Qubits und Co: Erste Schritte zum Quantum Computing

Matthias Homeister, THB

Security-Forum, 19.1.2023

Eine allgemeinverständliche Einführung…

24. Oktober 2019, Adrian Kreye in der SZ:

- eine gesellschaftliche Debatte über Chancen und Risiken des Quantum Computing
- jenseits von „halbinformierter Angst“ und „blinder Fortschrittsbegeisterung“
- Schwierigkeit der Thematik

Erste Leitfrage dieser Präsentation:

Werden Quantencomputer unsere *klassischen* Computer ablösen?

Klassische Berechnungen

Ein Beispiel…

$$\begin{array}{r} 117 \\ +114 \\ \hline 231 \end{array}$$

$$\begin{array}{r} 10 \\ +\ 11 \\ \hline 101 \end{array}$$

0 = 0

1 = 1

10 = 2

11 = 3

100 = 4

101 = 5

Vom Bit zum Qubit

Ein *klassisches* Bit nimmt die Zustände 0 und 1 an.

Ein Quantenbit kann auch im Zustand

$$0{,}6\,|0> + 0{,}8\,|1>$$

sein.

Superposition der klassischen Zustände 0 und 1.

Wollen wir das Qubit auslesen wird die Superposition zerstört.

Mit Wahrscheinlichkeit 0,36 erhalten wir |0>, mit der Wahrscheinlichkeit 0,64 das Messergebnis |1>.

Weitere Beispiele

Weitere Beispiele:

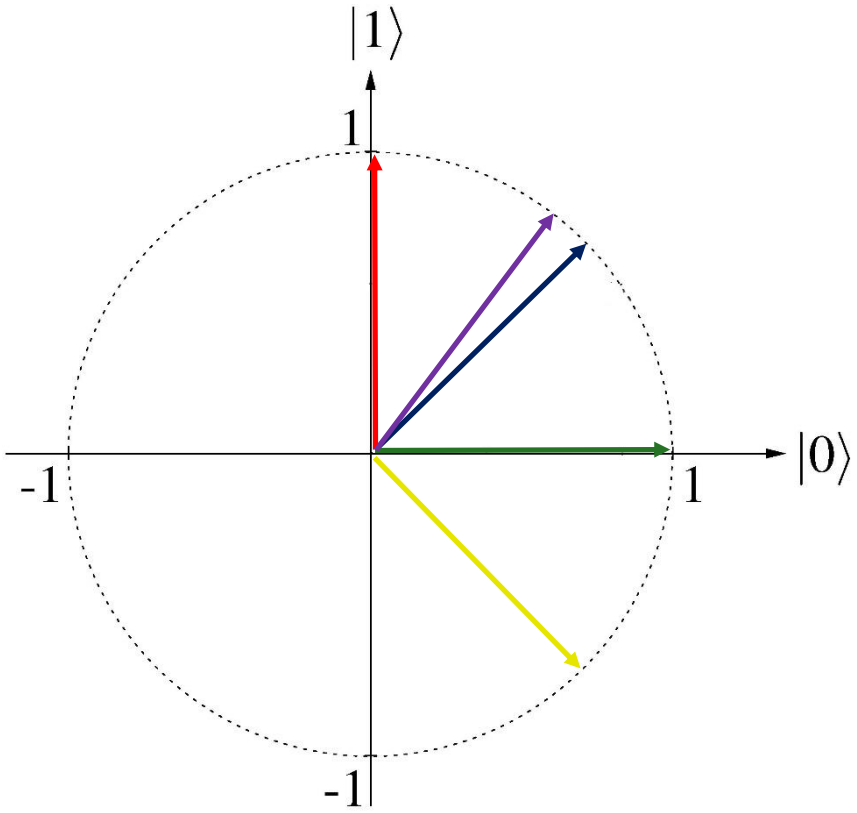
$|0>$

$|1>$

$\frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1>$

$\frac{1}{\sqrt{2}}|0> - \frac{1}{\sqrt{2}}|1>$

$0{,}6|0> + 0{,}8|1>$



Jeder solche Vektor: möglicher Qubit-Zustand.

