

Quantenalgorithmen

gehalten von: Prof. Dr. Alexander May

WS 11/12

Mitschrift von Michael Breuer

Weiterführende Literatur

Mermin, "Quantum Computer Science", Cambridge, 2007

Homeister, "Quantum Computing verstehen", Vieweg, 2005

Chuang, Nielsen, "Quantum Computation and Quantum Information"

D. Aharonov, Quantum Computation, <http://arxiv.org/pdf/quant-ph/9812037>

Inhaltsverzeichnis

1	Warum Quantenalgorithmen?	4
2	Klassische vs. Quanten-Berechnung	4
2.1	Klassische probabilistische Systeme	4
2.1.1	Beispiel: klassischer Münzwurf	5
2.1.2	Warscheinlichkeitsbaum des Münzwurfs	5
2.1.3	Weiteres Beispiel eines Warscheinlichkeitbaumes	5
2.1.4	Geometrische Interpretation	6
3	1-Qubit-System	6
3.1	Definition: Qubit	6
3.2	Exkurs/Notation für komplexe Vektorräume \mathbb{C}^n	6
3.3	Satz über orthonormale Basen im \mathbb{C}^n	6
3.3.1	Beispiel	7
3.4	Definiton über den Zustand eines Qubits	7
3.5	Definiton über den Zustand eines Quantensystems	7
3.6	Bezeichnungen	7

3.7	Vergleich Wahrscheinlichkeitsverteilung und Superposition	8
3.8	Quantenmünzwurf	8
4	Operationen auf 1-Qubit-Systemen	8
4.1	Definition unitärer Abbildungen	9
4.2	Satz über unitäre Matrizen als unitäre Abbildungen	9
4.2.1	Beispiel: Hadamar-Walsh-Matrix	9
4.3	Entwicklung eines Qubits unter einer unitären Abbildung U (Operator U)	9
4.3.1	Beispiel: Quanten-NOT	10
4.3.2	Beispiel: Wurzel des NOT	10
4.3.3	Beispiel: Hadamar-Walsh (2)	10
4.3.4	Beispiel: Flip	11
4.4	Definition über die Äquivalenz von zwei Zuständen	11
5	Exkurs über Tensorprodukte	11
5.1	Definition des Tensorprodukts	11
5.1.1	Beispiele	11
5.2	Rechenregeln für das Tensorprodukt	12
5.2.1	Distributivität	12
5.2.2	Skalare Multiplikation	12
5.2.3	Skalarprodukt	12
5.2.4	Norm des Tensorprodukts	12
5.3	Lemma über die Orthonormalität einer Basis aus dem Tensorprodukt zweier orthonormalen Basen	12
5.3.1	Beispiel	13
5.4	Notationen	13
6	2-Quanten-Register	13
6.1	Definition des Zustands eines 2-Qubit-Systems	13
6.2	Messung eines 2-Qubit-Systems:	13
6.3	Messung eines einzelnen Qubits eines 2-Qubit-Systems	14
6.4	Definition von separabel und verschränkt	14
6.4.1	Beispiel eines separablen Zustands	14
6.4.2	Beispiel eines verschränkten Zustands	15
6.4.2.1	Bezeichnung (EPR-Paar)	16
6.5	Fakt	16
6.5.1	Beispiel: CNOT	16
6.6	Definition einer Permutationsmatrix	16
6.6.1	Beispiel	16
6.7	Bezeichnung (lokal unitär)	16
6.7.1	Spezialfälle	17

6.8	Definition des Tensor- bzw. Kronecker-Produkts von Matrizen	17
6.8.1	Beispiel	17
6.9	Satz über die Beschreibung der Anwendungen von A und B als Tensorprodukt von Matrizen	17
6.9.1	Beispiel	18
6.10	Beispiel	18
6.11	Satz über unitäre Abbildungen, die sich nicht als Tensorprodukt von Matrizen schreiben lassen	18
6.12	Definition einer Quantenkopiermaschine	19
6.13	Satz über die Nichtexistenz von Quantenkopiermaschinen	19
7	n-Qubit-Zustände (Register)	20
7.1	Definition: n-Qubit-System	20
7.1.1	Notation	20
7.2	Zustandsübergänge	21
7.2.1	Beobachtung:	21
7.3	Definition: Separabilität	21
7.3.1	Beispiel	21
7.4	Quantenteleportation (Bennett et al. 1993)	21
7.4.1	Szenario	21
7.5	Superdense Coding (Bennet, Wiesner 1992)	23
7.5.1	Szenario	23

Tabellenverzeichnis

1	Messung der beiden Qubits von Alice - Wahrscheinlichkeit jeweils $\frac{1}{4}$	23
2	Bobs Operation in Abhängigkeit von Alices Messergebnis	23
3	Zustände des Qubits nach Alices Operation beim Superdense Coding	24
4	Bobs Berechnung der ursprünglichen Bits	24

1 Warum Quantenalgorithmen?

1. Notwendigkeit:

- Moores Gesetz (Integrationsdichte verdoppelt sich alle zwei Jahre)
- Rechner werden kleiner
- Bei atomaren Größen gelten quantenmechanische Gesetze

2. Potential:

- Quantencomputer können klassische Rechner simulieren und eventuell mehr
- Effizient faktorisieren & Dlog berechnen
- Quadratischer Speed-up bei Datenbanksuche ($\Theta(\sqrt{N})$ statt $\Theta(N)$)
- Exponentieller Speed-up in relativen Modellen
- Quantenkryptographie/- kodierung

2 Klassische vs. Quanten-Berechnung

Klassisch: Bits / Boolesche Funktionen: $F2^n \rightarrow F2^n$

Turingmaschine, Boolesche Schaltkreise / Bits

$EINGABE \rightarrow Berechnung \rightarrow AUSGABE$

Quanten: Qubits / Reversible Funktionen, lineare Funktionen $F2^n \rightarrow F2^n$

Quanten-Turingmaschine, Quanten-Schaltkreise kein kopieren von Qubits möglich

Quantenparallelität, Intefferenz / Messung liefert Qubits

Probleme bei Implementierung:

- Dekohärenz, Skalierbarkeit
- Quantenfehlerkorrektur

2.1 Klassische probabilistische Systeme

Seien $[x_1], \dots, [x_n]$ Basiszustände. Warscheinlichkeits-Verteilung auf Basiszuständen:

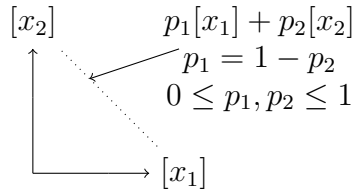
$$p_1[x_1] + p_2[x_2] + \dots + p_n[x_n] \quad (2.1)$$

mit

$$0 \leq p_i \leq 1, \sum_{i=1}^n p_i = 1 \quad (2.2)$$

Strategie: Maximiere die WS von günstigen Basiszuständen (=korrektes Ergebnis)

2.1.4 Geometrische Interpretation



3 1-Qubit-System

3.1 Definition: Qubit

Ein Qubit ist ein Einheitsvektor im \mathbb{C}^2 .

