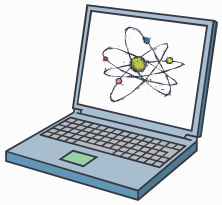
Quantenbits, -gatter, -register

Seminar über Quantencomputer

Jörg Meltzer
& Axel Steinacker



Inhalt

- Klassisches Modell
- Vektorielle Zustandsbeschreibung klassischer Register
- Einfache Gatter
- Was sind Qubits, Quantenregister
- Quantengatter, Quantenschaltkreise
- Quantenparallelismus
- Probleme

Einleitung

- Das Herz des klassischen Computers (die ALU) besteht aus einer Reihe geeignet miteinander verschalteter logischer Gatter.
- Von einem abstrakt logischen Standpunkt aus gesehen, heißt Rechen die Manipulation von Bits, die in den Registern der ALU bzw. des Hauptspeichers zur Verfügung gehalten werden.
- Dieses Konstruktionsprinzip wiederholt sich auch bei der Realisierung eines QC mit zwei wesentlichen Variationen einerseits haben die Bits eine allgemeinere Bedeutung und andererseits erfolgt ihre Verarbeitung auf reversible Weise.

Klassische Betrachtungsweise

- Bit wird realisiert als skalarer Wert

(Spannung/Magnetisierung in einem Speicherelement)

- Wert kann je nach Zustand als 0 oder 1 interpretiert werden.
- zweielementige Bitmenge abstrakt als $B = \{0,1\}$
- n Bits $B^n = B \times B \times .. \times B$

Vektordarstellung der Bits

- B = $\{|0\rangle,|1\rangle\}$,
- B = $\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\}$

  $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix},|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$
- Wörter aus 2 Bits sind durch die Elemente des Kartesischen Produktes gegeben
- B x B = {00,01,10,11}

Vektordarstellung der Bits 2

Direktes Produkt zweier Vektoren:

$$\begin{pmatrix}a_1\\a_2\end{pmatrix}\otimes\begin{pmatrix}b_1\\b_2\end{pmatrix}\equiv\begin{pmatrix}a_1b_1\\a_1b_2\\a_2b_1\\a_2b_2\end{pmatrix}$$

Direktes Produkt zweier Matrizen:

$$\begin{pmatrix}A_{11}&A_{12}\\A_{21}&A_{22}\end{pmatrix}\otimes\begin{pmatrix}B_{11}&B_{12}\\B_{21}&B_{22}\end{pmatrix}=\begin{pmatrix}A_{11}\begin{pmatrix}B_{11}&B_{12}\\B_{21}&B_{22}\end{pmatrix}&A_{12}\begin{pmatrix}B_{11}&B_{12}\\B_{21}&B_{22}\end{pmatrix}\\A_{21}\begin{pmatrix}B_{11}&B_{12}\\B_{21}&B_{22}\end{pmatrix}&A_{22}\begin{pmatrix}B_{11}&B_{12}\\B_{21}&B_{22}\end{pmatrix}\end{pmatrix}$$

Vektordarstellung und Register

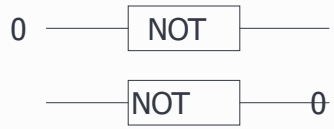
- folglich ist:
  B x B = $\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}$

  $|q1\rangle\otimes|q2\rangle=|q1q2\rangle$

  $|0\rangle_2=\begin{pmatrix}1\\0\\0\\0\end{pmatrix},|1\rangle_2=\begin{pmatrix}0\\1\\0\\0\end{pmatrix},$
- abgekürzt
- B x B ={ $|0\rangle_2,|1\rangle_2,|2\rangle_2,|3\rangle$}

  $|2\rangle_2=\begin{pmatrix}0\\0\\1\\0\end{pmatrix},|3\rangle_2=\begin{pmatrix}0\\0\\0\\1\end{pmatrix},$
- Ein Register allgemein $|q1\rangle\otimes|q2\rangle\otimes|q3\rangle\otimes\ldots\otimes|qn\rangle=|q1q2q3\ldots qn\rangle$

NOT Gatter



NOT ist Reversibel

NOT $|0\rangle=|1\rangle$, NOT $|1\rangle=|0\rangle$ NOT= $\begin{pmatrix}0&1\\1&0\end{pmatrix}$

Spezielle Reversible Gatter

Reversibles Rechnen bei Funktionen $B^n \to B^m$ mit m<n

Beispiel:

