

MIT QUANTEN KANN MAN RECHNEN



- bit ↔ qubit
- neue Algorithmen
- experimentelle Umsetzung





bit 0, 1

Informationsträger: Lichtpuls, Strom, Spannung, Ladung, Magnetisierung....



stetige Steigerung der Rechenleistung durch fortschreitende Miniaturisierung









Informationsverarbeitung: konventionell – mit Quanten



bit 0, 1 Informationsträger : Lichtpuls, Strom, Spannung, Ladung ...



Miniaturisierung

→ Quanteneffekte vermeiden ? VERWENDEN!

qubit $|\Psi\rangle = a_0 |0\rangle + a_1 |1\rangle$ Informationsträger: Photonen, Atome, Elektronen,...

- Superposition
 Unschärfeprinzip
 Zufallszahlen
 Quantenkryptographie
- Verschränkung
 Quantenteleportaation
 Quantencomputer



bit ↔ qubit



 bit 0, 1 zwei möglicher Werte

- qubit $|0\rangle$, $|1\rangle$
- beliebige Superpositionen der beiden Zustände

 $|\Psi\rangle = a_0|0\rangle + a_1|1\rangle$



XP bit → qubit Informationsträger

" <mark>0</mark> "	"1"	bit
	\leq	CD:
no bump	bump	pattern
		Pixel
white	black	brightness
1		hard disk
Ν	S	magnetic orientation
		TTL-signals
0V	5V	voltage level
\bigcirc		high speed glass fiber connection
off	on	light
	+	RAM-memory
not charged	charged	charge of capacitance

"0" "1"	qubit				
↑ ↔	photon:				
	linear				
	polarization				
\cap \cap	superconducting current:				
L angle R angle	orientation				
$ +\frac{1}{2}\hbar\rangle -\frac{1}{2}\hbar\rangle$	electron, neutron, atomic nucleus:				
	5pm				
g>	atom, ion: <i>internal stat</i> es				
	quantum dots:				
	energy levels				
$ a\rangle$ $ b\rangle$ $ a'\rangle$ $ b'\rangle$	any particle: directions at beam splitter				



bit 0, 1
 zwei möglicher Werte

• strings 0, 1, 1, 0

- Berechnung irreversibel (reversibel ↔ Permutation)
- Ergebnis auslesen "r"

- qubit $|0\rangle, |1\rangle$ • beliebige Superpositionen der beiden Zustände $|\Psi\rangle = a_0 |0\rangle + a_1 |1\rangle$
- qubit strings $|0,1,1,0\rangle$ in beliebiger Superposition $|\Psi\rangle = \sum_{i=0...00,...,1.11} a_i |i\rangle$
- Berechnung reversibel $|\Psi\rangle \xrightarrow{\text{calculation}} \mathcal{U}|\Psi\rangle$

Quantenparallelismus

 Messung "r" → ein Resultat ein einziges !?!





- QC kann die Komplexität eines Problems reduzieren
 - Komplexität bezüglich Zahl der Operationen, Speicherbedarf (abhängig von Zahl der Eingabestellen)

■ z.B.:	Summe	11+23=?	O(n)
	Produkt	11*23=?	0(n ²)
	Faktorisieren	253=a*b	O(exp(n ^{1/3}))

- Vorteil, wenn gemeinsame Eigenschaften der Resultate gesucht sind
 - (z.B. Eigenschaft, Parameter einer Funktion)
 - → Faktorisierung, (Suche)

→ nutze Quantenparallelismus !

Reviews zu Quantenalgorithmen:

A. Ekert, R. Jozsa, RMP 68, 733 (1996), A. Montanaro, NPJ Quantum Information 2, 15023 (2015) M-H Yung et. al, arXiv:1203.1331 (Adv. Chem. Phys. 157, 67 (2014))



• genügt für alle n-qubit gates !



