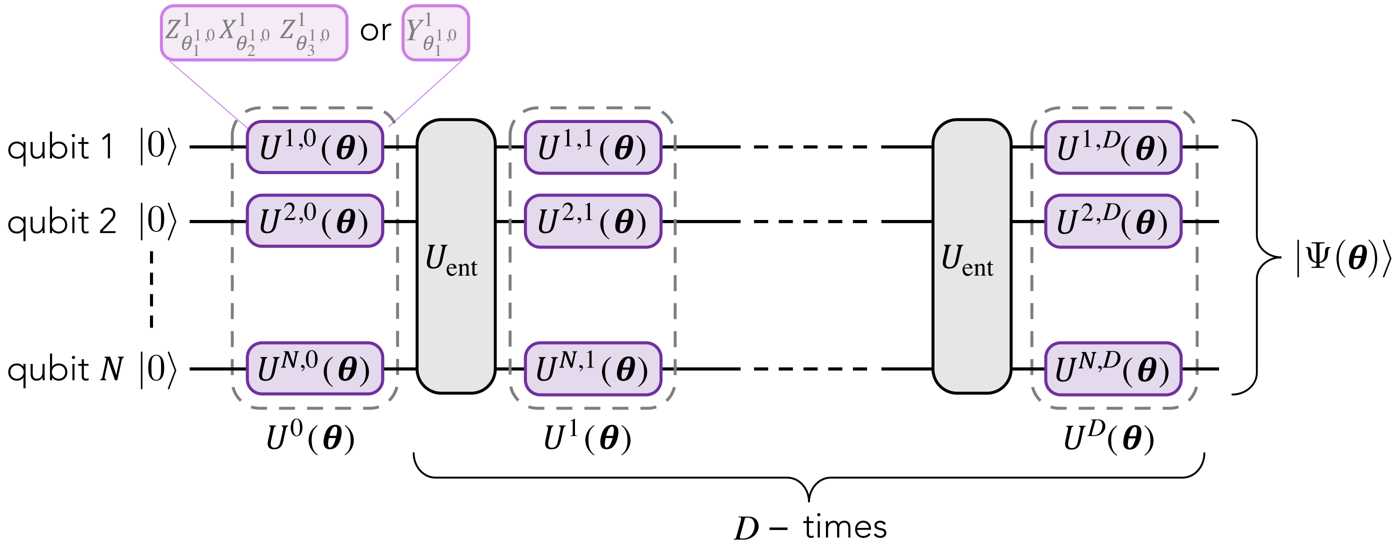


Source: Moll et al. (2018)

A. Peruzzo et al. “A variational eigenvalue solver on a photonic quantum processor”. Nat. Commun. 5, 4213 (2014)
A. Kandala et al. “Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets”. Nature 549, 242–246 (2017)
Moll, N. et al. “Quantum optimization using variational algorithms on near-term quantum devices”. Quantum Sci. Technol. 3, 030503 (2018)

Hybrid classical-quantum computing and QVE

QVE: quantum variational eigensolver



Source: Moll et al. (2018)

