Hauptseminar Quantencomputer SS2003
Quantenschaltkreise

Martin Ratajczak

12. Mai 2003

Inhaltsverzeichnis

1 Zusammenfassung

Im folgenden Artikel werden klassische Gatter und Quantengatter verglichen, Qubits und Quantenregister eingeführt, ihre spezifischen Eigenschaften herausgestellt und mit Beispielen erläutert. Es wird auf den Messprozess eingegangen. Schließlich wird die Simulation von Quantengattern auf einer QTM angesprochen und die Universalität von bestimmten, endlichen Mengen von Gattern gezeigt. Zuletzt werden die arithmetischen Gatter beschrieben.

2 Klassische reversible Gatter

2.1 Motivation

Das grösste Hindernis zur Miniaturisierung von klassischen Computern ist das zweite termodynamische Gesetz, d.h. irreversible Zustandsänderungen produzieren Wärme. Nach Landauer's Prinzip gilt: Um 1 Bit klassischer Information zu löschen, muss man 1-Bit-Entropie an die Umgebung abgeben (meist in Form von Wärme).
NOT und AND oder nur das NAND Gatter sind universell. Das bedeutet, dass diese Gatter ausreichen, um Schaltkreise für jede beliebige boolsche Funktion

$$f \in \mathcal{B}_n^m = \{g | g : \{0,1\}^n \to \{0,1\}^m\}$$

zu konstruieren. Jedoch sind das AND und das NAND Gatter irreversible boolsche Operationen, d.h. aus dem Output lässt sich nicht auf den Input schließen.

2.2 Klassische reversible Gatter

Nach Definition lässt sich aus dem Output eines reversiblen Gatters auf den Input schließen. Mit dem NOT, CONTROL NOT(CNOT) und
CONTROL CONTROL NOT(CCNOT,Toffoli Gatter)

$$T_2(a,b,c) = (a, b \oplus (a \wedge c), c),\ T_3(a,b,c) = (a, b, b \oplus (a \wedge b))$$

lassen sich beliebige reversible boolsche Funktionen in $\mathcal{B}_n^m$, $n \geq 3$ konstruieren.
Das Fredkin Gatter

$$F(a,b,c) = (a, ab \vee \overline{a}c, \overline{a}b \vee ac)$$

ist ebenfalls universell und reversibel.

Beweis der Universalität der Fredkin und Toffoli Gatter:
Toffoli Gatter:
$a = 1 \Rightarrow b' = b \oplus c$;
$b = 0 \Rightarrow b' = a \wedge c$;
$a = 1 \wedge c = 1 \Rightarrow b' = \overline{b}$

Fredkin Gatter:
$c = 0 \Rightarrow b' = a \wedge b$;
$b = 0 \wedge c = 1 \Rightarrow b' = \overline{a}$
Damit ist bewiesen, dass AND und NOT Gatter mit Fredkin und Toffoli Gattern realisierbar sind, folglich sind sie auch universell.

2.3 Reversible boolsche Funktionen

Für eine Funktion
$$f : a \rightarrow f(a)$$
existiert nicht immer eine reversible Berechnung.
Für die Funktion
$$f_0 : a \rightarrow (a, f(a))$$
existiert eine reversible Berechnung, im Spezialfall einer boolschen Funktion hat sie folgende Form:

$$f_0 : (x, b) \rightarrow (x, b \oplus f(x)).$$

Diese Resultate werden in heutigen reversiblen CMOS Prozessoren verwendet, bei welchen mehr oder weniger Dissipation entsteht.