Algorithmen





- are the two sides of a coin equal ?
- i.e., determine, whether function is constant or balanced

$$\begin{array}{ccccccc} f_1(0) = 0 & f_2(0) = 1 & f_3(0) = 0 & f_4(0) = 1 \\ f_1(1) = 0 & f_2(1) = 1 & f_3(1) = 1 & f_4(0) = 0 \\ & & \text{constant} & & \text{balanced} \end{array}$$

• classical solution: calculate function 2x

Deutsch-Josza, quantum solution



- use two qubits, initially in state |0,1
 angle
- define function: $U_f | x, y \rangle = | x, y \oplus f(x) \rangle$
- apply Hadamard on both: $|\psi_1\rangle = \mathbf{H}_a \mathbf{H}_b |0,1\rangle = \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle) = \frac{1}{2} (|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle)$



$$|1\rangle$$
—H—

Deutsch-Josza, quantum solution



- use two qubits, initially in state |0,1
 angle
- define function: $U_f | x, y \rangle = | x, y \oplus f(x) \rangle$
- apply Hadamard on both: $|\psi_1\rangle = \mathbf{H}_a \mathbf{H}_b |0,1\rangle = \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle) = \frac{1}{2} (|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle)$
- evaluate function $|\psi_2\rangle = \mathbf{U}_f |\psi_1\rangle = \frac{1}{2} (|0, f(0)\rangle + |0, f(1)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$



Deutsch-Josza, quantum solution



- use two qubits, initially in state $|0,1\rangle$
- define function: $U_f | x, y \rangle = | x, y \oplus f(x) \rangle$
- apply Hadamard on both: $|\psi_1\rangle = \mathbf{H}_a \mathbf{H}_b |0,1\rangle = \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle) = \frac{1}{2} (|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle)$
- evaluate function $|\psi_2\rangle = \mathbf{U}_f |\psi_1\rangle = \frac{1}{2} (|0, f(0)\rangle + |0, f(1)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$
- two cases: constant f(1) = f(0) $|\psi_2\rangle = \frac{1}{2} (|0, f(0)\rangle + |0, f(0)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(0)\rangle) =$ $= \frac{1}{2} (|0\rangle + |1\rangle) (|f(0)\rangle - |1 \oplus f(0)\rangle)$





- evaluate function $|\psi_2\rangle = \mathbf{U}_f |\psi_1\rangle = \frac{1}{2} (|0, f(0)\rangle + |0, f(1)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$
- two cases: constant f(1) = f(0) $|\psi_2\rangle = \frac{1}{2} (|0, f(0)\rangle + |0, f(0)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(0)\rangle) =$ $= \frac{1}{2} (|0\rangle + |1\rangle) (|f(0)\rangle - |1 \oplus f(0)\rangle)$

■ balanced $f(1)=1\oplus f(0)$ $|\psi_2\rangle = \frac{1}{2}(|0,f(0)\rangle + |1,1\oplus f(0)\rangle - |0,1\oplus f(0)\rangle - |1,f(0)\rangle) =$ $= \frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$ → to measure first qubit solves the question

p search algorithm (Grover)



- unsorted database "oracle" $f(x_s) = 1$ (if x_s solution), f(x) = 0 otherwise
- manipulate amplitude of all possible data-elements (a_i), such that the correct one dominates at a certain time
- 1. prepare superposition of all elements $|\psi_{1}\rangle = \mathbf{H}^{\otimes n} |00...0\rangle = N^{-1/2} \sum_{x=0..N-1} |x\rangle \qquad (N = 2^{n})$ 2. apply oracle $\mathbf{I}_{x_{s}}$: $\mathbf{U}_{f(x)} |x\rangle = (-1)^{f(x)} |x\rangle$ 3. apply inversion around the average $|\psi'\rangle = \mathbf{H}^{\otimes n} \mathbf{I}_{0} \mathbf{H}^{\otimes n} |\psi\rangle$ $\mathbf{I}_{0} |x\rangle = -(-1)^{\delta_{0,x}} |x\rangle$ • repeat 2.,3.,

$$|\psi_k\rangle = \left(\mathbf{H}^{\otimes n}\mathbf{I}_0\mathbf{H}^{\otimes n}\mathbf{O}\right)^k |\psi_1\rangle = \cos\frac{2k+1}{2}\theta |x_s\rangle + \sin\frac{2k+1}{2}\theta |x_{others}\rangle$$

