Quantencomputer - Eine Einführung

Inhalt

- Allgemeines
- Geschichte
- Modelle
- Reversibilität

Computer betrachtete man im:
19. Jh. -> rein geistige Prozesse
20. Jh. -> maschinelle Prozesse
21. Jh. -> Naturprozesse (großes Potenzial: Quantencomputer, Molekularcomputer)

alte Tradition der Informatik die Natur nachzuahmen

- bereits endliche Automaten sind entstanden als eine Abstraktion neuronaler Aktivitäten
- (künstliche) neuronale Netze als Simulation der Aktivitäten des Gehirns
- in Zukunft auch genetische Computer

Warum Quantencomputer?

Entwicklung klassische Computer macht immer noch enorme Fortschritte, gleichzeitig ist die Entwicklung von QC ist sehr ungewiss und kostspielig

- **unsere Welt ist von Grund auf quantenmechanisch** -> klassische Computer können nie das Potential der Physik voll ausschöpfen

  dennoch schränken QC die fundamentale Church-Turing These über die Berechnbarkeit nicht ein – sie können nichts berechnen, was klassische Computer nicht berechnen könnten; ihr Hauptvorteil liegt darin, dass sie einige wichtige Aufgaben wesentlich effizienter lösen können

- die **anhaltende Miniaturisierung** der Computer hat zur Folge, dass in kürzester Zeit (schätzungsweise 2012-2020) der atomare Level erreicht sein wird, der sowieso völlig durch quantenmechanische Gesetze bestimmt ist (ein „single electron transistor" ist bereits in der Entwicklung)

  bei anhaltenderer Steigerung der Leistungsfähigkeit in 50 Jahren Chips mit 10^5 Gattern und 10^{14} (100 Billionen) Hz Takt -> 10^{30} Logikoperationen pro Sek.

  ➔ Quantenphysik unumgänglich

(trotzdem gilt: auch wenn auf Hardwareebene die Gesetze der Quantenmechanik dominieren bleibt eine Haupt-Anwendung der Computer eine deterministisch geprägt
(QC werden klassische Computer wahrscheinlich nicht ersetzen können (aber Kooperation möglich)); es ist auch nicht gesagt, dass die bisherige Form der QC die einzig mögliche oder gar beste Variante darstellt)

- für einige bedeutende Anwendungen sind QC **exponentiell schneller** als herkömmliche (bspw. Faktorisierungsalgorithmus von Shor in polynomieller Zeit, schnellere Suche in unsortierten Datenbanken);
  ➔ Erkenntnis hat wesentlich die Forschungsaktivitäten auf diesem Gebiet verstärkt

- die Entwicklung von QC ist ein **Motor bei der Erweiterung unseres Wissens** über die Quantenmechanik und beeinflusst gar die traditionelle physikalische Herangehensweise an die Quantenmechanik. So existieren in der Physik seit Anfang der 90er Jahre Bemühungen, die Rolle von Informationen in der Physik zu ergründen. Heute geht man sogar von Information als eine physikalische Größe, fundamentaler als Materie und Energie aus.
  Außerdem besteht in Atom- und Quanten-Physik ein großer Bedarf an QC um die Art und Komplexität der dort anfallenden Daten handhaben zu können

- QC bieten erstaunliches Potenzial für zukünftige **Kommunikationstechnologien** - sie ermöglichen (nach heutiger Sicht) uneingeschränkte und mit klassischen Computern nicht erreichbare Sicherheit bei der Informationsübertragung (Quanten-Kryptographie), die Überwindung von Raum (Quanten-Teleportation) und fehlertolerantes Berechnen (Quanten-Fehlerkorrektur)
  ➔ QC dürften die Sicherheits- und Kommunikationstechnologien revolutionieren

Unterschiede zwischen klassischen Informationen und Quanten-Informationen

klassische Informationen können:
- gelesen werden
- durch beliebige Medien übertragen werden
- vervielfältigt werden

Quanten-Informationen können:

- nicht gelesen oder vervielfältigt werden ohne dabei zerstört zu werden (begründet in der Zufälligkeit der Ausgabe)
- teleportiert werden

Warum sind Quantencomputer so schnell?