3 Qubits und Register

3.1 Qubits

Definition: Ein Qubit (quantum bit) ist ein Quantenzustand

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle,$$

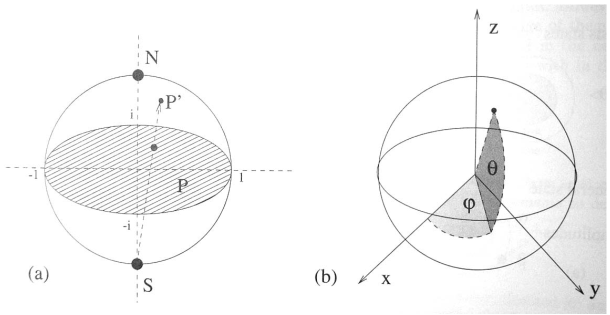
wobei $\alpha, \beta \in \mathbb{C}$ und $|\alpha|^2 + |\beta|^2 = 1$.
$\mathcal{B} = \{|0\rangle, |1\rangle\}$ ist die Orthonormalbasis (Standardbasis) eines zweidimensionalen Quantensystems.

Oft verwendet man auch eine duale Basis

$$\mathcal{D} = \{|0'\rangle, |1'\rangle\} : |0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1'\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Ein Qubit besteht bekanntlich aus einem 2-Zustands-Quantensystem. Denkbar wären auch Mehr-Zustands-Quantensysteme. Ob diese Verallgemeinerung bei Quantencomputern einen Vorteil bringt, ist unerforscht.

Ein Qubit kann mit Hilfe einer Riemann Kugel und einer Bloch Kugel grafisch dargestellt werden.



Aus einer Projektionsmessung kann man nur ein klassisches Bit an Information extrahieren, obwohl ein Qubit unendlich viele Quantenzustände repräsentiert. Misst man eine Observable E_0, die dem Zustand $|0\rangle$ entspricht, so mißt man in der Standardbasis das klassische Bit 0 mit Wahrscheinlichkeit $|\alpha|^2$ und das Qubit kollabiert in den Zustand $|0\rangle$.
Die Messung in der Standardbasis entspricht dem Projektionsoperator

$$\frac{1}{2}(I \pm \sigma_z), \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

3.2 Qubit-Evolution

Die Evolution eines Qubits wird durch eine unitäre Matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

bestimmt und führt zum folgenden Zustand:

$$(a\alpha + b\beta)\,|0\rangle + (c\alpha + d\beta)\,|1\rangle\,.$$

Beispielsweise wird mittels der Hadamard Matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

eine Hadamard Transformation ausgeführt, die die Standardbasis in die Dualbasis überführt:

$$H\left|0\right\rangle = \left|0'\right\rangle, H\left|0'\right\rangle = \left|0\right\rangle, H\left|1\right\rangle = \left|1'\right\rangle, H\left|1'\right\rangle = \left|1\right\rangle oder H\left|i\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + (-1)^i \left|1\right\rangle).$$

Es gilt: $H^2 = I$

Wendet man

$$H' = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

auf die Standardbasis

$$H'^2\left|0\right\rangle = -\left|1\right\rangle, H'^2\left|1\right\rangle = \left|0\right\rangle$$

an, verhält sie sich wie die NOT-Operation bis auf ein Vorzeichen.

Theorem:
Jede unitäre Matrix U vom Grad 2 kann in folgender Form geschrieben werden:

$$U = e^{i\gamma} \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \begin{pmatrix} cos(\theta) & i\,sin(\theta) \\ i\,sin(\theta) & cos(\theta) \end{pmatrix} \begin{pmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix}.$$

Beweis:

Multipliziert man die obere Matrix aus, erhält man:

$$U = \begin{pmatrix} e^{i(\alpha+\beta+\gamma)}cos(\theta) & e^{i(\alpha-\beta+\gamma)}i\,sin(\theta) \\ e^{i(-\alpha+\beta+\gamma)}i\,sin(\theta) & e^{i(-\alpha-\beta-\gamma)}cos(\theta) \end{pmatrix}$$

und

$$U^+ = \begin{pmatrix} e^{-i\gamma}cos(\theta)e^{-i(\alpha+\beta)} & -ie^{-i\gamma}sin(\theta)e^{i(\alpha-\beta)} \\ -ie^{-i\gamma}sin(\theta)e^{-i(\alpha-\beta)} & e^{-i\gamma}cos(\theta)e^{i(\alpha+\beta)} \end{pmatrix}$$

daraus folgt $UU^+ = 1 \Leftrightarrow$U ist eine unitäre Matrix.

