Freie Universität Berlin
Institut für Informatik

Seminar über Algorithmen für Quanten-Computer

Vortrag Nr. 4
Quantenbits, -gatter, -register

Jörg Meltzer
& Axel Steinacker

Inhalt

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

Das Bit wird als skalarer Wert realisiert, z.B. durch Spannung/Magnetisierung in einem Speicherelement. Dieser Wert kann je nach Zustand als 0 oder 1 interpretiert werden.

Daraus ergibt sich eine zweielementige Bitmenge $B = \{0,1\}$

Die Anzahl von n Bits würde man demnach so schreiben: $B^n = B \times B \times .. \times B$

Vektordarstellung der Bits

Man kann das Bit auch in der, für uns besser zu gebrauchenden Notation als Vektor schreiben:
B = $\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\}$.

Um nun aber mit den für Quantencomputer mathematischen Räumen, hier der Hilbertraum, rechnen zu können, werden wir die Vektoren in der sog. Ket –Schreibweise notieren:
B = $\{|0\rangle,|1\rangle\}$, wobei die Entsprechungen hier verdeutlicht werden

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

Daraus folgt, Wörter aus 2 Bits durch die Elemente des Kartesischen Produktes gegeben sind.

B x B = {00,01,10,11}

Vektordarstellung der Bits 2

Nun ein kleiner Ausflug in die Welt der Vektorrechnung: Das Tensor Produkt. Man beachte das quadratische Wachstumsverhalten der Ergebnismatrix.

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:

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

Vektordarstellung und Register

Mit den neuerworbenen Kenntnissen ist:

$$B \times B = \left\{ \begin{pmatrix} \mathbf{1} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \end{pmatrix}, \begin{pmatrix} \mathbf{0} \\ \mathbf{1} \\ \mathbf{0} \\ \mathbf{0} \end{pmatrix}, \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{0} \end{pmatrix}, \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{1} \end{pmatrix} \right\}$$

$$|0\rangle_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |1\rangle_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|2\rangle_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |3\rangle_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

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

Man schreibt aber abgekürzt:

Somit kann man B x Bauch als $\{|0\rangle_2, |1\rangle_2, |2\rangle_2, |3\rangle_2\}$ schreiben

Ein Register allgemein beschreibt man wie folgt:

$$|q1\rangle \otimes |q2\rangle \otimes |q3\rangle \otimes \ldots \otimes |qn\rangle = |q1\,q2\,q3 \ldots qn\rangle$$

Elemente des Quantencomputers

NOT Gatter

Not ist reversible, also umkehrbar. Ich weiß also hinter dem Gatter noch, was ich vorne

reingesteckt habe.

Die doppelte Verneinung bringt das ursprüngliche Ergebnis.

$$\text{NOT} \quad |0\rangle = |1\rangle \;, \quad \text{NOT} \quad |1\rangle = |0\rangle \qquad \text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Spezielle Reversible Gatter

$$B^n \rightarrow B^m$$

Reversibles Rechnen bei Funktionen mit m<n

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

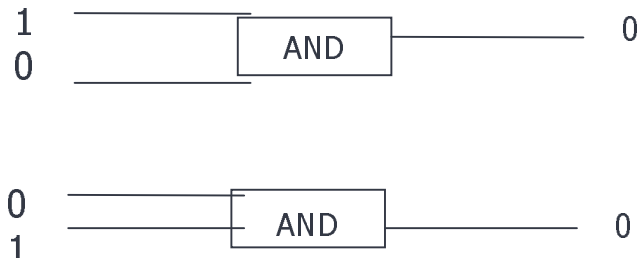
$$\text{XOR}\,|q1\rangle \otimes |q2\rangle = |q1\rangle \otimes |q1+q2\rangle \text{ , } q_i \in \{0,1\}$$

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

Beispiel:

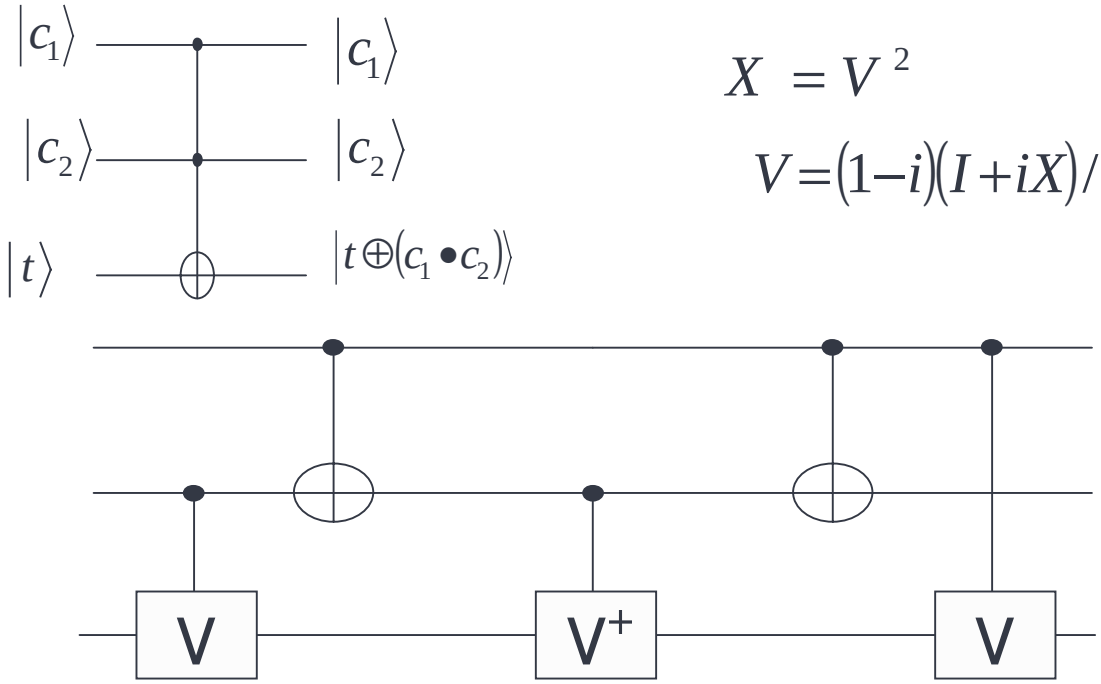
Das CNOT – Gatter wirkt auf 2 Bitsysteme: das hintere Bit wird geändert, wenn das vordere Bit gesetzt (wahr) ist.

AND Gatter



AND ist nicht umkehrbar. Wir können hinter dem Gatter nicht mehr darauf schließen, welche Werte vorne, in welcher Reihenfolge reingesteckt wurden.
Es gibt keine Irreversiblen Rechnungen beim Quantencomputer, damit der Anfangszustand nicht verloren gehen kann, der ja im Ergebnistupel enthalten ist.

Toffoli Gatter



$$X = V^2$$

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

Es werden zwei Typen von elementaren Gattern verwendet:
Die Hadamardtransformation H, die lokal auf die entsprechenden Leitungen ausgeführt wird und das Toffoli Gatter, das als reversibles Analogon zur klassischen UND-Verknüpfung angesehen werden kann.
Es wirkt auf eine 3-Qubit-System: das letzte Bit wird geswappt, wenn das 1. und 2. Bit wahr sind.

Fredkin Gatter

Kontrolliertes Bit-Swapping-Gatter:

Das Fredkin Gatter wirkt auch auf 3 Bit-Systeme, aber werden hier die vorderen Bits geswappt, wenn das hinterste (letzte) gesetzt wird.

Ionenfallen (Ion Traps)

Um ein Quantenbit zu erzeugen werden Atom- und Kernzustände benutzt.
Geladene Atome (Ionen) werden isoliert, indem sie in elektromagnetischen Traps gefangen gehalten werden.
Die Rotation der Atome (ihrer Elektronenhülle) wird nahezu angehalten, d.h. es dreht sich nur noch der Atomkern selber. Das Atom hat nur noch „Spinenergie“.
Mit Hilfe von monochromatischem Licht können Spinzustände geändert werden
Dieser Spin ist das Quantenmechanische Objekt in dem wir den quantenmechanischen Zustand speichern.

Das gemeine Qubit

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

$|\uparrow\rangle$ = $|0\rangle$ oder $|\downarrow\rangle$ = $|1\rangle$ an. Das System „kollabiert“ sozusagen.

Upspin Downspin

Unbeobachtet ist er aber eine Überlagerung der beiden Zustände

$$|\cdot\rangle = \frac{1}{\sqrt{2}}(|\downarrow\rangle + |\uparrow\rangle)$$

Der Punkt heißt, es ist weder ein Up – noch ein Downspin.

Qubits & QRegister

Einzelnes Qubit allgemein: $|\psi\rangle = \alpha\,|\downarrow\rangle + \beta\,|\uparrow\rangle$

Normierung: $|\alpha|^2 + |\beta|^2 = 1$

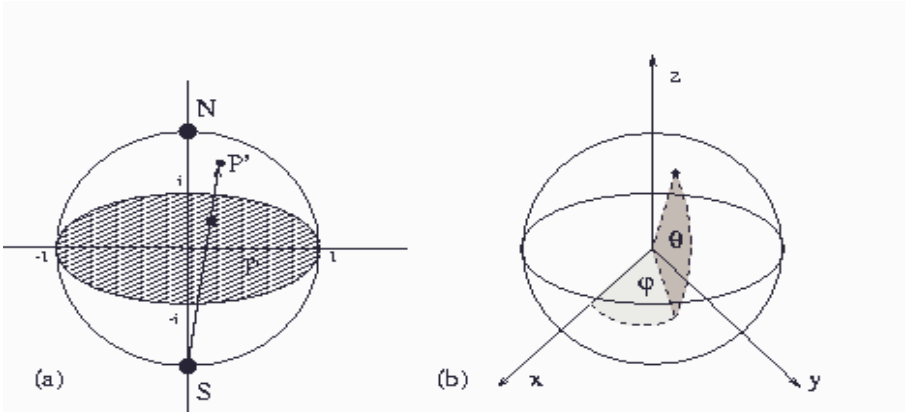
Vektordarstellung: $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

