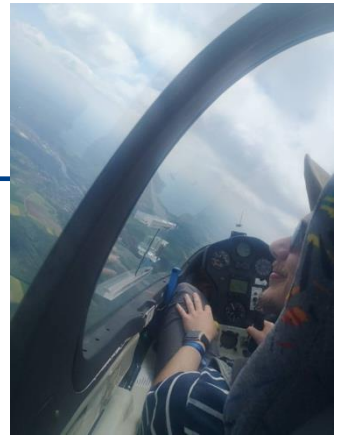
Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Was können Quantencomputer?

Yorick Reum

Offenes Informatik-Kolloquium
Mittwoch, 3. Juli 2024

Über mich



Theorie

B.Sc. in Physik und B.Sc. in Informatik

Bachelorarbeit in Kooperation
Theoretische Physik 3 + Lehrstuhl X

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

M.Sc. in Physik

Auslandsjahr: TEXAS The University of Texas at Austin

Quanteninformation bei
Prof. Dr. Scott Aaronson

Masterarbeit: *Design of Circular Bragg Grating Resonators for Quantum Dot Cluster State Sources in the Telecom C-Band*

PhotonQ
Technische Physik
Universität Würzburg

Praxis

aktuell:
Promotion zu neuartigen Quantenlichtquellen
bei Dr. Andreas Pfenning

Roadmap

Theorie

Praxis

Klassische und quantenmechanische Berechenbarkeit
→ (quanten-)erweiterte Church-Turing These
→ Quanten-Komplexitätstheorie

Informatik & Physik

Die Zutaten: Superposition und Verschränkung
→ Deutsch‘ Problem
→ Bellsche Ungleichung

Quantum 101 & Algorithmen

Physikalische Realisierung
→ DiVincenzo‘s Kriterien
→ Supraleitende und photonische Qubits

Hardware

Disclaimer

Es ist spät – ich habe trotzdem Formeln und Theoreme in den Slides.

Keine Sorge: Wir machen das nicht rigoros.

→ Ich erlaube mir Unsauberkeiten, normalisiere nicht, etc., …

Die erweiterte Church-Turing These

Informatik & Physik

Informatische Formulierung		Physikalische Formulierung	Wir vermuten…
intuitiv berechenbar = auf Turing-Maschine berechenbar	→	jeder physikalische Prozess = auf Turing-Maschine mit beliebiger Genauigkeit simulierbar	✓ klassisch ✓ quantum
+ *Laufzeitunterschied zwischen verschiedenen Berechnungsmodellen maximal polynomiell.*	+	*Beim Simulieren höchstens polynomielle Vergrößerung von Zeit, Raum, anderen Rechenressourcen.*	✓ klassisch ✗ quantum

Was verbindet die Mathematik mit der Realität?
→ Nicht die Physik, sondern die Informatik – durch die Church-Turing These.

[Deutsch David. 1985. Quantum theory, the Church–Turing principle and the universal quantum computer. Proc. R. Soc. Lond. doi.org/10.1098/rspa.1985.0070]

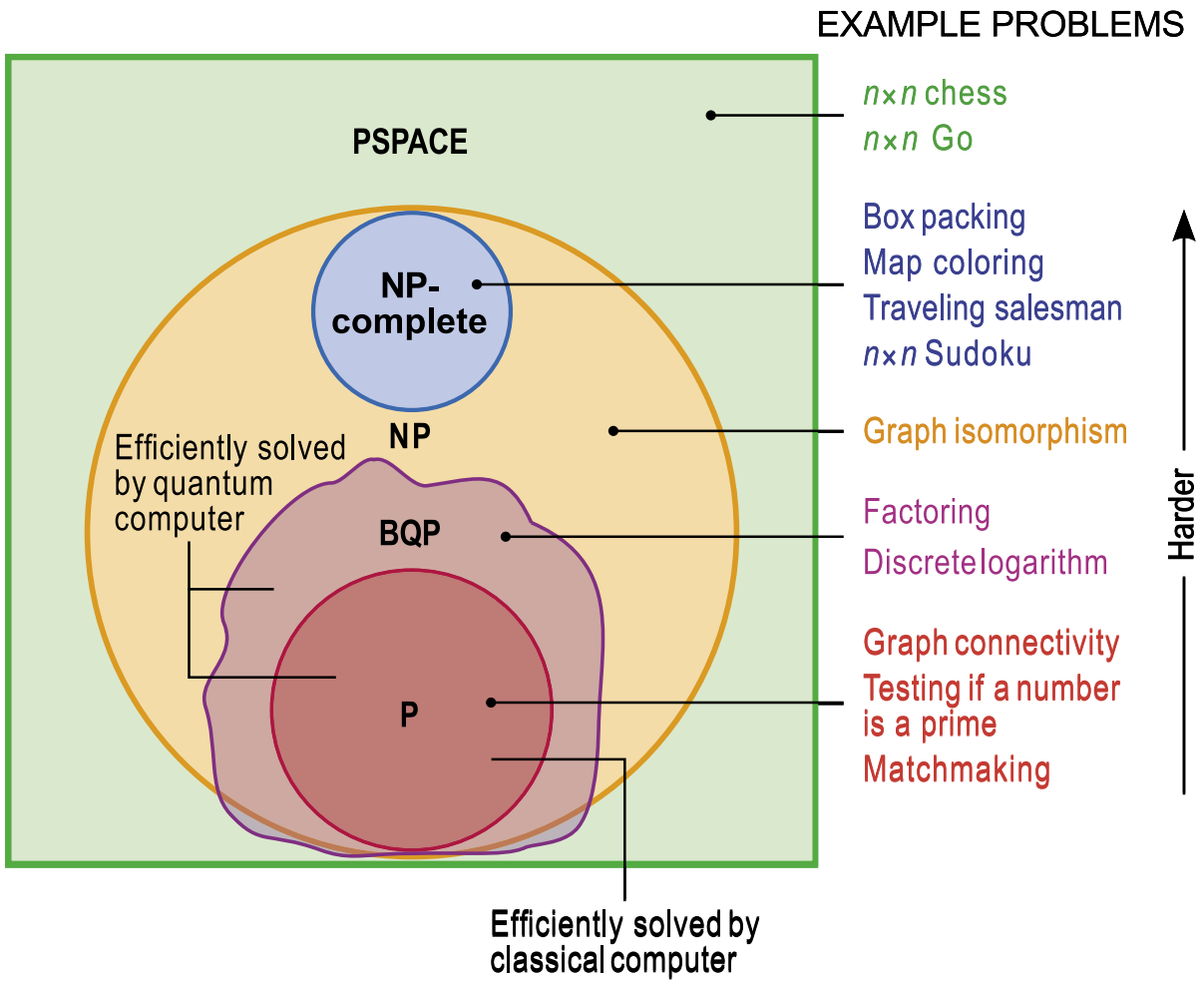
Die Ursprünge

Richard Feynman, 1982
Vorlesung über die Simulation von quantenmechanischen Systemen
(Moleküle, Festkörper, Chemie, …)