3.3 2-Qubit Register

Ein 2-Qubit Register ist ein Tensorprodukt aus 2-Qubits.
Die Standardbasis eines 2-Qubit Registers hat folgende Form:

$$|0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad |1\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|2\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \qquad |3\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Ein Zustand eines 2-Qubit Quantenregisters hat folgende Form:

$$|\Psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle\,, |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

Die Messung des Zustandes $|\Psi\rangle$ zur Standardbasis ergibt 2 Bits ij mit Wahrscheinlichkeit $|\alpha_{ij}|^2$ und kollabiert in den Zustand $|ij\rangle$.

Möchte man nur das erste (das zweite) Qubit messen, muss man zur Basis $\{|i0\rangle\,, |i1\rangle\}, i = 0, 1$ messen. Die Wahrscheinlichkeit für das Ergebnis Bit 0 ist $|\alpha_{00}|^2 + |\alpha_{01}|^2$ und der nachfolgende Zustand hat folgende Form:

$$|\Psi\rangle = \frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

Beispiel einer Evolution eines 2-Qubits ist die unitäre Transformation

$$XOR : |x, y\rangle \rightarrow |x, x \oplus y\rangle$$

und kann mit folgender Matrix dargestellt werden:

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

Die XOR Matrix stellt das CNOT Gatter dar, es gibt jedoch unendlich viele Darstellungen:

$$|x, y\rangle \rightarrow e^{i\theta}\,|x, x \oplus y\rangle\,,\ mit\,\theta = 2\pi k,\ k = 0, 1, \ldots.$$

3.4 No-Cloning (copying) Theorem

Theorem:

Ein unbekannter Quantenzustand kann nicht kopiert werden, d.h. es existiert keine unitäre Transformation U, so dass für ein 1-Qubit Zustand $|\Psi\rangle$ folgt:

$$U(|\Psi 0\rangle) = |\Psi\Psi\rangle \ (*).$$

Beweis:

Sei U eine unitäre Transformation mit obiger Eigenschaft(*), $|\alpha\rangle, |\beta\rangle$ seien zwei verschiedene orthogonale Zuständ und

$$U(|\alpha 0\rangle) = |\alpha\alpha\rangle, U(|\beta 0\rangle) = |\beta\beta\rangle, |\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle).$$

Dann gilt:

$U(|\gamma 0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\alpha\rangle + |\beta\beta\rangle)$
$\neq |\gamma\gamma\rangle = |\gamma\rangle |\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)\frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)$
$= \frac{1}{2}(|\alpha\alpha\rangle + |\alpha\beta\rangle + |\beta\alpha\rangle + |\beta\beta\rangle).$ $\square$

Das No-Cloning Theorem besagt nur, dass keine unitäre Transformation für das perfekte Kopieren eines Quantenzustandes existiert ohne das Original zu zerstören.
Man kann jedoch einen Quantenzustand teleportieren, d.h. ein Quantenzustand wird von einem Ort zu einem anderen transportiert, wobei das Original zerstört wird.

3.5 n-Qubit Register

Die Standardbasis eines n-Qubit Registers ist das Tensorprodukt von n Qubits:

$$\mathcal{B} = \{|i\rangle \, | i \in \{0,1\}^n\} = \{|i\rangle \, | 0 \leq i < 2^n\}.$$

Ein Zustand eines n-Qubit Registers hat folgende Form:

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i \, |i\rangle \, , \, \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