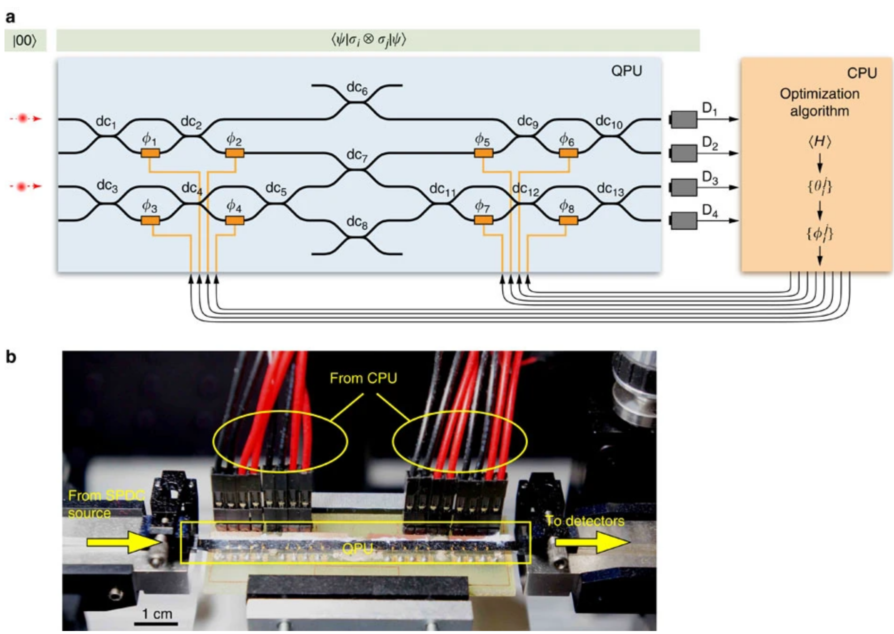
A. Peruzzo et al. “A variational eigenvalue solver on a photonic quantum processor”. Nat. Commun. 5, 4213 (2014)
A. Kandala et al. “Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets”. Nature 549, 242–246 (2017)
Moll, N. et al. “Quantum optimization using variational algorithms on near-term quantum devices”. Quantum Sci. Technol. 3, 030503 (2018)

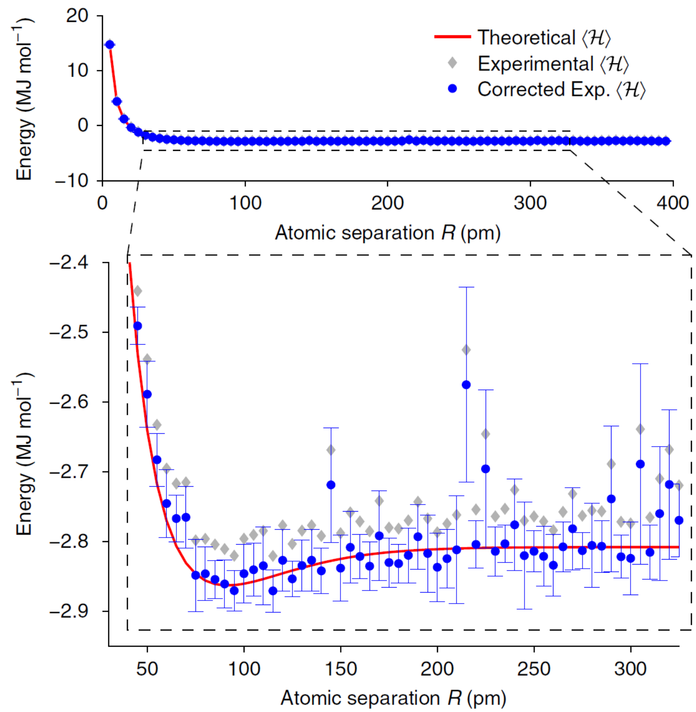
Quantum variational eigensolver (QVE)

Minimal model Hamiltonian (dimension 4×4), for bond dissociation of He-H$^+$

$$H(R) = \sum_{i\alpha} h^i_\alpha(R)\sigma^i_\alpha + \sum_{ij\alpha\beta} h^{ij}_{\alpha\beta}(R)\sigma^i_\alpha\sigma^j_\beta$$