1.) QC bieten enorme Parallelität
ein Quantenbit kann sich in einem von potenziell unendlich vielen Zuständen befinden (Superposition)
➔ Quantensysteme können sich gleichzeitig in exponentiell vielen Basiszuständen befinden
➔ eine exponentiell große Anzahl an Operationen kann in lediglich einem Schritt durchgeführt werden

2.) zeitgleiche Informationsübertragung durch Quantenteleportation

Schwierigkeiten

- eine Projektion kann aus einer großen Superposition lediglich ein (zufällig gewähltes) klassisches Ergebnis abbilden; alle anderen Ergebnisse werden irreversibel zerstört
(dennoch erlauben clevere Algorithmen, die die sog. Quanteninterferenz nutzen, von der Superposition zu profitieren, s.u.)

- eine Reaktion eines Quants mit seiner Umwelt kann zu sog. Dekohärenz-Effekten führen und den subtilen Quanten-Interferenz-Mechanismus stark beeinflussen oder ganz zerstören
➔ (längere) Berechnungen werden praktisch unmöglich

Aktueller Stand

große Fortschritte im Bereich der Quantenkryptographie

Geschichte

erste Idee eines QC durch Physiker mit Kenntnissen der Theoretischen Informatik

60iger Jahre Entwicklung klassischer reversibler Gatter
(andere Gründe -> Hitze!)

1973 von Benette bewiesene Existenz einer universal reversiblen Turing-Maschine

1980 Beweis von Benioff, dass Quantencomputer mindestens so mächtig wie klassische Computer sind, indem er zeigte, dass ein Quantensystem eine klassische reversible Turing-Maschie simulieren kann (allerdings war sein QC kein reiner QC)

weitreichende Konsequenzen: Physik und Informatik begannen gemeinschaftlich umfassendere und tiefreichendere Forschungen.

1982 fand der amerikanischer Physiker Richard Feynmann die Antwort auf die Frage, ob klassische Computer Quantensysteme simulieren können: er zeigte, dass ein Quantensystem durch eine randomisierte Turing-Maschine lediglich bei einer exponentiellen Abnahme der Geschwindigkeit simuliert werden kann. Anders formuliert: QC könnten exponentiell schneller sein als klassische Computer!

1993 zeigten Bernstein und Vazirani die Existenz einer universellen QTM, die es ermöglichte, andere QTM in polynomieller Laufzeit zu simulieren. Die Veröffentlichung von Bernstein und Vazirani bildeten den Grundstein der Quanten-Komplexitäts-Theorie. Außerdem zeigten sie, dass QTM und Quantenschaltkreise in polynomieller Zeit dieselbe Klasse an Funktionen berechnen können.

1994/1997 Shor zeigte wie man darauf basierend mit QC in polynomieller Zeit Faktorisierungen und diskrete Logarithmen berechnen kann – eine für die public-key-Kryptographie bedrohliche Erkenntnis

➔ von nun an stießen QC auf breites wissenschaftliches und nicht wissenschaftliches Interesse

1995 Entdeckung von Fehler-Korrektur Codes durch Shor ermöglichte den Umgang mit Dekohärenz und operativen Ungenauigkeiten bei der Übertragung und Speicherung von Quanteninformationen

Modelle

kurze Wiederholung: Turingmaschine

Turingmaschine (TM) = 7 Tupel

$M = (Q, \Sigma, \Gamma, \delta, q_0, B, F)$, mit

Q = endliche Menge an Zuständen
Σ = endliche Menge Eingabealphabet
Γ = endliche Menge Bandalphabet ($\Sigma \subset \Gamma$)
$q_0 \in Q$ (Startzustand)
$B \in \Gamma \setminus \Sigma$ (Leerzeichen)
$F \subset Q$ (Endzustände)

δ: $Q \times \Gamma \rightarrow Q \times \Gamma \times \{L,R\}$ (Überführungsfunktion)

Randomisierte Turingmaschine (Probabilistic Turing Machine, PTM)

repräsentieren heutzutage das wichtigste Model der klassischen Computer und stehen für die Machbarkeit polynomieller Berechnungen auf klassischen Computern

δ: $\Sigma \times Q \times \Sigma \times Q \times \{\leftarrow, \downarrow, \rightarrow\} \rightarrow [0,1]$

Konfiguration = vollständige Beschreibung des globalen Zustands der PTM, bspw.
$w_1 q w_2$ mit
$w_1 w_2$ = vollständiger Inhalt des Bandes,
q = aktueller Zustand,
aktuelle Position des Kopfes der PTM auf erstes Symbol von w_2