3.2 Exkurs/Notation für komplexe Vektorräume \mathbb{C}^n

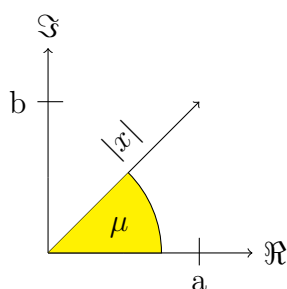
$$|x\rangle \in \mathbb{C}^n \Leftrightarrow |x\rangle = (x_1, \dots, x_n) \text{ "ket"-Notation} \quad (3.1)$$

$$\langle x| \in \mathbb{C}^n \Leftrightarrow \langle x| = (x_1^*, \dots, x_n^*) \text{ "bra"-Notation} \quad (3.2)$$

$$x \in \mathbb{C} \text{ mit: } x = a + ib, a, b \in \mathbb{R}, i^2 = -1 \text{ und } x^* = a - ib \quad (3.3)$$

$$\text{Norm: } \|x\| := |x| = \sqrt{xx^*} \text{ für } x \in \mathbb{C} \quad (3.4)$$

$$\text{Für } x \in \mathbb{C}^n : \|x\| := |x| = \sqrt{\langle x| \cdot |x\rangle} = \sqrt{\sum_{i=1}^n x_i^* x_i} \quad (3.5)$$



$$\sin(\mu) = \frac{b}{|x|}, \cos(\mu) = \frac{a}{|x|} \quad (3.6)$$

$$\Rightarrow x = (\cos(\mu) + i \cdot \sin(\mu))|x| = e^{i\mu}|x| \quad (3.7)$$

$$\text{Insbesondere gilt: } e^{2\pi i} = 1 \quad (3.8)$$

$$|x\rangle, |y\rangle \text{ orthogonal} \Leftrightarrow \langle x|y\rangle = 0 \quad (3.9)$$

3.3 Satz über orthonormale Basen im \mathbb{C}^n

Die Vektoren $|x_1\rangle, \dots, |x_n\rangle \in \mathbb{C}^n$ bilden eine orthonormale Basis des \mathbb{C}^n falls:

$$1. \langle x_i | x_j \rangle \quad \forall i = j \quad (3.10)$$

$$2. ||x_i\rangle| = 1 \quad \forall i = 1, \dots, n \quad (3.11)$$

3.3.1 Beispiel

1. Orthonormale Basis des \mathbb{C}^2 ::

$$(1, 0), (0, 1) \in \mathbb{C}^2 \text{ bzw. } (e^{i\mu}, 0), (0, e^{i\mu}) \quad (3.12)$$

2. Orthonormale Basen des \mathbb{C}^4 ::

$$|0\rangle = (1, 0, 0, 0), |1\rangle = (0, 1, 0, 0), |x\rangle = (0, 0, 1, 0), |y\rangle = (0, 0, 0, 1) \quad (3.13)$$

$$\frac{1}{5}(1, 2, 2, 4), \frac{1}{5}(2, -1, 4, -2), \frac{1}{5}(2, 4, -1, -2), \frac{1}{5}(4, -2, -2, 1) \quad (3.14)$$

3.4 Definiton über den Zustand eines Qubits

Seien $|0\rangle, |1\rangle = (1, 0), (0, 1)$ eine orthonormale Basis des \mathbb{C}^2 .

Der Zustand eines Qubits ist ein Einheitsvektor im \mathbb{C}^2 der Form $|q\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ mit $\alpha_1 \in \mathbb{C}$.

Übung: $|\alpha_0|0\rangle + \alpha_1|1\rangle| = 1 \Leftrightarrow |\alpha_0|^2 + |\alpha_1|^2 = 1$

3.5 Definiton über den Zustand eines Quantensystems

Seien $|0\rangle, \dots, |n\rangle$ eine orthonormale Basis des \mathbb{C}^n (auch H_n für Hilbertraum). Dann ist der Zustand eines Quantensystems: $\alpha_1|x_1\rangle + \dots + \alpha_n|x_n\rangle$ mit $|\alpha_1|^2 + \dots + |\alpha_n|^2 = 1$
Messung: x_i mit Warscheinlichkeit $|\alpha_i|^2$

3.6 Bezeichnungen

- Basisvektoren $|x_i\rangle$ werden Basiszustände genannt.
- α_i heißen Amplituden.
- Allgemeiner Zustand ist Superposition der Basiszustände (Überlagerung).
- $\psi(x_i) = \alpha_i$ heißt Wellenfunktion.
- $|x\rangle = e^{i\mu}|y\rangle \Leftrightarrow$ Zustände $|x\rangle$ und $|y\rangle$ heißen äquivalent.

3.7 Vergleich Wahrscheinlichkeitsverteilung und Superposition

Wahrscheinlichkeitsverteilung: $x_i \rightarrow p_{i1}[x_1] + \dots + p_{in}[x_n] \sum_{i=1}^n p_i = 1$

Superposition: $\alpha_1|x_1\rangle + \dots + \alpha_n|x_n\rangle \sum_{i=1}^n |\alpha_i|^2 = 1$ d.h. α_i WS-Verteilung.