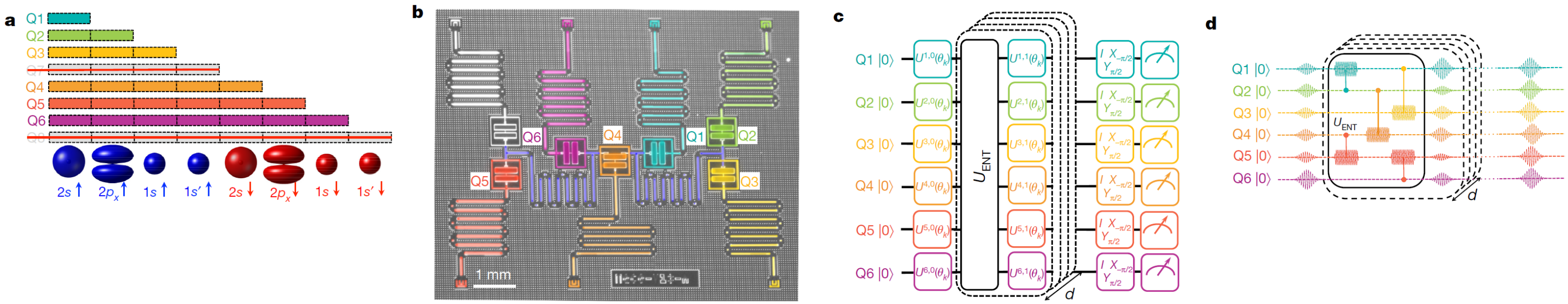
expectation values $\langle\psi|\,\sigma^i_\alpha\sigma^j_\beta\,|\psi\rangle$

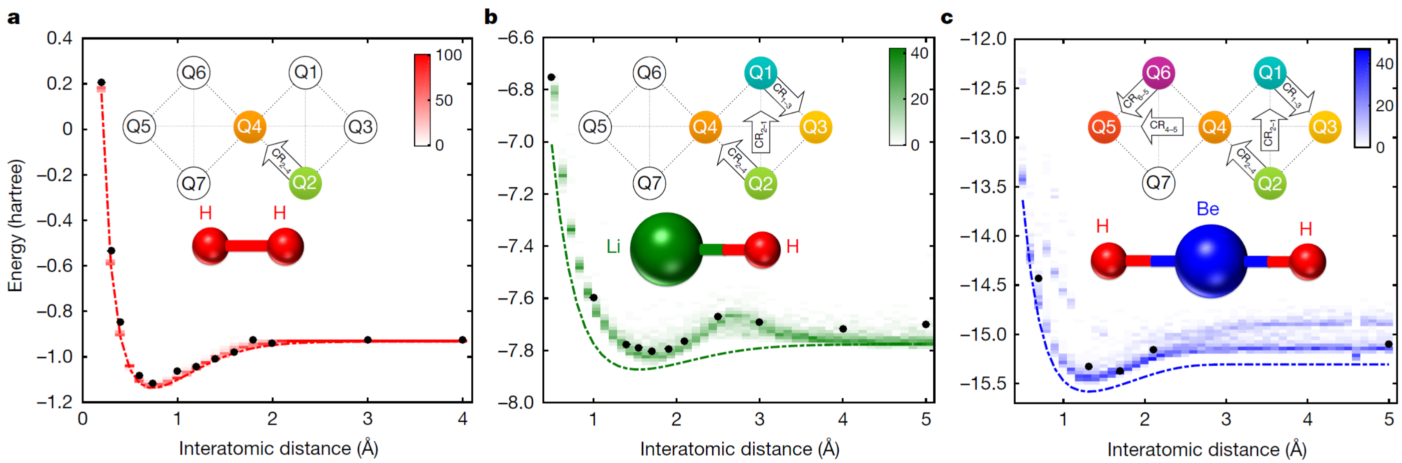




A. Peruzzo et al. “A variational eigenvalue solver on a photonic quantum processor”. Nat. Commun. 5, 4213 (2014)
J.-G. Liu et al. “Variational quantum eigensolver with fewer qubits”. Phys. Rev. Research 1, 023025 (2019)

Quantum variational eigensolver (QVE), cont.