> ***Nature isn't classical, dammit***, *and* ***if you want to make a simulation of nature, you'd better make it quantum mechanical***, *and by golly it's a wonderful problem, because it doesn't look so easy.*
>
> – Richard Feynman, 1982

(Quanten-)Komplexität: BQP & NP

Informatik & Physik



[The Limits of Quantum, Scott Aaronson, Scientific American, 2008]

BQP

=

Bounded-Error Quantum Polynomial-Time

$BQP \subseteq PP$

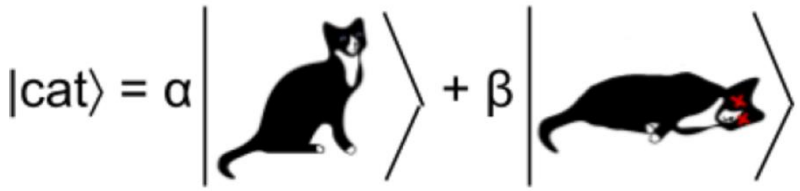
[L. Adleman, J. DeMarrais, M. Huang. Quantum computability. 1997]

Quantum 101

**Was hat die Quantenmechanik anzubieten,
das uns schneller rechnen lässt?**

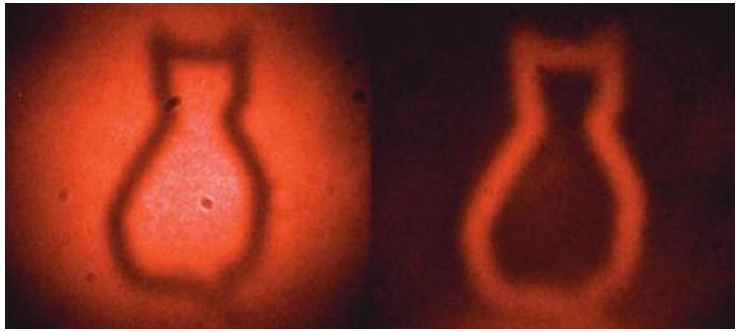
Die Zutaten

Superposition



[Perry, Anastasia, et al. "Quantum computing as a high school module." *arXiv preprint arXiv:1905.00282* (2019).]

Verschränkung



Lemos, Gabriela Barreto, et al. "Quantum imaging with undetected photons." Nature 512.7515 (2014): 409-412.

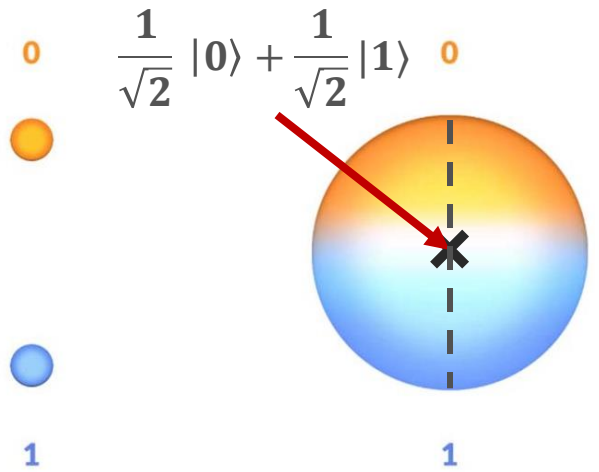
Quantenzustände und Wellenfunktionen

Von Bits und Quantenbits (Qubits).

Zwei Level, $|0\rangle$ oder $|1\rangle$.

Nur nicht binär, nicht entweder-oder.

Sondern Überlagerung: $\alpha\,|0\rangle + \beta\,|1\rangle$



Aber nach Messung trotzdem nur eins von beiden!

Wir messen das Level $|0\rangle$ mit der Wahrscheinlichkeit $|\alpha|^2$,
das Level $|1\rangle$ mit der Wahrscheinlichkeit $|\beta|^2$.

(Born‘sche Regel)

Amplituden und Wahrscheinlichkeiten

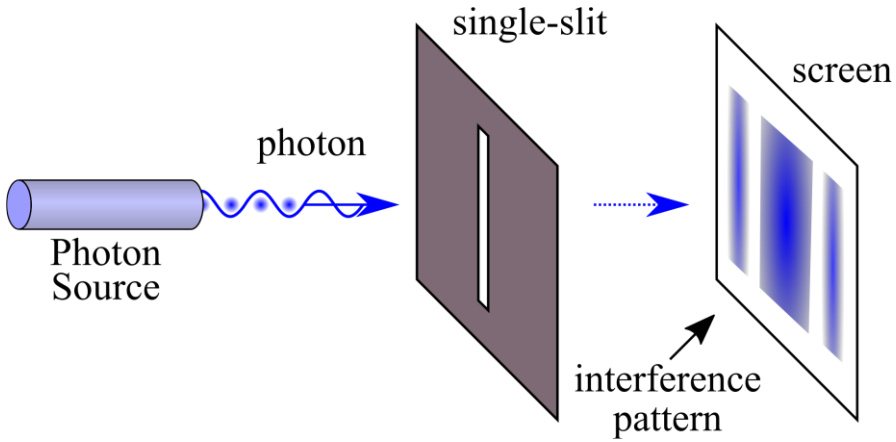
Wellenfunktion eines Qubits: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.

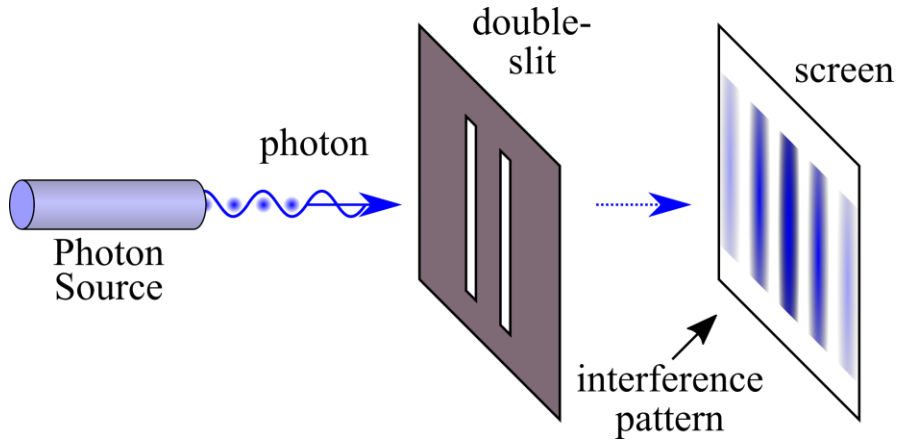
Also ist ein Qubit nur ein zufälliges Bit?

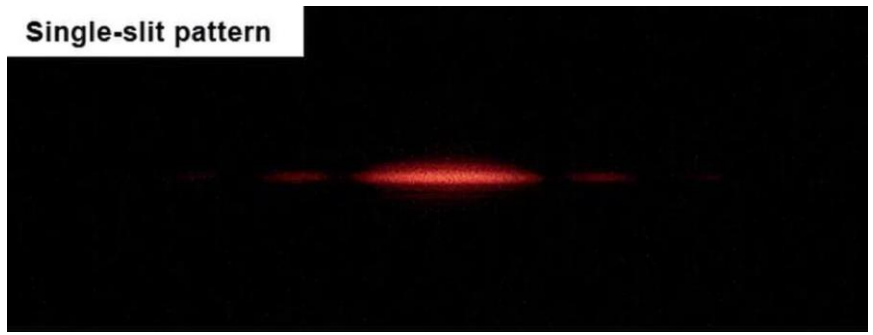
Nein. Die Amplituden $\alpha, \beta \in \mathbb{C}$ können negativ sein!

