erste Quantenalgorithmen

Nannette Kase
kase@informatik.hu-berlin.de

Peter Liske
liske@informatik.hu-berlin.de

25. Mai 2004

Der vorliegende Text ist die schriftliche Ausarbeitung
zum Vortrag *„erste Quantenalgorithmen“*
im Rahmen des Seminars „Quantenrechner“,
durchgeführt im Sommersemester 2004
am Institut für Informatik der Humboldt-Universität zu Berlin.
Leiter: Prof. Dr. Johannes Köbler, Olaf Beyersdorff

Inhaltsverzeichnis

1 Einleitung

1.1 Rückblick

In den vergangenen Vorträgen haben wir das mathematische Modell der Quantensysteme kennengelernt, ihre Schreibweise als Quantengatter und -schaltkreise und verschiedene Komplexitätsklassen für Quantenrechnermodelle.

Hadamard Die Quantengatter, Repräsentanten für unitäre Transformationen im Vektorraum, lassen sich in vielfältiger Weise zu komplexen Quantenschaltkreisen zusammensetzen. Ganz besonders interessant ist das sogenannte Hadamard-Gatter, weil es die Erzeugung gleichverteilter Zufallszahlen ermöglicht.

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad |0\rangle \; \text{—}\boxed{H}\text{—} \; \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

als unitäre Matrix | als Quantengatter (mit $|\Phi\rangle = |0\rangle$)

Abbildung 1: der Hadamard-Baustein

Funktionen als Blackbox Da in Quantensystemen niemals Information verlorengehen kann, müssen alle Quantengatter genauso viele Aus- wie Eingänge haben. Eine beliebige Funktion $f : \{0,1\}^n \to \{0,1\}^k$ lässt sich allgemein durch einen Schaltkreis wie in der Abbildung 2 dargestellt realisieren.

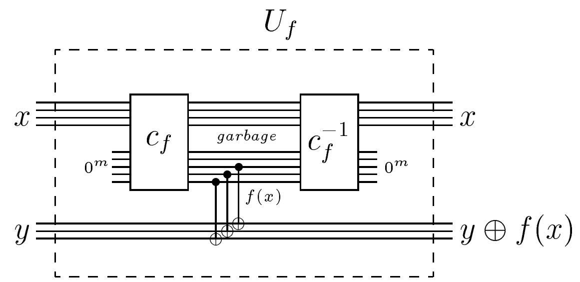

Abbildung 2: allgemeine Funktionsberechnung

Daraus ergibt sich für die weiteren Betrachtungen eine unitäre Transformation U_f, dargestellt als Blackbox, die die Eingänge $|x\rangle$ und $|y\rangle$ und die Ausgänge $|x\rangle$ und $|y \oplus f(x)\rangle$ besitzt.

1.2 Quantenalgorithmen

Algorithmusbegriff In [Gru99] wird der Begriff des Quantenalgorithmus wie folgt eingeführt:

> „Quantenalgorithmen sind Methoden, die Quantennetzwerke und -prozessoren benutzen, um algorithmische Probleme zu lösen.“

Wir haben bisher die Möglichkeit kennengelernt, Quantenprogramme in Form von Schaltkreisen bzw. als Quanten-Turingmaschine anzugeben. Für kleine, theoretische Überlegungen ist diese Art der Darstellung völlig ausreichend. Hingegen wird die Darstellung eines komplexeren Quantenalgorithmus sehr schnell sehr unübersichtlich. Allerdings existieren komplexe Quantenalgorithmen bislang nur in der Theorie. Die Techniken zum Bau funktionstüchtiger Quantencomputer sind nämlich erst in der Entwicklung. Für das Problem der Darstellung komplexer Quantenprogramme gibt es auch die Möglichkeit, Quantenflussdiagramme nud die Programmiersprache QPL zu verwenden. Mehr Informationen dazu findet man in [Sch03].

Erstellen von Quantenalgorithmen Die Schwierigkeit bei der Erstellung eines Quantenalgorithmus ist, eine komplexe unitäre Transformation (den gewünschten Algorithmus) darzustellen als Kombination vieler kleiner, elementarer, unitärer Transformationen.
Weiterhin wirft das Modell des Quantencomputers die Frage auf, ob Quantenalgorithmen überhaupt schneller sind als vergleichbare klassische oder probabilistische Algorithmen. Bisher kennt man in der Tat nur wenige praktische Problemstellungen, die mit Quantenalgorithmen schneller gelöst werden können. Dabei werden die folgenden drei Eigenschaften von Quantensystemen immer wieder ausgenutzt:

Verwicklung: Die Antwort auf die Frage, wo genau sich die Quanteninformation befindet, ist nicht leicht zu erklären. Zwischen den physikalischen Eigenschaften, die als Qubit interpretiert werden, können gewisse Abhängigkeiten bestehen – selbst dann, wenn sich die physikalischen Objekte an entfernten Orten befinden. In diesen Korrespondenzen steckt nun gewissermaßen die Quanteninformation. Man nennt das Phänomen Verwicklung von Information (entanglement).

