Quantencomputing

Modul 7270

Martin Rehberg

Hessen3C / Hochschule RheinMain

Inhaltsverzeichnis

1. Grundlagen des Quantencomputing
   - Einleitung
   - Exkurs: Berechenbarkeit & Turingmaschinen
   - Grundlagen der Quantenmechanik
   - Quantenzufallsgenerator & Problem von Deutsch
   - Tensorprodukt, Messen von Registern & Verschränkung
2. Quantencomputing und Kryptographie
   - Das RSA-Verfahren & periodische Funktionen
   - Schnelle- & Quanten-Fouriertransformation
   - Simons- & Shors Algorithmus
3. Quantum Key Distribution (*optional*)

Inhaltsverzeichnis

1. Grundlagen des Quantencomputing
   - Einleitung
   - Exkurs: Berechenbarkeit & Turingmaschinen
   - Grundlagen der Quantenmechanik
   - Quantenzufallsgenerator & Problem von Deutsch
   - Tensorprodukt, Messen von Registern & Verschränkung
2. Quantencomputing und Kryptographie
   - Das RSA-Verfahren & periodische Funktionen
   - Schnelle- & Quanten-Fouriertransformation
   - Simons- & Shors Algorithmus
3. Quantum Key Distribution (*optional*)

Einleitung

Ziele von Quantencomputing:

- Quantencomputer bauen
- Quantenalgorithmen entwickeln / untersuchen

Einleitung

Ziele von Quantencomputing:

- Quantencomputer bauen
- Quantenalgorithmen entwickeln / untersuchen

Ziel der Vorlesung:

- Einführung in die grundlegende Funktionsweise von Quantencomputern
  - physikalischen Grundlagen als *gegeben* annehmen
  - Mathematik werden wir nach Bedarf erarbeiten / wiederholen
- Anwendungen mit Blick auf Verschlüsselungsverfahren

Einleitung

Literatur:[1]

- Matthias Homeister - Quantencomputing verstehen (**Hauptquelle**), 5. Auflage, Springer, 2018.
- Artuhr Pittenger - An Indroduction to Quantum Computing Algorithms, Birkhäuser, 2001.
- Michael Nielsen, Isaac Chuang - Quantum Computation and Quantum Information, 10. Auflage, Cambridge University Press, 2010.
- Dirk Hoffmann - Theoretische Informatik, 2. Auflage, Hanser, 2011.

[1]verwendete Grafiken sind allesamt dem Buch von M. Hohmeister oder Wikipedia (public domain) entnommen

Einleitung

Klassische Welt

- mechanische Rechenmaschinen
  - Difference Engine, Analytical Engine - Charles Babbage
  - Schachmaschine - Leonardo Quevedo
- elektromechanische Rechenmaschinen
  - Z3, Z4 - Konrad Zuse
  - Kryptoanalyse - Colossus
- *moderne* Rechenmaschinen

Einleitung

Beobachtung

Ein **klassisches Bits** kann genau zwei unterschiedliche Zustände annehmen: 0 und 1. Sie haben zwei wesentliche Eigenschaften

- **Realismus:** Der Wert eines Bits ist zu jedem Zeitpunkt der Berechnung eindeutig bestimmt, d.h. entweder 0 oder 1. Er kann ausgelesen werden und der Prozess des Auslesens ändert den Wert des Bits nicht.
- **Lokalität:** Wird der Wert eines bestimmten einzelnen Bits verändert, so ändert das nicht den Wert *irgendeines* anderen Bits.

Einleitung

Quantenwelt

- Quantencomputer rechnen mit Quantenbits
- Quantenbits folgen den Gesetzen der Quantenmechanik
- Quantenbits sind in einem Zustand der *Superposition*, d.h. sind von der Form $\alpha|0\rangle + \beta|1\rangle$
- Quantenbits können in einem *verschränkten* Zustand sein

Einleitung

Beobachtung

Ein **Quantenbit** ist in einem Zustand der Superposition. Im Vergleich zum klassischen Bit stellen wir fest:

- **Veränderung beim Messen:** Wird ein Quantenbit gemessen, so wird der Zustand der Superposition aufgehoben und das Quantenbit wechselt in einen der beiden (klassischen) Zustände 0 oder 1. Durch den Messvorgang wird das Quantenbit mit dem entsprechenden Werte 0 oder 1 überschrieben.
- **Verschränkung:** Die Veränderung eines Quantenbits kann unmittelbar (also im selben Augenblick) die Eigenschaft eines anderen Quantenbits verändern.

