Quanteninformatik

MATHEMATISCHE GRUNDLAGEN UND Q-BITS

Seminararbeit

Alexander Hentschel

hentsche@informatik.hu-berlin.de

Institut für Informatik, Humboldt Universität Berlin

Wintersemester 2004

mathematische Grundlagen

Wiederholung

komplexe Zahlen

komplexe Zahlen

Motivation:

Lösung für

$$x^2 = -1$$

Einführung von **imaginäre Einheit**:

$$i := \sqrt{-1}$$

komplexe Zahlen

Karthesischen Darstellung:

$$z = x + iy \text{ mit } x, y \in \mathbb{R}$$

Definition:

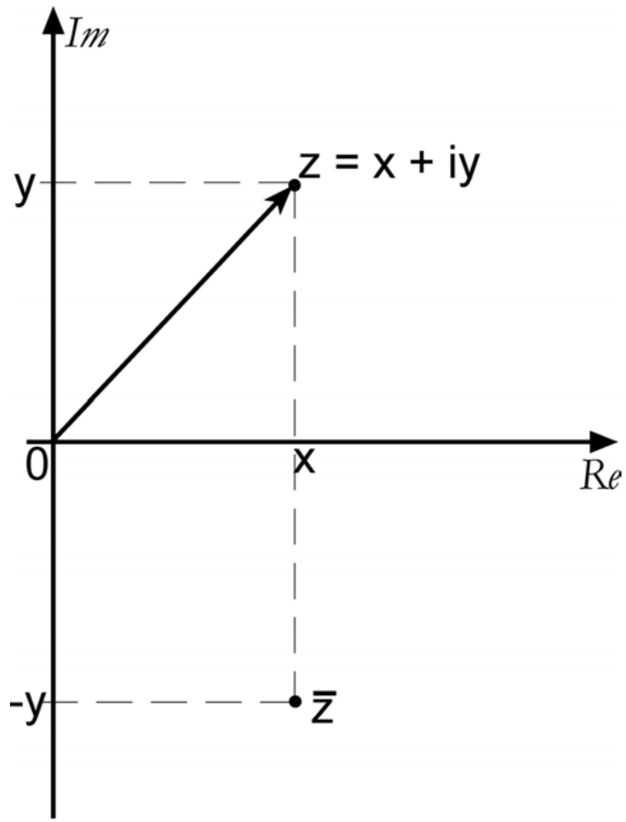
$$\textbf{\textit{Re}(z)} := x$$

$$\textbf{\textit{Im}(z)} := y$$

komplex konjugierte Zahl : $\overline{z} := \overline{x + iy} = x - iy \quad$ zu $z = x + iy$

komplexe Zahlen

Deutung: $z = x + iy$ als Punkt in der Ebene mit karthesischen Koordinaten (x,y):



komplexe Zahlen

Betrag: Länge des Zugehörigen Vektors

$$|z| := \sqrt{x^2 + x^2}$$

Korollar:
wegen $z \cdot \overline{z} = (x + iy)(x - iy) = x^2 + y^2$

$$|z|^2 = z \cdot \overline{z}$$

komplexe Zahlen

Rechenregeln:
wie üblich, unter Beachtung von $i^2 = -1$

- $(a + ib) + (x + iy) = (a + x) + i(b + y)$
- $(a + ib) \cdot (x + iy) = a \cdot x + i^2 b \cdot y + i \cdot b \cdot x + a \cdot iy = (ax - by) + i(ay + bx)$

Euler-Darstellung komplexer Zahlen

e^z-Funktion über unendliche Reihe definiert.
Daraus folgt für $z = iy$ mit $y \in \mathbb{R}$:

$$e^{iy} = \cos(y) + i\sin(y)$$

nach Pythagoras gilt:

$$|e^{iy}| = \sqrt{\cos^2(y) + \sin^2(y)} = \sqrt{1} = 1$$

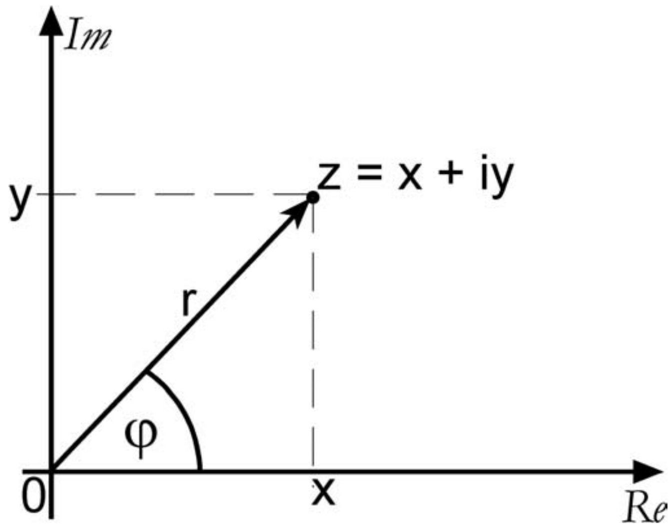
für $z = x + iy$ gilt wegen $e^z = e^{x+iy} = e^x e^{iy}$:

$$e^{x+iy} = e^x(\cos y + i\sin y)$$

Euler-Darstellung komplexer Zahlen

In *Zylinderkoordinaten* (Abbildung rechts):

$$z = r(\cos\varphi + i\sin\varphi)$$



φ — Winkel des Vektors z mit x-Achse

r — Länge des Vektors z

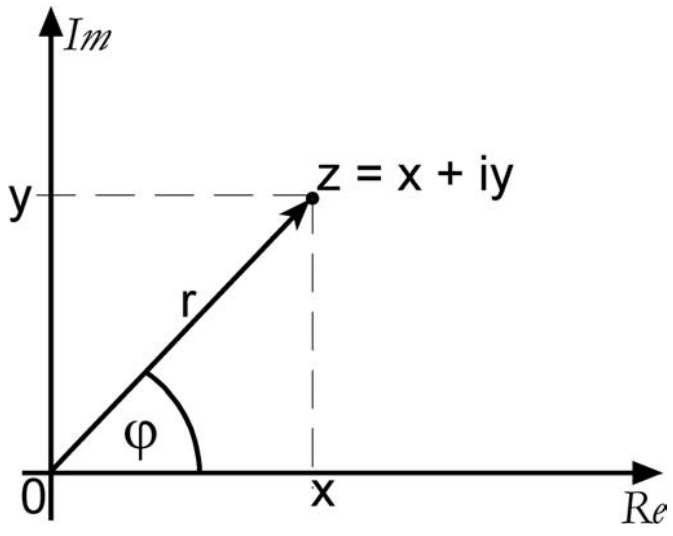
Euler-Darstellung komplexer Zahlen

$z = r(\cos\varphi + i\sin\varphi)$ mit

$$\tan(\varphi) = \frac{y}{x} = \frac{\mathit{Im}(z)}{\mathit{Re}(z)}$$

$$\Rightarrow \varphi = \arctan(\frac{\mathit{Im}(z)}{\mathit{Re}(z)})$$

$$|z| = \sqrt{z \cdot \overline{z}} = r\sqrt{\cos^2 y + \sin^2 y} = r$$



mit $e^{i\varphi} = \cos(\varphi) + i\sin(\phi)$

$$z = r(\cos\varphi + i\sin\varphi) = r \cdot e^{i\varphi}$$

Zusammenfassung: komplexe Zahlen

Darstellungen:

karthesisch: $z = x + iy \quad$ mit $x, y \in \mathbb{R}$ (1)

eulersch: $z = r \cdot e^{i\varphi} \quad$ mit $r = |z|$ und $\varphi = arctan(\frac{y}{x})$ (2)

$$Re(z) := x$$
$$Im(z) := y$$
$$\overline{z} := \overline{x + iy} = x - iy$$

In **Physik**:
zu $z = x + iy$ **komplex konjugierte Zahl** bezeichnet mit z^*:

$$z^* = \overline{z} = x - iy$$

mathematische Grundlagen

Wiederholung

endliche Vektorräume

endliche Vektorräume

Definition: linearer Raum (Vektorraum)
Eine Menge M heißt *linearer Raum* oder *Vektorraum* über $\mathbb{C}$, falls:

- jedem geordneten Paar (u, v) mit $u, v \in M$ eindeutig ein durch $u + v$ bezeichnetes Element aus M zugeordnet wird
- jedem Paar (α, v) mit $\alpha \in \mathbb{C}$ und $u \in M$ eindeutig ein mit αu bezeichnetes Element aus M zugeordnet wird

so dass für alle $u, v, w \in M$ und alle $\alpha, \beta \in \mathbb{C}$ folgendes gilt:

endliche Vektorräume

Fortsetzung Definition: linearer Raum (Vektorraum)
M heißt *linearer Raum* oder *Vektorraum* über $\mathbb{C}$, falls für alle $u, v, w \in M$ und alle $\alpha, \beta \in \mathbb{C}$ folgendes gilt:

1. $u + v = v + u$ (Kommutativität)
2. $(u + v) + w = u + (v + w)$ (Assoziativität)
3. $\exists! o \in M : z + o = z$ für alle $z \in M$ (Existenz eines Nullelements)
4. Zu jedem $z \in M$ gibt es ein eindeutig bestimmtes Element in M, welches mit $(-z)$ bezeichnet wird, so daß $z + (-z) = o$ (inverses Element)
5. $\alpha(u + v) = \alpha u + \alpha v$ (Distributivität)
6. $(\alpha\beta)u = \alpha(\beta u)$

endliche Vektorräume

Definition: Skalarprodukt
Sei M ein linearer Raum über $\mathbb{C}$.
Das *Skalarprodukt* ist eine Funktion die jedem Vektorpaar $u, v \in M$ eine Zahl $(u, v) \in \mathbb{C}$ zuordnet, so dass für alle $u, v, w \in M$ und alle $\alpha, \beta \in \mathbb{C}$ gilt:

1. $(u, u) \geq 0$ mit $(u, u) = 0$ genau dann, wenn $u = 0$
2. $(w, \alpha u + \beta v) = \alpha(w, u) + \beta(w, v)$
3. $\overline{(u, v)} = (v, u)$

Aus den letzten beiden Punkten der Definition ergibt sich sofort:

$$(\alpha u + \beta v, w) = \overline{\alpha}(u, w) + \overline{\beta}(u, w)$$

endliche Vektorräume

Definition des *Skalarprodukts* läßt die konkrete Festsetzung der Funktion offen

übliche komplexe Skalarprodukt $\langle\cdot|\cdot\rangle$ auf $\mathbb{C}^n$:

$$\langle x|y\rangle = \sum_{i=1}^{n} \overline{x_i} y_i \quad \text{für } x, y \in \mathbb{C}^n$$

Beachte: linker Vektor wird komplex konjugiert.

endliche Vektorräume

Definition: Basis
Es sei M ein *linearer Raum (Vektorraum)*.
Ein System $b_1, ..., b_n$ von Elementen des linearen Raumes M heißt genau dann eine Basis von M, wenn sich jedes $u \in M$ eindeutig in der Form

$$u = \alpha_1 b_1 + ... + \alpha_n b_n$$

darstellen läßt, wobei gilt: $\alpha_1, ..., \alpha_n \in \mathbb{R}$.

Man nennt u eine **Linearkombination** aus den Basisvektoren.

endliche Vektorräume

Besonders wichtig: **orthonormale Basen**

Definition Orthonormalität:
Für bel. Basisvektoren b_n und b_m gilt:

$$\langle b_n | b_m \rangle = \delta_{n,m} = \begin{cases} 1 & \text{falls } n = m, \\ 0 & \text{falls } n \neq m. \end{cases}$$

$$|b_n| = 1$$

Ist eine nicht orthonormale Basis bekannt, so läßt sich diese mittels Gram-Schmidt in eine orthonormale Basis überführen.

endliche Vektorräume

lineare Abbildungen:
Es sei:

Matrix $A \in \mathbb{C}^{m \times n}$
Vektor $v \in \mathbb{C}^n$

$$\Rightarrow \quad Av \in \mathbb{C}^m$$

Somit: Matrizen sind Abbildungen zwischen linearen Räumen: $A : \ \mathbb{C}^n \longrightarrow \mathbb{C}^m$

- mathematische Modell der Quantenmechanik operiert in linearen Räumen
- physikalische Prozesse durch Abbildungen in linearen Räumen mittels Matrizen, genannt **Operatoren** modelliert

endliche Vektorräume

Spezielle Operatoren (Matrizen):

adjungierter Operator:
ist $A : M \to M$ ein linearer Operator, dann wird ihm auf eindeutige Weise ein linearer Operator $A^+ : M \to M$ zugeordnet, welcher folgender Relation genügt:

$$\langle u|Av\rangle = \langle A^+u|v\rangle \quad \text{für alle } u, v \in M$$

Für *übliche komplexe Skalarprodukt* auf $\mathbb{C}^n$:
A^+ ist transponierte Matrix (Vertauschen von Zeilen und Spalten) mit komplex konjugierten Werten

endliche Vektorräume

Spezielle Operatoren (Matrizen):

unitärer Operatoren:
adjungierter Operator für den gilt:

$$AA^{+} = \widehat{1}$$

($\widehat{1}$ ist die Einheitsmatrix)

endliche Vektorräume

Der Hilbertraum
ist Erweiterung eines *endlichen linearen Raumes* auf die Dimension abzählbar unendlich

Quantenmechanik operiert im Hilbertraum

bei Quanteninformatik nur Systeme mit endlich vielen Zuständen: Hilbertraum $\longrightarrow$ linearen Raum

endliche Vektorräume

Nomenklatur im Hilbertraum:

- Elemente aus $\mathcal{H}$ mit $|f\rangle$ bezeichnet (Schreibweise nach Dirac in Anlehnung an Skalarproduktes: $\langle g|f\rangle$)
- analog zum linearen Raum gilt:

$$\langle g|(\alpha|f_1\rangle + \beta|f_2\rangle) = \alpha\langle g|f_1\rangle + \beta\langle g|f_2\rangle$$
$$\langle g|f\rangle = \langle f|g\rangle^*$$

- Hilbertraum hat eine orthnormale Basis $\{|u_n\rangle\}$ (unendlicher Dimension):

$$\langle u_m|u_n\rangle = \delta_{m,n} = \begin{cases} 1 & \text{für } m = n, \\ 0 & \text{für } m \neq n. \end{cases}$$

endliche Vektorräume

Nomenklatur im Hilbertraum (Fortsetzung):

- $$\| \, |f\rangle \, \| := \sqrt{\langle f|f\rangle}$$
- wie bei Skalarprodukt:
  linker Vektor $\langle f|$ von $\langle g|f\rangle$ komplex konjugiert.

Bezeichnung:
$\langle g|$ mit Bra-Vektor
$|f\rangle$ als Ket-Vekrot
(von Bra-c-Ket)

Grundlagen der Quantenmechanik

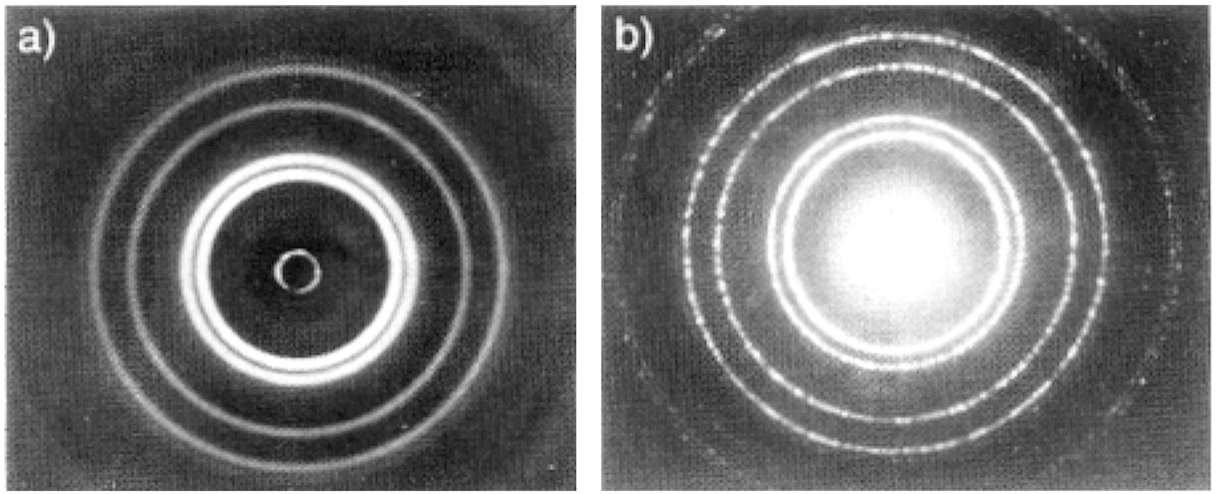
Einleitung

Grundlagen der Quantenmechanik

klassischen Physik:

Teilchen (Elektronen, Protonen, Atome, Ionen, Moleküle)
wie Billardkugeln beschrieben

Jedoch Experiment:
a) Röntgenbeugung b) Elektronenbeugung an dünner Folie



Grundlagen der Quantenmechanik

klassischen Physik:
Teilchen (Elektronen, Protonen, Atome, Ionen, Moleküle) wie Billardkugeln beschrieben

Quantenmechanik:
in mikroskopischen Größenordnungen haben Teilchen Welleneigeneigenschaften

Grundlagen der Quantenmechanik

Quantenmechanisches Kastenpotential:

Teilchenwelle muß stehende Welle im Potentialtopf sein

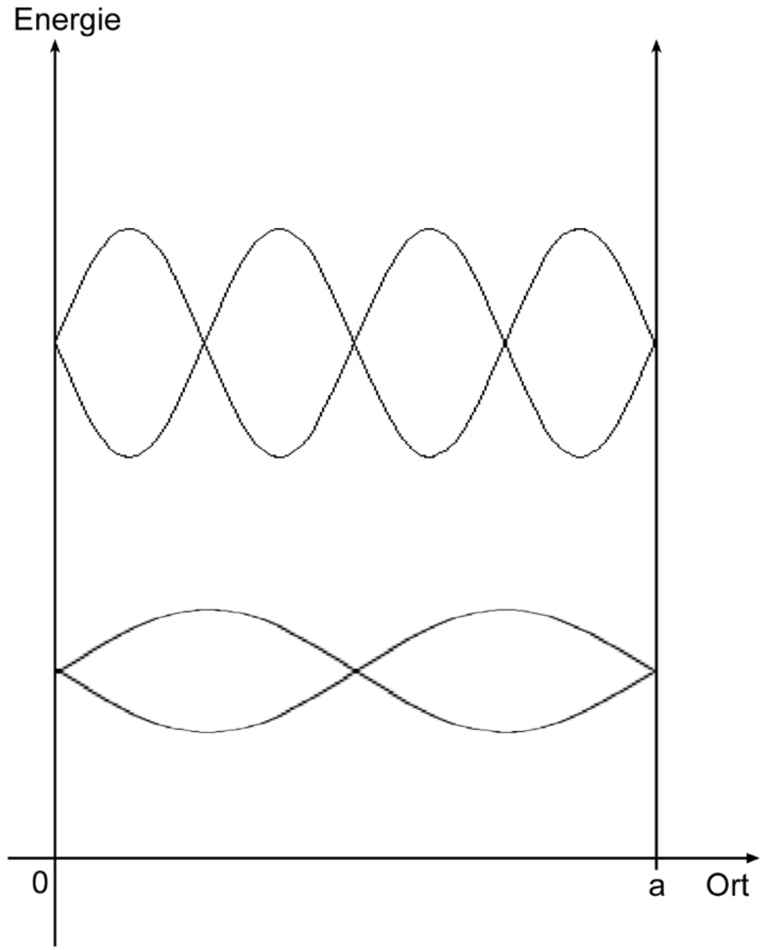
$\Rightarrow \quad n\lambda = 2a$

deBroglie-Wellenlänge λ eines Teilchens:

$\lambda = \frac{h}{p} \Leftrightarrow p = \frac{h}{\lambda} = \frac{hn}{2a}$

$\Rightarrow \quad E_{kin} = \frac{p^2}{2m} = \frac{h}{8ma^2} n^2$

Energie ist quantisiert!



Grundlagen der Quantenmechanik

Teilchen im Potentialtopf kann unendlich viele diskrete Eneriewerte annehmen

Jeder Energie $E(n)$ entspricht eine Wellenfunktionen Ψ_n.

Postulat der Quantenmechanik:
Ein Quantensystem kann sich in einer Überlagerung - genannt Superposition - von beliebig vielen seiner diskreten Quantenzustände befinden.

Grundlagen der Quantenmechanik

Darstellung von Superpositionszuständen:
Wellenfunktionen Ψ_n als Basisvektoren des Hilbertraumes:

Basis: $\{|\Psi_n\rangle\}$

Überlagerung durch Linearkombination aus Basis:

resultierenden Zustandsvektor

$$|\psi\rangle = \alpha|\Psi_1\rangle + \beta|\Psi_2\rangle \quad \text{mit } \alpha, \beta \in \mathbb{C}$$

Grundlagen der Quantenmechanik

Zustandsvektor:

$$|\psi\rangle = \alpha|\Psi_1\rangle + \beta|\Psi_2\rangle \quad \text{mit } \alpha, \beta \in \mathbb{C}$$

Born'sche Wahrscheinlichkeitsinterpretation:

Die Wahrscheinlichkeit ein Teilchen mit der Wellenfunktion $|\psi\rangle = ... + \alpha|\Psi_i\rangle + ...$ im Zustand $|\Psi_i\rangle$ zu finden (messen) ist $|\alpha|^2 = \parallel \langle\Psi_i|\psi\rangle \parallel^2$.

Grundlagen der Quantenmechanik

Folgen der Born'schen Deutung:
Sei System ausschließlich im ersten Energieniveau:
$|\psi\rangle = |\Psi_1\rangle$

- Wahrscheinlichkeit es im dritten Energieniveau $|\Psi_3\rangle$ zu messen ist null
  Mathematisch: $\| \langle\Psi_3|\psi\rangle \|^2 = \| \langle\Psi_3|\Psi_1\rangle \|^2 = 0$!
- jede Messung des Energiezustandes liefert Ergebnis Zustand 1:
  $\Rightarrow \| \langle\Psi_1|\psi\rangle \|^2 = \| \langle\Psi_1|\Psi_1\rangle \|^2 = 1$
- also $\langle\Psi_m|\Psi_n\rangle = \delta_{m,n} = \begin{cases} 1 & \text{für } m = n, \\ 0 & \text{für } m \neq n. \end{cases}$

Grundlagen der Quantenmechanik

Messung eines Quantenzustandes:
Wie bei Teilchen im Potentialtopf:
für Quantensystem nur diskrete Energiewerte zugelassen, also messbar

Messung eines Systems im Superpositionszustand:
Durch Messung wird Systems auf einen konkreten (an der Superposition beteiligten!) Eigenzustand festgelegt.