Quantenregister: Direktes Produkt mehrerer Qubits

$$|\psi_1\psi_2\psi_3..\psi_n\rangle \equiv |\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle \in \mathrm{H}_n$$

Wichtig: dim(H_n) = 2^n
Klassische Register dim(Z_2^n)=n
Zu beachten ist, wie bereits weiter oben erwähnt, die Matrizen wachsen exponentiell, im klassischen nur linear (n Bits in n Registern). Hier kann ich aber mit einem n Bit breiten Register 2^n klassische Werte darstellen.

Riemann & Bloch Sphäre



Ein Weg den Zustand eines Qubits zu repräsentieren, ist als Punkt auf der Oberfläche einer Einheits-Riemann-Sphere (links). Dort entsprechen Nord und Süd den klassischen Bitwerten 0 und 1.

Ebenso als Punkt auf einer Bloch-Sphere (rechts) unter Verwendung des spherischen Koordinatensystems. Dieses basiert auf dem Fakt, das jedes Qubit als cos $\theta/2|0\rangle + e^{i\phi} \sin \theta/2|1\rangle$ dargestellt werden kann.

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 überabzählbar groß ist.
Es drängt sich die Frage auf, ob solch große unitäre Matrizen in mehrere kleinere, besser zu handhabende, transformiert werden können.

Kohärenzgatter

Kohärenzgatter = $\sqrt{NOT}$

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

Wird verwendet, um einen klassischen Zustand 0 in ein Quantenbit (kohärenter Quantenzustand) zu überführen. Bewirkt eine Drehung des Urspin um 90°. Doppelt ausgeführt, ergibt sich somit die Negation des Ursprungszustandes.

Phasenschieber

$$P = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon \end{pmatrix}, \qquad |\varepsilon|^2 = 1$$

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

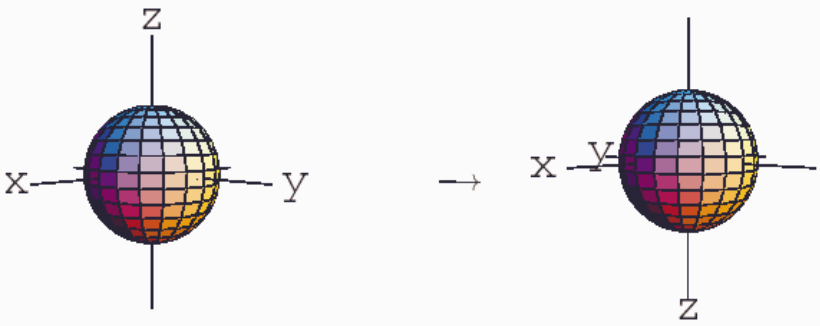


Abbildung 3: Bewegung eines quantenmechanischen Spins. Bsp. 1: Rotation um x–Achse mit Winkel 180°. Diese vertauscht Nord- und Südpol und entspricht auf B einer Negation.

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

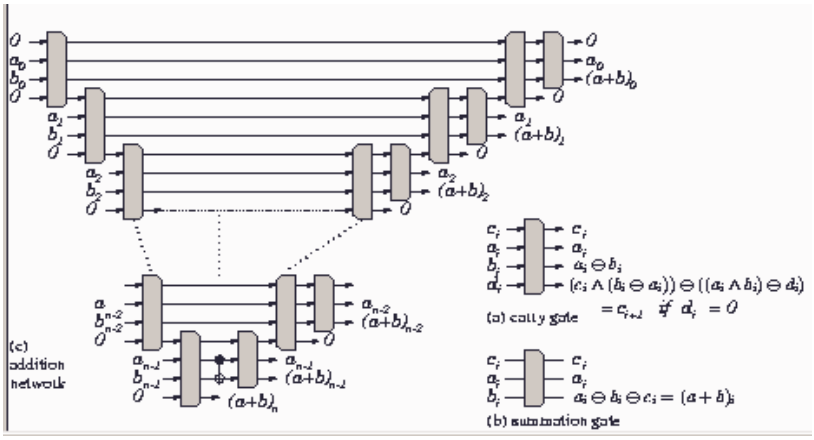
$$\mathbf{v = \sum_{y \in \{0,1\}^m} \alpha_y |y>,}$$

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

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

So schön das Thema auch anmuten mag, noch hat es seine Grenzen und die sind physikalischer Natur. Die QRegister sind nicht fehlerfrei realisierbar: Zeitpropagation *nicht* völlig kohärent.
Auch die Gatter sind 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 ist das 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

Quellen

Folgende Quellen wurden zur Erstellung dieser Arbeit verwandt:

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