Überlagerung: Der Zustand eines Quantensystems stellt sich im allgemeinen als Überlagerung (superposition) mehrerer Basiszustände dar, die alle bei einer Messung zum Messergebnis führen könnten.

Parallelität: Die Neuerungen der ersten Quantenalgorithmen gegenüber den bisherigen Berechnungsverfahren beruhen vor allem auf der Quantenparallelität. Daher wird diese im nächsten Abschnitt näher erläutert.

1.3 Quantenparallelismus

Sei U_f die Blackbox, die die Funktion $f : \{0,1\} \rightarrow \{0,1\}$ simuliert.

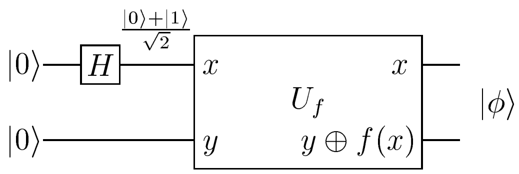

Abbildung 3: Blackbox für $f : \{0,1\} \rightarrow \{0,1\}$

U_f ist die Transformation $(x,y) \rightarrow (x, y \oplus f(x))$. Wählen wir als Eingabe für die Blackbox $x = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ und $y = |0\rangle$, so erhält man $|\phi\rangle = \frac{|0\, f(0)\rangle + |1\, f(1)\rangle}{\sqrt{2}}$.
Für eine Funktion $f : \{0,1\}^n \rightarrow \{0,1\}$ ist der Schaltkreis wie in Abbildung 4 gegeben.
Das Ergebnis ist $|\phi\rangle = \sum\limits_{i \in \{0,1\}^n} \frac{|i\, f(i)\rangle}{\sqrt{2^n}}$. Das einmalige Anwenden der Funktion liefert also alle 2^n Ergebnisse gleichverteilt als Überlagerunszustand. Exponentieller Rechenaufwand ist somit mit linearem Platz möglich. Dieses grundlegende Phänomen der Quantensysteme nennt man „Quantenparallelismus“.

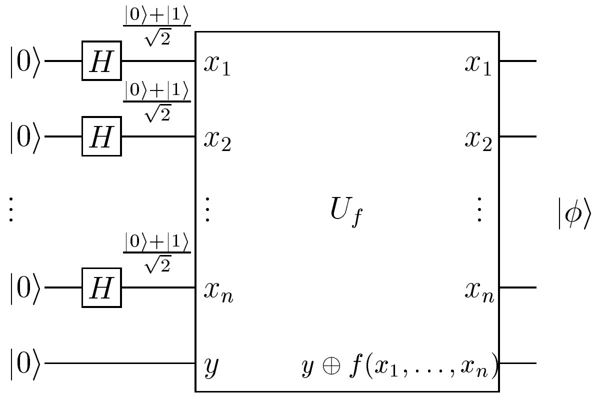

Abbildung 4: Blackbox für $f : \{0,1\}^n \to \{0,1\}$

2 Das Deutsch-Problem

2.1 Der Deutsch-Algorithmus

Definitionen

Promise-Problem: Ein Promise-Problem ist eine Fragestellung, bei der einige Eigenschaften des zu untersuchenden Objektes als gegeben vorausgesetzt werden können.

balanciert: Eine Funktion $f : \{0,1\}^n \to \{0,1\}$ heißt balanciert, wenn die Anzahlen der Urbilder der 0 und der 1 gleich sind.
Formal: $|\{x \mid f(x) = 0\}| = |\{x \mid f(x) = 1\}| = 2^{n-1}$

Deutsch-Problem: Bei einer gegebenen Funktion $f : \{0,1\} \to \{0,1\}$ ist das Deutsch-Problem, zu entscheiden, ob f balanciert oder konstant ist.
Das Deutsch-Problem heißt auch Deutsch's XOR-Problem, da entschieden wird, ob $f(0) \oplus f(1) = 0$ oder $f(0) \oplus f(1) = 1$. Interpretiert werden kann dieses Problem dahingehend, dass man entscheiden soll, ob eine Münze gefälscht (auf beiden Seiten gleich) oder echt ist.