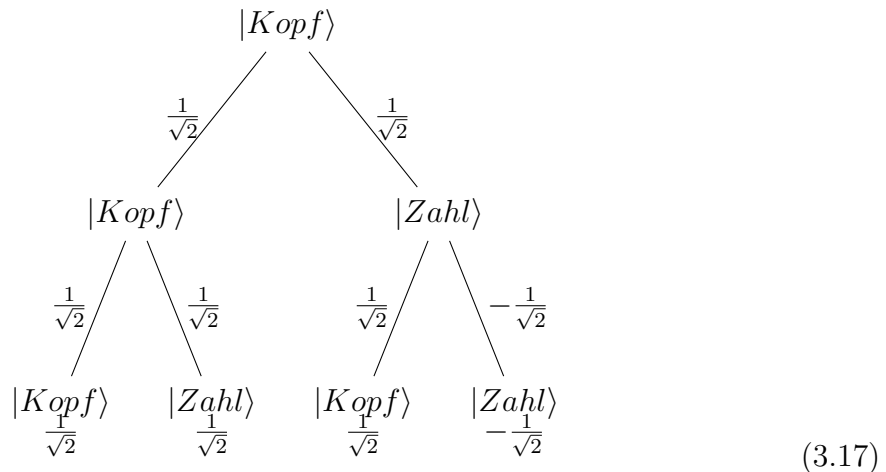
Trotzdem fundamental verschieden! Amplituden können sich gegenseitig auslöschen und verstärken (Interferenz).

3.8 Quantenmünzwurf

$$|Kopf\rangle \rightarrow \frac{1}{\sqrt{2}}|Kopf\rangle + \frac{1}{\sqrt{2}}|Zahl\rangle \quad (3.15)$$

$$|Zahl\rangle \rightarrow \frac{1}{\sqrt{2}}|Kopf\rangle - \frac{1}{\sqrt{2}}|Zahl\rangle \quad (3.16)$$

Strategie: Maximiere die QS von günstigen Basiszuständen (= korrektes Ergebnis)



$|Kopf\rangle$ hat Amplitude 1, $|Zahl\rangle$ Amplitude 0.

4 Operationen auf 1-Qubit-Systemen

Forderungen aus Quantenmechanik:

- Abbildungen müssen reversibel (umkehrbar) sein.
- Abbildungen müssen linear sein.
- Da Qubits Einheitsvektoren beschrieben, muss die Abbildung längenerhaltend sein.

4.1 Definition unitärer Abbildungen

Eine lineare Abbildung $U : \mathbb{C}^n \rightarrow \mathbb{C}^n$ heißt unitär, falls $\forall |x\rangle \in \mathbb{C}^n$:

$$|U|x\rangle| = ||x\rangle|. \tag{4.1}$$

D.h. U ist längenerhaltend.

Eine Matrix $U \in \mathbb{C}^{n \times n}$ heißt unitär falls:

$$(U^*)^T = U^{-1}. \tag{4.2}$$

4.2 Satz über unitäre Matrizen als unitäre Abbildungen

Jede unitäre Matrix $U \in \mathbb{C}^{n \times n}$ definiert eine unitäre Abbildung.

Beweis $\forall A \in \mathbb{C}^{m \times m}, |x\rangle, |y\rangle \in \mathbb{C}^m$ gilt:

$$\langle\langle x|A|y\rangle\rangle = \langle\langle (A^*)^T|x\rangle\rangle \tag{4.3}$$

$$\Rightarrow |U|x\rangle| = \sqrt{\langle\langle U|x\rangle|U|x\rangle\rangle} = \sqrt{\langle\langle (U^*)^T U|x\rangle| |x\rangle\rangle} = \sqrt{\langle x|x\rangle} = ||x\rangle| \tag{4.4}$$

4.2.1 Beispiel: Hadamar-Walsh-Matrix

$$W_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4.5}$$

W_2 ist unitär:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{4.6}$$

Anmerkung: W_2 beschreibt den Quantenmünzwurf (vgl. Abschnitt 3.8)

4.3 Entwicklung eines Qubits unter einer unitären Abbildung U (Operator U)

Sei $|0\rangle = (1, 0)$ und $|1\rangle = (0, 1)$, $U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Dann gilt:

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ d.h. } |0\rangle \xrightarrow{U} a|0\rangle + b|1\rangle \tag{4.7}$$

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix} = c \begin{pmatrix} 1 \\ 0 \end{pmatrix} + d \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ d.h. } |1\rangle \xrightarrow{U} c|0\rangle + d|1\rangle \tag{4.8}$$

4.3.1 Beispiel: Quanten-NOT

Ziel: $|0\rangle \Rightarrow |1\rangle$ und $|1\rangle \Rightarrow |0\rangle$

$$M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (4.9)$$

$$(1, 0) \mapsto (0, 1) \Rightarrow |0\rangle \mapsto |1\rangle \quad (0, 1) \mapsto (1, 0) \Rightarrow |1\rangle \mapsto |0\rangle \quad (4.10)$$

M_2 ist unitär, denn $M_2(M_2^*)^T = M_2 \cdot M_2 = I_2$.

4.3.2 Beispiel: Wurzel des NOT

$$\sqrt{M_2} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \quad (4.11)$$

$$\begin{aligned} |0\rangle &\xrightarrow{\sqrt{M_2}} \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \\ &\xrightarrow{\sqrt{M_2}} \frac{1+i}{2} \left(\frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \right) + \frac{1-i}{2} \left(\frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle \right) \end{aligned} \quad (4.12)$$

$$= \left(\left(\frac{1+i}{2} \right)^2 + \left(\frac{1-i}{2} \right)^2 \right) |0\rangle + 2 \cdot \frac{1-i^2}{4} |1\rangle \quad (4.13)$$

$$= \frac{1 + 2i + i^3 + 1 - 2i + i^2}{4} |0\rangle + |1\rangle = |1\rangle \quad (4.14)$$

Messen liefert $|0\rangle$ mit WS $|\frac{1+i}{2}|^2 = \frac{1-i}{2} \cdot \frac{1+i}{2} = \frac{1-i^2}{4} = \frac{1}{2}$

Analog:

$$|1\rangle \xrightarrow{\sqrt{M_2}} \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle \xrightarrow{\sqrt{M_2}} |0\rangle \quad (4.15)$$

Übung $\sqrt{M_2}$ ist unitär.