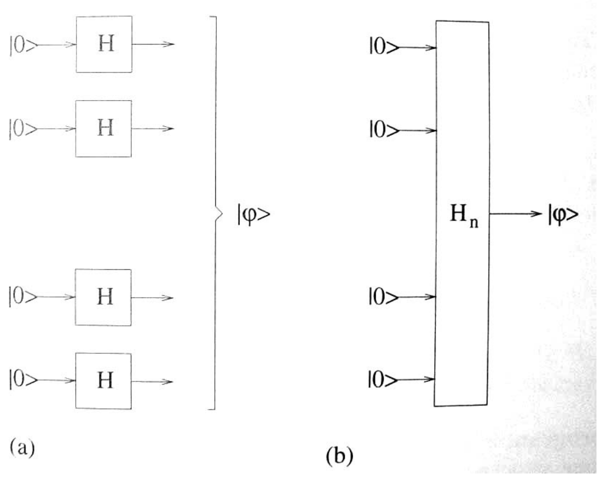
Die Zahl der Zustände und die Grösse der Superpositionen wachsen exponentiell mit der Anzahl der Qubits.
Ein n-Qubit Register kann exponentiell mehr Information speichern als ein n-Bit Register, jedoch kann man maximal n Bit aus einem n-Qubit Register verlässlich durch Messung wiederherstellen.

Beispiel:
Die Hadamard Transformation H_n transformiert zwischen der Standard- und der Dualbasis:

$$H_n = \bigotimes_{i=1}^{n} H,$$

$$H_n \, |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{xy} \, |y\rangle \, .$$

Durch Anwendung von H auf die einzelnen Qubits des QRegisters $|0^{(n)}\rangle$ kann man in linearer Anzahl von Operationen eine gleichgewichtete Superposition von Basiszuständen erzeugen.



4 Quantenschaltkreise

4.1 Quantengatter

Definition:
Ein Quantengatter mit n Inputs und n Outputs wird durch einen unitären Operator

$$U : \mathcal{H}_{2^n} \rightarrow \mathcal{H}_{2^n}$$

bestimmt und wird durch eine unitäre Matrix vom Grad 2^n repräsentiert, wobei $\mathcal{H}_{2^n}$ das 2^n-fache Tensorprodukt des Hilbertraumes darstellt.

Definition:
Ein Quantenschaltkreis ist eine Menge von azyklisch verbundenen Quantengattern. Die Größe und Tiefe der Schaltkreise stellt die Anzahl der Knoten und die Tiefe des Graphen dar.

Die Quantenverdrahtungen sind nur im übertragenen Sinne zu verstehen, in Wirklichkeit existieren auf dem Quantenniveau keine Verdrahtungen. Effekte wie z.B. Feldinteraktionen zwischen Qubits stellen eine "Verdrahtung" her.
Quantengatter können durch "Wahrheitstafeln" der Zustände beschrieben werden und aufgrund der Linearität kann man den Output aller möglichen Inputs beschreiben.

Beispiele:
Hadamard Gatter repräsentiert durch Matrizen:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$H' = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$
$$H'' = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Rotationsgatter:

$$R_x(\theta) = \begin{pmatrix} cos(\theta) & i\,sin(\theta) \\ i\,sin(\theta) & cos(\theta) \end{pmatrix}$$
$$R_y(\theta) = \begin{pmatrix} i\,cos(\theta) & sin(\theta) \\ sin(\theta) & i\,cos(\theta) \end{pmatrix}$$
$$R_z(\theta) = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

Diese Gatter werden bei der Konstruktion des Deutsch Gatters verwendet.

Inverse XOR Gatter:

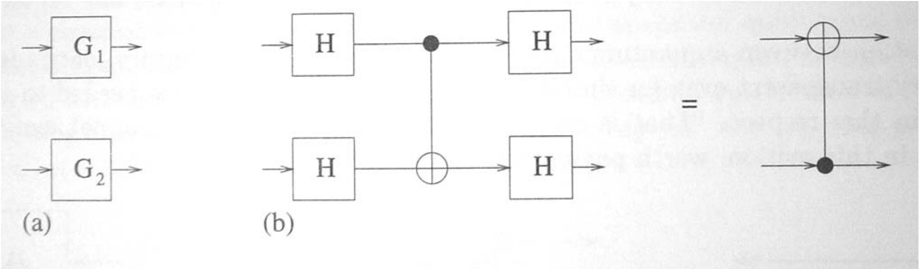


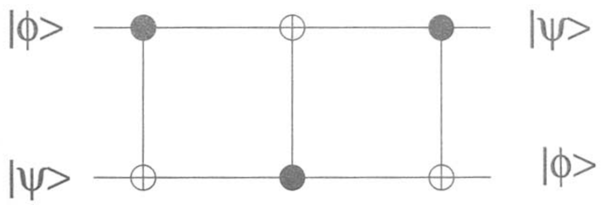
Figure 2.11: An implementation of the inverse of the XOR gate.

