Vorlesungsmitschrift

Quantencomputer

WS

2002/2003

Prof. Dr. Grädel

Jan Möbius,David Bommes

9. Dezember 2002

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Historischer Überblick

- 1982 Richard Feynman :
  Spekulation über die Möglichkeit, Quantencomputer zu realisieren, welche gewisse Aufgaben effizienter lösen können als klassische Computer.

  inhärente Parallelität in QM-Prozessen
- 1985-93 Deutsch, Bernstein-Vazirani,Yao :
  - Modelle für Quanten-Computer (QTM,Quantum gate arrays)
  - Quanten-Komplexität
  - einfache Algorithmen
- 1994 Peter Shor :
  Polynomzeit Algorithmus für QC um natürliche Zahlen zu faktorisieren. Basis : Quanten-Fourier-Transformation
- 1996 Grover :
  Suchalgorithmus, der eine Nadel in einem Heuhaufen der Größe N in O($\sqrt{N}$) Schritten findet.
- 2001 :
  QC mit 7 Qubit,
  $\rightarrow 15 = 3 \cdot 5$ (Shor)

Probleme :

- Mehr Algorithmen?
- Welche Probleme kann man mit QC effizient lösen?
- kann man QC vernünftiger Größe bauen?

1.2 Experiment

Polarisierungsfilter: polarisieren Licht horizontal, vertikal, bzw. 45°.

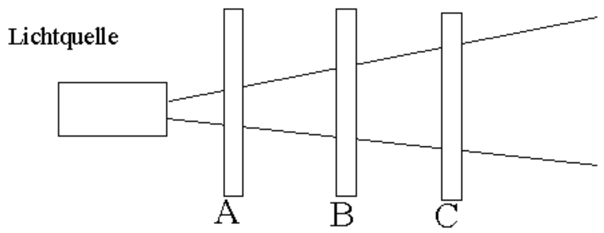

Abbildung 1.1: Experiment

1.2.1 Erklärung

Der Polarisierungszustand eines Photons ist beschrieben durch den Vektor $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\rightarrow\rangle$ in einem zwei dimensionalen Vektorraum mit der Basis $\{|\uparrow\rangle, |\rightarrow\rangle\}$.
Nur die Richtung ist wesentlich $\rightarrow$ Einheitsvektoren $|\alpha|^2 + |\beta|^2 = 1$
Die Basiswahl ist beliebig. Statt $\{|\uparrow\rangle, |\rightarrow\rangle\}$ geht auch $\{|\nearrow\rangle, |\nwarrow\rangle\}$.
(jedes Paar von orthogonalen Einheitsvektoren ist zulässig).

1.2.2 Messung eines Zustandes

Messung : Projektion bezüglich Orthonormalbasis.
Zu einer Messapparatur gehört eine Basis, wie zum Beispiel $\{|\uparrow\rangle, |\rightarrow\rangle\}$.
Die Messung von $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\rightarrow\rangle$ projiziert $|\psi\rangle$ entweder auf $|\uparrow\rangle$ (mit Wahrscheinlichkeit $|\alpha|^2$) oder auf $|\rightarrow\rangle$ (mit Wahrscheinlichkeit $|\beta|^2$). Nach der Messung ist $|\psi\rangle$ zerstört, transformiert in einen Basiszustand. Jede weitere Messung würde das selbe Resultat ergeben.
Zu verschiedenen Messapparaturen gehören verschiedene ON-Basen.

Polarisierungsfilter bezüglich Polarisierung ζ :
Messung des polarisations Zustands $|\psi\rangle$ bezüglich der Basis $\{\sin\zeta|\uparrow\rangle + \cos\zeta|\rightarrow\rangle, \cos\zeta|\uparrow\rangle - \sin\zeta|\rightarrow\rangle\}$

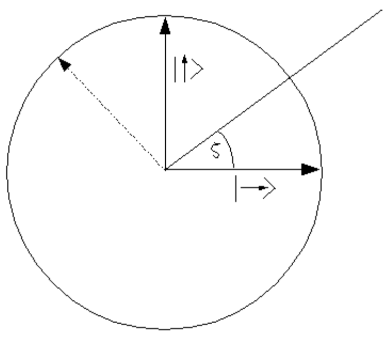

Abbildung 1.2: Messung des Pol. Zustands

Die Photonen, die nach der Messung der Polarisation entsprechen werden durchgelassen, die anderen reflektiert.