randomisierter Quantenalgorithmus 1985 veröffentlichte David Deutsch eine randomisierte Lösung für das Deutsch-Problem [De85] und damit das erste Beispiel für einen Quantenalgorithmus, der nachweislich schneller ist als klassische Algorithmen. Der Schaltkreis für die Lösung lautet:

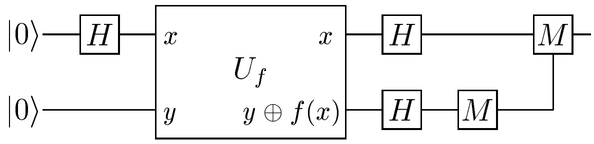

Abbildung 5: Lösung für das Deutsch-Problem

Der Eingabewert $\frac{|0\rangle+|1\rangle}{\sqrt{2}}\,|0\rangle$ wird durch den Schaltkreis U_f zu $\frac{1}{\sqrt{2}}(|0\,f(0)\rangle + |1\,f(1)\rangle)$. Nach Anwendung des Hadamard-Schaltkreises erhält man:

$f(0)$	$f(1)$	$H_2\left(\frac{1}{\sqrt{2}}(\|0\,f(0)\rangle + \|1\,f(1)\rangle)\right)$
0	0	$\frac{1}{\sqrt{2}}(\|0\,0\rangle + \|0\,1\rangle)$
0	1	$\frac{1}{\sqrt{2}}(\|0\,0\rangle + \|1\,1\rangle)$
1	0	$\frac{1}{\sqrt{2}}(\|0\,0\rangle - \|1\,1\rangle)$
1	1	$\frac{1}{\sqrt{2}}(\|0\,0\rangle - \|0\,1\rangle)$

Die allgemeine Formel für den erhaltenen Quantenzustand lautet

$$\frac{1}{\sqrt{2}}(|0\,0\rangle + (-1)^{f(0)}\,|f(0) \oplus f(1)\,1\rangle).$$

Ist das zweite Qubit bei der Messung 0, so handelt es sich um den Zustand $|00\rangle$. Hieraus lassen sich keine Rückschlüsse auf die Funktion ziehen. Die Wahrscheinlichkeit, diesen Zustand bei der Messung zu erhalten, ist $\frac{1}{2}$. Wenn das zweite Qubit hingegen 1 ist, so steckt Information über f im ersten Qubit. Bei einer konstanten Funktion ist dann das erste Qubit 0, bei 1 ist f balanciert.

Inzwischen sind sogar verschiedene deterministische Quantenalgorithmen bekannt, die das Deutsch-Problem mit nur einer Anwendung der Blackbox lösen. Eine verallgemeinerte Variante wird im nächsten Teil vorgestellt.

2.2 Das Deutsch-Josza-Problem

Das Deutsch-Josza-Problem besteht darin, zu entscheiden, ob eine gegebene Funktion $f : \{0,1\}^n \to \{0,1\}$ konstant oder balanciert ist [DJ92]. Es handelt sich hier wieder um ein Promise-Problem.

deterministischer Algorithmus Im schlimmsten Fall müssen $2^{n-1}+1$ (verschiedene) Eingaben geprüft werden, falls die ersten 2^{n-1} Funktionswerte gleich sind. Sobald man zwei verschiedene Funktionswerte erhalten hat, kann man stoppen, da dann klar ist, dass die Funktion balanciert sein muss.

probabilistischer Algorithmus Als probalistische Herangehensweise wählt man solange zufällig Stichproben x und bestimmt $f(x)$, bis man sich mit einer vorgegebenen Wahrscheinlichkeit sicher sein kann, die richtige Antwort zu kennen.
Die Wahrscheinlichkeit, $k+1$ mal denselben Funktionswert zu erhalten, obwohl f balanciert ist, beträgt

$$P(\text{Fehler}) = 1 \cdot \frac{2^{n-1}-1}{2^n-1} \cdot \frac{2^{n-1}-2}{2^n-2} \cdot \ldots \cdot \frac{2^{n-1}-k}{2^n-k} < \left(\frac{1}{2}\right)^k .$$

Bei vorgegebener Fehlerwahrscheinlichkeit P_F werden also nur eine konstante Anzahl Stichproben benötigt ($-\log_2 P_F$), um dieses Problem probabilistisch zu entscheiden.

Quantenalgorithmus Der folgende Schaltkreis löst das Deutsch-Josza-Problem.