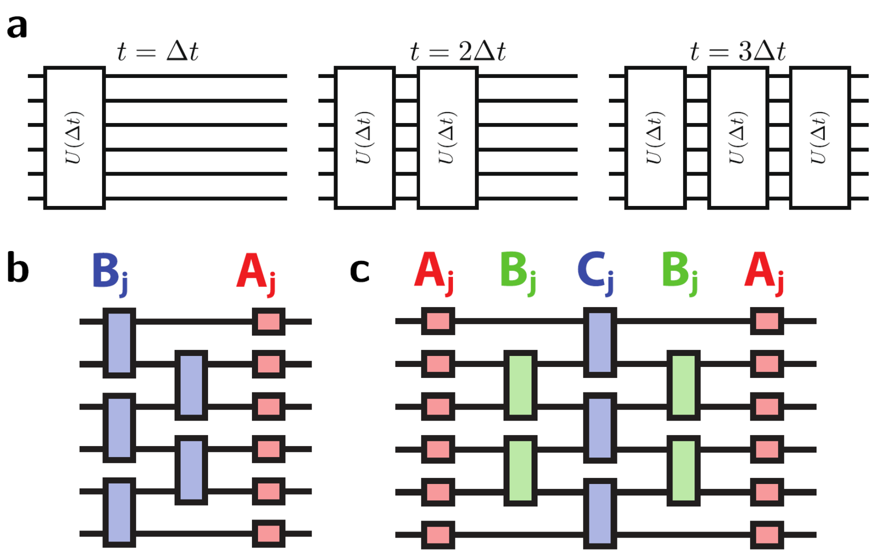


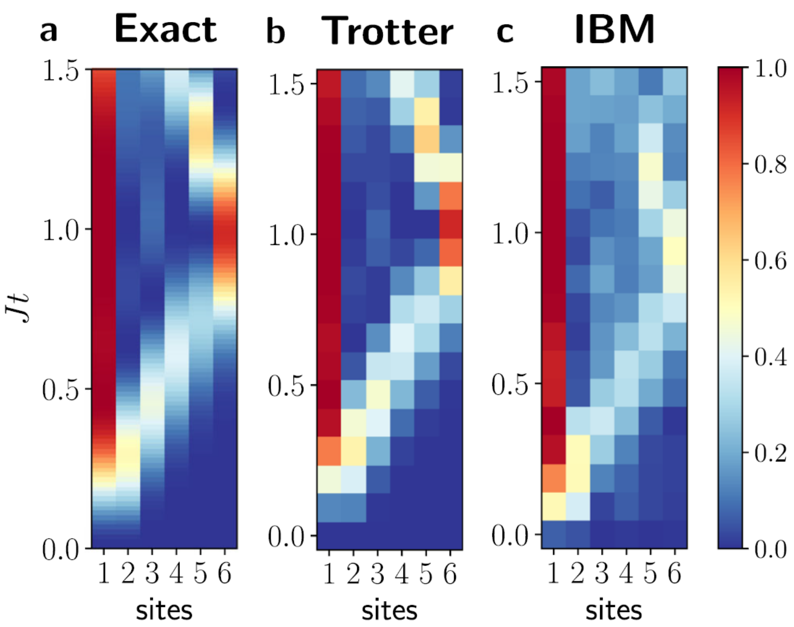
Source: A. Kandala et al. (2017), IBM

A. Kandala et al. “Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets”. Nature 549, 242–246 (2017)
F. Arute et al. “Hartree-Fock on a superconducting qubit quantum computer”. arXiv:2004.04174 (2020)

Simulating quantum many-body dynamics

Setup: spin-$\frac{1}{2}$ chain





Smith, Kim, Pollmann, Knolle. “Simulating quantum many-body dynamics on a current digital quantum computer”. npj Quantum Information 5, 106 (2019)