- **Filter A :**
  Polarisierung : $|\rightarrow\rangle$
  Basis : $\{|\uparrow\rangle, |\rightarrow\rangle\}$
  50% der Photonen werden auf $|\rightarrow\rangle$ projeziert und durchgelassen.

- **Filter B :**
  Polarisierung : $|\uparrow\rangle$
  Basis : $\{|\uparrow\rangle, |\rightarrow\rangle\}$

- **Filter C :**
  Polarisierung : $|\nearrow\rangle$
  Basis : $\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle), \{\frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle)\}$

  Beachte :

- $|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\nwarrow\rangle)$
- $|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle)$

Filter B reflektiert alle auf $|\rightarrow\rangle$ polarisierten Photonen. Nun setzt man den Filter C zwischen die Filter A und B. C projeziert die Photonen mit dem Zustand $|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle$ mit der Wahrscheinlichkeit $\frac{1}{2}$ auf $|\nearrow\rangle$.
Die durchgelassenen Photonen mit der Polarisierung $|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$ wieder mit Wahrscheinlichkeit $\frac{1}{2}$ auf $|\uparrow\rangle$ projeziert und durchgelassen.

1.3 Einige Grundlagen der QM

1.3.1 Zustände

Zustand : vollständige Beschreibung eines physikalischen Systems.
In QM sind die Zustände Einheitsvektoren in einem Hilbertraum.

1.3.2 Hilbertraum

Hilbert Vektorraum über $\mathbb{C}$, mit einem inneren Produkt
$\langle\cdot|\cdot\rangle : H \times H \to \mathbb{C}$ mit

- $\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^*$
- $\langle\psi|\psi\rangle \geq 0$ und $\langle\psi|\psi\rangle = 0$ gdw. $\psi = 0$
- $\langle\psi|\alpha\varphi_1 + \beta\varphi_2\rangle = \alpha\langle\psi|\varphi_1\rangle + \beta\langle\psi|\varphi_2\rangle$

induzierte Norm : $||\psi|| = \sqrt{\langle\psi|\psi\rangle}$

(Für unendlich-dimensionale Hilberträume ist zusätzlich zu fordern, dass H vollständig ist bezüglich $||\ ||$. Jede Cauchy Folge hat einen Grenzwert in H). **Hier :** (fast) ausschließlich endl.-dimensionale Räume.

1.3.3 Dirac-Notation

$|\psi\rangle$ (ket) (Ausnahme Nullvektor 0 (nicht $|0\rangle$))
$\langle\varphi|$ ist der duale Vektor zu $|\varphi\rangle$ (lra)
$\langle\varphi| : H \to \mathbb{C}$; $|\psi\rangle \mapsto \langle\varphi|\psi\rangle$

1.3.4 Qubits

- **Bit :**
  elementarer Baustein eines klassischen Rechners mit zwei Zuständen (0 1)

- **Qubit :**
  Superpositionen der beiden Basiszustände $|0\rangle$und $|1\rangle$bilden Orthonormalbasis eines Hilbertraums H_2. Ein Qubit ist ein Vektor $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ mit $|\alpha|^2 + |\beta|^2 = 1$.

Die Messung des Qubits ψ führt mit Wahrscheinlichkeit $|\alpha|^2$ zum Zustand $|0\rangle$ und mit Wahrscheinlichkeit $|\beta|^2$ zum Zustand $|1\rangle$. Jede wiederholte Messung führt zum selben Resultat. Obwohl ein Qubit unendlich viele Zustände haben kann, kann man nur ein Bit Information extrahieren. Dieser Extraktionsprozess (Messung) ist probabilistisch.