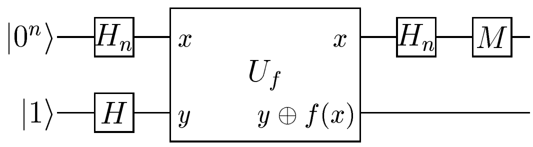

Abbildung 6: Lösung für das Deutsch-Josza-Problem

Die Eingaben $|0^n\rangle$ und $|1\rangle$ werden durch die Hadamard-Schaltkreise zu $\sum\limits_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
Nach der Blackbox erhält man $\sum\limits_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \frac{|0\oplus f(x)\rangle-|1\oplus f(x)\rangle}{\sqrt{2}} = \sum\limits_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \frac{(-1)^{f(x)}(|0\rangle-|1\rangle)}{\sqrt{2}}$.
Nach dem letzten Übergang ist der Zustand des Systems

$$\sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} \frac{1}{\sqrt{2^n}} |z\rangle (-1)^{xz+f(x)} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

$$= \sum_{z\in\{0,1\}^n} |z\rangle \underbrace{\sum_{x\in\{0,1\}^n} \frac{1}{2^n} (-1)^{xz+f(x)}}_{\alpha_z} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Der Wert $|\alpha_z|^2$ ist die Wahrscheinlichkeit, bei der Messung der ersten n Qubits $|z\rangle$ zu erhalten. Für $z = 0^n$ vereinfacht sich die Formel zu

$$\alpha_{0^n} = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}.$$

Ist nun f konstant, so gilt $\alpha_{0^n} = \frac{1}{2^n} \sum\limits_{x \in \{0,1\}^n} (-1)^{f(0^n)} = \pm 1$. Die Wahrscheinlichkeit, 0^n zu messen, ist demnach $|\alpha_{0^n}|^2 = 1$.
Ist f balanciert, so gilt $\alpha_{0^n} = \frac{1}{2^n} \left(\sum\limits_{x \in \{x' | f(x')=0\}} (-1)^0 + \sum\limits_{x \in \{x' | f(x')=1\}} (-1)^1 \right) = \frac{1}{2^n} \left(2^{n-1} - 2^{n-1}\right) = 0$. Bei balanciertem f erhält man daher mit Wahrscheinlichkeit $|\alpha_{0^n}|^2 = 0$ den Wert 0^n.

Es gilt also: Ergibt die Messung den Wert 0^n, so ist die Funktion f mit Sicherheit konstant, bei jedem anderen Messergebnis ist sie balanciert. Die Blackbox muss also nur ein einziges Mal angewendet werden, um das richtige Ergebnis zu berechnen.

3 Simons Problem

Der in diesem Abschnitt vorgestellte Algorithmus von Simon [Si97] stellt die Grundlage dar für den späteren Algorithmus von Shor zur Faktorisierung ganzer Zahlen [Sh97]. Im Gegensatz zu Deutsch's Algorithmus und seinen Verallgemeinerungen, welche eher dem theoretischen Interesse dienen, findet sich Simons Algorithmus somit auch in praktischen Anwendungen wieder.

3.1 Problemstellung

Sei eine Funktion $f : \{0,1\}^n \to \{0,1\}^m$ gegeben, für die eine Zahl $s \in \{0,1\}^n$ existiert, sodass

$$\forall x \neq x' : f(x) = f(x') \quad \Longleftrightarrow \quad x' = x \oplus s.$$

Die Aufgabe ist nun, dieses sogenannte Periode s anhand der Blackbox zu bestimmen.

Wie wir sehen werden, ist Simons Algorithmus ebenso wie der ursprüngliche Algorithmus von Deutsch nur ein probabilistischer Quantenalgorithmus, aber dennoch viel schneller als klassische Lösungsverfahren.

3.2 klassische Herangehensweisen

deterministischer Algorithmus Da jede beliebige n-Bit-Zahl als mögliche Periode in Frage kommt, müsste eine deterministische Herangehensweise zwangsläufig systematisch alle Eingaben für f durchprobieren, bis die Funktionswerte zweier Eingaben x_i und x_j gleich sind (dann ist $s = x_i \oplus x_j$). Bei k unterschiedlichen, getesteten Zahlen kann man $\binom{k}{2}$ verschiedene Funktionswertepaare auf Gleichheit testen. Genau soviele Möglichkeiten für s lassen sich dadurch ausschließen. Damit nur noch eine Zahl übrig bleibt, muss gelten

$$2^n - 1 - \binom{k}{2} = 1 \implies k = \Omega\left(2^{\frac{n}{2}}\right).$$

probabilistischer Algorithmus Man kann die Stichproben $x_1, \ldots, x_k$ auch zufällig gleichverteilt vornehmen und die Wahrscheinlichkeit betrachten, dass ein s', welches noch nicht ausgeschlossen wurde, die gesuchte Periode von f

darstellt. Durch Überlegung stellt man fest, dass alle s' dieselbe Wahrscheinlichkeit besitzen. Somit müssen ebenfalls $\Omega\left(2^{\frac{n}{2}}\right)$ Stichproben tätigen, um eine konstante Fehlerwahrscheinlichkeit zu unterschreiten.