Unendlich viele!

Wachstumsrate

Lineares Wachstum:

Äpfel	Preis
1	1 €
2	2 €
3	3 €
4	4 €
10	10 €
100	100 €

Quadratisches Wachstum:

Äpfel	Preis
1	1 €
2	4 €
3	9 €
4	16 €
10	100 €
100	10000 €

Exponentielles Wachstum:

Äpfel	Preis
1	2 €
2	4 €
3	8 €
4	16 €
5	32 €
6	64 €
10	1024 €
20	1 Million €
30	1 Milliarde €
100	*30 Stellen*

Mehrere klassische Bits

Belegungen bzw. Binärzahlen:

1 Bit: 0, 1

2 Bits: 00, 01, 10, 11

3 Bits: 000, 001, 010, 011, 100, 101, 110, 111

10 Bits: 1024 verschiedene Belegungen bzw. Zahlen

20 Bits: ca. 1 Million verschiedene Zahlen

30 Bits: ca. 1 Milliarde verschiedene Zahlen

100 Bits: ca. 10^{30} verschiedene Zahlen

Mehrere Quantenbits

1 Qubit: 0, 1 als Superposition

2 Quits: 00, 01, 10, 11 als Superposition

$$(\frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1>)(\frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1>)$$

$$= (\frac{1}{2}|00> + \frac{1}{2}|01> + \frac{1}{2}|10> + \frac{1}{2}|11>)$$

3 Qubits: 000, 001, 010, 011, 100, 101, 110, 111 als Superposition

10 Qubits: 1024 Zahlen als Superposition

20 Qubits: 1 Million Zahlen als Superposition

30 Qubits 1 Milliarde Zahlen als Superposition

Quantenparallelismus

Wir müssen einen Algorithmus auf alle möglichen Bitkombinationen anwenden.

Quantencomputer mit n Qubits:

1) Erzeuge Superposition aller 2^n Belegungen

2) In einem Durchlauf 2^n Ergebnisse (Funktionswerte) ermittelbar.

Der Haken:

Alle diese Ergebnisse bilden eine *Superposition*.

Diese ist unerkennbar. Bei der Messung erhalten wir eines per Zufall.

Das gleiche Resultat: Würfele *zuvor* die n Bits aus.

Ermittle für diese Kombination das Ergebnis.

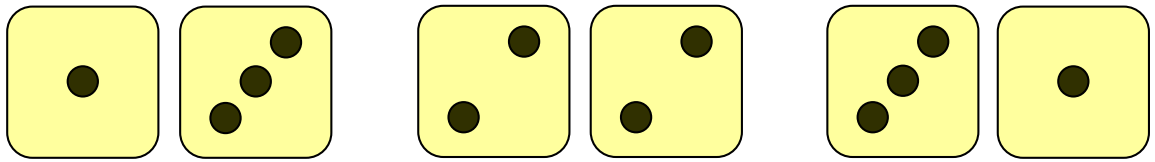
Interferenz

Wir nutzen folgendes aus:

Amplituden führen bei der Messung zu Wahrscheinlichkeiten.

Sie selbst sind aber *keine* Wahrscheinlichkeiten.

Wir werfen zwei Würfel: Summe 4?