Einleitung

Verschränkung von Quantenbits hat weitreichende Folgen, etwa

- Primfaktorisierung $\rightsquigarrow$ RSA-Verfahren
- diskreter Logarithmus $\rightsquigarrow$ Elliptic Curve Diffie-Hellman
- Suche in Datenbanken, u.v.m.

Einleitung

Verschränkung von Quantenbits hat weitreichende Folgen, etwa

- Primfaktorisierung $\rightsquigarrow$ RSA-Verfahren
- diskreter Logarithmus $\rightsquigarrow$ Elliptic Curve Diffie-Hellman
- Suche in Datenbanken, u.v.m.

Es gibt aber nicht nur Vorteile:

- No-Cloning Theorem
- (vermutlich) können Quantencomputer NP-vollständige Probleme nicht effizient lösen
- Fehlerkorrektur

Berechenbarkeit und Turingmaschinen

Berechnung (intuitiv)

Einem *Berechnungsgerät* wir eine Eingabe übergeben. Anschließend führt das Gerät deterministisch Berechnungen durch.
Eine *Berechnung* ist eine Folge von Zuständen des Berechnungsgerätes. Jeder Rechenschritt ist ein Übergang zwischen den Zuständen und hängt allein vom aktuellen Zustand ab.

Berechenbarkeit und Turingmaschinen

Definition: Alphabet, Zeichen, Wort, formale Sprache

- Ein *Alphabet* Σ ist eine endliche Menge von Symbolen.
- Ein Element $\sigma \in \Sigma$ heißt *Zeichen* des Alphabets.
- Ein Element $\omega \in \Sigma^* := \bigcup_{i=0}^{\infty} \Sigma^i$ wird *Wort* über Σ genannt, wobei $\Sigma^0 := \{\varepsilon\}$. Man nennt ε das *leere Wort*.
- Eine Teilmenge $L \subseteq \Sigma^*$ wird *formale Sprache* über Σ genannt.

Berechenbarkeit und Turingmaschinen

Definition: Alphabet, Zeichen, Wort, formale Sprache

- Ein *Alphabet* Σ ist eine endliche Menge von Symbolen.
- Ein Element $\sigma \in \Sigma$ heißt *Zeichen* des Alphabets.
- Ein Element $\omega \in \Sigma^* := \bigcup_{i=0}^{\infty} \Sigma^i$ wird *Wort* über Σ genannt, wobei $\Sigma^0 := \{\varepsilon\}$. Man nennt ε das *leere Wort*.
- Eine Teilmenge $\mathrm{L} \subseteq \Sigma^*$ wird *formale Sprache* über Σ genannt.

Beispiel Palindromsprache

Für $\Sigma = \{a, b, c, ..., x, y, z\}$ sei L die Menge aller spiegelbildlich angeordneten Zeichenketten. In dieser Sprache sind die Wörter *aabaa*, *anna* und *otto* enthalten. Nicht enthalten sind *abab*, *abc* oder *aaba*.

Berechenbarkeit und Turingmaschinen

Definition: Turingmaschine

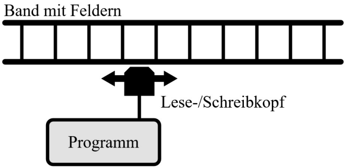
Eine (deterministische) *Turingmaschine* (TM) ist ein 7-Tupel $(S, \Sigma, \Pi, \delta, s_0, \Box, E)$, bestehend aus

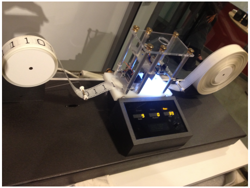
- der endlichen *Zustandsmenge* S,
- dem endlichen *Eingabealphabet* Σ,
- dem *Bandalphabet* Π mit $\Pi \supset \Sigma$,
- der *Zustandsübergangsfunktion* $\delta : S \times \Pi \to S \times \Pi \times \{\leftarrow, \to\}$,
- dem *Startzustand* s_0,
- dem *Blank-Symbol* $\Box \in \Pi \setminus \Sigma$,
- der Menge der *Endzustände* $E \subseteq S$.