3.3 Quantenalgorithmus von Simon

Simons Lösung dieses Problems sieht wie folgt aus:

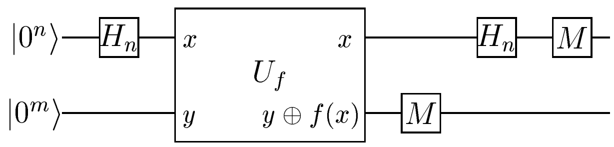

Abbildung 7: Simons Lösungs für das Problem

An dieser Stelle wird wieder der Quantenparallelismus ausgenutzt, sodass sich hinter der Transformation U_f der Zustand $\frac{1}{\sqrt{2^n}} \sum\limits_{i \in \{0,1\}^n} |i\rangle\, |f(i)\rangle$ ergibt.
Die anschließende Messung der unteren n Bits legt den Funktionswert auf ein $f(i)$ fest. Damit beinhalten die ersten n Bit nur noch die Urbilder von $f(i)$. Wegen der vorgegebenen Funktionseigenschaft sind das genau i und $i \oplus s$. Der Postmessungs-Zustand ist demnach $\frac{1}{\sqrt{2}} \left(|i\rangle + |i \oplus s\rangle\right) |f(i)\rangle$.
Nun wird auf die ersten n Bits wieder das Hadamard-Gatter H_n angewandt und man erhält

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} |z\rangle \left((-1)^{iz} + (-1)^{(i \oplus s)z}\right) |f(i)\rangle = \sum_{z \in \{0,1\}^n} \alpha_z\, |z, f(i)\rangle.$$

Hierbei ist $\alpha_z = \frac{(-1)^{iz}(1+(-1)^{sz})}{\sqrt{2^{n+1}}}$, sodass sich für $sz = 0$ eine Amplitude von $\alpha_z = \pm\frac{1}{\sqrt{2^{n+1}}}$ ergibt und für $sz = 1$ der Wert $\alpha_z = 0$. Bei der endgültigen Messung ergibt sich also in jedem Fall ein zu s orthogonaler Vektor.
Nach $\mathcal{O}(n)$ Anwendungen des Schaltkreises erhält man dadurch $n-1$ Vektoren, die zu s orthogonal und untereinander linear unabhängig sind. Aus dem linearen Gleichungssystem ergibt sich sofort der gesuchte Vektor s.

3.4 Varianten

Man kann auch die erste Messung der unteren Bits einfach weglassen und den Algorithmus dadurch etwas vereinfachen [Gru99]. Die Rechnung wird

allerdings umständlicher und soll hier nicht weiter ausgeführt werden.
Auch für diesen Algorithmus konnte durch Abänderung inzwischen eine deterministische Variante gefunden werden, siehe [Br97]. Dabei werden die Algorithmen von Simon und Grover geschickt kombiniert. Weil Grover's Algorithmus allerdings erst in einem späteren Vortrag Thema sein wird, wollen wir an dieser Stelle nicht näher darauf eingehen.

Literatur

[Br97] Brassard, G., Hoyer, P.; *An Exact Quantum Polynomial-Time Algorithm for Simon's Problem*, quant-ph/9704027, 1997

[De85] Deutsch, David; *Quantum Theory, the Church-Turing principle and the universal quantum computer*, Proc. Roy. Soc. London A, Volume 400, Seiten 97-117, 1985

[DJ92] Deutsch, David, Josza, Richard; *Rapid solution of problems by quantum computation*, Proc. Roy. Soc. London A, Volume 439, Seiten 553-558, 1992

[Gru99] Gruska, Jozef; *Quantum Computation*, McGraw-Hill Publishing Company, 1999

[Lea01] Leander, Gregor; *Quantencomputer*, Diplomarbeit im August 2001

[Sch03] Schroeder, Andreas; *Quantenflussdiagramme und die Quantenprogrammiersprache QPL*, unveröffentlicht, 2003

[Sh97] Shor, Peter W.; *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing, Volume 26, Number 5, Seiten 1484-1509, 1997

[Si97] Simon, Daniel R.; *On the Power of Quantum Computation*, SIAM Journal on Computing, Volume 26, Number 5, Seiten 1474-1483, 1997

[To03] Toran, Jacobo; Vorlesung *Quantencomputer*, Sommersemester 2003 an der Universität Ulm