• stop after about $\frac{\pi}{4}\sqrt{N}$ iterations with $|\psi_1\rangle = \cos\frac{\theta}{2}|x_s\rangle + \sin\frac{\theta}{2}|x_{others}\rangle$, if only 1 solution





- difficult problem, best known classical algorithm O(exp(n^{1/3}))
- fact that factorization is difficult, is used to warrant security of public-key encryption
- a (not very fast) factoring algorithm:
 - choose y, coprime with N; evaluate $F_N(a) = y^a \mod N$
 - find period r of $F_N(a) \Rightarrow y' \equiv 1 \mod N$

 $(y^{r} = kN + 1 \Longrightarrow y^{r+1} = kNy + y \Longrightarrow$ $\Rightarrow y^{r+1} \mod N = y \mod N \Longrightarrow r \text{ period of } F_{N})$

- if r even, set $x = y^{r/2} \Rightarrow x^2 \equiv 1 \mod N \Rightarrow$ $\Rightarrow x^2 - 1 = (x - 1)(x + 1) \equiv 0 \mod N$
- x 1 or x + 1 cannot be multiples of N, thus they must have a common factor

 $\Rightarrow p,q = gcd(x \pm 1,N)$ are factors of N

- all tasks can be calculated efficiently except finding the period F_N
 - ⇒ Shor: use quantum Fourier transform



- use quantum parallelism to calculate $F_N(a)$ for many a
- use Fourier transform to calculate period r
 - two registers: source register with K qubits, where $N^2 \leq Q = 2^K \leq 2N^2$ target register with $L \ge \log_2 N$

 - 1. initialize: $|\psi_1\rangle = H^{\otimes K} |0\rangle |0\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0..Q-1} |q\rangle |0\rangle$ 2. calculate $F_N(q)$: $|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0..Q-1} |q\rangle |y^q \mod N\rangle$ all values are calculated in parallel and available for the next step
 - 3. measure target register, suppose result Z, where $z = y' \mod N$. Since $y' \equiv y'' \mod N$ source register is in state

$$|\phi_l\rangle = \frac{1}{\sqrt{A+1}} \sum_{j=0..A} |jr+l\rangle$$

measurement gives one value of kr+l, but, I random, different in every run, not useful.



4. Fourier transform to extract $r: \mathbf{U}_{F_q}: |q\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{q'=0..Q-1} \exp\left(2\pi i \frac{q'q}{Q}\right) |q'\rangle$

$$\Rightarrow \left|\phi_{l}'\right\rangle = \frac{1}{\sqrt{Q(A+1)}} \sum_{q'=0..Q-1} \sum_{j=1..A} \exp\left(2\pi i \frac{q'(jr+l)}{Q}\right) \left|q'\right\rangle = \frac{1}{\sqrt{Q(A+1)}} \sum_{q'=0..Q-1} \exp\left(2\pi i \frac{q'l}{Q}\right) \sum_{\substack{Q/r \text{ for } q' \text{ multiple of } Q/r; 0 \text{ otherwise}}} \left|q'\right\rangle$$

$$U_{F_{Q}}\left|\phi_{I}\right\rangle = \frac{1}{\sqrt{r}}\sum_{j=0..r-1}\exp\left(2\pi i\frac{Ij}{r}\right)\left|j\frac{Q}{r}\right\rangle$$

- 5. measure source register, result $\lambda Q/r$, independent of *I*
- 6. repeat 1...5, several values of $\lambda_i Q/r \rightarrow$ determine r



example: factor N=15

• choose y, coprime with N, e.g. y=7, evaluate $F_{N_f}(a) = 4 \Longrightarrow x = 7^2 = 49$