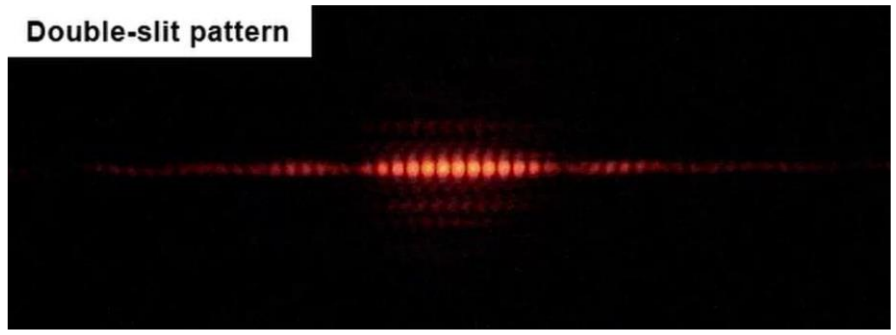
Superposition in Aktion – am Doppelspalt

Amplituden sind mehr als nur Wahrscheinlichkeiten.





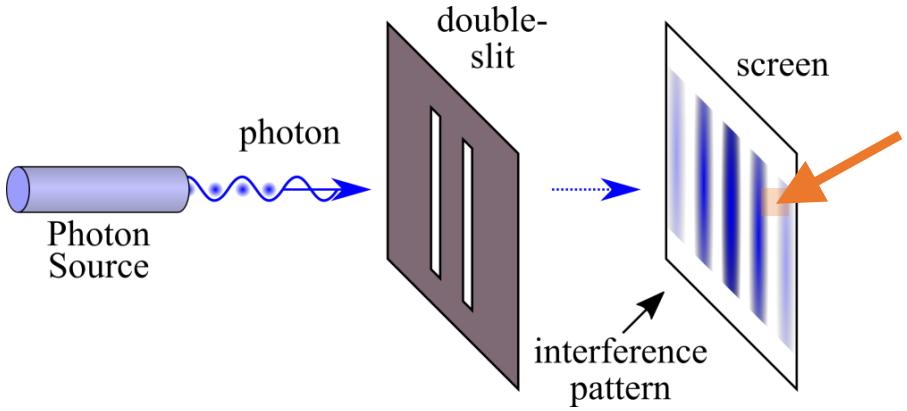


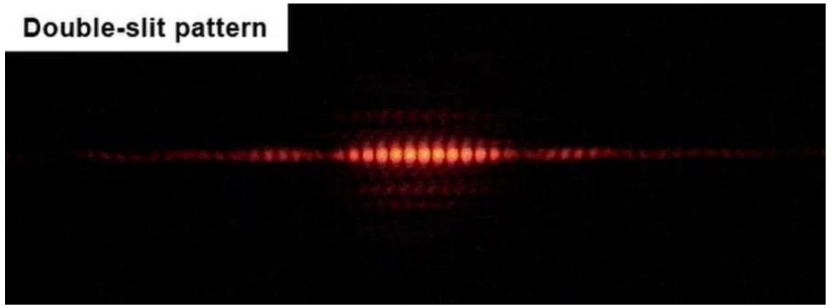


Superposition in Aktion – am Doppelspalt

Amplituden sind mehr als nur Wahrscheinlichkeiten.

> The weirdness isn't that "God plays dice," but rather that "these aren't normal dice"!
> – *Scott Aaronson*





Klassisch

P_1: Wahrscheinlichkeit für Photon hier wenn Spalt 1 offen
P_2: Wahrscheinlichkeit für Photon hier wenn Spalt 2 offen

→ Wahrscheinlichkeit für Photon hier $P = P_1 + P_2$.
→ Nur 0 wenn P_1 und $P_2 = 0$.

Quantenmechanisch

α: Amplitude für Photon hier wenn Spalt 1 offen.
β: Amplitude für Photon hier wenn Spalt 2 offen.

→ Wahrscheinlichkeit für Photon hier $P = |\alpha + \beta|^2$.
→ **Auch 0 wenn $\boldsymbol{\beta = -\alpha}$!**

$$|\text{Photon hier}\rangle = \alpha\ |\ \text{Spalt 1 offen}\rangle + \beta\ |\text{Spalt 2 offen}\rangle + \gamma\ |\text{kein Spalt offen}\ \rangle$$

Nochmal, aber (natur-)philosophisch

fünften Solvay-Konferenz
im Jahr 1927 in Brüssel

Nochmal, aber (natur-)philosophisch

Die **Wahrscheinlichkeitsfunktion** vereinigt objektive und subjektive Elemente.

Sie enthält **Aussagen über Wahrscheinlichkeiten oder besser Tendenzen** (Potentia in der aristotelischen Philosophie), und **diese Aussagen sind völlig objektiv**, sie hängen nicht von irgendeinem Beobachter ab.

Außerdem enthält sie Aussagen über unsere Kenntnis des Systems, die natürlich subjektiv sein müssen, insofern sie ja für verschiedene Beobachter verschieden sein können.

In besonders günstigen Fällen kann das subjektive Element in der Wahrscheinlichkeitsfunktion gegenüber dem objektiven Element ganz vernachlässigt werden. Die Physiker sprechen dann von einem *reinen Fall*.

– Die Kopenhagener Deutung der Quantentheorie (Werner Heisenberg, 1958)

Quantenzustände und Information

Die Amplituden $\alpha, \beta \in \mathbb{C}$ haben beliebig viele Nachkommastellen.

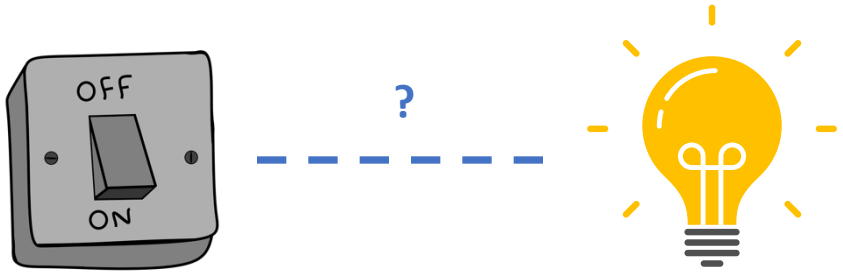
→ Einzelnes Qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ enthält unendlich viel Information.

Aber nicht auslesbar.

Eine Messung des Qubits gibt uns nur einmal $|0\rangle$ oder $|1\rangle$.

Superposition als Rechenressource

Das Problem von David Deutsch.



Klassischer Algorithmus: Für beide Positionen des Schalters prüfen, ob die Glühbirne an ist. Zwei Abfragen.