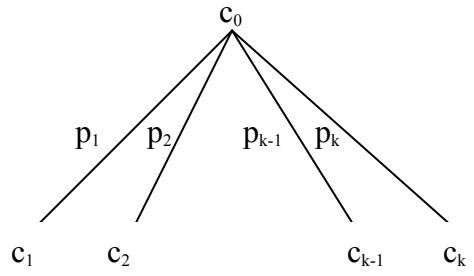
jede Konfiguration c_0 besitzt die Folgekonfigurationen $c_1, \ldots, c_k$
δ beschreibt die Wahrscheinlichkeit, dass von der Konfiguration c_0 die Nachfolgekonfiguration c_i mit $1 \leq i \leq k$ gewählt wird, so dass gilt:

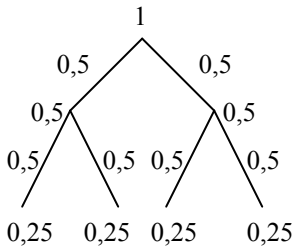
$$\sum_{i=1}^{k} p_i = 1$$ **lokale Wahrscheinlichkeitsbedingung**

anders notiert:

$$\sum_{(\sigma,q,d)\in\Sigma\times Q\times\{\leftarrow,\downarrow,\rightarrow\}} \delta(\sigma_1, q_1, \sigma, q, d) = 1$$

Konfigurationsbaum:





$p_1 + p_1 + \ldots + p_{k-1} + p_k = 1$

jede Kante, jeder Knoten (und jede Konfiguration, s.u.) kann mit einer Wahrscheinlichkeit versehen werden

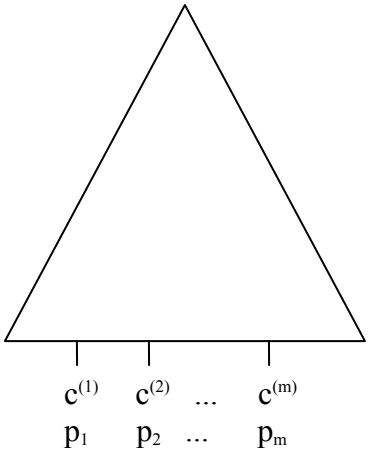
die Wahrscheinlichkeit an einer Kante ergibt sich direkt aus δ
(gibt die Wahrscheinlichkeit an, dass die Berechnung in die spezielle Richtung geht)

die Wahrscheinlichkeit der Wurzel ist 1

die Wahrscheinlichkeit eines Knotens ergibt sich als dass Produkt der Wahrscheinlichkeiten der Kanten auf dem Weg von der Wurzel zum Knoten

die Wahrscheinlichkeit eines Knoten ist somit die Wahrscheinlichkeit, dass eine bei der Wurzel startende Berechnung diesen Knoten erreicht

auf einem Level kann eine Konfiguration c mehrfach auftreten $c^{(1)}, \ldots, c^{(m)}$



dann ist die Wahrscheinlichkeit für das Auftreten von c

$$p_c = \sum_{i=1}^{m} p_i$$

sind c_1, …, c_k unterschiedliche Konfigurationen eines Levels, so muss die folgende Bedingung erfüllt sein:

$$\sum_{i=1}^{k} p_i = 1 \qquad \textbf{globale Wahrscheinlichkeitsbedingung}$$

Satz: Falls alle lokalen Wahrscheinlichkeitsbedingungen erfüllt sind, so ist auch die globale Wahrscheinlichkeitsbedingung erfüllt.

Beweis:

spezielle Formulierung einer lokalen Wahrscheinlichkeitsbedingung:

$F(c) = p_1 c_1 + p_2 c_2 + \ldots + p_k c_k$ "*lineare Superposition*"

mit $\sum_{i=1}^{k} p_i = 1$

beginnend wird beschreibt F(c) die Wurzel und ihre Folgekonfigurationen nun ist jede Folgekonfiguration c_i wiederum durch die Superposition ihrer Nachfolger substituierbar (für die wiederum gilt $\sum_{i=1}^{k} p_i = 1$) bis das Ende des Baumes erreicht ist. Aufgrund der Distributivität der Addition und Multiplikation der Wahrscheinlichkeiten ergibt sich nach dem Ausmultiplizieren eine Superposition dessen Wahrscheinlichkeitskoeffizienten die Summe 1 ergeben, die globale Wahrscheinlichkeitsbedingung ist erfüllt □