$|01\rangle \rightarrow^{H-Gatter} \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle)$
$\rightarrow^{XOR-Gatter} \frac{1}{2}(|00\rangle + |11\rangle - |01\rangle - |10\rangle)$
$\rightarrow^{H-Gatter} |11\rangle$

Definition von NOT,XOR und CCNOT bei Quantencomputern:

$NOT : |a\rangle \rightarrow |\overline{a}\rangle$
$XOR = CNOT : |a, b\rangle \rightarrow |a, a \oplus b\rangle$
$CCNOT : |a, b, c\rangle \rightarrow |a, b, (a \wedge b) \oplus c\rangle$

Vertauschen der Qubits:



Permutationsschaltkreis:

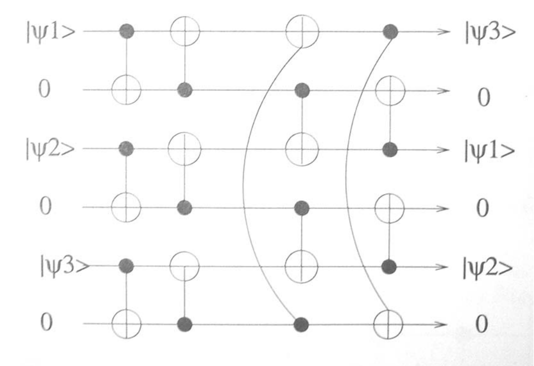


Figure 2.15: Permutation circuit

4.2 Simulation von Quantenschaltkreisen durch eine Quanturingmaschine (QTM)

Definition:
Jedem Quantenschaltkreis C mit Input-Variablen $x_1, \ldots, x_n$ und Output-Variablen $y_1, \ldots y_m, m \leq n$ wird für jeden Input $x \in \{0,1\}^n$ die Wahrscheinlichkeitsverteilung ρ_x über $\{0,1\}^m$ definiert durch:

$$v = \sum_{y \in 0,1^m} \alpha_y \left| y \right\rangle, \, \pi_x(y) = |\alpha_y|^2.$$

Wobei $\{\pi_x | x \in 0, 1^n\}$ die Wahrscheinlichkeitsverteilung induziert durch den Schaltkreis C ist.

Es stellt sich die Frage:
Kann eine QTM durch einen Quantenschaltkreis simuliert werdem wie bei klassischen Computern? Ja.

Definition:
Ein Quantenschaltkreis C mit n Inputvariablen (n,t)-simuliert eine QTM M, wenn für jedes $x \in \{0,1\}^n$ die Wahrscheinlichkeitsverteilung ρ_x indiziert durch C mit der Wahrscheinlichkeitsverteilung der Konfigurationen von M nach t Schritten mit x als Input übereinstimmt.

Theorem:
Wenn M eine QTM ist und $n, t \in N^{\geq 0}$, dann existiert ein boolscher Quantenschaltkreis C der Größe (Anzahl der Gatter) polynomiell in n und t, so dass M (n,t)-simuliert wird.

4.3 Quantenprogramme und Messgatter

Definition:
Ein Quantenprogramm ist ein Quantenschaltkreis mit Messgattern(am Ende).