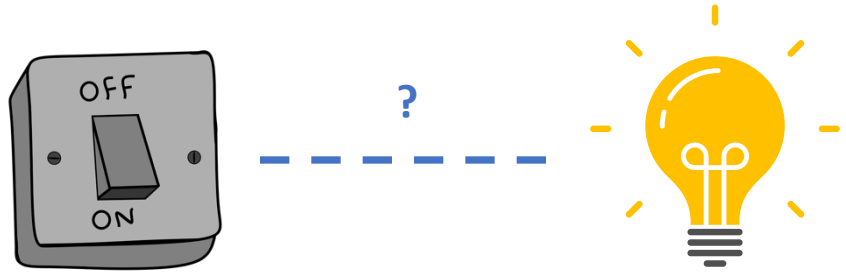
Glühbirne in Abhängigkeit von Schalter $f: \{0,1\} \rightarrow \{0,1\}$

Prüfen: $f(0) \neq f(1)$ → verbunden
$f(0) = f(1)$ → nicht verbunden

[Deutsch David. 1985. Quantum theory, the Church–Turing principle and the universal quantum computer. Proc. R. Soc. Lond. doi.org/10.1098/rspa.1985.0070]

Superposition als Rechenressource

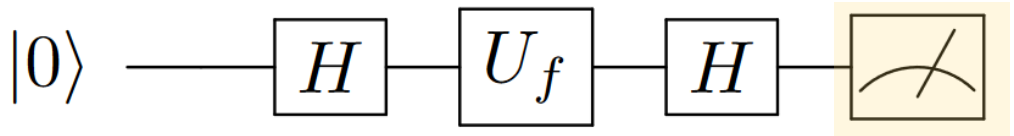
Das Problem von David Deutsch.



Quanten-Algorithmus: Für beide Positionen des Schalters **gleichzeitig** prüfen, ob die Glühbirne an ist. **Eine Abfrage.**

$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle = \begin{cases} |0\rangle + |1\rangle \text{ falls } f(0) = f(1) \\ |0\rangle - |1\rangle \text{ falls } f(0) \neq f(1) \end{cases}$$

$|0\rangle + |1\rangle$ erzeugt faire Superposition



Messergebnis:

$$f(0) = f(1) \Longrightarrow |0\rangle$$
$$f(0) \neq f(1) \Longrightarrow |1\rangle$$

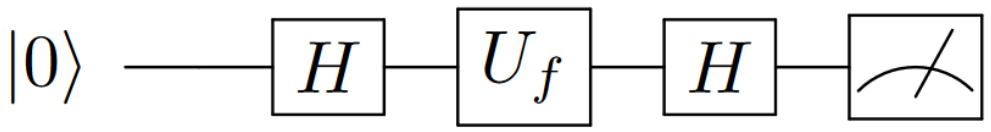
[Deutsch David. 1985. Quantum theory, the Church–Turing principle and the universal quantum computer. Proc. R. Soc. Lond. doi.org/10.1098/rspa.1985.0070]

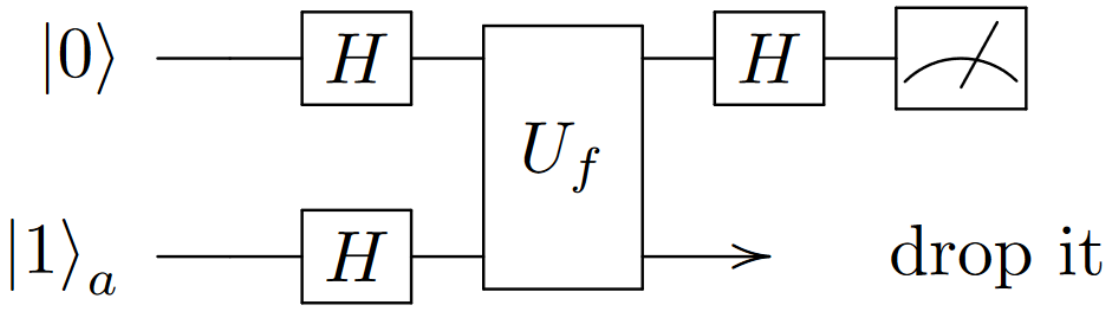
Deutsch‘s Problem & Reversibilität

In der Quantenmechanik ist alles (außer Messungen) reversibel.
Quantencomputer sind reversible Computer.

nur konzeptionell richtig!

Problem: verlieren Information → nicht reversibel





Deutsch‘s Problem mit Photonen

Photonisches Qubit, nutzen zum Beispiel

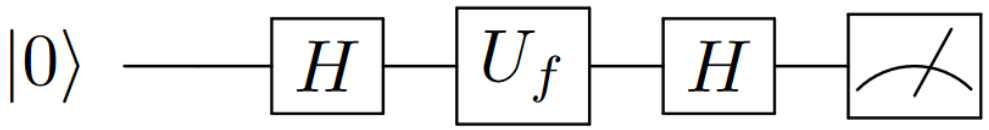
Pfad zu Kodierung

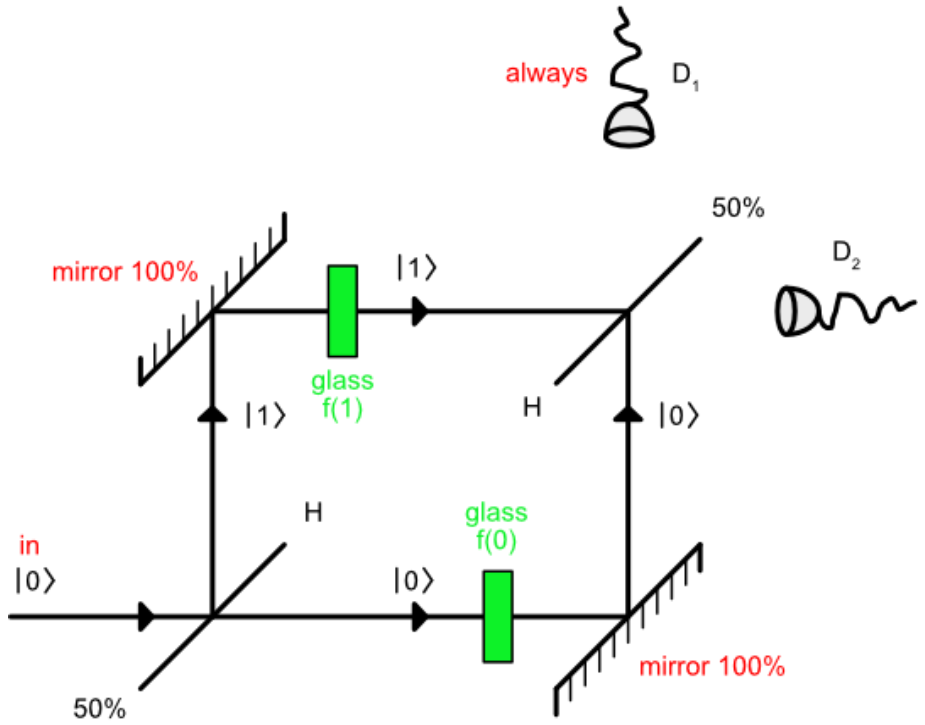
$|0\rangle$ = |Photon da⟩ $|1\rangle$ = |kein Photon da⟩

oder

Polarisationsrichtung zur Kodierung (= Spin-Achse des Photons)