B. Chiaro et al. “Growth and preservation of entanglement in a many-body localized system”. arXiv:1910.06024

Quantum optimization: QAOA algorithm

Maximize

$$C(z) = \sum_{\alpha=1}^{m} C_\alpha(z), \quad z = z_1 z_2 \ldots z_n$$

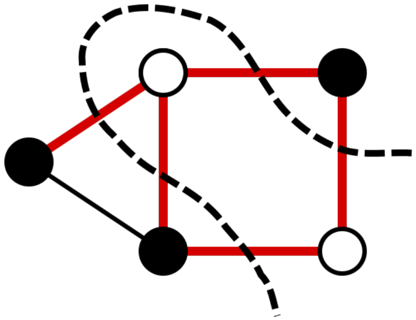
Ansatz: encode C as quantum Hamiltonian, maximize

$$\langle \psi_p(\gamma,\beta) | \, C \, | \psi_p(\gamma,\beta) \rangle$$

w.r.t. angles γ, β in

$$|\psi_p(\gamma,\beta)\rangle = \mathrm{e}^{-i\beta_p B} \mathrm{e}^{-i\gamma_p C} \cdots \mathrm{e}^{-i\beta_1 B} \mathrm{e}^{-i\gamma_1 C} |+\rangle^{\otimes n}$$

Application to Max-Cut:

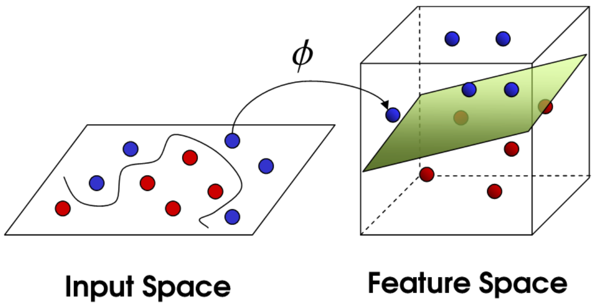


Source: Wikipedia

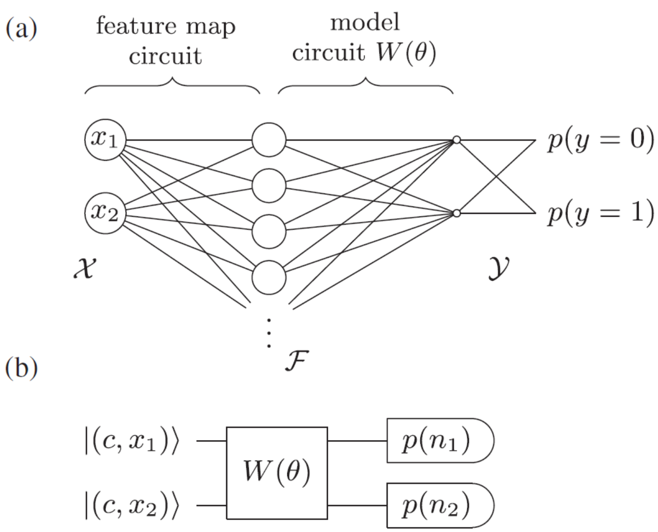
E. Farhi et al. "A quantum approximate optimization algorithm". arXiv:1411.4028

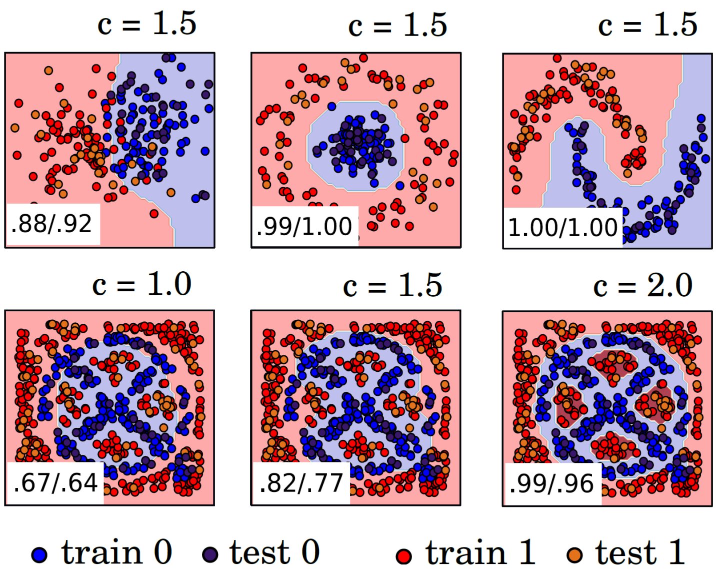
Quantum machine learning

Quantum Hilbert space as nonlinear feature map:



Source: towardsdatascience.com

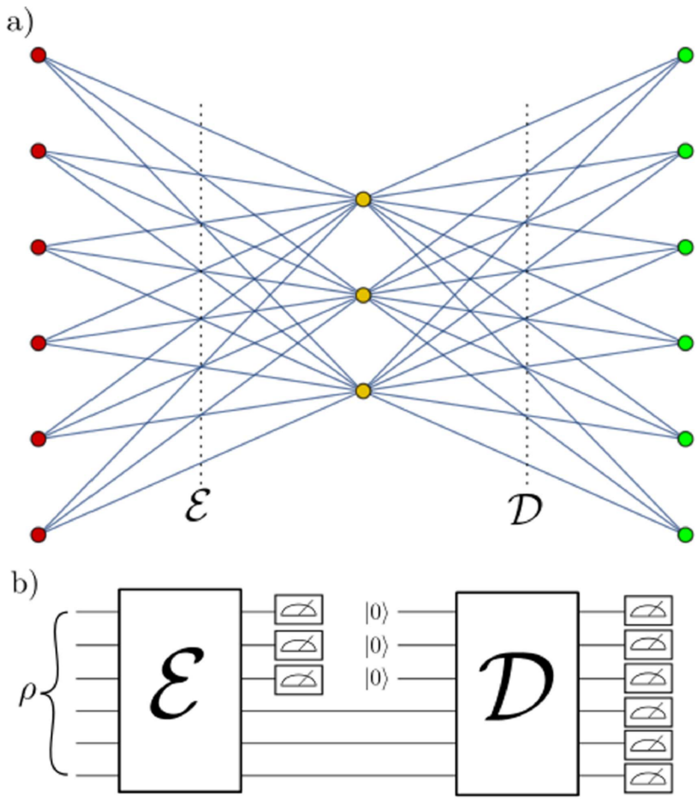


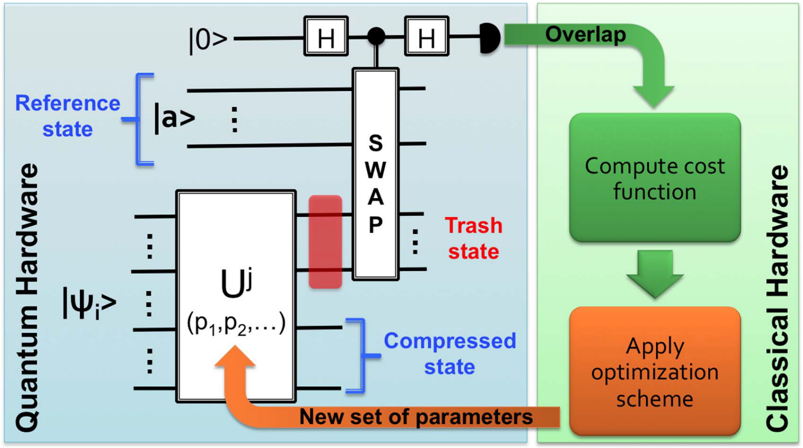


Review: J. Biamonte et al. “Quantum machine learning”. Nature 549, 195–202 (2017)

M. Schuld and N. Killoran. “Quantum machine learning in feature Hilbert spaces”. Phys. Rev. Lett. 122, 040504 (2019)

Quantum autoencoders

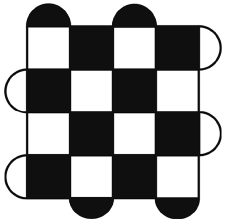




J. Romero, J. P. Olson, A. Aspuru-Guzik. "Quantum autoencoders for efficient compression of quantum data". Quantum Sci. Technol. 2, 045001 (2017)