Die Überführungsfunktion ist durch eine **Matrix** $M_{\mathcal{M}}$ beschreibbar (transition matrix):

- Reihen und Spalten enthalten alle möglichen Konfigurationen der PTM (unendliche Matrix möglich)
- $M_{\mathcal{M}}(i,j)$ ist die Wahrscheinlichkeit, dass c_i Folgekonfiguration von c_j ist

➔ alle Einträge sind Positiv und die Summe der Spalten ist 1
(wg. lokaler Wahrscheinlichkeitsbedingung)

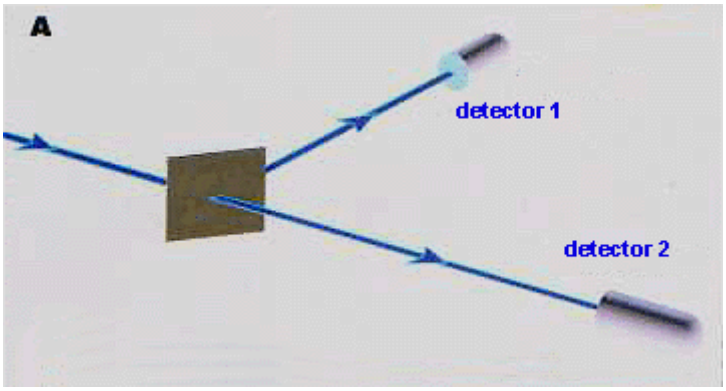
multipliziert man die *Überführungsmatrix* mit einem gleichdimensionierten Vektor, dessen Elemente nichtnegativ sind und die Summe der Elemente gleich 1 ist, so ist dieser Vektor als eine Superposition interpretierbar, das Ergebnis liefert die aus dem nächsten Rechenschritt resultierende Superposition (die dann auch die globale Wahrscheinlichkeitsbedingung erfüllt).

➔ die Überführungsmatrix repräsentiert die Evolution der PTM

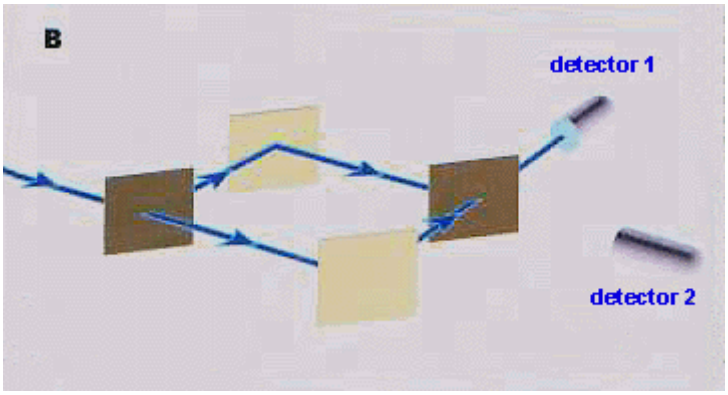
in einer Berechnung wird lediglich entsprechend den Wahrscheinlichkeiten **ein Weg** im Baum gegangen; die Wegbeschreitung ist während der **Berechnung beobachtbar** ohne die Berechnung zu beeinflussen, es wird **ein Ergebnis** geliefert

aufgrund der Komplexität ist es ist nützlich die Wahrscheinlichkeiten auf $\{0, \frac{1}{2}, 1\}$ einzuschränken

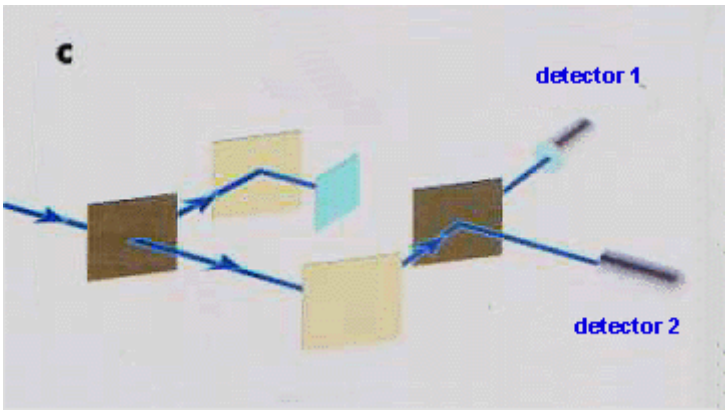
Exkurs Quanteninterferenz



$p_{d1} = p_{d2} = 0{,}5$



$p_{d1} = 1$; $p_{d2} = 0$!!!