1.3.5 n-Qubit System (Quantenregister)

Klassisches System mit n Bits hat 2^n Zustände
$0 \to 0, 0 \to 1, \ldots, 1 \to 1$

n-Qubit System hat Basiszustände
$|0-0\rangle, |0-0\rangle, \ldots, |1-1\rangle$
und kann sich in jeder Subposition
$\alpha_0|0-0\rangle + \alpha_1|0-0\rangle + \ldots + \alpha_{2^n-1}|1-1\rangle$
befinden, mit $\sum_{n=0}^{2^n-1} |\alpha_n|^2 = 1$

$H_{2^n} = \underbrace{H_2 \otimes \ldots \otimes H_2}_{\text{n mal}}$

klassisch: Kolineare Systeme mit Zustandsräumen
V mit Basis $v_1, \ldots, v_m$ $\quad V \cap W = 0$
W mit Basis $w_1, \ldots, w_n$
$\rightsquigarrow$ Produktraum $V \times W$ mit Basis $v_1, \ldots, v_m, w_1, \ldots, w_n$
$dim(V \times W) = dim(V) + dim(W)$

hier: Zustandsraum $V \otimes W$ mit Basis
$\{v_i \otimes w_j : i = 1, \ldots, m, j = 1, \ldots, n\}$
$dim(V \otimes W) = dim(V) \cdot dim(W)$
(exp. Wachstum der Dimension in der Anzahl der Komponenten)

1.3.6 Notation

- für $|0\rangle \otimes |0\rangle$ auch $|0\rangle|0\rangle$ oder $|00\rangle$
- $|0-0\rangle$ für $|0\rangle \otimes |0\rangle \otimes \ldots \otimes |0\rangle$
- Für jedes Paar: $|\psi\rangle = \sum_i a_i|v_i\rangle$ in V und $|\psi\rangle = \sum_j b_j|w_j\rangle$ in W
  haben wir in $V \otimes W$ den Vektor $|\psi\rangle \otimes |\varphi\rangle = \sum_{i,j} a_i b_j (|v_i\rangle \otimes |w_i\rangle)$
  Aber: nicht jeder Vektor $|v\rangle \in V \otimes W$ kann als Produkt $|v\rangle = |\psi\rangle \otimes |\varphi\rangle$ mit $|\psi\rangle \in V, |\varphi\rangle \in W$ geschrieben werden!

Beispiel :

$|v\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in H_2 \otimes H_2$
es gibt keine $|\varphi_1\rangle, |\varphi_2\rangle \in H_2$ mit $|v\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$

Beweis :

sonst existieren $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{C}$ mit
$|v\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \underbrace{\alpha_1\beta_2}_{=0}|01\rangle + \underbrace{\alpha_2\beta_1}_{=0}|10\rangle + \beta_1\beta_2|11\rangle$

$\Rightarrow \alpha_1\alpha_2 = 0$ oder $\beta_1\beta_2 = 0 \quad ↯$

Solche nicht-zerlegbaren Zustände heissen **entangled** (verschränkt)

1.3.7 Messung

Messung des ersten Qubits eines n-Bit-Zustands $|\psi\rangle = \sum_{v\in\{0,1\}^n} \alpha_v |v\rangle$ ergibt:

- $|0\rangle$ mit Wahrscheinlichkeit $p = \sum_{w\in\{0,1\}^{n-1}} |\alpha_{0w}|^2$
  und projiziert $|\psi\rangle$ auf den Zustand $|0\rangle \otimes \frac{1}{\sqrt{p}} \sum_{w\in\{0,1\}^{n-1}} \alpha_{0w}|w\rangle$

- $|1\rangle$ mit Wahrscheinlichkeit $q = \sum_{w\in\{0,1\}^{n-1}} |\alpha_{1w}|^2$
  und projiziert $|\psi\rangle$ auf den Zustand $|1\rangle \otimes \frac{1}{\sqrt{q}} \sum_{w\in\{0,1\}^{n-1}} \alpha_{1w}|w\rangle$

  $(q = 1 - p)$

1.3.8 Observable

Eigenschaft eines physikalischen Systems, welche prinzipiell messbar ist.

- Zerlegung des Zustandsraums in orthogonale Teilräume:
  $H = E_1 \oplus E_2 \oplus \ldots \oplus E_n$ mit $E_i \perp E_j$ $(i \neq j)$
  $|\psi\rangle = |\varphi_1\rangle + |\varphi_2\rangle + \ldots + |\varphi_n\rangle$ mit $|\varphi_i \in E_i\rangle$
- Messung bzgl. $\{E_1, \ldots, E_n\}$: Projektion von $|\psi\rangle$ auf ein $|\varphi_i\rangle$
- Resultat: $|\varphi_i\rangle$ mit Wahrscheinlichkeit $\|\ \varphi_i\ \|^2$