XOR= $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ =CNOT

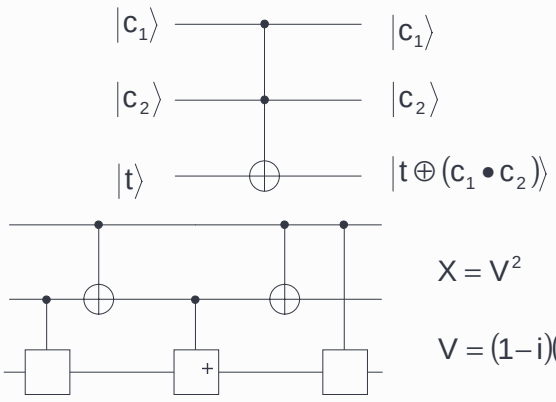
XOR $|q1\rangle \otimes |q2\rangle = |q1\rangle \otimes |q1 + q2\rangle$, $q_i \in \{0,1\}$

XOR $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, ... , XOR $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

AND Gatter

AND ist Irreversibel

Toffoli Gatter



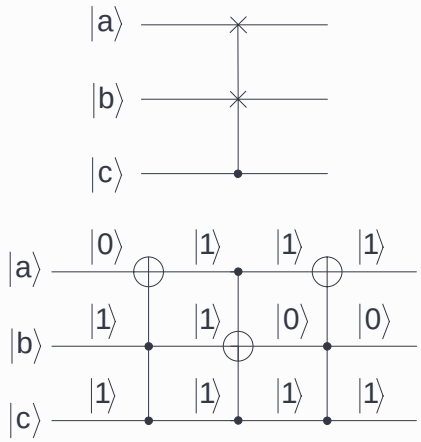
$X = V^2$

$V = (1-i)(I+iX)/2$

Fredkin Gatter

- Kontrolliertes Bit-Swapping-Gatter

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	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1



Ion Traps

- Atom- und Kernzustände werden benutzt geladene Atome (Ionen) werden isoliert, indem sie in elektromagnetischen Traps gefangen gehalten werden.
- Die Atome werden auf eine Energie abgekühlt, so daß ihre kinetische Energie viel geringer ist als ihre Spinenergie
- mit Hilfe von monochromatischem Licht können Spinzustände geändert werden
- Dieser Spin ist das Quantenmechanische Objekt in dem wir den quantenmechanischen Zustand speichern.

Qubits???

- Bei der Messung nimmt der Spin des zugrunde liegenden Quantenmechanischen Objekts die Werte

  $|\uparrow\rangle = |0\rangle$ oder $|\downarrow\rangle = |1\rangle$ an

- Unbeobachtet ist er aber eine Überlagerung der beiden Zustände
- $|\cdot\rangle = \frac{1}{\sqrt{2}}(|\downarrow\rangle + |\uparrow\rangle)$

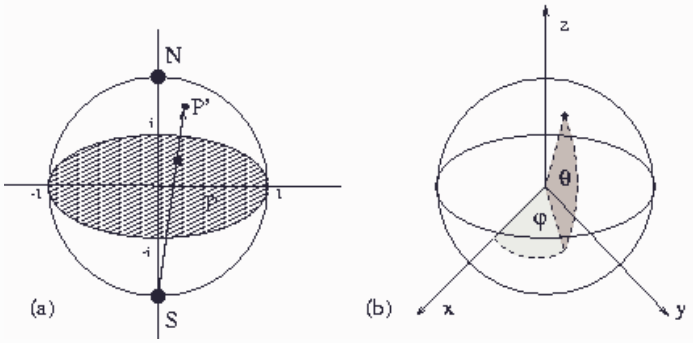
Qubits & QRegister

- Einzelnes Qubit allgemein: $|\psi\rangle = \alpha|\downarrow\rangle + \beta|\uparrow\rangle$
- Normierung: $|\alpha|^2 + |\beta|^2 = 1$
- Vektordarstellung: $|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$
- Quantenregister: Direktes Produkt mehrerer Qubits

  $|\psi_1\psi_2\psi_3..\psi_n\rangle \equiv |\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle \in H_n$

- Wichtig:dim(H_n) = 2^n
- Klassische Register dim(Z_2^n)=n

Riemann & Bloch Sphäre



Merkmale von Qregistern

- Die Anzahl von Basis Zuständen und der Superpositionen wächst exponentiell mit der Anzahl der Qubits. Schon für
  n = 200 ist die Gesamtanzahl von Zuständen einer Basis größer als die geschätzte Anzahl von Atomen im Universum.
- Trotz der exponentiellen Größe der Basiszuständen läßt sich ein QRegister in linearer Zeit von einem zum anderen Zustand umwandeln.