$p_{d1} = p_{d2} = 0{,}5$

➔ bei Quanten keine einfache Addition der Wahrscheinlichkeiten

Quantenturingmaschine (Quantum Turing Machine QTM)

Überführungsfunktion:

$$\delta: \Sigma \times Q \times \Sigma \times Q \times \{\leftarrow, \downarrow, \rightarrow\} \rightarrow \mathbb{C}_{[0,1]}$$

lifert eine sog. *Wahrscheinlichkeitsamplitude* (komplexe Zahl), dessen Betrag im Intervall [0,1] liegt

lokale Wahrscheinlichkeitsbedingung für alle Nachfolgekonfigurationen $c_1, \ldots, c_k$ einer Konfiguration c_0:

$$\sum_{i=1}^{k} |\alpha_i|^2 = 1$$

$|\alpha_i|^2$ wird als Wahrscheinlichkeit der Transition von c_0 zu c_i betrachtet

den Kanten des Konfigurationsbaums werden direkt die Wahrscheinlichkeitsamplituden zugewiesen

jedem Knoten wird das Produkt der Amplituden der Kanten auf dem Weg von der Wurzel zum Knoten zugewiesen (die Wurzel erhält 1)

tritt in einem Level eine Konfiguration c mehrfach auf $c^{(1)}, \ldots, c^{(m)}$, so wird ihr die Summe der entsprechenden Knoten-Amplituden zugewiesen:

$$\beta = \sum_{i=1}^{m} \alpha_i$$ (analog zur Addition der Wahrscheinlichkeiten bei der PTM)

sind $c_1, \ldots, c_k$ unterschiedliche Konfigurationen eines Levels, so muss die folgende Bedingung erfüllt sein:

$$\sum_{i=1}^{k} |\beta_i|^2 = 1$$ **globale Wahrscheinlichkeitsbedingung**

aus der Erfüllung aller lokalen Wahrscheinlichkeitsbedingungen folgt **nicht** die Erfüllung der globalen Wahrscheinlichkeitsbedingung!
(ergo: es existieren ungültige Berechnungen)

positive/konstruktive und negative/destruktive Interferenz:

tritt in einem Level eine Konfiguration c mehrfach auf $c^{(1)}, \ldots, c^{(m)}$ und es gilt die Ungleichung

$$\left|\sum_{i=1}^{m} \alpha_i\right|^2 > \sum_{i=1}^{m} |\alpha_i|^2 ,$$

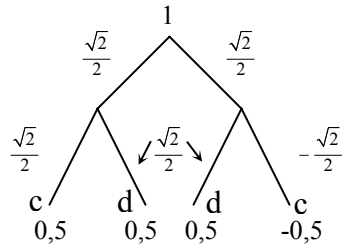
also $\beta_i^2 > \sum_{i=1}^{m} |\alpha_i|^2$, so spricht man von „positiver Interferenz".

gilt $\beta_i^2 < \sum_{i=1}^{m} |\alpha_i|^2$, so spricht man von „negativer Interferenz"

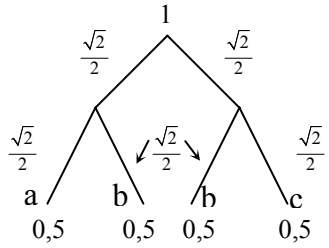
die rechte Seite der Ungleichung entspricht der Wahrscheinlichkeit des Auftretens der Konfiguration nach der klassischen Physik / PTM

die linke Seite ist die Wahrscheinlichkeit des Auftretens der Konfiguration durch die Quanteninterferenz / nach der QTM

ein Beispiel:



(a) QTM



(b) ungültige Berechnung

(b) ist ein Beispiel für eine ungültige Berechnung (globale Wahrscheinlichkeitsbedingung nicht erfüllt, trotz Erfüllung aller lokaler Wahrscheinlichkeitsbedingungen)

Im Beispiel (a) treten zwei Pfade zur Konfiguration d auf die, jeweils eine Wahrscheinlichkeitsamplitude von 0,5 ($\frac{\sqrt{2}}{2} * \frac{\sqrt{2}}{2}$) besitzen und damit einzeln betrachtet mit einer Wahrscheinlichkeit von 0,25 aufträten, d insgesamt würde also mit einer Wahrscheinlichkeit von 0,5 auftreten. Diese Wahrscheinlichkeitsbetrachtung ist aufgrund der Quanteninterferenz falsch. Tatsächlich tritt die Konfiguration d mit der *totalen* Wahrscheinlichkeit $(0,5+0,5)^2 = 1$ auf und damit doppelt so häufig, als es (klassisch gesehen) scheint!