Beispiel:

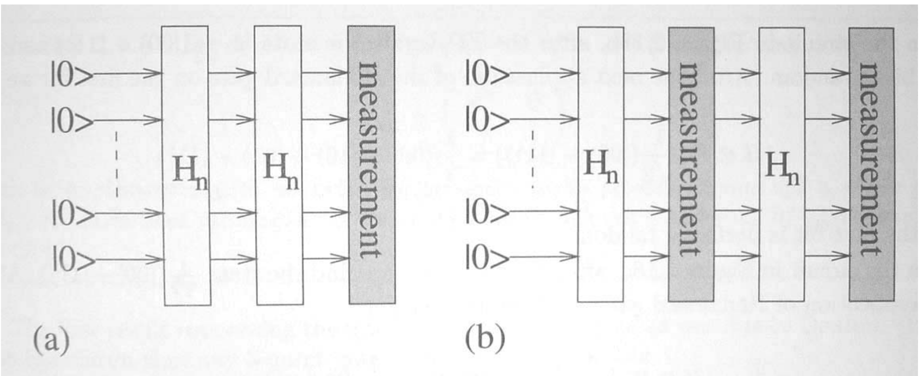
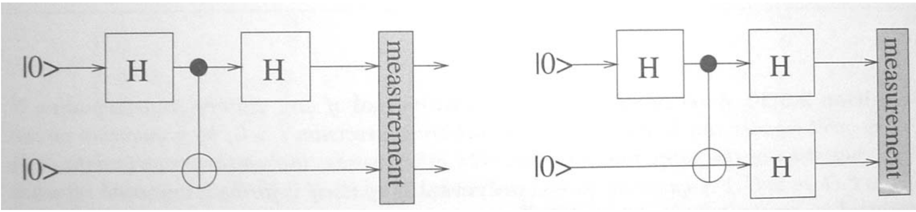


Figure 2.17: Measurement gates and their role

Eine Hintereinanderschaltung von $H_n, Messgatter, H_n, Messgatter$ auf $|0^n\rangle$ erzeugt einen gleichverteilten n-Bit String mit Wahrscheinlichkeit $\frac{1}{2^n}$.

Theorem: Es ist möglich ein Zufallsergebnis zu generieren ohne zwischendurch zu messen:



Beweis:
1.Schaltkreis:

$$|00\rangle \rightarrow^{H\oplus I,\,XOR} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow^{H\oplus I} \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle)$$

1.Schaltkreis:

$$|00\rangle \rightarrow^{H\oplus I,\,XOR} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow^{H\oplus H} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

4.4 Universalität von Quantengattern

Der Unterschied zwischen klassischen Computern und Quantencomputern ist, dass es eine unendliche Anzahl für n Input und Output Quantengatter gibt. Es stellt sich die Frage: Lassen sich alle größeren unitären Matrizen durch eine kleine Anzahl von unitären Matrizen von kleinem Grad konstruieren?

Definition:
Eine Matrix M ist eine ϵ-Approximation von U, wenn

$$\|U - M\| \leq \epsilon.$$

Definition:
Eine Menge von Quantengattern G ist universell, wenn eine beliebige unitäre Transformation U auf ein Qubit-Register mit einer beliebigen Präzision $\epsilon > 0$ durch einen Quantenschaltkeis $C_{U,\epsilon}(G)$ approximiert werden kann.

Ein Quantengatter ist universell,wenn es selbst eine universelle Menge von Gattern beschreibt, die auf $|0\rangle, |1\rangle$ angewendet werden.

Beispiel:

Φ_0 sei ein irrationaler Bruchteil von π.
Mit
$U_\Phi = \begin{pmatrix} e^{i\Phi} & 0 \\ 0 & 1 \end{pmatrix}$,
kann jedes beliebige Gatter approximiert werden.

Beispiel: Deutsch Gatter

Theorem:
Jedes 3-qubit Gatter mit einer unitären Matrix

$$D(\theta) = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{R}_y(\theta) \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{1} & & & \mathbf{0} & \\ & 1 & 0 & 0 & 0 \\ \mathbf{0} & 1 & 1 & 0 & 0 \\ & 0 & 0 & i\,cos(\theta) & \mathbf{s}in(\theta) \\ & 0 & 0 & sin(\theta) & i\,cos(\theta) \end{pmatrix}, mit\,\theta\ irrational$$

ist universell.