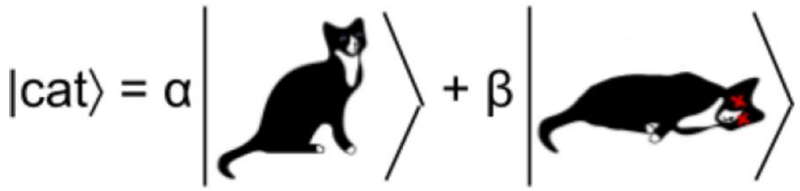
$|0\rangle = |\leftrightarrow\rangle$ $|1\rangle = |\updownarrow\rangle$





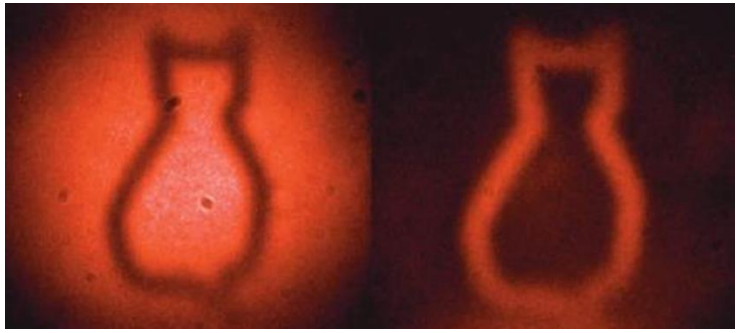
Die Zutaten

Superposition



[Perry, Anastasia, et al. "Quantum computing as a high school module." *arXiv preprint arXiv:1905.00282* (2019).]

Verschränkung



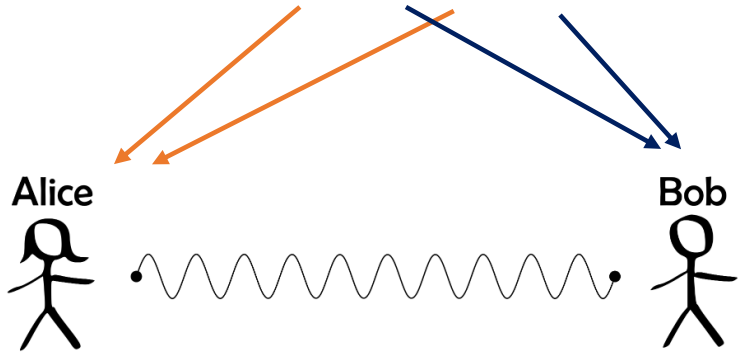
Lemos, Gabriela Barreto, et al. "Quantum imaging with undetected photons." Nature 512.7515 (2014): 409-412.

Verschränkung und Kommunikation

Was ist Verschränkung?
→ „spukhafte Fernwirkung“ (Albert Einstein)
→ Korrelation, über das klassische Maß hinaus

Ein Qubit: $|0\rangle + |1\rangle$

Zwei Qubits: $|0\rangle|0\rangle + |1\rangle|1\rangle$ (maximal verschränkter Zustand = 1 ebit)



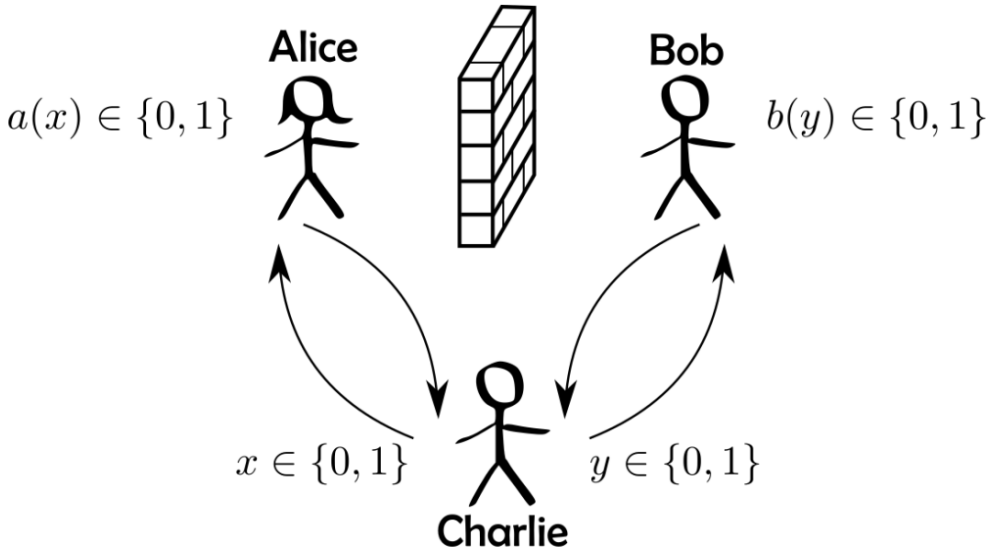
Alice misst. Sie erhält zufällig $|0\rangle$ oder $|1\rangle$.
Sagen wir, sie misst $|0\rangle$. Die Qubits kollabieren zu $|0\rangle|0\rangle$.
→ Anschließend wird Bob auch zwingend $|0\rangle$ messen!

Heißt das, wir können Informationen schneller als Lichtgeschwindigkeit übermitteln?
→ Nein, wir haben keinen Einfluss auf das Messergebnis.

No-Communication-Theorem
Messungen an einem quantenmechanischen Teilsystem können nicht benutzt werden können, um Informationen zu einem anderen Teilsystem zu übertragen.
[M. J. W. Hall, u.a. /Giancarlo Ghirardi u. a., 1988]

Verschränkung als Rechenressource

Das CHSH-Spiel (Bell‘s Ungleichung).



Ablauf

1. Alice und Bob einigen sich auf eine Strategie.
2. A & B dürfen ab nur noch zufällige Bits kommunizieren.
3. A & B kriegen jeweils ein zufälliges Bit von Charlie, x und y.

Ziel

Alice und Bob wollen Bits a und b ausgeben,
sodass $a + b = x \cdot y \pmod 2$.

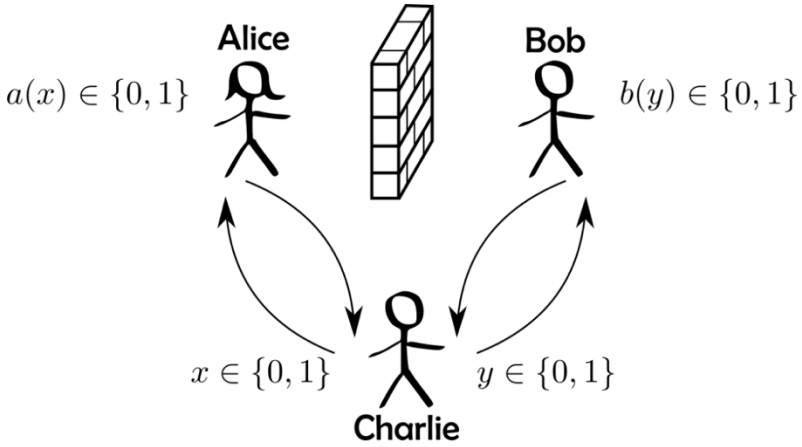
Eine (optimale) klassische Strategie

Alice und Bob wählen immer $a = b = 0$. Sie gewinnen dann 75 % der Spiele.