(positive Interferenz) Die Konfiguration c tritt demzufolge nie auf ($(0,5-0,5)^2=0$, negative Interferenz).

Die totale Wahrscheinlichkeit gibt also an, mit welcher Wahrscheinlichkeit ein Beobachter eine Konfiguration als Ergebnis einer Berechnung erhält, falls eine Beobachtung (und damit Terminierung) durchgeführt wird.

Um QC nützlich zu machen, müssen die Berechnungen so konzipiert werden, dass korrekte bzw. gewünschte Ergebnisse aufgrund von positiver Interferenz mit hoher Wahrscheinlichkeit und falsche bzw. ungewünschte mit geringer Wahrscheinlichkeit auftreten.

Es existiert eine transparentere Bedingung als die der globalen Wahrscheinlichkeit, die diese aber impliziert:

Analog zur PTM kann für jede QTM eine **Überführungsmatrix M_M** aufgestellt werden dessen Elemente M(i,j) komplexe Zahlen sind, die die Wahrscheinlichkeitsamplitude eines Übergangs von der Konfiguration c_i zur Konfiguration c_j bedeuten.
Die lokale Wahrscheinlichkeitsbedingung impliziert, dass die Euklidische Norm der Spalten (und damit auch die Summe der lokalen Wahrscheinlichkeiten) der Matrix gleich 1 ist:

Euklidische Norm:

für alle Elemente x_i eines n-dimensionalen Vektors gilt: $\sqrt{\sum_{k=1}^{n} x_k^2} = 1$

Matrix **unitär** $\Rightarrow$ alle globalen Wahrscheinlichkeitsbedingungen erfüllt

unitär - z.B. es existiert die konjugiert transponierte Matrix M^{-1},
so dass gilt $M*M^{-1}=I$

Matrix **unitär** $\Rightarrow$ Berechnungen der QTM **reversibel**
$\Rightarrow$ jede vorherige Superposition ist ableitbar

eine QTM folgt allen Wegen im Konfigurationsbaum **gleichzeitig** (daher der Begriff „Superposition" als Zusammenfassung mehrerer gleichzeitiger Zustände)

da die Anzahl der Knoten mit den Berechnungsschritten exponentiell steigt, können in einer Superposition gleichzeitig zur Anzahl der Schritte **exponentiell viele Konfigurationen** berechnet werden

eine Beobachtung der Evolution eines Quantensystems führt zur Beeinflussung der Quanten, die u.U. zum völligen Verlust der Quanteninformation führen kann
➔ die Berechnung der QTM ist **nicht beobachtbar**
(aber zurückverfolgbar/reversibel)

am Ende einer Berechnung kann diese gelesen werden. Dabei erhält man ein Ergebnis entsprechend ihrer totalen Wahrscheinlichkeiten. Alle **nicht ausgegebenen Ergebnisse geht verloren**.

um die Komplexität beherrschbar zu machen, hat es sich als günstig erwiesen, lediglich folgende Amplituden zu verwenden: $\{-1, -\frac{4}{5}, -\frac{3}{5}, 0, \frac{3}{5}, \frac{4}{5}, 1\}$

Klassische reversible Gatter und reversible Berechnung

„Braucht man zum Rechnen Energie?"

die große theoretische Vorarbeit hierzu wurde bereits in den 60er Jahren begonnen

ursprüngliche Motivation zur Erforschung reversibler Berechnungen war die Vermeidung von immer größerer Wärmeabgabe bei zunehmender Miniaturisierung, da aufgrund des **2. Gesetzes der Thermodynamik** jede irreversible Zustandsänderung Wärme erzeugen muss.

für klassische Berechnungsoperationen berechnete Landauer eine energetische untere Grenze von 1kT ln2 (k–Bolzmannkonstante, T-Temperatur, ln2-Phasenvolumen = ln von Anzahl der Zustände; Entropie S = 1k*ln2)