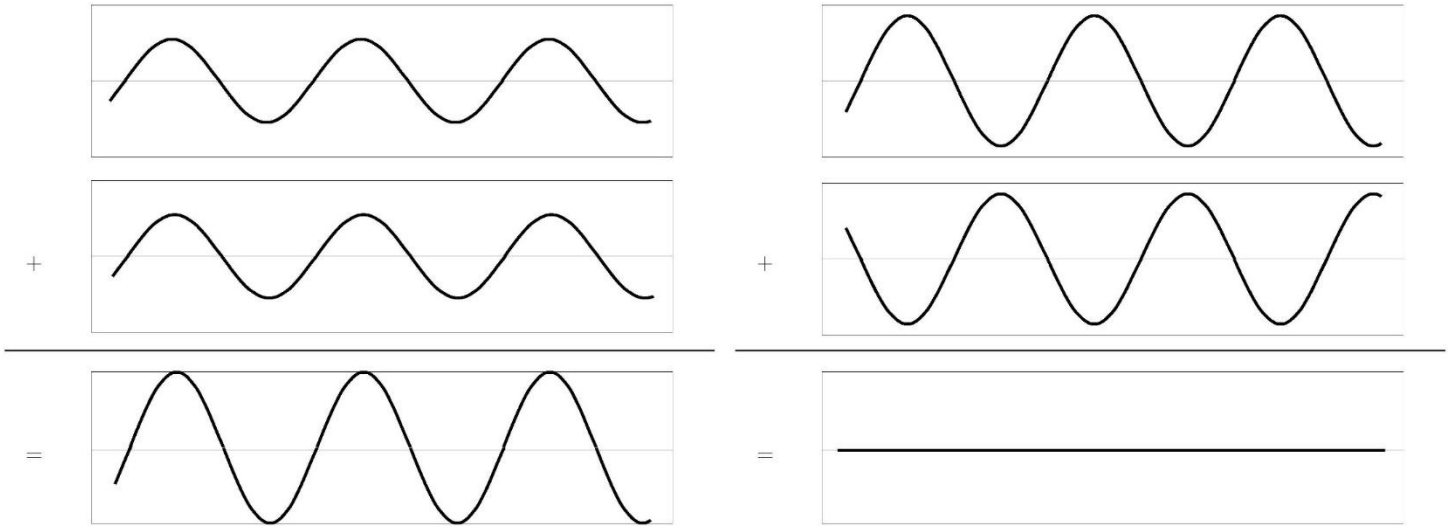
Wahrscheinlichkeit: $\frac{1}{36}+\frac{1}{36}+\frac{1}{36}=\frac{1}{12}$

Wahrscheinlichkeiten addieren sich stets.

Interferenz –(2)

Amplituden können sich gegenseitig auslöschen:

$$\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} = 0$$



Quantenalgorithmen nutzen Interferenz.

Ein Beispiel für virtuosen Einsatz von Interferenz:

Shors Algorithmus

Peter Shor (geb. 1959):

1994: Mit Quantencomputern ist die Faktorisierung effizient ausführbar!

… einer der Gründe für die heutige Veranstaltung.

Faktorisierung

Aufgabenstellung: Finde die Primfaktorzerlegung einer beliebigen ganzen Zahl:

45 = ?

$= 3 \cdot 3 \cdot 5$

21290246318258757547497882016271517497806703963277216278233383215381949984056495911366573853021918316783107387995317230889569230873441936471

= ?

Mit klassischen Rechnern nicht effizient ermittelbar.

Darauf beruht (vereinfacht gesagt) die Sicherheit der RSA-Kryptographie.

Erste Leitfrage dieser Präsentation:

Werden Quantencomputer unsere *klassischen* Computer ablösen?

Antwort: Nein.

Quantencomputer können spezielle Aufgaben lösen, an denen klassische Rechner scheitern.

So besteht auch Shors Algorithmus selbst aus einem Quantenteil und einem klassischen Teil.