Berechenbarkeit und Turingmaschinen

Startkonfiguration:

- TM ist im Startzustand s_0
- zu verarbeitendes Eingabewort $\omega \in \Sigma^*$ steht auf dem Band
- Lese-/Schreibkopf über dem ersten Eingabezeichen positioniert
- alle Felder links und rechts des Eingabewortes sind mit dem Blank-Symbol $\square$ beschrieben

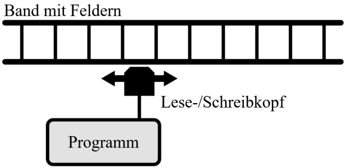


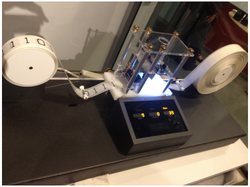


Berechenbarkeit und Turingmaschinen

Programmablauf:

- Der Lese-/Schreibkopf liest das aktuelle Bandzeichen σ ein
- Der Funktionswert $(s', \sigma', r) = \delta(s, \sigma)$ wird berechnet
- Das Bandzeichen wird durch σ' ersetzt
- Der Kopf wird nach links $(\leftarrow)$ oder rechts $(\rightarrow)$ bewegt
- Der Folgezustand s' wird angenommen





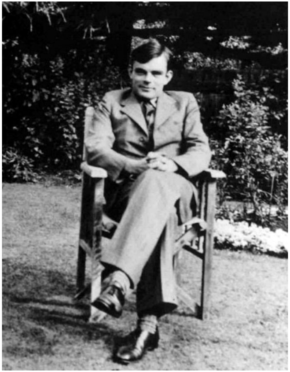
Berechenbarkeit und Turingmaschinen

Definition: (Turing-) Berechenbarkeit

Eine Funktion $f : \Sigma^* \to \Sigma^*$ heißt *(turing-) berechenbar*, wenn eine TM $T = (S, \Sigma, \Pi, \delta, s_0, \Box, E)$ existiert, die für alle $\omega \in \Sigma^*$ mit $f(\omega)$ auf dem Band anhält oder in eine Endlosschleife gerät, wenn $f(\omega)$ nicht definiert ist.

Variationen von TM:

- mehrere Bänder / Folgezustände
- Folgezustände per Münzwurf



Alan Turing

Berechenbarkeit und Turingmaschinen

These von Church (1936)

Jede im intuitiven Sinn berechenbare Funktion ist durch eine Turingmaschine berechenbar.

Mehr noch: Alles was mit einem QC berechenbar ist, kann auch mit einer TM berechnet werden.
Aber: Wahrscheinlich gibt es praktisch relevante Probleme, die mit QC *schneller* gelöst werden können.

Alonzo Church

Grundlagen der Quantenmechanik

Ziel: Eine Idee für die Beobachtungen der Physik gewinnen, nicht aber die physikalischen Beobachtungen in der Quantenwelt erklären.

Wir wollen die Begriffe *Superposition* und *Messen* veranschaulichen.

Gedankenexperiment:
Schrödingers Katze

Erwin Schrödinger

Grundlagen der Quantenmechanik

Klassisch: Eine Katze sitzt in einer undurchsichtigen Box. Diese enthält einen (klassischen) Mechanismus, der die Katze mit Wahrscheinlichkeit $1/2$ sofort tötet.

Die Katze ist *entweder* tot *oder* lebendig.

Grundlagen der Quantenmechanik

Modifikation: Der Mechanismus wird mit einem quantenmechanischen Prozess gekoppelt, etwa dem Zerfall eines radioaktiven Atoms.