System unmittelbar vor der Messung im Zustand
$|\psi\rangle = \alpha|\Psi_1\rangle + \beta|\Psi_2\rangle$
Messung liefert mit Wahrscheinlichkeit $|\alpha|^2$ den Eigenwert von $|\Psi_1\rangle$.
System befindet nach Messung im Zustand $|\Psi_1\rangle$.

Grundlagen der Quantenmechanik

System vor Messung im Zustand $|\psi\rangle = \alpha|\Psi_1\rangle + \beta|\Psi_2\rangle$
System nach Messung im Zustand $|\Psi_1\rangle$

Superpositionszustand wird durch die Messung zerstört

Man nennt diesen Effekt:

Reduktion des Zustandes oder auch
Informationskollaps

(da fast sämtliche im Quantensystem gespeicherte Information verloren geht)

Q-Bits

Quanten-Bits

Systeme mit einem Q-Bit

Q-Bits

Quantensysteme mit zwei diskreten Zuständen:

- Polarisation eines Photons
- Elektronenspin
- Ausrichtung eines Kernspins im Magnetfeld
- zwei unterschiedliche Anregunsgzustände eines Atoms

Grundzustand meist mit $|0\rangle$ bezeichnet
erste angeregte Niveau mit $|1\rangle$

Forderung: System nun in diesen Zuständen
(und deren Superposition)

Q-Bits

Definition:

Standard-Basis: $\mathcal{B} = \{|0\rangle, |1\rangle\}$ mit $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Wellenfunktion des Bits (in Standardbasis):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{mit } \alpha, \beta \in \mathbb{C}$$

Q-Bits

Wellenfunktion des Bits (in Standardbasis):
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ mit $\alpha, \beta \in \mathbb{C}$

System soll sich nur in Zuständen $|0\rangle$ und $|1\rangle$ befinden:
$|\alpha|^2 + |\beta|^2 = 1$

mit Eulerformel:

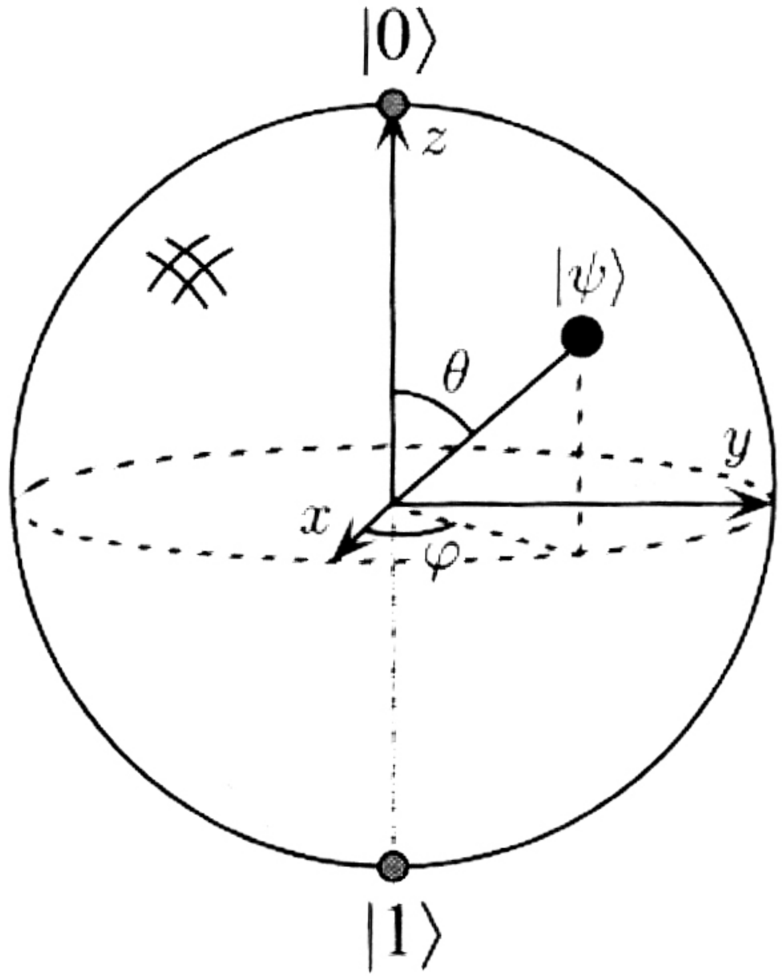
$$|\psi\rangle = (\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle)$$