а	1	2	3	4	5	6	7
$F_N(a)$	7	4	13	1	7	4	13

$$p = \gcd(49 - 1, N) = 3$$

 $q = \gcd(49 + 1, N) = 5$

• quantum Fourier transform to find *r*:



initialize, evaluate $F_N(a)$

measure 2^{nd} register, superposition in 1^{st} register random shift by I_i

QFT, measure first register \Rightarrow period $Q/r \Rightarrow r$



example: factor N=15

• choose y, coprime with N, e.g. y=7, evaluate $F_{N_f}(a) = 4 \Longrightarrow x = 7^2 = 49$

а	1	2	3	4	5	6	7
$F_N(a)$	7	4	13	1	7	4	13

$$p = \gcd(49 - 1, N) = 3$$

 $q = \gcd(49 + 1, N) = 5$

• quantum Fourier transform to find *r*:



initialize, evaluate
$$F_N(a)$$

 $F_N(q): |\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0..Q-1} |q\rangle |y^q \mod N\rangle$

measure 2^{nd} register, superposition in 1^{st} register random shift by I_i

 $\left|\phi_{I}\right\rangle = \frac{1}{\sqrt{A+1}} \sum_{j=0..A} \left|jr+I\right\rangle$

QFT, measure first register \Rightarrow period $Q/r \Rightarrow r$





Feynman:

- Ein Quantensystem auf einem Computer zu simulieren ist exponentiell aufwändig
- Ein Quantensystem evolviert in Echtzeit, d.h., es kann sich selbst in Echtzeit simulieren
- Kann diese Quantensystem derart manipuiert werden, dass es ein anderes Quantensystem (in Echtzeit) simuliert?





- Digitale Quantensimulation
 - Evolution durch Hamiltonoperator bestimmt

$$H = T + V$$

• T und V gleichzeitig in Ort/Impulsbasis diagonalisieren



effizient – Aufwand polynomial





- Analoge Quantensimulation
 - Kopplung der qubits (atome, Xmon, …) entspricht der Kopplung von Spins o. Elektronen in Festkörper o. Molekülen, in Gittermodel für Feldtheorie, etc.
 - gleiche Geometrie (aber nicht notwendig)
 - verfolge direkte Evolution
 - manipuliere Parameter (Gitterkonstante, Kopplungen etc.)
- Adiabatische Optimierung
 - suche Lösung bei geg. Randbedingungen
 - beginne bei bekanntem H variiere H "langsam", sodass RB abgebildet werden – Grundzustand von H ist Lösung.



Umsetzung

Anforderungen für "qubit" in experimenteller Umsetzung



- qubits
- Initialisierung
- Quantengatter

- Auslesen
- (De-) Kohärenz

- definiere 2 unterscheidbare Zustände
- Möglichkeit, die qubits (auf 0) zu setzen
- Operationen zur Erzeugung verschränkter Zustände (starke Kopplung notwendig)
 - Messung einzelner qubits nach Operation
- renz Zeit während der Quanteneigenschaften überwiegen muss ausreichend lang sein



- nuclear magnetic resonance
- spin ¹/₂ ¹H,¹³C,¹⁵N,¹⁹F,²⁹Si

 $\Delta E = \mu \cdot \hbar B_0$ liquids – individual processors (weak coupling: $2\pi J_{ij} << |\omega_i - \omega_j|$):









• pseudo-pure states

$$\rho \approx \frac{1}{2^n} (1 - \varepsilon) \cdot \underline{1} + \varepsilon \prod_i |\psi\rangle_i \langle \psi|_i$$



• CNOT-gate



refocussing







- nuclear magnetic resonance
- factorize 15



- 7 qubits
- 11.4T, 470MHz (¹⁹F) und 125MHz (¹³C)
- ~300 pulses, 720ms total time
 L. M. K. Vandersypen, et al., Nature 414, 883 (2001).