Quantenmechanisch: Das Atom ist *gleichzeitig* unverändert bzw. zerfallen, also ist die Katze *gleichzeitig* tot und lebendig (Zustand der Superposition). Wird die Box geöffnet, dann ist die Katze *entweder* tot *oder* lebendig. Das öffnen der Box entspricht dem Messen.

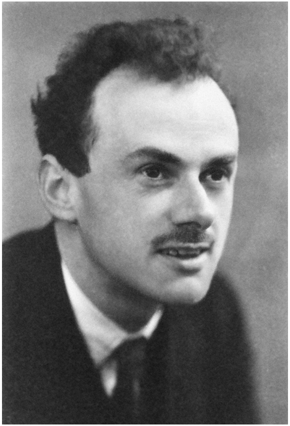
Grundlagen der Quantenmechanik

Für die Beschreibung quantenmechanischer Zustände verwendet man die auf Paul Dirac zurückgehende *ket-Notation*.

Definition: Quantenbit

Ein *Quantenbit* (*Qubit*) nimmt Zustände der Form $\alpha|0\rangle + \beta|1\rangle$ mit $\alpha, \beta \in \mathbb{C}$ an. Die Zahlen α, β heißen *Amplituden* und genügen der Bedingung $|\alpha|^2 + |\beta|^2 = 1$.

Klassische Bits: $|0\rangle$, $|1\rangle$.



Paul Dirac

Grundlagen der Quantenmechanik

Beispiel: Zulässige Zustände sind $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ oder $\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$, denn $\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = 1$ bzw. $\left(\frac{1}{\sqrt{3}}\right)^2 + \left(\sqrt{\frac{2}{3}}\right)^2 = 1$.

Während wir den Zustand klassischer Bits durch *lesen* feststellen können, ist das bei Qubits nicht ohne Weiteres möglich.
Bei Qubits müssen wir *messen* und das Messergebnis hängt von den Amplituden ab.

Grundlagen der Quantenmechanik

Messen eines Quantenbits

Messen wir ein Qubit im Zustand $\alpha|0\rangle + \beta|1\rangle$, wird die Superposition zerstört. Anschließend ist es mit Wahrscheinlichkeit $|\alpha|^2$ im Zustand $|0\rangle$ und mit Wahrscheinlichkeit $|\beta|^2$ im Zustand $|1\rangle$. Diesen Zustand nach dem Messen können wir beobachten.

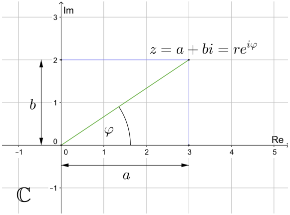
Beispiel: Das Qubit $\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$ ist nach dem Messen mit Wahrscheinlichkeit $1/3$ im Zustand $|0\rangle$ und mit Wahrscheinlichkeit $2/3$ im Zustand $|1\rangle$.

Übung: Was beobachten Sie beim Messen der Qubits $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ und $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$?

Grundlagen der Quantenmechanik

Erinnerung: Jede komplexe Zahl $z \in \mathbb{C}$ kann in der Form $z = a + ib$ mit $a, b \in \mathbb{R}$ und $i := \sqrt{-1}$ geschrieben werden. Die Zahl $\overline{z} := a - ib$ heißt die *Konjugierte* von z. Der *Betrag* einer komplexen Zahl ist $|z| := \sqrt{a^2 + b^2}$.

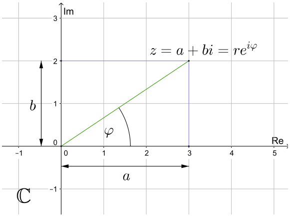
Die *Polarkoordinatendarstellung* einer komplexen Zahl ist $z = re^{i\varphi}$, wobei r der Betrag ist und φ die *Phase*.



Grundlagen der Quantenmechanik

Wissen: Gilt $|z| = |z'|$ für $z \neq z'$ mit $z, z' \in \mathbb{C}$, so unterscheiden sich die komplexen Zahlen nur in der Phase.

Wie selbstverständlich identifizieren wir $\mathbb{C}$ mit $\mathbb{R}^2$ mittels $\mathbf{1} = (1, 0)$ und $i = (0, 1)$.