Jedem Winkelpaar (θ, φ) ist eindeutig umkehrbar ein Punkt auf der Einheitskugel zugeordnet

Q-Bits

$$|\psi\rangle = (\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle)$$

Anschauliches Modell:
Bloch Sphere

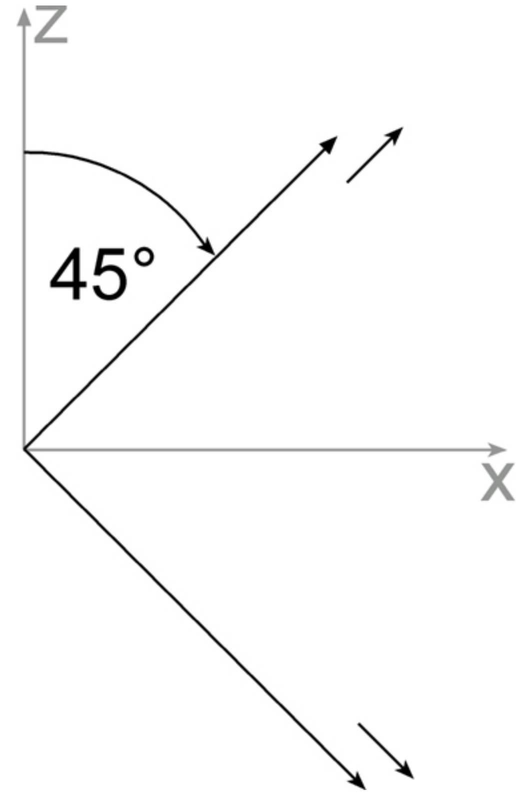


Q-Bits

andere Basis:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \qquad \text{(normiert)}$$

$$|\searrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \qquad \text{(normiert)}$$



Q-Bits

andere Basis:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \qquad \text{(normiert)}$$

$$|\searrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \qquad \text{(normiert)}$$

$$\Rightarrow$$

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|\nearrow\rangle + |\searrow\rangle\right) \quad \text{und} \quad |1\rangle = \frac{1}{\sqrt{2}}\left(|\nearrow\rangle - |\searrow\rangle\right)$$

Für Superpositionszustand:

$$|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|\nearrow\rangle + \frac{\alpha-\beta}{\sqrt{2}}|\searrow\rangle$$

Q-Bits

$$|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|\nearrow\rangle + \frac{\alpha-\beta}{\sqrt{2}}|\searrow\rangle$$

Für Q-Bit im Zustand $|\psi\rangle = |0\rangle$:
$\alpha = 1$ und $\beta = 0$

Messung in Basis $\{|\nearrow\rangle, |\searrow\rangle\}$:
Wahrscheinlichkeit $\frac{1}{2}$ für beide Zustände

Mit einem Quantencomputer ist die Erzeugung *echter* Zufallszahlen möglich !

Q-Bits

Zustand $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ durch Operation A verändern:

$$A : \mathcal{H}_2 \longrightarrow \mathcal{H}_2 \qquad \text{mit } A : |\psi\rangle \mapsto |\phi\rangle$$

muss wieder gelten: $\| \, |\phi\rangle \, \| = 1$

Per Postulat sind **Operatoren unitär**

Q-Bits

Hadamard Gatter H und Paulimatrizen σ_x, σ_y und σ_z:

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

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Systeme von Q-Bit

Systeme von Q-Bit

Systeme von Q-Bit

System aus zwei Q-Bits klassisch in 4 Zuständen möglich:

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

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

Systeme von Q-Bit

Sei $|\varphi\rangle = a|0\rangle + b|1\rangle$ und $|\phi\rangle = c|0\rangle + d|1\rangle$

$$\begin{aligned}
|\psi\rangle := |\varphi\phi\rangle := |\varphi\rangle|\phi\rangle &= (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) \\
&= ac|0\rangle|0\rangle + ad|0\rangle|1\rangle + bc|1\rangle|0\rangle + bd|1\rangle|1\rangle \\
&= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle
\end{aligned}$$

Nach der Born'schen Deutung:
System mit der Wahrscheinlichkeit:

- $|ac|^2$ im Zustand $|00\rangle$
- $|ad|^2$ in $|01\rangle$

Systeme von Q-Bit

$$|\psi\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

Erste Bit hat mit Wahrscheinlichkeit $|ac|^2 + |ad|^2$ Wert 0.