4.3.3 Beispiel: Hadamar-Walsh (2)

$$W_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (4.16)$$

$$|0\rangle \xrightarrow{\sqrt{W_2}} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\xrightarrow{\sqrt{W_2}} \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \quad (4.17)$$

$$= \left(\frac{1}{2} + \frac{1}{2}\right)|0\rangle + \left(\frac{1}{2} - \frac{1}{2}\right)|1\rangle = |0\rangle \quad (4.18)$$

4.3.4 Beispiel: Flip

$$F = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (4.19)$$

$$|0\rangle \mapsto |0\rangle \quad |1\rangle \mapsto -|1\rangle \quad (4.20)$$

Allgemein:

$$F_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad (4.21)$$

$$|0\rangle \mapsto |0\rangle \quad |1\rangle \mapsto e^{i\theta}|1\rangle \quad (4.22)$$

4.4 Definition über die Äquivalenz von zwei Zuständen

Zwei Zustände $|x\rangle, |y\rangle \in \mathbb{C}^n$ heißen genau dann äquivalent, wenn $|x\rangle = e^{i\theta}|y\rangle$.

Flip transformiert $|1\rangle$ in einen äquivalenten Zustand. Messung von $|1\rangle$ mit gleicher WS.

5 Exkurs über Tensorprodukte

5.1 Definition des Tensorprodukts

Seien $|x\rangle = (x_1, \dots, x_n) \in \mathbb{C}^n, |y\rangle = (y_1, \dots, y_m) \in \mathbb{C}^m$. Dann ist das Tensorprodukt von $|x\rangle$ und $|y\rangle$ definiert als:

$$|x\rangle \otimes |y\rangle = (x_1y_1, \dots, x_1y_m, x_2y_1, \dots, x_2y_m, \dots, x_ny_1, \dots, x_ny_m) \in \mathbb{C}^{nm} \quad (5.1)$$

5.1.1 Beispiele

$$|0\rangle = (1, 0), |1\rangle = (0, 1), \quad |0\rangle \otimes |1\rangle = (0, 1, 0, 0) \quad (5.2)$$

$$|x\rangle = \frac{1}{\sqrt{2}}(1, -1), |y\rangle = \frac{1}{\sqrt{2}}(1, 1), \quad |x\rangle \otimes |y\rangle = \frac{1}{2}(1, 1, -1, -1) \quad (5.3)$$

d.h. $|x\rangle \otimes |y\rangle \neq |y\rangle \otimes |x\rangle$

5.2 Rechenregeln für das Tensorprodukt

5.2.1 Distributivität

$$\forall |x\rangle \in \mathbb{C}^n, |y\rangle, |z\rangle \in \mathbb{C}^m : |x\rangle \otimes (|y\rangle + |z\rangle) = |x\rangle \otimes |y\rangle + |x\rangle \otimes |z\rangle \quad (5.4)$$

$$\forall |x\rangle, |y\rangle \in \mathbb{C}^n, |z\rangle \in \mathbb{C}^m : (|x\rangle + |y\rangle) \otimes |z\rangle = |x\rangle \otimes |z\rangle + |y\rangle \otimes |z\rangle \quad (5.5)$$

5.2.2 Skalare Multiplikation

$$\forall |x\rangle \in \mathbb{C}^n, |y\rangle \in \mathbb{C}^m, c \in \mathbb{C} : (c|x\rangle) \otimes |y\rangle = c(|x\rangle \otimes |y\rangle) = |x\rangle \otimes (c|y\rangle) \quad (5.6)$$

5.2.3 Skalarprodukt

$$\forall |v\rangle, |x\rangle \in \mathbb{C}^n, |y\rangle, |z\rangle \in \mathbb{C}^m : \langle |v\rangle \otimes |y\rangle | |x\rangle \otimes |z\rangle \rangle = \langle v|x\rangle \langle y|z\rangle \quad (5.7)$$

5.2.4 Norm des Tensorprodukts

$$\forall |x\rangle \in \mathbb{C}^n, |y\rangle \in \mathbb{C}^m : \||x\rangle \otimes |y\rangle\|^2 = \||x\rangle\|^2 \cdot \||y\rangle\|^2 \quad (5.8)$$

5.3 Lemma über die Orthonormalität einer Basis aus dem Tensorprodukt zweier orthonormalen Basen

Seien $|x_1\rangle, \dots, |x_n\rangle, |y_1\rangle, \dots, |y_m\rangle$ orthonormale Basen des \mathbb{C}^n bzw. \mathbb{C}^m . Dann ist:

$$|x_1\rangle \otimes |y_1\rangle, \dots, |x_n\rangle \otimes |y_m\rangle \in \mathbb{C}^{nm} \quad (5.9)$$

eine orthonormale Basis des \mathbb{C}^{nm} .

Beweis Normalität: Für $|x_i\rangle, |y_j\rangle$ gilt:

$$\||x_i\rangle \otimes |y_j\rangle\| = \||x_i\rangle\| \cdot \||y_j\rangle\| = 1 \cdot 1 = 1 \quad (5.10)$$

Orthogonalität: Für $|x_i\rangle \otimes |y_j\rangle$ und $|x_k\rangle \otimes |y_l\rangle$ mit $(i, j) \neq (k, l)$ gilt:

$$\langle |x_i\rangle \otimes |y_j\rangle | |x_k\rangle \otimes |y_l\rangle \rangle = \langle x_i|x_k\rangle \langle y_j|y_l\rangle = 0 \quad (5.11)$$



5.3.1 Beispiel

Tensor von $|0\rangle, |1\rangle$ liefert

$$|0\rangle = (1, 0), |1\rangle = (0, 1)$$

$$|0\rangle \otimes |0\rangle = (1, 0, 0, 0)$$

$$|0\rangle \otimes |1\rangle = (0, 1, 0, 0)$$

$$|1\rangle \otimes |0\rangle = (0, 0, 1, 0)$$

$$|1\rangle \otimes |1\rangle = (0, 0, 0, 1)$$

$$|x\rangle = \frac{1}{\sqrt{2}}(1, -1), |y\rangle = \frac{1}{\sqrt{2}}(1, 1)$$

$$|x\rangle \otimes |x\rangle = \frac{1}{2}(1, -1, -1, 1)$$

$$|x\rangle \otimes |y\rangle = \frac{1}{2}(1, 1, -1, -1)$$

$$|y\rangle \otimes |x\rangle = \frac{1}{2}(1, -1, 1, -1)$$

$$|y\rangle \otimes |y\rangle = \frac{1}{2}(1, 1, 1, 1)$$

5.4 Notationen

Seien $|x\rangle \otimes |y\rangle$ abkürzend als $|xy\rangle$ bezeichnet. Insbesondere ist $|0\rangle \otimes |0\rangle = |00\rangle, \dots, |1\rangle \otimes |1\rangle = |11\rangle$

6 2-Quanten-Register

6.1 Definition des Zustands eines 2-Qubit-Systems

Seien $\alpha_i \in \mathbb{C}, i \in \{0, 1, 2, 3\}$. Ein Zustand eines 2-Qubit-Systems ist ein Einheitsvektor der Form

$$|v\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle \in \mathbb{C}^n \quad (6.1)$$

Es gilt:

$$|v\rangle \text{ Einheitsvektor} \Leftrightarrow |\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1. \quad (6.2)$$

D.h. die Amplitudenquadrate liefern eine WS-Verteilung.