1.3.9 Evolution

Evolution eines qm-Systems via unitärer Transformationen $|\psi\rangle \mapsto U|\psi\rangle$

- U lineare Abbildung von H nach H
- U unitär: $\langle U_\varphi | U_\psi \rangle = \langle \varphi | \psi \rangle$
- Für die Beschreibung der Transformation durch eine Matrix U bedeutet dies, dass
  $U^* = U^{-1}$ (U^* konjugiert transponierte Matrix zu U)
- Insbesondere sind unitäre Transformationen **invertierbar** d.h. **reversibel**
  $\rightarrow$ Berechnungen von QL sind aus reversiblen Basisschritten zusammengesetzt.
  (Ausnahme: Messung !)

1.3.10 No Cloning Theorem

Es gibt für $n > 1$, keine unitäre Transformation
Copy : $H_n \otimes H_n \rightarrow H_n \otimes H_n$
so dass für ein $|a\rangle \in H_n$ und alle $|\psi\rangle \in H_n$

$$Copy(|\psi\rangle \otimes |a\rangle) = (|\psi\rangle \otimes |\psi\rangle) \qquad \text{(Notation: } |\psi, \varphi\rangle = |\psi\rangle|\varphi\rangle = |\psi\rangle \otimes |\varphi\rangle)$$

Beweis :

Annahme : Copy existiert.
Für $n > 1$ existiert ein zu $|a\rangle$ orthogonaler Zustand $|\varphi\rangle$

Setze $|\psi\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |\varphi\rangle)$

$$\begin{aligned}
Copy(|\Phi\rangle|a\rangle) &= \frac{1}{\sqrt{2}}[Copy(|a\rangle|a\rangle) + Copy(|\varphi\rangle|a\rangle)] \\
&= \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |\varphi\rangle|\varphi\rangle) \\
&\neq |\psi\rangle|\psi\rangle \\
|\psi\rangle|\psi\rangle &= \frac{1}{\sqrt{2}}(|aa\rangle + |a\varphi\rangle + |\varphi a\rangle + |\varphi\varphi\rangle)
\end{aligned}$$

1.4 Quantum Gates und QGA

1.4.1 Definition

Ein Quantum Gate auf m Qubits ist eine unitäre Transformation $U : H_{2^m} \to H_{2^m}$ auf dem $2^m - dim$ Hilbertraum.

1.4.2 Gates auf 2^1 dimensionalem Hilbertraum (m=1)

Gates auf einem Qubit $U : H_2 \to H_2$
Betrachte Standardbasis $|0\rangle, |1\rangle$ von H_2

$$\begin{aligned}
U: \quad & |0\rangle \mapsto a|0\rangle + b|1\rangle \quad \rightsquigarrow \begin{pmatrix} a \\ b \end{pmatrix} \\
& |1\rangle \mapsto c|0\rangle + d|1\rangle \quad \rightsquigarrow \begin{pmatrix} c \\ d \end{pmatrix} \\
\rightsquigarrow \quad & Matrix \begin{pmatrix} a & c \\ b & d \end{pmatrix}
\end{aligned}$$

U unitär : $\begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

Beispiel :

- $M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ("not" Gate)
  $M_\neg|0\rangle = |1\rangle, M_\neg|1\rangle = |0\rangle$
- Sei $M = \frac{1}{2}\begin{pmatrix} i+1 & 1-i \\ 1-i & 1+i \end{pmatrix}$ unitär, da
  $M^*M = \frac{1}{4}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 2\cdot(1-i^2) & (1-i)^2+(1+i)^2 \\ (1-i)^2+(1+i)^2 & 2\cdot(1-i^2) \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$
  $MM = \frac{1}{4}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = M_\neg$
  also $M = \sqrt{M_\neg}$
- Hadamard (Hadamard-Walsh)
  $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

transformiert Standardbasis $|0\rangle$, $|1\rangle$in Hadamard-Basis (Fourier - Basis)

$|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

und zurück,

$$H|0'\rangle = H \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$
$$H|1'\rangle = H \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$
S(Phase)=$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{\varphi}} \end{pmatrix}$$

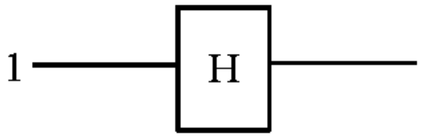

Abbildung 1.3: Quantum Gate (m=1)