Quanten Gatter

- Quantengatter implementieren unitäre Operatoren
- Werden dargestellt als unitäre Matrix mit 2^n Einträgen.
  (n Ein/Ausgänge)
- Die Anzahl von Ein- und Ausgängen ist wegen der Reversibilität mindestens gleichgroß
- So wie klassische Gatter können Quantengatter durch Wahrheitstabellen beschrieben werden. Somit können wir die Ausgabe für alle möglichen Eingaben bestimmen
- Ein wichtiger Unterschied zwischen dem Klassischen- und Quantenrechnen ist, das für beliebige n die Anzahl der n Eingang-/Ausgang-Quantengatter nicht zählbar ist.
- Es drängt sich die Frage auf, ob solch große unitäre Matrizen in mehrere kleinere, besser zu handhabende, transformiert werden können.

Kohärenzgatter

- Kohärenzgatter = $\sqrt{NOT}$

$$|\uparrow\rangle \longrightarrow \boxed{\sqrt{NOT}} \longrightarrow |\cdot\rangle$$

- Überführt das Bit in ein Quantenbit (kohärenter Quantenzustand)
- allg. Quantenregister nimmt alle 2^n Zustände an

Phasenschieber

- P = $\begin{pmatrix} 1 & 0 \\ 0 & \varepsilon \end{pmatrix}$ $\quad |\varepsilon|^2 = 1$
- Im Falle ε =1 bleibt die Phase gleich
- Im Falle ε =-1 erfolgt eine 180 Drehung
- Universelles 2-Qubit Gatter

$$A \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha}\cos\theta & -ie^{i(\alpha-\phi)}\sin\theta \\ 0 & 0 & -ie^{i(\alpha+\phi)}\sin\theta & e^{i\alpha}\cos\theta \end{pmatrix}$$

- ist *universell*, falls α, ϕ , θ irrationale Vielfache von sich und π sind.

3d-Qubit Zustandsraum

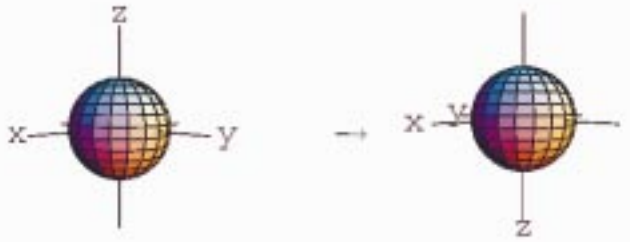


Abbildung 3: Bewegung eines quantenmechanischen Spins. Bsp. 1: Rotation um z–Achse mit Winkel 180°. Diese vertauscht Nord- und Südpol und entspricht auf B einer Negation.

Quantenschaltkreise

- Ein Quanten-Schaltkreis ist eine „Ansammlung“ von Quantengattern, die jeweils über physische Qubits oder über Felder interagieren.
- Für irgendein Quantengatter C mit den Eingangvariablen $x_1...x_n$ und den Ausgängen $y_1,...y_m$ $m \geq n$, setzen wir zu jedem Eingang $x \in \{0,1\}^n$ die mögliche Verteilung zu p_x über $\{0,1\}^m$.
- Für beliebige Eingaben x hat der finale Quantenzustand v die Form
- $$v = \sum_{y \in \{0,1\}^m} \alpha_y |y\rangle,$$

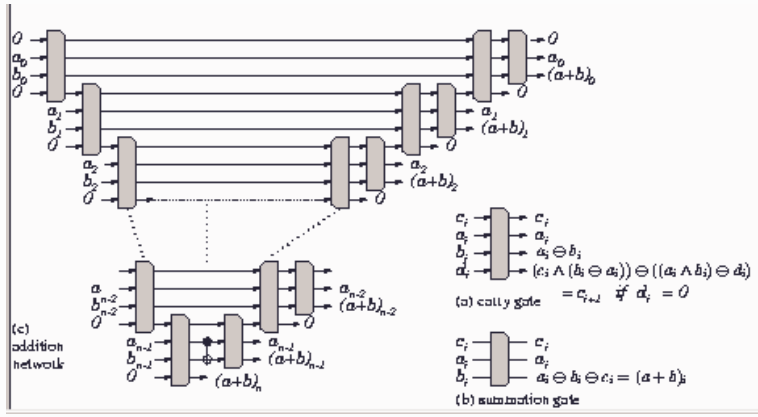
α_y ist die Amplitude, die man durch die Projektion von v erhält, wenn der Ausgang auf y gesetzt ist.
$pi_x(y) = |\alpha_y|^2$ ist die zugehörige Wahrscheinlichkeit und
$\{pi_x \mid x \in \{0,1\}^n\}$ ist die von C erzeugte Verteilung.