6.2 Messung eines 2-Qubit-Systems:

Messung von $|v\rangle$ liefert:

- Basiszustand $|00\rangle$ mit WS $|\alpha_0|^2$.
- Basiszustand $|01\rangle$ mit WS $|\alpha_1|^2$.
- Basiszustand $|10\rangle$ mit WS $|\alpha_2|^2$.

- Basiszustand $|11\rangle$ mit WS $|\alpha_3|^2$.

Nach der Messung befindet sich das 2-Qubit-System im gemessenen Basiszustand. (Kollaps der Wellenfunktion, irreversibel)

6.3 Messung eines einzelnen Qubits eines 2-Qubit-Systems

Messung des 1. Qubits von $|v\rangle$ liefert:

- $|0\rangle$ mit WS $|c_0|^2 + |c_1|^2$
- $|1\rangle$ mit WS $|c_2|^2 + |c_3|^2$

Nach der Messung befinden sich das System im Zustand

$$\frac{c_0|00\rangle + c_1|01\rangle}{\sqrt{|c_0|^2 + |c_1|^2}} \text{ falls } |0\rangle \text{ im 1. Qubit gemessen wurde,} \quad (6.3)$$

$$\frac{c_2|10\rangle + c_3|11\rangle}{\sqrt{|c_2|^2 + |c_3|^2}} \text{ falls } |1\rangle \text{ im 1. Qubit gemessen wurde.} \quad (6.4)$$

Man beachte:

$$\begin{aligned} \left| \frac{c_0|00\rangle + c_1|01\rangle}{\sqrt{|c_0|^2 + |c_1|^2}} \right| &= \frac{1}{\sqrt{|c_0|^2 + |c_1|^2}} \cdot |c_0|00\rangle \\ &+ c_1|01\rangle \Big| = \frac{1}{\sqrt{|c_0|^2 + |c_1|^2}} \cdot \sqrt{|c_0|^2 + |c_1|^2} = 1 \end{aligned} \quad (6.5)$$

D.h. der neue Zustand ist weder ein Einheitsvektor im \mathbb{C}^4 .

6.4 Definition von separabel und verschränkt

Wir nennen den Zustand $|z\rangle \in \mathbb{C}^4$ eines 2-Qubit-Systems separabel, falls $|z\rangle = |x\rangle \otimes |y\rangle$ für $|x\rangle, |y\rangle \in \mathbb{C}^2$. Ein Zustand, der nicht separabel ist, heißt verschränkt.

6.4.1 Beispiel eines separablen Zustands

$$|z\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \quad (6.6)$$

ist separabel. Gesucht: $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{C}$ mit:

$$|z\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \quad (6.7)$$

$$= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle \quad (6.8)$$

$$\text{Gleichungssystem } \begin{cases} \alpha_0\beta_0 = \frac{1}{2} \\ \alpha_0\beta_1 = \frac{1}{2} \\ \alpha_1\beta_0 = \frac{1}{2} \\ \alpha_1\beta_1 = \frac{1}{2} \end{cases} \text{ erfüllt für } \alpha_0 = \beta_0 = \alpha_1 = \beta_1 = \frac{1}{\sqrt{2}} \quad (6.9)$$

Sei $|z\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$ ein separabler Zustand.

Frage: Wie groß ist die WS, $|0\rangle$ im 1. Qubit zu messen?

$$|z\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle \quad (6.10)$$

Messung von $|0\rangle$ im 1. Qubit mit WS :

$$|\alpha_0\beta_0|^2 + |\alpha_1\beta_1|^2 = |\alpha_0|^2 \underbrace{(|\beta_0|^2 + |\beta_1|^2)}_{=1} = |\alpha_0|^2 \quad (6.11)$$

Nach Messung von $|0\rangle$ befindet sich das 2-Qubit-System im Zustand

$$\frac{\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle}{\sqrt{|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2}} = \frac{\alpha_0|0\rangle \otimes (\beta_0|0\rangle + \beta_1|1\rangle)}{\sqrt{|\alpha_0|^2 \underbrace{(|\beta_0|^2 + |\beta_1|^2)}_{=1}}} = \frac{\alpha_0}{\sqrt{|\alpha_0|^2}} |0\rangle \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \quad (6.12)$$

äquivalent zu $|0\rangle$

Analog:

- Mit WS $|\alpha_1|^2$ Messung $|1\rangle$ im 1. Qubit. Nach Messung: $|1\rangle \otimes (|\beta_0|^2 + |\beta_1|^2)$
- Mit WS $|\beta_0|^2$ Messung $|0\rangle$ im 2. Qubit. Nach Messung: $(|\alpha_0|^2 + |\alpha_1|^2) \otimes |0\rangle$
- Mit WS $|\beta_1|^2$ Messung $|1\rangle$ im 2. Qubit. Nach Messung: $(|\alpha_0|^2 + |\alpha_1|^2) \otimes |1\rangle$

Man beachte: Bei separablen 2-Qubit-Systemen können die einzelnen Qubits unabhängig voneinander betrachtet werden.

6.4.2 Beispiel eines verschränkten Zustands

$$|z\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (6.13)$$

Schreibe

$$|z\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \quad (6.14)$$

$$\Rightarrow \text{Gleichungssystem } \begin{cases} \alpha_0\beta_0 = \frac{1}{\sqrt{2}} \Rightarrow \alpha_0 \neq 0 \wedge \beta_0 \neq 0 \\ \alpha_0\beta_1 = 0 \Rightarrow \alpha_0 = 0 \vee \beta_0 = 0 \\ \alpha_1\beta_0 = 0 \Rightarrow \alpha_0 = 0 \vee \beta_0 = 0 \\ \alpha_1\beta_1 = \frac{1}{\sqrt{2}} \Rightarrow \alpha_1 \neq 0 \wedge \beta_1 \neq 0 \end{cases} \not\Leftarrow \text{ nicht erfüllbar.} \quad (6.15)$$

6.4.2.1 Bezeichnung (EPR-Paar) Ein 2-Qubit-System im Zustand $|z\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ wird als EPR-Paar (Einstein, Podolski, Rosen) bezeichnet.