> ***Landauer's principle:*** *To erase a bit of classical information within a computation, 1 bit of entropy must be expelled into the computer's environment (typically in the form of waste heat).*

heutiger "Energieverbrauch" liegt bei etwa kT ln 10^8

reversible Berechnungen benötigen theoretische keine Energie

klassische reversible Berechnungen sind ein Spezialfall der Quanten-Berechnungen
➔ für QC von Interesse

reversible Gatter

in den 60iger Jahren wurden zunächst reversible Gatter entwickelt

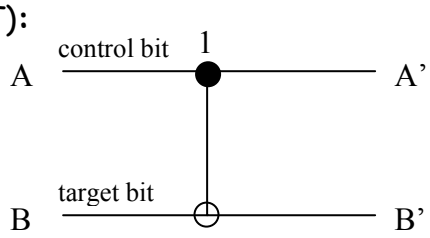
irreversibel: AND, NAND, OR, …

Grund: aus den Ausgabewerten können nicht wieder die Eingabewerte bestimmt werden, während der Berechnung gehen Informationen verloren

reversibel: NOT, CN , CCN, Fredkin-Gatter

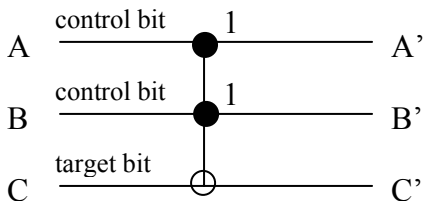
CONTROL NOT (CN, CNOT):

A=A'
falls A=0 -> B'=B
falls A=1 -> B'= $\overline{B}$



A	B	A'	B'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

CONTROL CONTROL NOT:
(CCN, CCNOT,(Petri-) Toffoli-Gate)



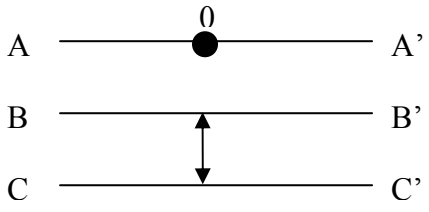
A=A'
B=B'
falls A=B=0 -> C'=C
falls A=B=1 -> C'= $\overline{C}$

A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

$$f(a,b,c) = (a,b,c \oplus (a \wedge b))$$

N, CN und Toffoli-Gate können alle reversiblen Booleschen Funktion B_n^m mit $n \geq 3$ berechnen
das Toffoli- sowie das Fredkin-Gate bilden eine logische Basis

Fredkin-Gatter:
(Petri-Fredkin-Gate)



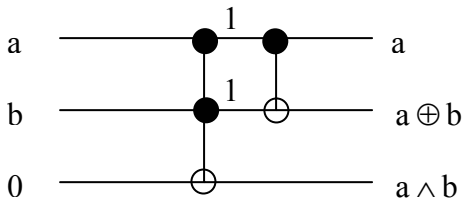
A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	0	0	1
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	1	1	1

A=A'
falls A=0 -> B'=B, C'=C
falls A=1 -> B'=C, C'=B

$f(a,b,c) = a, ab \vee \bar{a}c, \bar{a}b \vee ac)$

reversible Gatter werden interessant, wenn eine Boolesche Funktion reversibel ist. Eine nicht reversible Funktion $f: a \to f(a)$ kann durch eine kleine Erweiterung reversibel (injektiv) gemacht werden: $f_0: a \to (a, f(a))$

Beispiel: reversibler 2-bit-Adder
aus $(a,b) \to (a \oplus b, a \wedge b)$ wird $(a,b) \to (a, a \oplus b, a \wedge b)$
realisierbar durch ein CN-Gate und ein CNN-Gate mit Eingang c=0:

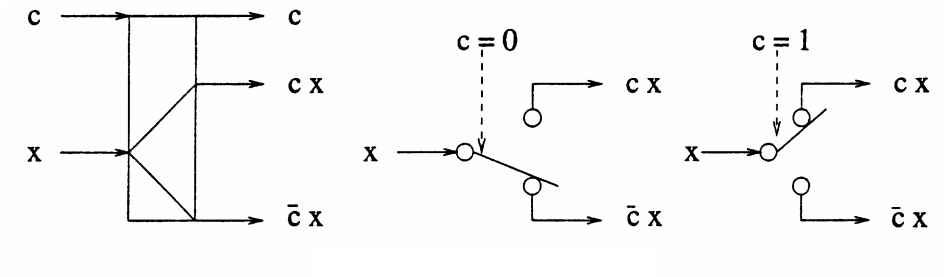


nach diesem Erfolg wurde vom gleichen Team der Wissenschaftler ein „Rechner" modelliert, der alle möglichen Informationen reversibel verarbeiten kann. Er soll im Prinzip wie ein Billardspiel (daher sein Name: „Billard-Kugel-Rechner") funktionieren: Die aufeinander treffenden Kugeln repräsentieren jeweils die Bits, ihre Bewegung die Schaltungsfunktionen.