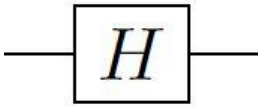
Agenda

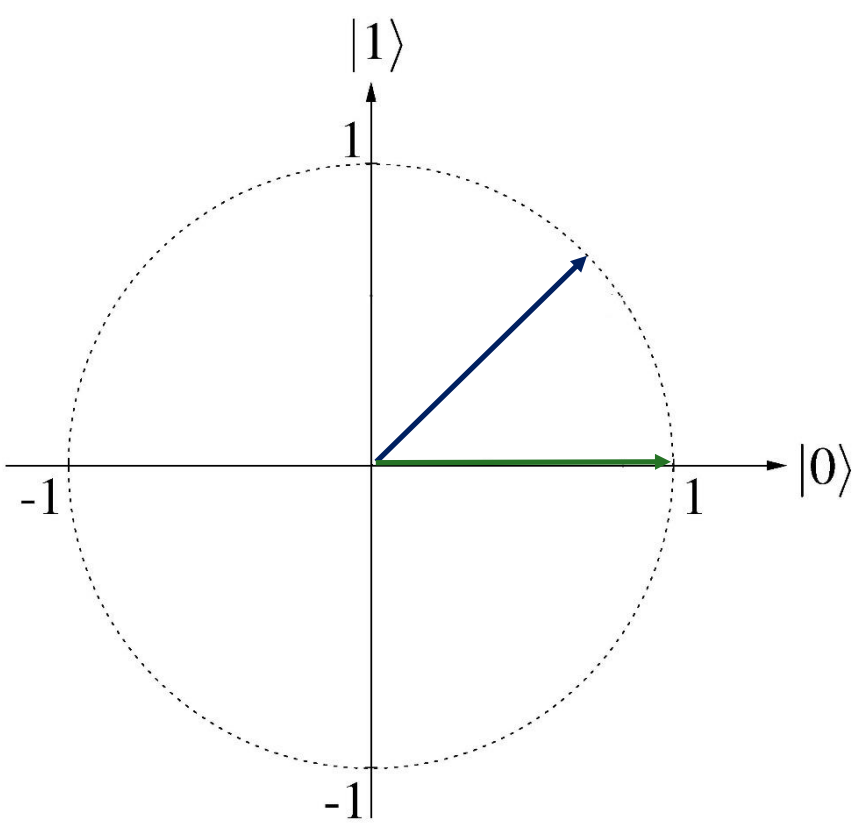
- **Kurzgefasst: Gatter**
- Kurzgefasst: Verschränkung

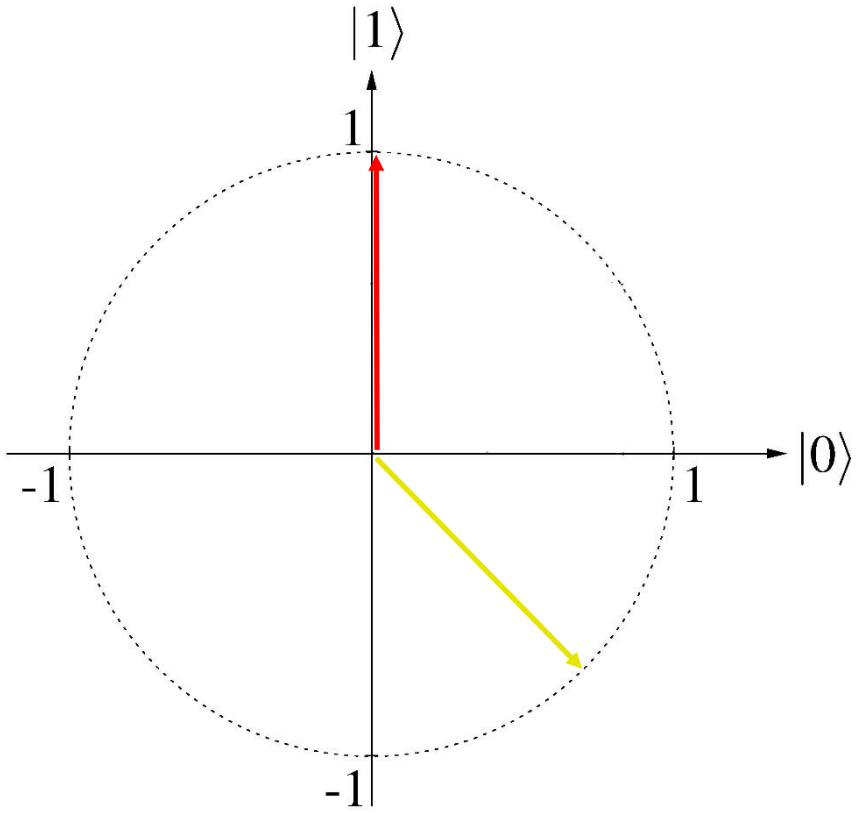
Quantengatter

Quantengatter bilden Qubit-Zustände auf Qubit-Zustände ab.