Messung des 1. Qubits eines EPR-Paares liefert $|0\rangle$ mit WS $\frac{1}{2}$, nachher im Zustand

$$\frac{\frac{1}{\sqrt{2}}|00\rangle}{\frac{1}{\sqrt{2}}} = |00\rangle \quad (6.16)$$

D.h. aber: Messung des 2. Qubits liefert ebenfalls Null! (Qubits sind abhängig)

6.5 Fakt

2-Qubit-Systeme entwickeln sich gemäß unitärer Abb. $M \in \mathbb{C}^{4 \times 4}$.

6.5.1 Beispiel: CNOT

$$M_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \begin{array}{l} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |01\rangle \end{array} \quad (6.17)$$

Controlled-NOT: Das 2. Bit wird genau dann invertiert, wenn das 1. (Kontroll-)Bit gesetzt ist.

Man überprüfe, dass $M_{CNOT} \cdot (M_{CNOT}^*)^T = I_2$

6.6 Definition einer Permutationsmatrix

$M \in \mathbb{C}^{m \times m}$ heißt Permutationsmatrix genau dann wenn M in jeder Zeile und Spalte genau eine Eins und sonst Nullen enthält.

6.6.1 Beispiel

M_{CNOT} ist eine Permutationsmatrix.

Übung Permutationsmatrizen sind unitär.

6.7 Bezeichnung (lokal unitär)

Eine unitäre Abbildung, die nur auf einem Teil der Qubits agiert, heißt lokal unitär. Sei $|z\rangle = (c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle)$ ein Qbit und $A, B \in \mathbb{C}^{2 \times 2}$ unitär.

$$c_0(A|0\rangle \otimes B|0\rangle) + c_1(A|0\rangle \otimes B|1\rangle) + c_2(A|1\rangle \otimes B|0\rangle) + c_3(A|1\rangle \otimes B|1\rangle) \quad (6.18)$$

heißt Anwendung von A auf das 1. Qubit und Anwendung von B auf das 2. Qubit.

6.7.1 Spezialfälle

$B = I_2$ liefert eine lokal unitäre Abbildung auf dem 1. Qubit.

$A = I_2$ liefert eine lokal unitäre Abbildung auf dem 2. Qubit.

6.8 Definition des Tensor- bzw. Kronecker-Produkts von Matrizen

Seien

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \in \mathbb{C}^{m \times m}, \quad B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \in \mathbb{C}^{n \times n} \quad (6.19)$$

dann ist das Tensorprodukt von A und B definiert als:

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mm}B \end{pmatrix} \in \mathbb{C}^{mn \times mn}. \quad (6.20)$$

6.8.1 Beispiel

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \quad (6.21)$$

$$\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix} \in \mathbb{C}^{mn \times mn}. \quad (6.22)$$

6.9 Satz über die Beschreibung der Anwendungen von A und B als Tensorprodukt von Matrizen

Seien $A, B \in \mathbb{C}^{2 \times 2}$ unitär. Ferner sei $|z\rangle \in \mathbb{C}^{4 \times 4}$ ein 2-Qubit-System. Die Anwendung von A auf das 1. Qubit und B auf das 2. Qubit wird beschrieben durch $A \otimes B|z\rangle$.

Beweis Für $|00\rangle$, andere Basiszustände folgen analog:

$$A \otimes B|00\rangle = a_{11}b_{11}|00\rangle + a_{11}b_{21}|01\rangle + a_{21}b_{11}|10\rangle + a_{21}b_{21}|11\rangle \quad (6.23)$$

$$= a_{11}|0\rangle \otimes (b_{11}|0\rangle + b_{21}|1\rangle) + a_{21} \otimes (b_{11}|0\rangle + b_{21}|1\rangle) \quad (6.24)$$

$$= (a_{11}|0\rangle + a_{21}|1\rangle) \otimes (b_{11}|0\rangle + b_{21}|1\rangle) \quad (6.25)$$

$$= A|0\rangle \otimes B|0\rangle \quad (6.26)$$

Aus der Linearität von $A \otimes B$ folgt: Gilt obige Identität für alle Basiszustände, so gilt sie auch für die Linearkombinationen von Basiszuständen. Daraus folgt: Die Identität gilt für beliebiges $|z\rangle \in \mathbb{C}^{4 \times 4}$



Man beachte Lokal unitäre Abbildungen auf separablen Zuständen $|z\rangle = |x\rangle \otimes |y\rangle$ liefern stets einen separablen Zustand:

$$|z\rangle \xrightarrow{A \otimes B} A|x\rangle \otimes B|y\rangle \quad (6.27)$$

D.h. lokal unitäre Operatoren allein können keine Verschränkung erzeugen.

6.9.1 Beispiel

Anwendung von W_2 auf das 1. Qubit: $W_2 \otimes I_2$

$$W_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad W_2 \otimes I_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \quad (6.28)$$

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}} \underbrace{(|0\rangle + |1\rangle)}_{W_2} \otimes |0\rangle \quad (6.29)$$

6.10 Beispiel

$$W_4 = W_2 \otimes W_2 \quad W_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad (6.30)$$

$$(6.31)$$

Zustandsübergang für Basiszustand $|x_0x_1\rangle, x_0, x_1 \in \{0, 1\}$:

$$W_4|x_0x_1\rangle = \frac{1}{2}(|00\rangle + (-1)^{x_1}|01\rangle + (-1)^{x_0}|10\rangle + (-1)^{x_0+x_1}|11\rangle) \quad (6.32)$$

$$= \frac{1}{\sqrt{2}} \underbrace{(|0\rangle + (-1)^{x_0}|1\rangle)}_{W_1|x_0\rangle} \otimes \frac{1}{\sqrt{2}} \underbrace{(|0\rangle + (-1)^{x_1}|1\rangle)}_{W_2|x_1\rangle} \quad (6.33)$$