1.4.3 Gates auf 2^2 dimensionalem Hilbertraum (m=2)

2-Qubit Gates $U : H_4 \to H_4$

Standard Basis $\underbrace{|00\rangle}_{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}} \underbrace{|01\rangle}_{\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}} \underbrace{|10\rangle}_{\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}} \underbrace{|11\rangle}_{\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}}$

Beispiel : CNOT (controlled-NOT)

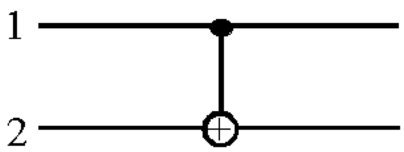

Abbildung 1.4: Notation M_{CNOT}

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

$M_{CNOT}|00\rangle = |00\rangle$
$M_{CNOT}|01\rangle = |01\rangle$
$M_{CNOT}|10\rangle = |11\rangle$
$M_{CNOT}|11\rangle = |10\rangle$

$M_{CNOT} = |ij\rangle = |i \;\; i \otimes j\rangle$

Allgemein :

Sei U eine unitäre Transformation auf <u>einem</u> Qubit.

Controlled-U (C-U) Transformation auf zwei Qubits:
C-U $|ij\rangle = |i\rangle \otimes$ if i then $U|j\rangle$ else $|j\rangle$

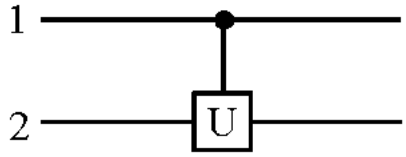

Abbildung 1.5: allgemeine Notation

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & \\ & & U \end{pmatrix}$$

Interessantes Gate : C-C-NOT = Toffoli-Gate (Tf)

$\mathrm{Tf}|ijk\rangle = |ij \;\; ij \otimes k\rangle$

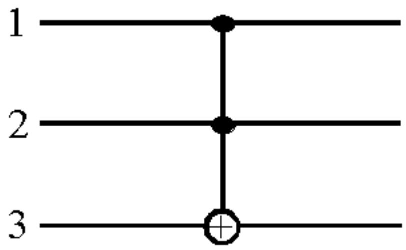

Abbildung 1.6: Notation C-C-NOT

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{pmatrix}$$

Tf als klassisches Gate :

$$\begin{aligned} \mathrm{Tf}: \{0,1\}^3 &\rightarrow \{0,1\}^3 \\ (i,j,k) &\mapsto (i,j,ij \oplus k) \end{aligned}$$

Jeder klassische Schaltkreis kann durch einen Schaltkreis aus Tf-Gates simuliert werden.
Zu $f: \{0,1\}^n \rightarrow \{0,1\}^m$ betrachten wir die reversible Funkition

$$\begin{aligned} f': \{0,1\}^n \times \{0,1\}^m &\rightarrow \{0,1\}^n \times \{0,1\}^m \\ (x,y) &\mapsto (x, f(x) \oplus y) \end{aligned}$$

Die Menge Ω von reversiblen Gates ist vollständig (für klassische reversible Berechnungen) wenn zu jeder reversiblen Funktion
$g: \{0,1\}^n \rightarrow \{0,1\}^n$ ein reversibler Schaltkreis aus Ω-Gates gebaut werden kann, welcher eine Funktion
$h: \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n \times \{0,1\}^k$ realisiert, so dass für ein festes $u \in \{0,1\}^k$
$h(x,u) = (g(x), v)$

Satz :

$\{\mathrm{Tf}\}$ ist vollständig (für klassische reversible Berechnungen)

Beweis : Jede Funktion kann durch einen klassischen Schaltkreis über $\{$ NAND$\}$ berechnet werden