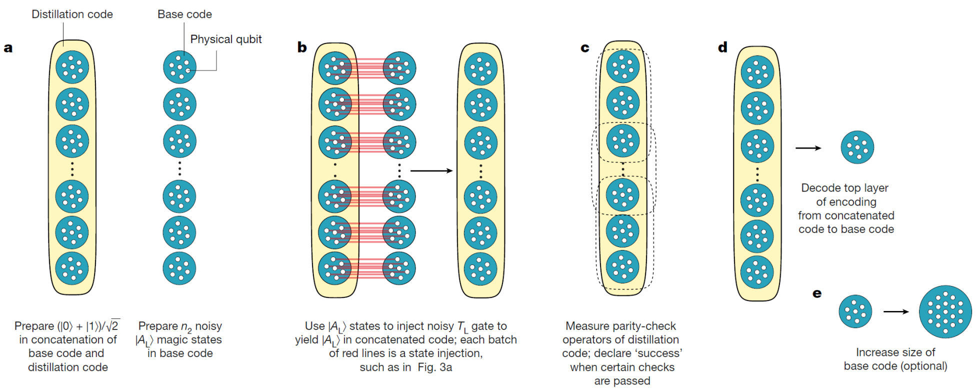
Quantum error correction and fault-tolerant comput.

- Surface codes



E. Dennis et al. “Topological quantum memory”. J. Math. Phys. 43, 4452–4505 (2002)
B. J. Brown et al. “Poking holes and cutting corners to achieve Clifford gates with the surface code”. Phys. Rev. X 7, 021029 (2017)

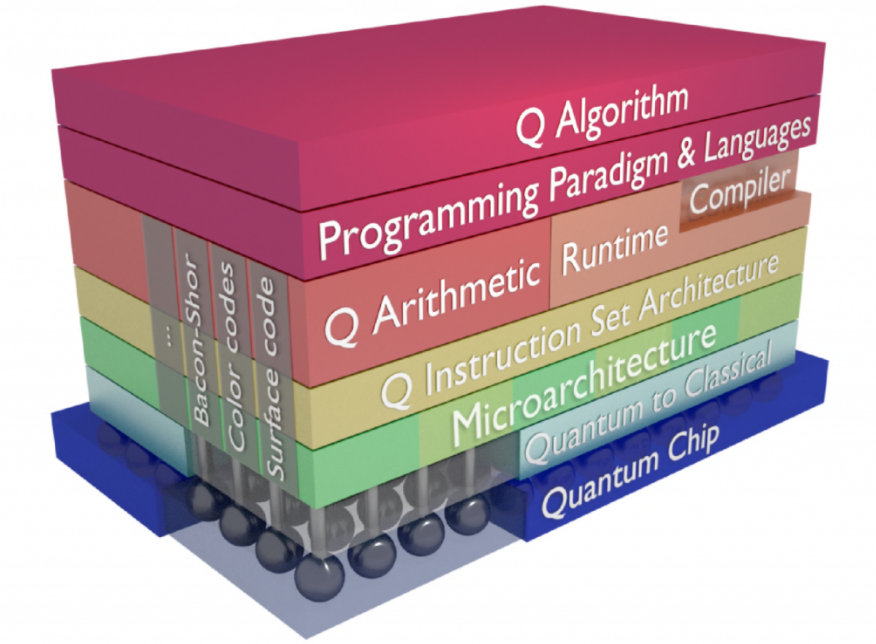
- Magic state distillation



S. Bravyi and A. Kitaev. “Universal quantum computation with ideal Clifford gates and noisy ancillas”. Phys. Rev. A 71, 022316 (2005)

E. Campbell, B. Terhal, C. Vuillot. “Roads towards fault-tolerant universal quantum computation”. Nature 549, 172–179 (2017)
R. Sweke et al. “Reinforcement learning decoders for fault-tolerant quantum computation”. arXiv:1810.07207 (2018)

Quantum software stack



Source: https://qutech.nl/newsroom/events/workshop-quantum-computing/

- Qiskit (IBM)
- Cirq, TensorFlow Quantum (Google)
- ProjectQ (ETH)
- Microsoft Q#
- Silq (silq.ethz.ch)
- Cambridge Quantum Computing
- PennyLane / Strawberry Fields (Xanadu)
- github.com/Qaintum/Qaintessent.jl (TUM)

...