[www.scottaaronson.com/qclec.pdf, Vorlesungen 13 und 14]

Verschränkung als Rechenressource

Das CHSH-Spiel (Bell‘s Ungleichung).



A & B teilen sich nun verschränkte Qubits $|0\rangle|0\rangle + |1\rangle|1\rangle$.

Eine (optimale) Quanten-Strategie
Je nachdem, was x (y) ist, dreht Alice (Bob) an den Amplituden ihres Qubits.
Dann miss jeder und wählt a (b) je nach Messergebnis.

Wenn sie clever drehen, gewinnen sie $\cos(\pi/8)^2 \approx 85\ \%$ der Spiele!

Ohne dabei kommuniziert zu haben.

Diese Verletzung der *Bell‘schen Ungleichung* wurde experimentell nachgewiesen (Nobelpreis für Physik 2022).

[www.scottaaronson.com/qclec.pdf, Vorlesungen 13 und 14]

Lokalität und Realismus

real = Messergebnisse sind auch ohne Messung bereits definiert

lokal = Information wird maximal mit Lichtgeschwindigkeit transportiert

Jede klassische Theorie ist lokal und real. → Jede klassische Theorie erfüllt Bellsche Ungleichung.

Aus der experimentellen Verletzung von Bellsche Ungleichung wissen wir, **dass die Realität nicht real-lokal ist.**

→ Keine „verborgenen lokale Variablen“, etc., Messergebnisse sind wirklich zufällig, …

We live in a world where there’s no classical local realism, but no faster-than-light communication either.
Or, to put it another way, a **purely classical simulation of our universe would have to include faster-than-light communication, but our universe itself does not**.
– Scott Aaronson

Superdense Coding

Man kann Qubits verschicken (z.B. Photonen über Glasfaser-Kabel).

Wie viel Information kann dabei transportiert werden?

Ohne Verschränkung: 1 bit pro qubit (Holevo’s Theorem)

Mit 1 ebit Verschränkung: 2 bits pro qubit

Noch mehr Qubits?

Die Anzahl der Amplituden wächst exponentiell mit der Anzahl der Qubits.

2 Qubits: $\alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle + \gamma|1\rangle|0\rangle + \delta\ |1\rangle|1\rangle$

3 Qubits: $\alpha_1|0\rangle|0\rangle|0\rangle + \alpha_2|0\rangle|1\rangle|0\rangle + \alpha_3|1\rangle|0\rangle|0\rangle + \alpha_4|1\rangle|1\rangle|0\rangle +$
$\alpha_5|0\rangle|0\rangle|0\rangle + \alpha_6|0\rangle|1\rangle|0\rangle + \alpha_7|1\rangle|0\rangle|0\rangle + \alpha_8|1\rangle|1\rangle|0\rangle$

…

Um n verschränkte Qubits auf einem klassischen Computer zu simulieren, muss 2^n-dimensionaler Vektor verwaltet werden.

Ohne Verschränkung reichen $2n$ Dimensionen.

$(\alpha_0|0\rangle + \beta_0|1\rangle)(\alpha_1|0\rangle + \beta_1|1\rangle) \cdots (\alpha_{n-1}|0\rangle + \beta_{n-1}|1\rangle)$

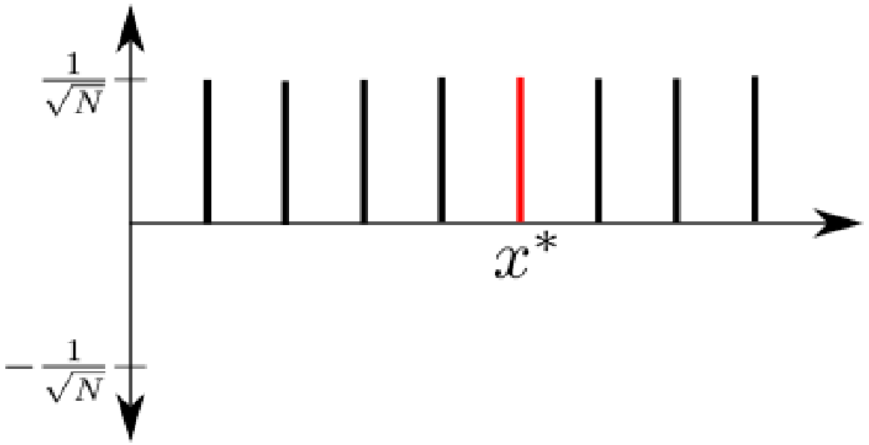
Grovers Algorithmus: Suchen in unsortierter Liste

Ziel: Wir durchsuchen einen n-bit-string nach einer 1.

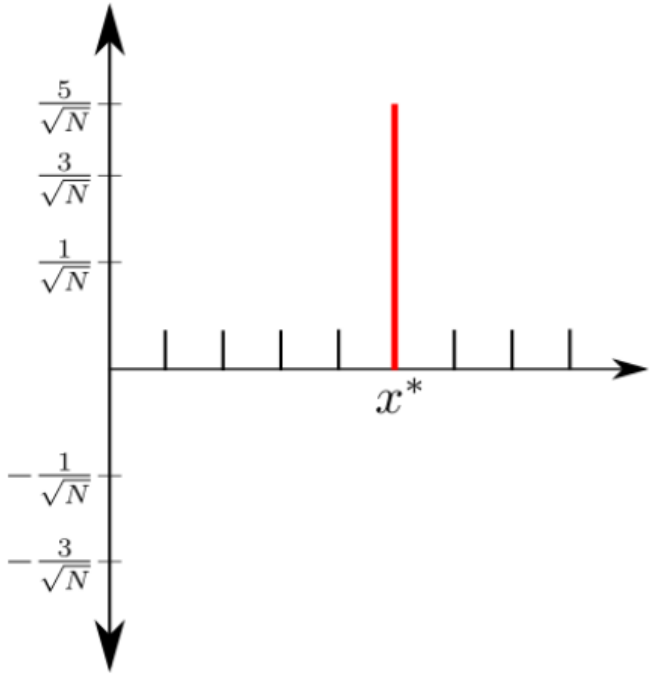
Mit Formeln: Finde x^* sodass $f(x^*) = 1$.

Klassisch: Lineare Suche ist optimal, $\mathrm{O}(n)$ Rechenschritte.

Quantenmechanisch: $\mathrm{O}(\sqrt{n})$ Schritte genügen!



$$U_f|x\rangle = \left((-1)^{f(x)}|x\right\rangle$$



Shor‘s Algorithmus – ganz grob

Faktorisierung ist reduzierbar zu Periodenfindung,

2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, … mod 15

2, 4, 8, 1, 2, 4, 8, 1, 2, 4, … → period 4

dafür Quanten Fourier-Transformation ausnutzbar

… die über Superposition effizient Amplituden Fourier transformiert.