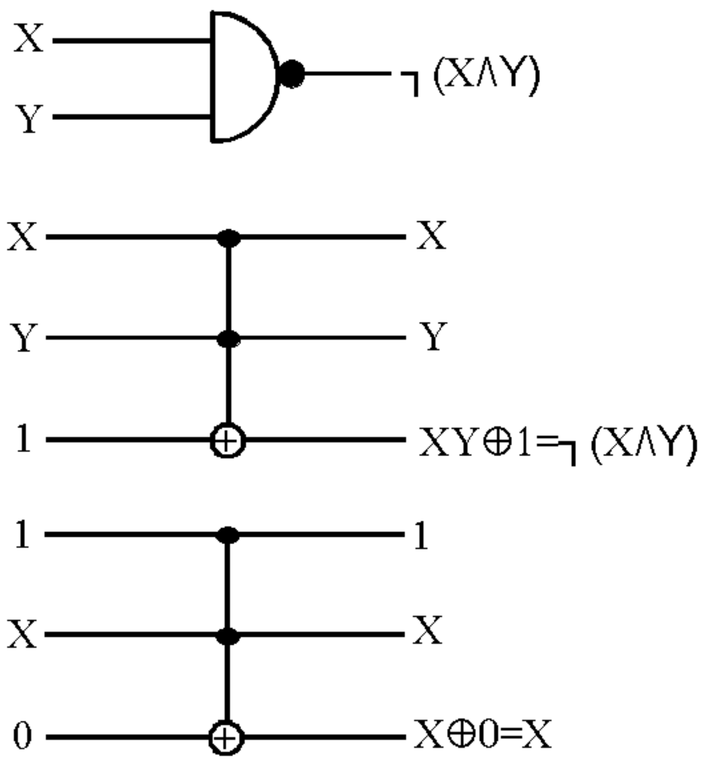

Abbildung 1.7: NAND

$|ij\rangle \mapsto |i\rangle \otimes$ if $i = 0$ then $U|j\rangle$ else $|j\rangle$

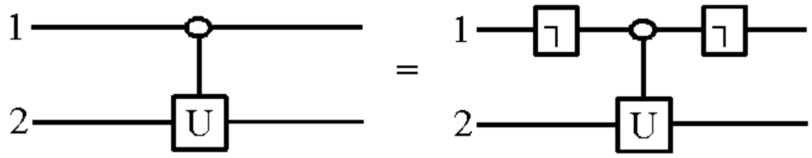

Abbildung 1.8: Kontrolle durch 0 statt 1

1.4.4 Tensorprodukt von Matrizen

Definition :

Sei $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$ (mxn)-Matrix

$B = \begin{pmatrix} b_{11} & \cdots & b_{1s} \\ \vdots & \ddots & \vdots \\ b_{r1} & \cdots & b_{rs} \end{pmatrix}$ (rxs)-Matrix

Dann ist die $(mr \times ns)$-Matrix $A \otimes B := \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}$

Seien A, B (2×2)-Matrizen, welche Quanten-Gates auf einem Qubit beschreiben, dann wird die simultane Aktion von A auf dem ersten und B auf dem zweiten Qubit durch die Matrix $A \otimes B$ beschrieben :

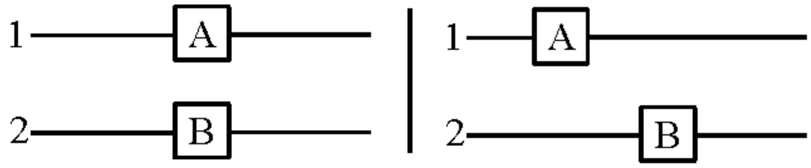

Abbildung 1.9: simultane Aktion

Begründung :

ausrechen
In den Spalten der Matrix stehen, in Koordinatenschreibweise, die Bilder der Basisvektoren
Operation : $\underbrace{|i\rangle \otimes |j\rangle}_{=|ij\rangle} \mapsto A|i\rangle \otimes B|j\rangle$

$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$ $B = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix}$

$$\begin{aligned} A|i\rangle \otimes B|j\rangle &= (a_{0i}|0\rangle + a_{1i}|1\rangle) \otimes (b_{0j}|0\rangle + b_{1j}|1\rangle) \\ &= a_{0i}b_{0j}|00\rangle + a_{0i}b_{1j}|01\rangle + a_{1i}(b_{0j}|10\rangle + a_{1i}b_{1j}|11\rangle \end{aligned}$$

In der zu $|ij\rangle$ gehörenden Spalte der Produktmatrix steht also : $\begin{pmatrix} a_{0i} \cdot b_{0j} \\ a_{0i} \cdot b_{1j} \\ a_{1i} \cdot b_{0j} \\ a_{1i} \cdot b_{1j} \end{pmatrix}$

Dies ist genau die entsprechende Spalte von $A \otimes B$. Dies gilt für Räume beliebiger Dimensionen. Wenn A und B (unitäre) Transformationen auf H_n bzw. H_m beschreiben, dann beschreibt $A \otimes B$ die Operation auf $H_n \otimes H_m$ die der simultanen Kombination der beiden Operationen entspricht(Reihenfolge egal). $A \otimes B$ führt kein Entanglement ein.