Solid state NMR – quantum computer

- NMR in semiconductors
- single Phosphor atoms
- coupling controlled via gate voltages
- P-P: 10-20nm



 manipulate e- wavefunction with A gates



 couple qubits via J-gates: SWAPgate





CP trapped ions

- ions trapped by rf-fields
- linear trap (ω_{ax} ~0.7-2Mhz. ω_{rad} ~5MHz)
- effective two level system









control bit

- motional states of the ion chain in harmonic potential
- \Rightarrow qubit states "dressed" with motional states
- possible also for distant ions:
- state of the atom can be transferred to the motional state of the chain and back
- phase shift on a single ion, depending on its ion-phonon state (CPhase)
- transfer state of first ion back to the ion



→perform CNOT operation for the two ions



interaction with laser light depends also on the motional state of atoms



14 ion GHZ-state lacksquare

TABLE I. Populations, coherence, and fidelity with a N-qubit GHZ state of experimentally prepared states. Entanglement criteria supported by σ standard deviations. All errors in parenthesis, 1 standard deviation.

Number of ions	2	3	4	5	6	8	10	12	14
Populations, %	99.50(7)	97.6(2)	97.5(2)	96.0(4)	91.6(4)	84.7(4)	67.0(8)	53.3(9)	56.2(11)
Coherence, %	97.8(3)	96.5(6)	93.9(5)	92.9(8)	86.8(8)	78.7(7)	58.2(9)	41.6(10)	45.4(13)
Fidelity, %	98.6(2)	97.0(3)	95.7(3)	94.4(5)	89.2(4)	81.7(4)	62.6(6)	47.4(7)	50.8(9)
Distillability criterion [14], σ	283	151	181	100	95	96	40	18	17
Entanglement criterion [15], σ	265	143	167	101	96	92	25	-6	0.7





T. Monz et al., PRL 106, 130506 (2011)





- atoms trapped in optical lattice
- first Bose-Einstein condensate to ensure high density



ramp up opical lattice to transfer atoms







 $\pi/2$

φ

 $\pi/2$

neutral atoms

- atoms can be moved, when shifti the standing light fields
- phase shift for (s-wave) scattering of atoms
- state dependent traps
- →state dependent phase shift
- →between all neighbouring atoms entangle more than 10 atoms
- individual readout difficult
- → "cluster-state" one-way quantum computing

time i+2 i+1 Lattice Site 0.6 0.5 0.4 Visibility 0.3 0.2 0.1

100

0

200

300

Hold time (us)

400

500



• read out via single atom imaging



Atoms in 2D optical lattice

Quantum Simulation: Spin Transport in Heisenberg Quantum Magnets



- $\hat{H} = -J_{ex} \sum_{i} \left[\frac{1}{2} (\hat{S}_{i}^{+} \hat{S}_{i+1}^{-} + \hat{S}_{i}^{-} \hat{S}_{i+1}^{+}) + \Delta \hat{S}_{i}^{z} \hat{S}_{i+1}^{z} \right]$ study change of spin orientation for J>0
 - initalize atoms from BEC in 2D lattice in ground state
 - π/2 pulse + field gradient to generate spin-spiral
 - evolution for varying J
 - single-site read out
 + correlation analysis
 - observe decay of correlations between spins



Superconducting qubits

- superconducting qubits
- quantized current/charge in loop with Josephson-junctions: qubits demonstrated ("entanglement")
- anharmonisches Potential Übergänge mit unterschiedlicher Frequenz
 adressierbar







 coupling of sc-qubits via µ-wave resonators





3 qubit experiments, 2 CPhase operations





M. Baur et al., PRL **108**, 040502 (2012)



quantum gates at fault tollerant threshold





- D-Wave
 - adiabatic solver
- Google



- supraleitende qubits, playground, Al
- NASA
 - QuAIL mit D-Wave Rechner
- Microsoft
 - Quantum Architectures and Computation (QArC)
 - Anwendungen in Chemie (Fe₂S₂)
- NTT, IBM
 - superconducting qubit architectures

• Quantenparallelismus $|\Psi\rangle = a_0 |0\rangle + a_1 |1\rangle$

Zusammenfassung

- Neue Algorithmen
 - Faktorisieren
 - Quantensimulation
- Quantengatter durch Wechselwirkung

 $|\Psi\rangle$ \longrightarrow $U|\Psi\rangle$

- Algorithmen mit wenigen qubits
- Unterschiedliche experimentelle Umsetzungen