Beispiel Hadamard-Gatter:





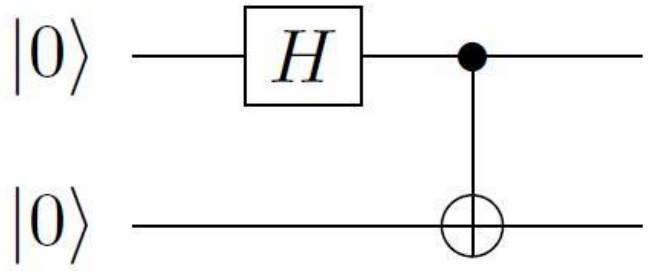


Quantengatter

Quantengatter mathematisch:

- Operationen, die u.a. linear, umkehrbar und winkelerhaltend sind.
- Genauer: unitär

Quantenschaltkreis:



Agenda

- Kurzgefasst: Gatter
- **Kurzgefasst: Verschränkung**

Verschränkte Qubits

Ergebnis des Schaltkreises:

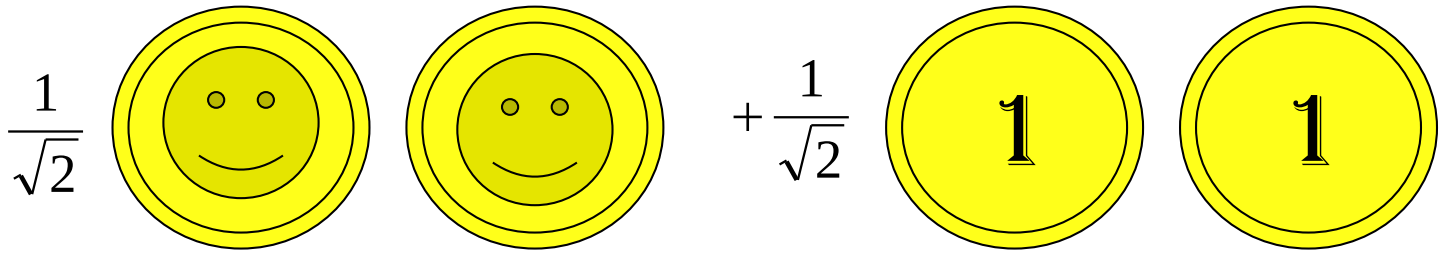
$$\frac{1}{\sqrt{2}}|0>|0>+\frac{1}{\sqrt{2}}|1>|1>,$$

Verschränkt:

- vor der Messung beide unbestimmt
- Eines der Qubits wird gemessen: Danach ist auch das andere festgelegt
- Räumliche Trennung spielt keine Rolle

Verschränkte Quanten-Münzen

Kopf oder Zahl?



Metapher für Qubits, Werfen entspräche der Messung …

Verschränkung

Wir verschränken zwei Qubits

- eins bleibt bei uns
- das andere wird zu einem Satelliten geschickt

Wir messen unser Bit: dann steht anschließend der Wert des anderen Bits fest!

- ohne ein Medium
- sofort

Bemerkung: Kommunikation mit Überlichtgeschwindigkeit damit nicht möglich!

Zusammenfassung

- Qubits
- Superposition
- Messung
- Quantenparallelismus
- Interferenz
- Quantengatter
- Verschränkung


Vielen Dank für Ihre Aufmerksamkeit!

Bildnachweis

Abbildungen:

[11] aus Homeister, Quantum Computing verstehen, Springer-Vieweg 2022.

[12] von Peter Shor zur Verfügung gestellt.

Alle anderen Abbildungen vom Verfasser erstellt.

Kontakt:

matthias.homeister@th-brandenburg.de