Fachhochschule
Dortmund
University of Applied Sciences and Arts

Quantencomputer

Werkzeuge für die Algorithmenimplementierung

Timo Grautstück

Fachhochschule Dortmund
FB 10: Informationstechnik

30. Mai 2022

Inhalt

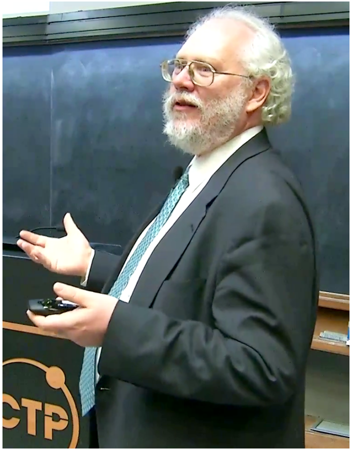
Grundlagen Quantencomputer

Werkzeuge zur Implementierung

Quantenalgorithmen

Warum Quantencomputer?

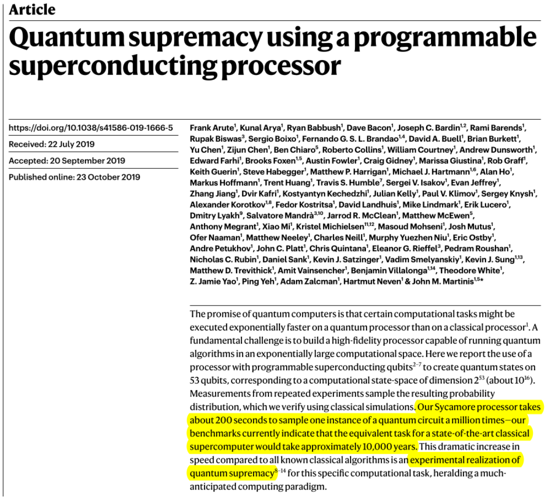
- → Shors Algorihmus: $\mathcal{O}((\log n)^3)$
- → Grover Algorithmus: $\mathcal{O}(\sqrt{N})$
- → Quantenkryptographie: key exchange problem
- → **Quantenüberlegenheit *(Quantum Supremacy)***



Peter Shor 2017

Bildquelle (wikimedia): `https://commons.wikimedia.org/wiki/File:Peter_Shor_2017_Dirac_Medal_Award_Ceremony.png`

Quanten supremacy



Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

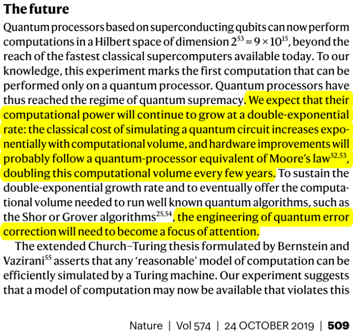
Received: 22 July 2019

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]*

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2–7] to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy[8–14] for this specific computational task, heralding a much-anticipated computing paradigm.



The future

Quantum processors based on superconducting qubits can now perform computations in a Hilbert space of dimension $2^{53} \approx 9 \times 10^{15}$, beyond the reach of the fastest classical supercomputers available today. To our knowledge, this experiment marks the first computation that can be performed only on a quantum processor. Quantum processors have thus reached the regime of quantum supremacy. We expect that their computational power will continue to grow at a double-exponential rate: the classical cost of simulating a quantum circuit increases exponentially with computational volume, and hardware improvements will probably follow a quantum-processor equivalent of Moore's law[52,53], doubling this computational volume every few years. To sustain the double-exponential growth rate and to eventually offer the computational volume needed to run well known quantum algorithms, such as the Shor or Grover algorithms[25,54], the engineering of quantum error correction will need to become a focus of attention.