Beispiel: Matrizen von Sleater und Weinfurter

$$S(\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{\frac{i\pi}{4}} cos\frac{\pi\tau}{2} & e^{\frac{-i\pi}{4}} sin\frac{\pi\tau}{2} \\ 0 & 0 & e^{\frac{-i\pi}{4}} sin\frac{\pi\tau}{2} & e^{\frac{i\pi}{4}} cos\frac{\pi r}{2} \end{pmatrix},$$

$$S^{-1}(\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{\frac{-i\pi}{4}} cos\frac{\pi\tau}{2} & e^{\frac{i\pi}{4}} sin\frac{\pi\tau}{2} \\ 0 & 0 & e^{\frac{i\pi}{4}} sin\frac{\pi\tau}{2} & e^{\frac{-i\pi}{4}} cos\frac{\pi r}{2} \end{pmatrix}$$

$\Rightarrow$

$$S^2(\tfrac{\tau}{2}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i\, cos\pi\frac{\pi\tau}{2} & sin\pi\frac{\pi\tau}{2} \\ 0 & 0 & sin\pi\frac{\pi\tau}{2} & i\, cos\pi\frac{\pi\tau}{2} \end{pmatrix}$$

$\Rightarrow S^2(\frac{1}{2}) = XOR.$

Mit $S(\frac{\tau}{2})$, $S^{-1}(\frac{\tau}{2})$ und XOR lässt sich ein allgemeines Toffoli Gatter implementieren.

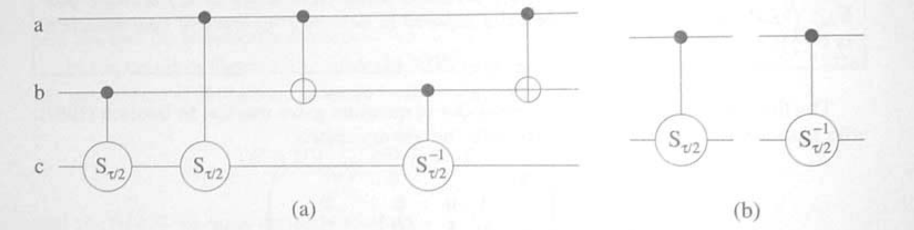


Figure 2.20: A circuit for the Toffoli gate

$S(\tau)$ (mit τ ist ein Vielfaches von π) ist ein universelles 2-qubit Gatter.
Deutsch, Barenco, Ekert und Lloyd zeigten, dass beinahe jedes nichttriviale 2-Qubit Gatter universell ist.

Beispiel:
Das XOR Gatter ist beim Quantencomputing nicht universell, jedoch das XOR Gatter und folgendes 1-Qubit Gatter :

$$\begin{pmatrix} e^{i(\delta+\frac{\alpha}{2}+\frac{\beta}{2})} cos\frac{\theta}{2} & e^{i(\delta+\frac{\alpha}{2}-\frac{\beta}{2})} sin\frac{\theta}{2} \\ -e^{i(\delta-\frac{\alpha}{2}+\frac{\beta}{2})} sin\frac{\theta}{2} & e^{i(\delta-\frac{\alpha}{2}-\frac{\beta}{2})} cos\frac{\theta}{2} \end{pmatrix}$$

.

4.5 Arithmetische Schaltkreise

Mit Hilfe von einem Carry-Gatter, eines Summationsgatters und eines XOR-Gatters lässt sich eine Additionsschaltung konstruieren. Die Umkehrung der Richtung dieses Additionsgatters ergibt ein Subtraktionsgatter für $b \geq a$ und für $b < a$ eine Modulo 2^n-Subtraktion, wobei a und b Input der Gatter ist.