Nach Messung des Ersten Bits:
zwei-Bit Quantenregister im Superpositionszustand aus $ac|00\rangle$ und $ad|01\rangle$

Post-Messungs-Zustand:

$$|\psi'\rangle = \frac{ac|00\rangle + ad|01\rangle}{\sqrt{|ac|^2 + |ad|^2}}$$

Normierungsfaktor: $\sqrt{|ac|^2 + |ad|^2}$

Systeme von Q-Bit

Register aus N Q-Bits in Basisraum mit 2^N Dimensionen:

$$\mathcal{B}^N := \{|i\rangle \ |i \in \{0,1\}^N\}$$

verkürzte Schreibweise:
Binärcode ersetzt durch Dezimalzahl
Bsp: $|101\rangle \equiv |5\rangle$

Zustand eines $|\psi\rangle$ des N-Q-Bit-Registers:

$$|\psi\rangle = \sum_{i\in\{0,1\}^N} \alpha_i |i\rangle\,, \qquad \text{mit} \sum_{i\in\{0,1\}^N} |\alpha_i|^2 = 1$$

Systeme von Q-Bit

Postulat der Quantenmechanik:
zeitliche Entwicklung eines Quantensystems durch einen *unitären* Operator $\widehat{U}$ (eine Matrix) beschrieben

Für unitäre Operatoren galt: $\exists \widehat{U}$ mit $\widehat{U}\widehat{U}^{-1} = \widehat{1}$

jeder Physikalische Prozess umkehrbar:
Mikroreversibilität $\Rightarrow$ jede logische Operation muss

umkehrbar sein

Systeme von Q-Bit

Betrachten:
zwei Q-Bit-Register
mathematische Operation R_2, die nur auf das zweite Bits wirkt

Register im Zustand: $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

$$R_2|\psi\rangle = a|0\,R(0)\rangle + b|0\,R(1)\rangle + c|1\,R(0)\rangle + d|1\,R(1)\rangle$$

einzelne Q-Bit-Operation wirkt *gleichzeitig* auf *alle* 2^N *Zustände* des Systems: **Quantenparallität**

Quantencomputer und Information

Quantencomputer und Information

Quantencomputer und Information

Quantenregister aus N Q-Bits:
Überlagerungszustand aus 2^N Basiszuständen möglich

$$|\psi\rangle = \alpha_1|0\rangle + \alpha_2|1\rangle + \alpha_{2^N}|2^N - 1\rangle \qquad \text{mit } \alpha_1, ...\alpha_{2^N} \in \mathbb{C}$$

2^N komplexe Zahlen (beliebiger Genauigkeit) speicherbar

Quantencomputer und Information

Problem: nur eine Messung um Ergebnis auszulesen, denn

- Information wird durch Messen zerstört
- Rechnung nicht (mit gleichem Ergebnis) wiederholbar, da Quantencomputer nur probabilistische Resultate liefert
- Ergebnis nicht kopierbar

Quantencomputer und Information

Problem: nur eine Messung um Ergebnis auszulesen, denn

- Information wird durch Messen zerstört
- Rechnung nicht (mit gleichem Ergebnis) wiederholbar, da Quantencomputer nur probabilistische Resultate liefert
- Ergebnis nicht kopierbar

No-Clonig-Theorem:
Es gibt keine unitäre Transformation $\widehat{U}$*, die ein Q-Bit kopieren kann.*

Quantencomputer und Information

Anforderungen an einen Quantencomputer (nach David DiVincenzo):

- Jedes Q-Bit gut charakterisiert (eindeutig ansprechbar)
- Erweiterbarkeit des Systems auf viele Q-Bits (Skalierbarkeit)
- Alle Q-Bits müssen in einem wohl definierten Anfangszustand präparierbar sein, z.B. in $|000..0\rangle$.
- Die möglichen Operationen auf dem System müssen einen universellen Satz von Quantenoperationen enthalten.

Quantencomputer und Information

Anforderungen an einen Quantencomputer (Fortsetzung):

- Überlagerungszustände der Q-Bits dürfen nur in Zeitskalen zerfallen, die viel länger als die Zeit einer elementaren Gatteroperation sind.
- Es muss eine Möglichkeit geben, den Zustand der Q-Bits zu messen un in eine klassische Anzeige auszulesen.

Literaturverzeichnis

Literatur

[1] **Teubner - Taschenbuch der Mathematik**

von: I.N.Bronstein und K.A. Semendjajew

Verlag: B.G. Teubner Verlagsgesellschaft Leipzig

[2] **Quantum Computation and Quantum Information**

von: Michael A. Nielsen & Isaac L. Chuang

Verlag: Cambridge University Press

Literaturverzeichnis

Literatur

[3] **Fundamentals of Quantum Information**
von: Dieter Heiss
Verlag: B.Springer-Verlag

[4] **Physik Journal Januar 2004**
Artikel: *Ein Atomarer Abakus* von: D. Leibfried & T. Schätz
Verlag: Wiley-VCH Verlag

Ende