Arithmetische Schaltkreise

- Die zwei grundlegendsten Probleme sind das Design von Additionswerken (a,b) -> (a,a+b)
  und Modulo-Addition (a,b) -> (a, (a+b) mod N) von n-bit Zahlen a und b mit $N = 2^n$.
- Mit einem einfachen Carry Gatter und einem Summationsgatter lässt sich ein Additionswerk designen.
- 1. Phase
  alle carry Bits werden unter Verwendung der n Carry Gatter berechnet

  2. Phase
  -speichern $a_{n-1} \oplus b_{n-1}$ in b_{n-1} mittels XOR Gatter
  -alle restlichen $(a+b)_i$ bit berechnen und alle carry bits auf 0 setzen
  für alle i = n-2,...,0
- Anordnungsumkehrung ergibt äquivalentes Subtraktionswerk.

Additionsnetzwerk



Quantenparallelismus

- Parallelismus ist die physikalische Grundlage des Funktionsprinzips eines Quantencomputers.
- Jedes mögliche Ergebnis muss in irgendeiner Art und Weise bereits in diesem verschränkten Zustand enthalten sein.
- Wichtig:Verschränkung muss erhalten bleiben.

  d.h. Qregister muss in Superpositionszustand sein.

  keine Messung während der Rechnung.
- Problem: Handhabung des berechneten Resultats

  Messung reduziert Informationsgehalt auf die Eigenzustände

Quantenparallelismus 2

- Lösung: Verschränkung mehrerer Qubits
- Exponentielle Zunahme des Informationsgehalts
- Damit sind alle Endzustände des Problems bereits im Quantensystem vorhanden
- Klassische Computer kann nur einen Zustand in einem Zeitpunkt annehmen (das Problem nur seriell bearbeiten)
- Herausforderung: Steuerung des Systems ohne zwischenzeitlichen Eingriff.
- Fazit: Der einzige Vorteil von Quantencomputer liegt in der Ausnutzung der quasiparallelen Verarbeitung von Informationen durch den Quantenparallelismus

Physikalische Grenzen

- Register nicht fehlerfrei realisierbar: Zeitpropagation *nicht* völlig kohärent.
- Gatter nicht perfekt realisierbar:
- Oft nur näherungsweise Umsetzung möglich
- Unterschied zu klassischen Schaltungen:
  - In klassischen Schaltungen korrigiert rücktreibender Effekt Abweichungen von den 0,1 - Zuständen.
  - Quantenmechanisch aufgrund der gewünschten Unitarität und Nutzen von Überlagerungen so nicht möglich!
- Ein n-qubit Register scheint in der Lage zu sein, exponentiell mehr Informationen als ein klassisches n-bit Register zu speichern. Wegen der Fehlertoleranz ist die maximale Kapazität beschränkt (Holevo-Theorem)

Fehlerkorrektur

Für ein klassisches Bit:

3-fache Redundanz korrigiert bel. Fehler an einem Bit.

Quantenmechanisch:

für ein Qubit mindestens 5-fache Redundanz nötig.

Beispiel (DiVincenzo):

$$
\begin{aligned}
|0\rangle_L = |00000\rangle \;&+\; |11000\rangle + |01100\rangle + |00110\rangle + |00011\rangle + |10001\rangle \\
&-\; |10100\rangle - |01010\rangle - |00101\rangle - |10010\rangle - |01001\rangle \\
&-\; |11110\rangle - |01111\rangle - |10111\rangle - |11011\rangle - |11101\rangle \\
|1\rangle_L = |11111\rangle \;&+\; \ldots
\end{aligned}
$$

Fazit

- Quantenregister spannen hochdimensionale Hilberträume auf
- Quantengatter stellen ein effektives Konzept dar
- Bereits realisiert: universelle 2-Bit Gatter.
- Fehlerfreie Quantenregister und -gatter physikalisch nicht realisierbar, Fehlerkorrektur jedoch möglich
- -> Quantencomputer *prinzipiell* realisierbar

Ende

Vielen Dank

für ihre Aufmerksamkeit

Quellen

- Textbuch von J. Gruska. Quantum Computing. McGraw-Hill, 1999.
- Die physikalische Realisierung von Quantencomputern (Christina Hölzer, TU-Darmstadt)
- Quantenregister & Quantengatter (Oliver Schulz) fuj.physik.uni-dortmund.de/~suter/Seminare/QC_Seminar_SS00/QuantenGatter.pdf
- www.informatik.uni-leipzig.de/~der/Vorlesungen/register.gatter.ps