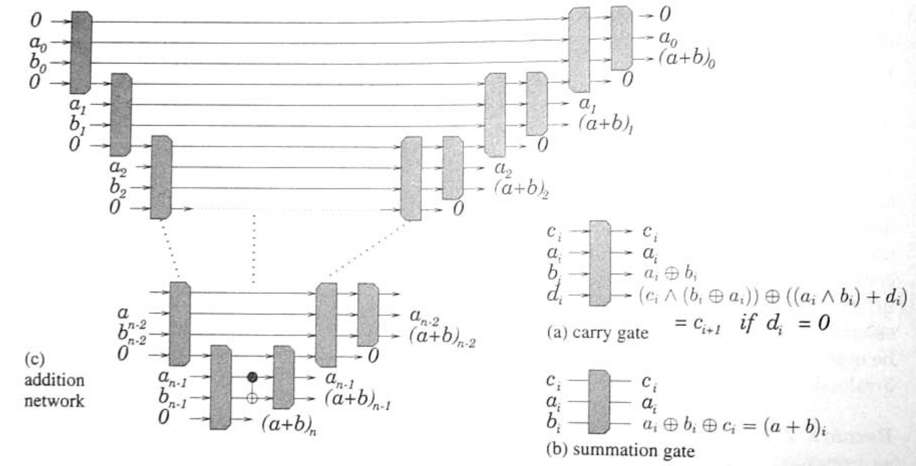
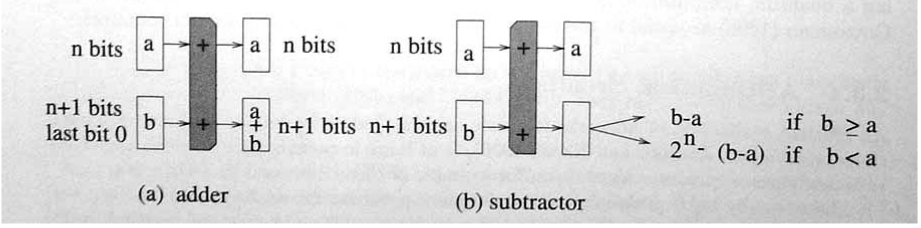


Figure 2.22: Quantum network for binary addition



Die Modulo-Addition lässt sich auf ähnliche Weise konstruieren:

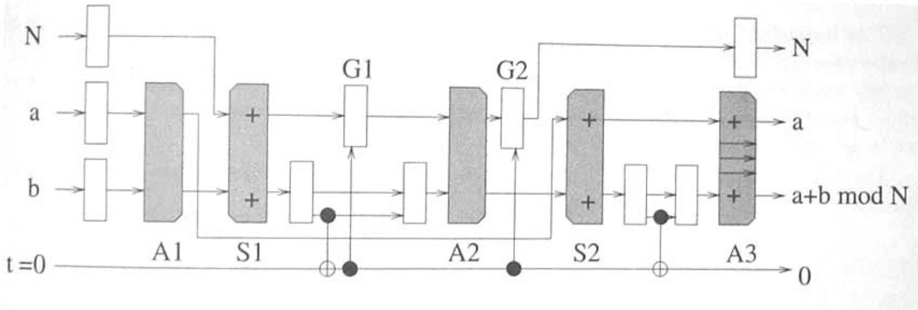


Figure 2.24: A quantum network for modular addition

Die Modulo Multiplikation $f_{a,N}(b) = ab$ lässt sich aus der Addition und Modulo Addition wie folgt zusammensetzen:

$$(b + \ldots + b)\, mod\ N = (\sum_{i=0}^{n-1} a 2^i b_i)\, mod\ N,$$

wobei $N = 2^n$.
Das Potenzieren lässt sich auf ähnliche Weise konstruieren:

$$g_{a,N}(b) = a^b\, mod\, N = a^{\sum_{i=0}^{n-1} b_i 2^i}\, mod\, N = \prod_{i=0}^{n=1} (a^{2^i})^{b_i}\, mod\, N.$$

Literatur

[1] Josef Gruska, Quantum Computing, McGraw-Hill, 1999

[2] Michael A.Nielsen and Isaac L.Chuang, Quanten Computation and Quantum Information, Cambridge University Press, 2000