References I

- Arute, F. et al. (2020). "Hartree-Fock on a superconducting qubit quantum computer". In: *arXiv:2004.04174*. URL: https://arxiv.org/abs/2004.04174.
- Biamonte, J. et al. (2017). "Quantum machine learning". In: *Nature* 549, pp. 195–202. DOI: 10.1038/nature23474.
- Bravyi, S. and Kitaev, A. (2005). "Universal quantum computation with ideal Clifford gates and noisy ancillas". In: *Phys. Rev. A* 71, p. 022316. DOI: 10.1103/PhysRevA.71.022316.
- Brown, B. J. et al. (2017). "Poking holes and cutting corners to achieve Clifford gates with the surface code". In: *Phys. Rev. X* 7, p. 021029. DOI: 10.1103/PhysRevX.7.021029.
- Campbell, E., Terhal, B., and Vuillot, C. (2017). "Roads towards fault-tolerant universal quantum computation". In: *Nature* 549, pp. 172–179. DOI: 10.1038/nature23460.
- Chiaro, B. et al. (2019). "Growth and preservation of entanglement in a many-body localized system". In: *arXiv:1910.06024*. URL: https://arxiv.org/abs/1910.06024.
- Dennis, E. et al. (2002). "Topological quantum memory". In: *J. Math. Phys.* 43, pp. 4452–4505. DOI: 10.1063/1.1499754.
- Farhi, E., Goldstone, J., and Gutmann, S. (2014). "A quantum approximate optimization algorithm". In: *arXiv:1411.4028*. URL: https://arxiv.org/abs/1411.4028.
- Gidney, C. and Ekerå, M. (2019). "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits". In: *arXiv:1905.09749*. URL: https://arxiv.org/abs/1905.09749.
- Kandala, A. et al. (2017). "Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets". In: *Nature* 549, pp. 242–246. DOI: 10.1038/nature23879.

References II

- Liu, J.-G. et al. (2019). "Variational quantum eigensolver with fewer qubits". In: *Phys. Rev. Research* 1, p. 023025. DOI: 10.1103/PhysRevResearch.1.023025.
- Moll, N. et al. (2018). "Quantum optimization using variational algorithms on near-term quantum devices". In: *Quantum Sci. Technol.* 3, p. 030503. DOI: 10.1088/2058-9565/aab822.
- Peruzzo, A. et al. (2014). "A variational eigenvalue solver on a photonic quantum processor". In: *Nat. Commun.* 5, p. 4213. DOI: 10.1038/ncomms5213.
- Romero, J., Olson, J. P., and Aspuru-Guzik, A. (2017). "Quantum autoencoders for efficient compression of quantum data". In: *Quantum Sci. Technol.* 2, p. 045001. DOI: 10.1088/2058-9565/aa8072.
- Schuld, M. and Killoran, N. (2019). "Quantum machine learning in feature Hilbert spaces". In: *Phys. Rev. Lett.* 122, p. 040504. DOI: 10.1103/PhysRevLett.122.040504.
- Shor, P. W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134. DOI: 10.1109/sfcs.1994.365700.
- Smith, A. et al. (2019). "Simulating quantum many-body dynamics on a current digital quantum computer". In: *npj Quantum Information* 5, p. 106. DOI: 10.1038/s41534-019-0217-0.
- Sweke, R. et al. (2018). "Reinforcement learning decoders for fault-tolerant quantum computation". In: *arXiv:1810.07207*. URL: https://arxiv.org/abs/1810.07207.