6.11 Satz über unitäre Abbildungen, die sich nicht als Tensorprodukt von Matrizen schreiben lassen

Wir wissen bereits, dass nicht jeder 2-Qubit-Zustand ein Tensorprodukt zweier 1-Qubit-Zustände ist. Analog ist nicht jede unitäre Abbildung $M \in \mathbb{C}^{4 \times 4}$ Tensorprodukt unitärer Matrizen $A, B \in \mathbb{C}^{2 \times 2}$

Beweis

$$M_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ ist unitär} \quad (6.34)$$

Annahme: M_{CNOT} sei Tensorprodukt zweier unitärer Abbildungen, d.h. $M_{CNOT} = A \otimes B$. Dann gilt:

$$|00\rangle \xrightarrow{W_2 \otimes I_2} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{A \otimes B} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \quad (6.35)$$

D.h. wir erhalten ein verschränktes EPR-Paar durch lokal unitäre Abbildungen auf dem separablen Zustand $|00\rangle$. (↯ zu 6.9, siehe Seite 17)

6.12 Definition einer Quantenkopiermaschine

Sei $|x\rangle \in \mathbb{C}^{2 \times 2}$ ein Qubit. Eine Quantenkopiermaschine ist eine unitäre Abbildung M mit:

$$M(|z\rangle \otimes |x\rangle) = |z\rangle \otimes |z\rangle \quad \forall |z\rangle \in \mathbb{C}^{2 \times 2} \quad (6.36)$$

6.13 Satz über die Nichtexistenz von Quantenkopiermaschinen

Es gibt keine Quantenkopiermaschine.

Beweis Annahme: Es gebe eine Quantenkopiermaschine M . Seien $|0\rangle, |1\rangle$ Basiszustände. Aufgrund der Kopiereigenschaft gilt:

$$M(W_2|0\rangle \otimes |1\rangle) = W_2|0\rangle \otimes W_2|0\rangle \quad (6.37)$$

ist separabel. Aufgrund der Linearität von M gilt aber ebenfalls

$$M(W_2|0\rangle \otimes |1\rangle) = M\left(\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) \quad (6.38)$$

$$= \frac{1}{\sqrt{2}}(M|01\rangle + M|11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (6.39)$$

ist verschränkt (EPR-Paar). ↯ zur Annahme.



Man beachte

$$M_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ ist Kopiermaschine für Basiszustände } |0\rangle, |1\rangle \quad (6.40)$$

$$\text{denn } |00\rangle \mapsto |00\rangle \wedge |01\rangle \mapsto |11\rangle \quad (6.41)$$

Allerdings gilt:

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)|0\rangle \xrightarrow{M_{CNOT}} \alpha_0|00\rangle + \alpha_1|11\rangle \neq (\alpha_0|0\rangle + \alpha_1|1\rangle)(\alpha_0|0\rangle + \alpha_1|1\rangle) \text{ für } \alpha_0, \alpha_1 \neq 0 \quad (6.42)$$

7 n-Qubit-Zustände (Register)

Seien $|0\rangle, |1\rangle$ eine orthonormale Basis des \mathbb{C}^2 . Das Basislemma liefert:

$$|0\rangle \otimes |0\rangle, |0\rangle \otimes 1, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle \quad (7.1)$$

als orthonormale Basis des \mathbb{C}^4 . Erneute Anwendung liefert orthonormale Basis $|b_0b_1b_2\rangle, b_j \in \{0, 1\}$ des \mathbb{C}^8 . Induktiv:

$$|b_0 \cdots b_{n-1}\rangle, b_j \in 0, 1 \quad (7.2)$$

ist orthonormale Basis des \mathbb{C}^{2^n}

7.1 Definition: n-Qubit-System

Ein n-Qubit-System ist ein Einheitsvektor im \mathbb{C}^{2^n} der Form.

$$|z\rangle = \sum_{x \in \{0,1\}^n} c_x |x\rangle \text{ mit } c_x \in \mathbb{C}, \sum_{x \in \{0,1\}^n} |c_x|^2 = 1 \quad (7.3)$$

7.1.1 Notation

Wir interpretieren $x = x_{n-1} \cdots x_0$ als Binärdarstellung der natürlichen Zahl

$$\sum_{j=0}^{n-1} x_j 2^{n-1-j} \quad (7.4)$$

Dann schreiben wir:

$$|z\rangle = \sum_{j=0}^{2^n-1} c_j |j\rangle \quad (7.5)$$

7.2 Zustandsübergänge

- Gemäß unitärer Abbildungen $M \in \mathbb{C}^{2^n \times 2^n}$.
- Lokal unitäre Abbildungen auf einzelnen Qubits.

7.2.1 Beobachtung:

- Beschreibung von n-Bit-Register erfordert 2^n Amplituden.
- Operationen besitzen Beschreibungsgröße von $(2^n)^2 \cdot 2^{2n}$.

Deshalb (Feynman):

”Quantenrechner sollten sich nicht effizient auf klassischen Rechnern simulieren lassen, da die Beschreibungsgröße exponentiell in der Anzahl n der Register ist.”

7.3 Definition: Separabilität

Ein n-Qubit-System $|z\rangle \in \mathbb{C}^{2^n}$ heißt separabel genau dann wenn

$$|z\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle \text{ für } |x_j\rangle \in \mathbb{C}^2 \quad (7.6)$$

Nicht separable Zustände heißen beschränkt.

7.3.1 Beispiel

$$|z\rangle = \frac{1}{\sqrt{3}}(|000\rangle - |001\rangle - |111\rangle) \quad (7.7)$$

ist verschränkt. Messung des 1. Qubits liefert $|0\rangle$ mit Wahrscheinlichkeit $\frac{2}{3}$. Danach in

$$\frac{\frac{1}{\sqrt{3}}(|000\rangle - |001\rangle)}{\sqrt{\frac{2}{3}}} = \frac{1}{\sqrt{2}}(|000\rangle - |001\rangle) \quad (7.8)$$

$|1\rangle$ mit WS $\frac{1}{3}$. Danach in

$$\frac{\frac{1}{\sqrt{3}}(|111\rangle)}{\sqrt{\frac{1}{3}}} = |111\rangle \quad (7.9)$$

7.4 Quantenteleportation (Bennett et al. 1993)

7.4.1 Szenario

Alice besitzt Qubit $|z\rangle = c_0|0\rangle + c_1|1\rangle$. Alice und Bob besitzen klassischen Kanal, d.h. sie können Bits versenden, aber keine Qubits. Alice und Bob teilen sich ein EPR-Paar $|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Alice besitzt das 1. Qubit, Bob besitzt das 2. Qubit.