Und noch einige Details.

Experimentelle Quantenüberlegenheit

- Zurzeit: Supremacy durch Sampling
- Stichprobenprobleme, statt Entscheidungsprobleme (SampBQP statt BQP)
  - *Ziel: einen n-bit String aus einer Wahrscheinlichkeitsverteilung ziehen, die klassisch hart zu erzeugen wäre*

- Benötigt keinen universellen Quantencomputer

- Photonisch: BosonSampling
- Supraleitend: Quantum (Pseudo-)Random Circuits

Anforderungen zur Implementierung von Quantencomputern

Wir brauchen

Experimentellen Zugang zu quantenmechanischen Eigenschaften

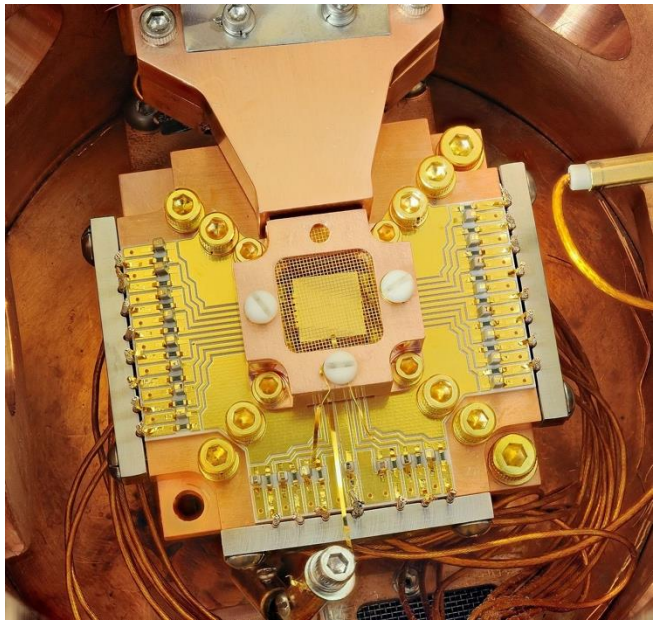
David DiVincenzo‘s Kriterien

- Skalierbares physikalisches System mit gut charakterisierten Qubits
- Initialisierbarkeit der Qubits
- Universeller Satz von Quantengattern
- Lange Kohärenzzeiten (länger als die Gatterzeiten)
- Fähigkeit, Qubit-spezifische Messungen durchzuführen

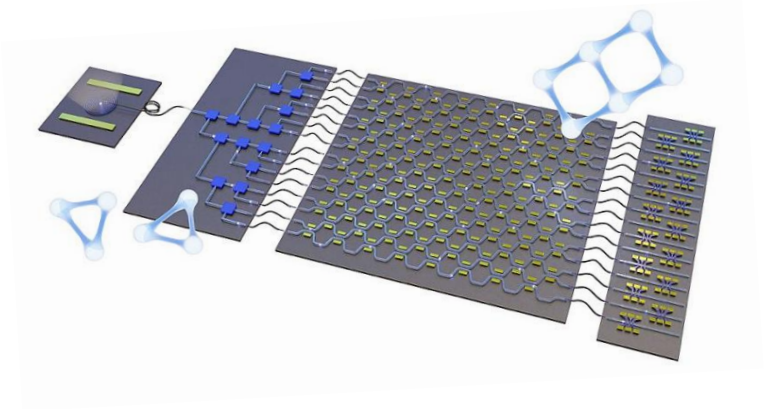
[DiVincenzo. "The physical implementation of quantum computation." Fortschritte der Physik: Progress of Physics 48.9-11 (2000): 771-783.]

Verschiedene Plattformen

Supraleitend



Ionenfallen



Photonisch

Und einige mehr…

Code your own supraleitende Qubits

Hardware

- IBM Qiskit (github.com/Qiskit)

Qiskit

- Python-API für Quanten-Schaltkreise
  - könnt ihr auf realen superconducting transmon qubits laufen lassen (IBM Quantum Platform)
  - oder simulieren (genauso schnell und rauschfrei…)

IBMs Q System One

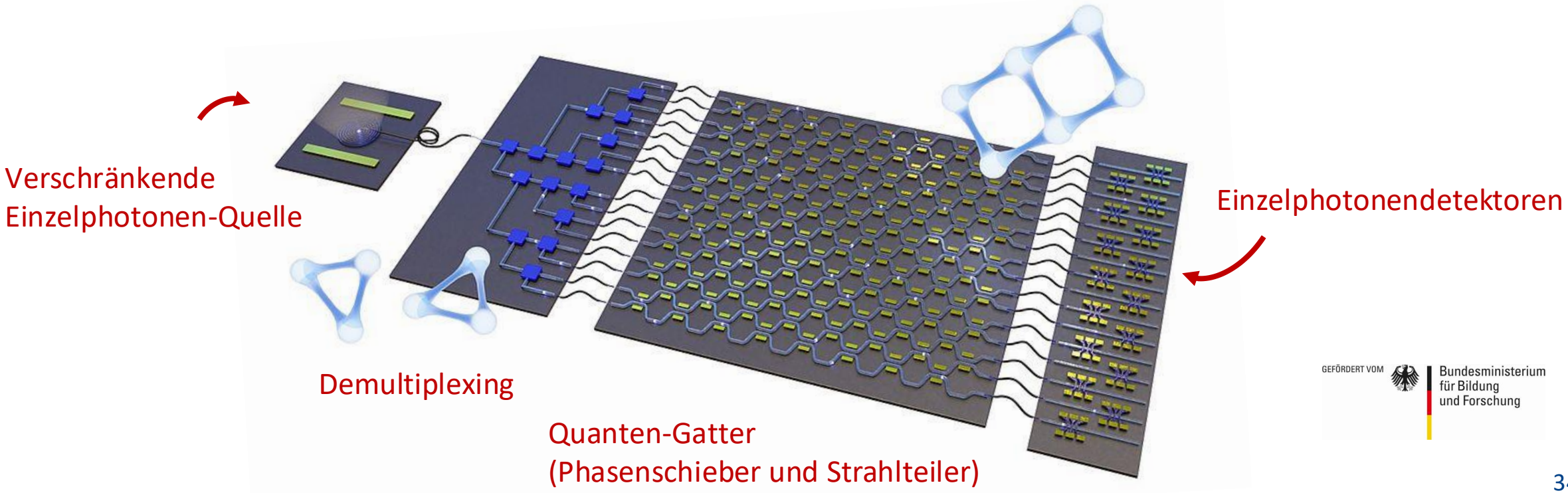
Photonischer Quantenprozessor

Hardware

→ www.photonq.de

PhotonQ baut einen photonischen Quantenprozessor.

Durch den Einsatz hochgradig verschränkter photonischer Zustände und adaptiver Messungen lässt sich universelles Quantencomputing realisieren.



GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

Post-Pizza-Botschaft

Quantenmechanik kann helfen, (sehr) besondere Aufgaben
bis zu exponentiell schneller zu lösen.