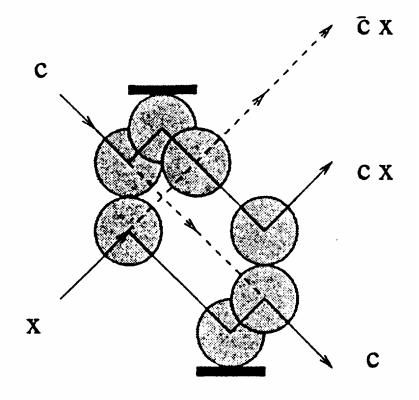
Billardball-Model

durch Billardkugeln ist ein reversibler logischer Schalter simulierbar, der theoretisch keine Energie umsetzt:

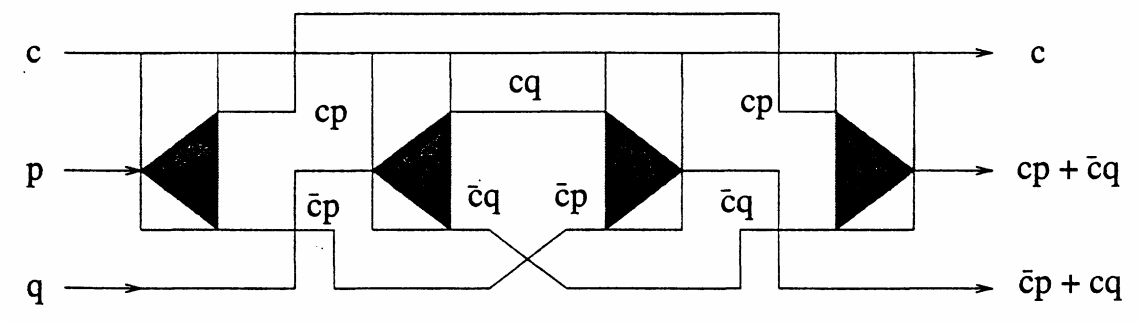
Schalter:



Billard-Simulation:



durch diesen Schalter lässt sich wiederum das Fredkin-Gatter darstellen:



alternativ entwickelte Bennett 1973 ein **molekular-dynamisches Computer-Model**, dass lediglich 20 bis 200 kT Joules je Operation umsetzt

allerdings boten all diese Entwicklungen noch keine Möglichkeit, Informationen zu speichern
erst Anfang der 80er Jahre erschien von Charles H. Bennett. Professor eine Arbeit, in der er ausführlich die erste reversible Turingmaschine vorstellte. Dabei inspirierte ihn eine chemische Reaktion von wichtiger biologischer Bedeutung: die DNA-Verdopplung

Die Reversible Turingmaschine

ein Computer ist reversibel, falls aus jeder Konfiguration die vorherige Konfiguration bestimmbar ist

es kann gezeigt werden, dass falls eine reversible TM

$$M = (\Sigma, Q, q_0, \delta)$$

existiert, auch eine TM

$$M' = (\Sigma, Q, q'_0, \delta')$$

existiert, so dass aus $M(c)=c' \Rightarrow M'(c')=c$

aus jeder nicht reversiblen ein-Band-TM kann eine reversible drei-Band-TM mit konstantem zusätzlichen Zeitbedarf und quadratischem zusätzlichen Speicherbedarf konstruiert werden:

in den 90er Jahren wurden ein reversibler Chip und eine reversible Programmiersprache entwickelt

die so genannte „Reversible Logic" stellt heute ein Gebiet der Informatik dar, auf dem sehr intensiv geforscht wird

trotzdem bisher keine Anwendungen für diese energielosen Modelle existieren führten sie zur Entwicklung der modernen reversiblen **CMOS**-Bausteine, die fast keine Energie mehr „verbrauchen"