The extended Church–Turing thesis formulated by Bernstein and Vazirani[55] asserts that any 'reasonable' model of computation can be efficiently simulated by a Turing machine. Our experiment suggests that a model of computation may now be available that violates this

Quantum supremacy using a programmable superconducting processor [1]

Quantenbits I

Basiszustände

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Zweizustandssystem

Kann sich in einer Superposition der Basiszustände befinden:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \qquad \alpha, \beta \in \mathbf{C}$$

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

→ ϕ und θ sind Kugelkoordinaten, der Radius $r = 1$

Quantenbits II

Normalisierung

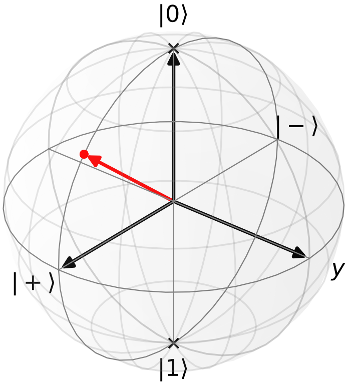
$$\langle\psi|\psi\rangle = 1$$

$$\Rightarrow |\alpha|^2 + |\beta|^2 = 1$$

Beispiel: ϕ=0 und θ=π/2

$$|\psi\rangle = \cos\left(\frac{\pi}{4}\right)|0\rangle + e^{i0}\sin\left(\frac{\pi}{4}\right)|1\rangle$$

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



Bloch-Kugel *(Blochsphere)*

Quantenbits III

Quantenregister

- → n Qubits besitzten 2^n Wahrscheinlichkeitsamplituden

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix}$$

- → Können durch Produkte der Basiszustände beschreiben werden

$$|0\rangle \otimes |0\rangle = |00\rangle = \begin{bmatrix} 1 \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 0 \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Quantengatter I

- → Manipulation von Qubits
- → Quantengatter die auf n Bits operieren sind unitäre $2^n \times 2^n$-Matrizen
- → Für diese Matrizen existieren Eigenvektoren

Unitär

$$\boxed{I = A^\dagger A} \qquad A^\dagger = A^{*T}$$

Eigenvektor & Eigenwert

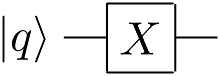
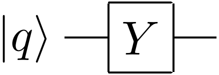
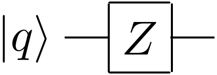
$$A|\psi\rangle = \lambda|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$$

Beispiel: X- & H-Gatter

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

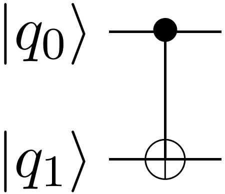
$$H = |0\rangle\langle +| + |1\rangle\langle -| = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Quantengatter II - *(Pauligatter)*

<table>
<tr><th>Matrix</th><th>Schaltungssymbol</th><th>Wahrheitstabelle</th></tr>
<tr><td>$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$</td><td>
</td><td><table><tr><th>Fall</th><th>$|q\rangle$</th><th>$X|q\rangle$</th></tr><tr><td>1</td><td>$|0\rangle$</td><td>$|1\rangle$</td></tr><tr><td>2</td><td>$|1\rangle$</td><td>$|0\rangle$</td></tr></table></td></tr>
<tr><td>$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$</td><td>
</td><td><table><tr><th>Fall</th><th>$|q\rangle$</th><th>$Y|q\rangle$</th></tr><tr><td>1</td><td>$|0\rangle$</td><td>$i|1\rangle$</td></tr><tr><td>2</td><td>$|1\rangle$</td><td>$-i|0\rangle$</td></tr></table></td></tr>
<tr><td>$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$</td><td>
</td><td><table><tr><th>Fall</th><th>$|q\rangle$</th><th>$Z|q\rangle$</th></tr><tr><td>1</td><td>$|0\rangle$</td><td>$|0\rangle$</td></tr><tr><td>2</td><td>$|1\rangle$</td><td>$-|1\rangle$</td></tr></table></td></tr>
</table>

Quantengatter III - *(kontrollierte Gatter)*

- → Alle Gatter können kontrolliert auf n Qubits angewandt werden
- → Ein Zielqubit und $n-1$ kontrollierende Qubits
- → Um eine Transformation auf einem Zielbit auszuführen, müssen sich alle kontrollierenden Bits im Zustand $|1\rangle$ befinden