Viele NP-Problem (wahrscheinlich) trotzdem nicht effizient berechenbar.

(Keine magische Parallelisierung.)

Aktuell viel Engineering zu tun.

Und jetzt nochmal genau, bitte!

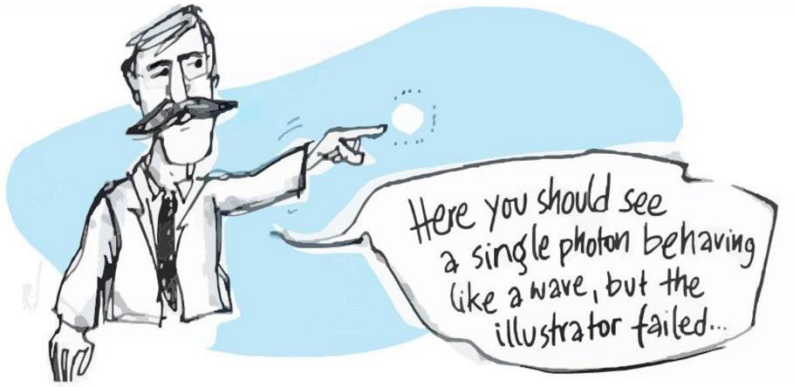
- Scott‘s Vorlesungsskripte: scottaaronson.com/qclec.pdf & qisii.pdf
- Scott‘s Blog: scottaaronson.blog
- Quantenheorie & Philosophie (Werner Heisenberg)
- …

Vorlesungen:

- Bachelor Physik: *Theo. Quantencomputer und Quanteninformation*
- Master Physik: *Exp. Quantencomputer und Quanteninformation*
- Master Informatik: *Quantum Communications* (Prof. Dr. Guido Dietl)

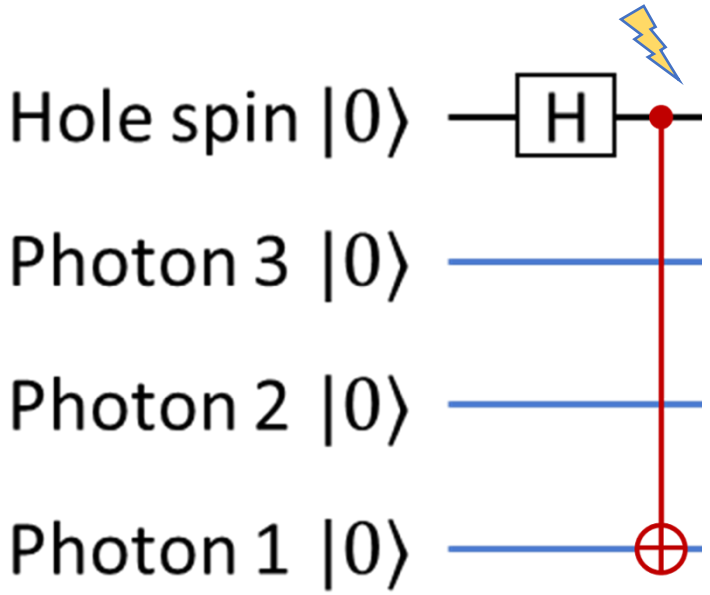
Danke für die Aufmerksamkeit!

Noch Fragen?



ZEISS Symposium Optics in the Quantum World, 2018

Photonic Cluster States from QDs



Superposition

Entanglement

$$|\Uparrow\Downarrow\uparrow\rangle + |\Uparrow\Downarrow\downarrow\rangle \rightarrow |\Uparrow, L\rangle + |\Downarrow, R\rangle$$

…and again…

$$\rightarrow |\Uparrow\rangle|L\rangle|L\rangle + |\Downarrow\rangle|R\rangle|L\rangle + \ldots$$

PRL 103, 113602 (2009) PHYSICAL REVIEW LETTERS week ending 11 SEPTEMBER 2009

Proposal for Pulsed On-Demand Sources of Photonic Cluster State Strings

Netanel H. Lindner[1] and Terry Rudolph[2,3]

[1]Department of Physics, Technion-Israel Institute of Technology, 32000 Haifa, Israel
[2]Optics Section, Blackett Laboratory, Imperial College London, London SW7 2BZ, United Kingdom
[3]Institute for Mathematical Sciences, Imperial College London, London SW7 2BW, United Kingdom

(Received 22 October 2008; revised manuscript received 8 March 2009; published 8 September 2009)

We present a method to convert certain single photon sources into devices capable of emitting large strings of photonic cluster state in a controlled and pulsed "on-demand" manner. Such sources would greatly reduce the resources required to achieve linear optical quantum computation. Standard spin errors, known to affect only 1 or 2 of the emitted photons at a time. This allows for the use that the photonic machine gun can be fired for arbitrarily we conclude high entangled-quantum dot

RESEARCH

RESEARCH ARTICLE

QUANTUM PHYSICS

Deterministic generation of a cluster state of entangled photons

I. Schwartz,[1*] D. Cogan,[1*] E. R. Schmidgall,[1,2] Y. Don,[1] L. Gantz,[1] O. Kenneth,[1] N. H. Lindner,[1] D. Gershoni[1†]

Photonic cluster states are a resource for quantum computation based solely on single-photon measurements. We use semiconductor quantum dots to deterministically generate long strings of polarization-entangled photons in a cluster state by periodic timed excitation of a precessing matter qubit. In each period, an entangled photon is added to the cluster state formed by the matter qubit and the previously emitted photons. In our prototype device, the qubit is the confined dark exciton, and it produces strings of hundreds of photons in which the entanglement persists over five sequential photons. The measured process map characterizing the device has a fidelity of 0.81 with that of an ideal device. Further feasible improvements of this device may reduce the resources

energy splitting $\Delta\varepsilon_2$ corresponding to a precession period of $T_{DE} = h/\Delta\varepsilon_2 \simeq 3$ nsec (27, 28). In addition to the DE, our experiment uses two states of a biexciton (BiE)—a bound state of two excitons—whose total spin projections on $\hat{z}$ are either +3 or −3, with a precession period of $T_{BIE} = h/\Delta\varepsilon_3 \simeq 5$ nsec. We denote these states by $|\pm 3\rangle$. The experimental protocol relies on the optical transition rules $|+2\rangle \leftrightarrow |+3\rangle$ and $|-2\rangle \leftrightarrow |-3\rangle$ through right $|R\rangle$ and left $|L\rangle$ hand circularly polarized photons, respectively (27, 28), in direct analogy with the original proposal (22). The energy-level diagram describing the DE, the BiE, and the optical transition rules is schematically summarized in Fig. 1C.

An ideal protocol for cluster-state generation

Before the protocol begins, the DE is deterministically initialized in its higher-energy spin eigenstate $|\psi_{DE}^{init}\rangle = |-X\rangle$ (31) by a short π-area picosecond pulse (29). A π-area pulse transfers the entire population from one quantum state to another.

The protocol, which begins immediately after the initialization, consists of repeated applications of a cycle. The cycle contains three elements: (i) a converting laser π-pulse, resonantly tuned to the DE-BiE optical transition. The pulse