Ziel Alice will $|z\rangle$ an Bob senden.

Probleme

- Alice kennt c_0, c_1 nicht. Messung lässt Wellenfunktion kollabieren.
- Approximieren der Amplitude durch Kopieren von $|z\rangle$ und wiederholtes Messen ist nicht möglich.
- Messung liefert nur Amplitudenquadrate $|c_0|^2, |c_1|^2$ nicht c_0, c_1 .
- Jede Methode die $|z\rangle$ aus klassischer Information konstruiert liefert Kopien von $|z\rangle$. Widerspruch zum No-Cloning-Theorem.

Ausweg Alice muss $|z\rangle$ übertragen, d.h. am Ende besitzt Bob $|z\rangle$, aber Alice nicht mehr. Nutze dafür die Verschränkung durch das EPR-Paar. Betrachte

$$|z\rangle \otimes |e\rangle = (c_0|0\rangle + c_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{7.10}$$

$$= \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|100\rangle + c_1|111\rangle) \tag{7.11}$$

Beachte: Die ersten beiden Bits gehören Alice, das dritte Bit gehört Bob. Alice führt folgenden Schaltkreis aus:

Erläuterungen

1. Alice wenden CNOT auf das 2.Qubit mit dem 1. Qubit als Kontrollbit an:

$$|ze\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|100\rangle + c_1|111\rangle) \tag{7.12}$$

2. Alice wendet nun auf das 1. Qubit die Hadamard-Walsh-Transformation W_2 an:

$$\frac{1}{\sqrt{2}} \left(\frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle + \frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|11\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle - |1\rangle)|10\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle - |1\rangle)|01\rangle \right) \tag{7.13}$$

$$= \frac{1}{2}(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|010\rangle - c_1|110\rangle + c_1|001\rangle + c_1|101\rangle) \tag{7.14}$$

$$= \frac{1}{2}(|00\rangle(c_0|0\rangle + c_1|1\rangle) + |01\rangle(c_0|1\rangle + c_1|0\rangle) + |10\rangle(c_0|0\rangle - c_1|1\rangle) + |11\rangle(c_0|1\rangle - c_1|0\rangle)) \tag{7.15}$$

3. Alice misst ihre beiden Qubits (siehe Tabelle 1) und teilt ihr Messergebnis Bob über den klassischen Kanal mit.

Tabelle 1: Messung der beiden Qubits von Alice - Warscheinlichkeit jeweils $\frac{1}{4}$

Qubit	Zustand nach Messung
$ 00\rangle$	$ 00\rangle(c_0 0\rangle + c_1 1\rangle)$
$ 01\rangle$	$ 01\rangle(c_0 1\rangle + c_1 0\rangle)$
$ 10\rangle$	$ 10\rangle(c_0 0\rangle - c_1 1\rangle)$
$ 11\rangle$	$ 11\rangle(c_0 1\rangle - c_1 0\rangle)$

Tabelle 2: Bobs Operation in Abhängigkeit von Alices Messergebnis

Messergebnis	Operation
$ 00\rangle$	Keine Operation, da Qubit im gewünschten Zustand
$ 01\rangle$	NOT: $c_0 1\rangle + c_1 0\rangle \xrightarrow{\text{NOT}} c_0 0\rangle + c_1 1\rangle$
$ 10\rangle$	Flip: $c_0 0\rangle - c_1 1\rangle \xrightarrow{\text{Flip}} c_0 0\rangle + c_1 1\rangle$
$ 11\rangle$	Flip \circ NOT: $c_0 1\rangle - c_1 0\rangle \xrightarrow{\text{Flip} \circ \text{NOT}} c_0 0\rangle + c_1 1\rangle$

- Bob führt entsprechend des gesendeten Qubits von Alice eine Operation durch (siehe Tabelle 2).

Bobs Operation als Schaltkreis: (Bild folgt)

7.5 Superdense Coding (Bennet, Wiesner 1992)

7.5.1 Szenario

- Alice und Bob besitzen Quantenkanal zum Versenden von Qubits.
- Alice und Bob teilen sich EPR-Paar.

Ziel Versand zweier klassischer Bits (b_0, b_1) mit Hilfe von einem Qbit. Alice führt folgende Operation auf ihrem Qubit aus: (Bild folgt)

$$f(b_0, b_1) = \begin{cases} \text{Flip auf 1. Qubit, falls } b_0 = 1 \\ \text{Not auf 1. Qubit, falls } b_1 = 1 \end{cases} \quad (7.16)$$

Liefert: (siehe Tabelle 3)

Alice sendet Zustand $|z\rangle$ über Quantenkanal an Bob. Bob führt folgende Operation aus (siehe auch Tabelle 4)(Bild folgt):

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix} \quad (7.17)$$

Tabelle 3: Zustände des Qubits nach Alices Operation beim Superdense Coding

b_0	b_1	Operation
0	0	$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
0	1	$\frac{1}{\sqrt{2}}(10\rangle + 01\rangle)$
1	0	$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
1	1	$\frac{1}{\sqrt{2}}(10\rangle - 01\rangle)$

Tabelle 4: Bobs Berechnung der ursprünglichen Bits

Berechnung	Interpretation
$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle) \xrightarrow{M} \frac{1}{2}(00\rangle + 10\rangle + 00\rangle - 10\rangle) = 00\rangle$	$(b_0, b_1) = (0, 0)$
$\frac{1}{\sqrt{2}}(10\rangle + 01\rangle) \xrightarrow{M} \frac{1}{2}(01\rangle - 11\rangle + 01\rangle + 11\rangle) = 01\rangle$	$(b_0, b_1) = (0, 1)$
$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle) \xrightarrow{M} \frac{1}{2}(00\rangle + 10\rangle - 00\rangle - 10\rangle) = 00\rangle$	$(b_0, b_1) = (1, 0)$
$\frac{1}{\sqrt{2}}(10\rangle - 01\rangle) \xrightarrow{M} \frac{1}{2}(- 01\rangle + 11\rangle + 01\rangle + 11\rangle) = 11\rangle$	$(b_0, b_1) = (1, 1)$