Beispiel :

Sei $A = B = H$ (Hadamard)

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

$$\begin{aligned} (H \otimes H)|ij\rangle &= \frac{1}{2}(|0\rangle + (-1)^i|1\rangle) \otimes (|0\rangle + (-1)^j|1\rangle) \\ &= \frac{1}{2}(|00\rangle + (-1)^j|01\rangle + (-1)^i|10\rangle + (-1)^{i+j}|11\rangle) \end{aligned}$$

zerlegbar ($|ij\rangle$ zerlegbar, $H \otimes H$ führt kein Entanglement ein)

Hingegen ist M_{CNOT} kein Tensorprodukt von (2×2) Matrizen.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Betrachte Operation von M_{CNOT} auf zerlegbarem Zustand :

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}((|0\rangle + |1\rangle) \otimes |0\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ M_{CNOT}|\psi\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \mathrm{EPR-Paar(entangled)} \end{aligned}$$

führt also ein Entanglement ein.

1.4.5 Hadamard Transformation revisited

$$\begin{aligned} H &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

Sei $H^{\otimes n} = \underbrace{H \otimes H \otimes \ldots \otimes H}_{m-Mal} : H_{2^n} \rightarrow H_{2^n}$

$$
\begin{aligned}
H^{\otimes n}|0-0\rangle &= H|0\rangle \otimes \ldots \otimes H|0\rangle \\
&= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \ldots \otimes (|0\rangle + |1\rangle)) \\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle
\end{aligned}
$$

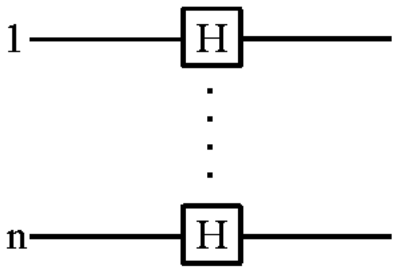

Abbildung 1.10: Hadamard auf mehreren Qubits

Mit linearem Aufwand (n Q-Gates) wird $|0-0\rangle$ in gleichmäßige Überlagerung aller 2^n Basisvektoren transformiert!

1.4.6 Quantum Gate Arrays (QGA)

Sei Ω eine Menge von Quanten-Gates. Ein Quanten Schaltkreis oder Quanten Gate Array(QGA) auf n Qubits ist eine unitäre Transformation $U : H_{2^n} \to H_{2^n}$, welche aus Q-Gates aus Ω zusammengesetzt ist.

Basisoperation :

Wende Gate G auf Qubits $i_1, \ldots, i_m$ an.

m=2 : $\underbrace{G}_{(4\times 4)-\text{Matrix}(2-\text{Qubits})} \otimes I_{2^{n-2}}$

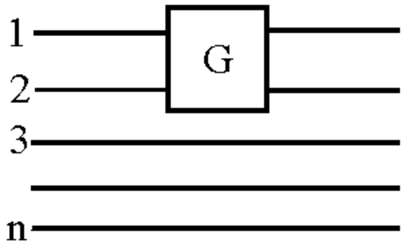

Abbildung 1.11: Basisoperation

$P^{-1}_{i_1 i_2}(G \otimes I_{2^{n-2}})P_{i_1 i_2}$

$P_{i_1 i_2}$: Permutation, welche Qubits i_1, i_2 auf Qubits 1,2 vertauscht.

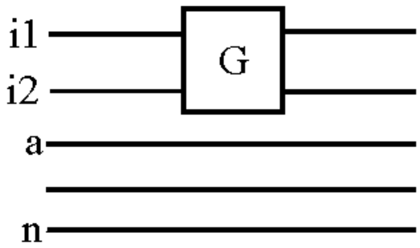

Abbildung 1.12: Basisoperation mit Permutation

Index

Abbildungsverzeichnis