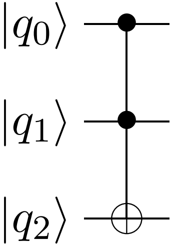


Kontrolliertes-Nicht-Gatter

Beispiel: CNOT

$$CX_{01} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

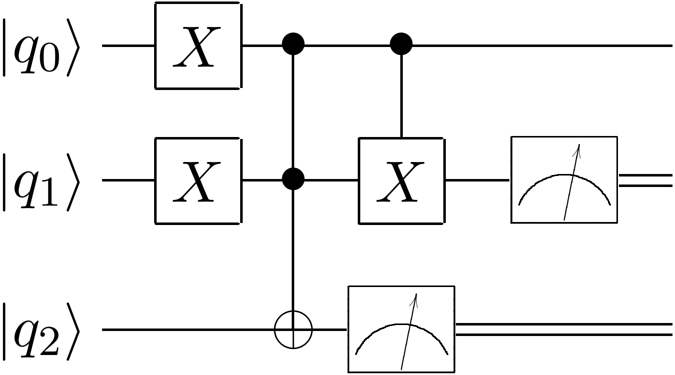
Quantengatter IV - *(Toffoli-Gate)*

<table>
<tr><th>Matrix</th><th>Schaltungssymbol</th><th>Wahrheitstabelle</th></tr>
<tr>
<td>$CCX_{012} = \begin{bmatrix} I_2 & 0_2 & 0_2 & 0_2 \\ 0_2 & I_2 & 0_2 & 0_2 \\ 0_2 & 0_2 & I_2 & 0_2 \\ 0_2 & 0_2 & 0_2 & X \end{bmatrix}$</td>
<td>
</td>
<td>
<table>
<tr><th>Fall</th><th>$\lvert q_0q_1q_2\rangle$</th><th>$CCX_{012}\lvert q_0q_1q_2\rangle$</th></tr>
<tr><td>1</td><td>$\lvert 000\rangle$</td><td>$\lvert 000\rangle$</td></tr>
<tr><td>2</td><td>$\lvert 001\rangle$</td><td>$\lvert 001\rangle$</td></tr>
<tr><td>3</td><td>$\lvert 010\rangle$</td><td>$\lvert 010\rangle$</td></tr>
<tr><td>4</td><td>$\lvert 011\rangle$</td><td>$\lvert 011\rangle$</td></tr>
<tr><td>5</td><td>$\lvert 100\rangle$</td><td>$\lvert 100\rangle$</td></tr>
<tr><td>6</td><td>$\lvert 101\rangle$</td><td>$\lvert 101\rangle$</td></tr>
<tr><td>7</td><td>$\lvert 110\rangle$</td><td>$\lvert 111\rangle$</td></tr>
<tr><td>8</td><td>$\lvert 111\rangle$</td><td>$\lvert 110\rangle$</td></tr>
</table>
</td>
</tr>
</table>

Toffoli-Gatter

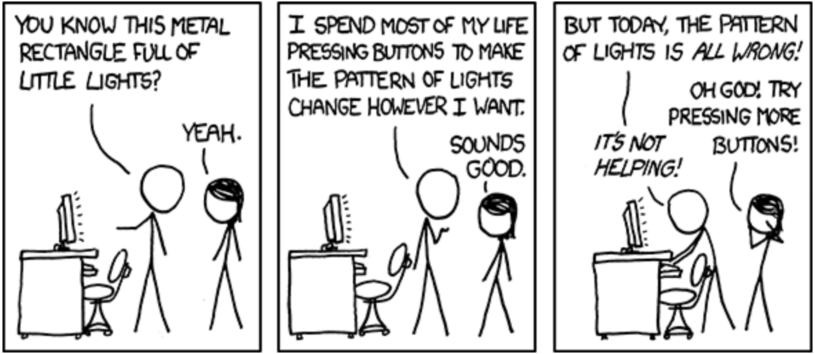
Quantenschaltungen

- → Grundlage für Quantenalgorithmen
- → Keine Rückführungen (azyklisch)
- → Kopieren und Zusammenführen von Qubits nicht erlaubt



Quantenschaltung für einen Halbaddierer

Frametitle II


YOU KNOW THIS METAL RECTANGLE FULL OF LITTLE LIGHTS?
YEAH.
I SPEND MOST OF MY LIFE PRESSING BUTTONS TO MAKE THE PATTERN OF LIGHTS CHANGE HOWEVER I WANT.
SOUNDS GOOD.
BUT TODAY, THE PATTERN OF LIGHTS IS ALL WRONG!
OH GOD! TRY PRESSING MORE BUTTONS!
IT'S NOT HELPING!

Your text here …

Your text here ...

The End

Thank you for your attention, are there any questions?

Literaturverzeichnis I

F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, and R. Barends, “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, pp. 505–510, Oct 2019.