Grundlagen der Quantenmechanik

Identifizieren wir $|0\rangle$ mit $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $|1\rangle$ mit $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, können wir ein Qubit als Kombination linear unabhängiger Vektoren darstellen:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle.$$

Unter der Bedingung $|\alpha|^2 + |\beta|^2 = 1$ an die Amplituden $\alpha, \beta \in \mathbb{C}$ erhalten wir, dass ein Qubit ein *Vektor* aus $\mathbb{C}^2$ der Länge 1 ist.

D.h. die Superposition ist eine *Linearkombination* der klassischen (nicht überlagerten) Zustände $|0\rangle$ und $|1\rangle$.

Achtung: $\alpha, \beta \in \mathbb{C}$, d.h. wie befinden uns im $\mathbb{C}^2$.

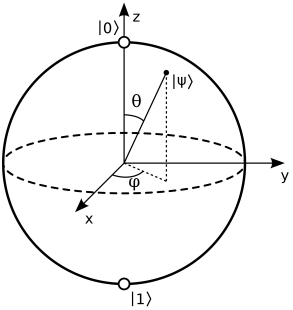
Grundlagen der Quantenmechanik

Mittels

$$\alpha = \cos\frac{\theta}{2}, \;\; \beta = e^{i\varphi}\sin\frac{\theta}{2}$$

können wir uns das Qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ auf der *Blochschen Sphäre* veranschaulichen.

Das Bild erinnert uns an die komplexen Zahlen mit der *Riemannschen Zahlenkugel*.



Grundlagen der Quantenmechanik

Rechenschritte auf Qubits: *unitäre* Matrizen (physikalisch begr.)

Definition (transponierte Matrix)

Sei

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

eine Matrix (mit komplexen Einträgen), dann heißt

$$A^T := \begin{pmatrix} a_{11} & \dots & a_{m1} \\ \vdots & & \vdots \\ a_{1n} & \dots & a_{mn} \end{pmatrix}$$

die *Transponierte* von A.

Grundlagen der Quantenmechanik

Definition (konjugierte und adjungierte Matrix)

Sei $A = (a_{ij}) \in \mathbb{C}^{m \times n}$. Die Matrix $\overline{A} := (\overline{a_{ij}}) \in \mathbb{C}^{m \times n}$ heißt die *Konjugierte* von A, und $A^\dagger := (\overline{A})^T$ die *Adjungierte* von A.

Definition (unitäre Matrix)

Eine Matrix $A = (a_{ij}) \in \mathbb{C}^{n \times n}$ heißt *unitär*, wenn $A^\dagger = A^{-1}$ gilt.

Es folgt sofort das unitäre Matrizen *invertierbar* sind, denn nach Definition gilt $A^\dagger A = AA^\dagger = I_n$.

Grundlagen der Quantenmechanik

Erinnerung: Die Multiplikation eines Vektors mit einer (quadratischen) Matrix beschreibt eine lineare Abbildung.

In unserem Fall liefert die Multiplikation eines Vektors mit einer unitären Matrix $A \in \mathbb{C}^{n \times n}$ eine unitäre Transformation

$$A : \mathbb{C}^n \to \mathbb{C}^n, v \mapsto Av.$$

Grundlagen der Quantenmechanik

Definition (Hadamard-Matrix)

Die Matrix

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

heißt *Hadamard-Matrix*.

Lemma

Die Hadamard-Matrix ist unitär.

Beweis: Übung.

Jacques Hadamard

Grundlagen der Quantenmechanik

Wir untersuchen die Wirkung der Hadamard-Transformation auf den Basiszuständen $|0\rangle$ und $|1\rangle$. Wegen

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\ 1\end{pmatrix}$$

gilt

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

Analog:

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Grundlagen der Quantenmechanik

Da $H = H^{-1}$ gilt, erhalten wir nach wiederholter Anwendung

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{H} |0\rangle$$

und

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{H} |1\rangle.$$

Übung: Konstruieren Sie alle unitäten Transformationen A, für die gilt

$$|0\rangle \xrightarrow{A} \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle.$$