Zur Idee des Quantencomputers

Franz Embacher[1]

Unterlagen zum Workshop "Quantenkryptographie und Quantencomputer"
im Rahmen der 58. Fortbildungswoche Physik/Chemie
Institut für Theoretische Physik der Universität Wien, 25. 2. 2004

1 Problemstellung

Um die Idee des Quantencomputers zu verstehen, betrachten wir ein einfaches Beispiel: Gegeben sei eine "Datenbank" mit zwei Einträgen, wobei jeder Eintrag entweder 0 oder 1 ist. Die Aufgabe besteht darin, herauszufinden, ob die beiden Einträge gleich sind.

Mathematisch wird eine solche Datenbank durch eine Funktion $f : \{0,1\} \to \{0,1\}$ beschrieben: $f(0)$ ist der erste, $f(1)$ der zweite Eintrag. Es gibt vier derartige Funktionen:

- die Identität $f(0) = 0, f(1) = 1$,
- die Vertauschung $f(0) = 1, f(1) = 0$,
- die konstante Funktion $f(0) = 0, f(1) = 0$ und
- die konstante Funktion $f(0) = 1, f(1) = 1$.

Die Aufgabe besteht darin, herauszufinden, ob $f(0) = f(1)$, d.h. ob f konstant ist.

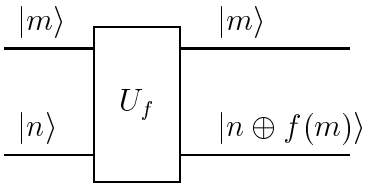
Jeder klassische Algorithmus, der diese Aufgabe löst, muss zwei Funktionsaufrufe (Datenbankabfragen) veranschlagen: einen, um $f(0)$ auszulesen und einen, um $f(1)$ auszulesen. Danach kann überprüft werden, ob $f(0) = f(1)$ ist.

Wir werden jetzt als Alternative zum klassischen Verfahren einen "Quanten-Algorithmus" besprechen.

[1] fe@ap.univie.ac.at

2 Funktionsaufruf

Dazu benötigen wir zunächst ein 2-Qubit-System und stellen uns vor, für jede der vier Funktionen f liege die Datenbank (der Funktionsaufruf) in Form eines Bauteils vor, der eine Wechselwirkung zwischen den beiden Qubits (Registern) bewirkt:



Dabei sind $m, n \in \{0, 1\}$, und $\oplus$ steht für die Addition modulo 2 (insbesondere gilt $1 \oplus 1 = 0$). Durch eine Formel ausgedrückt, ist die Wirkungweise dieses "Gatters" durch

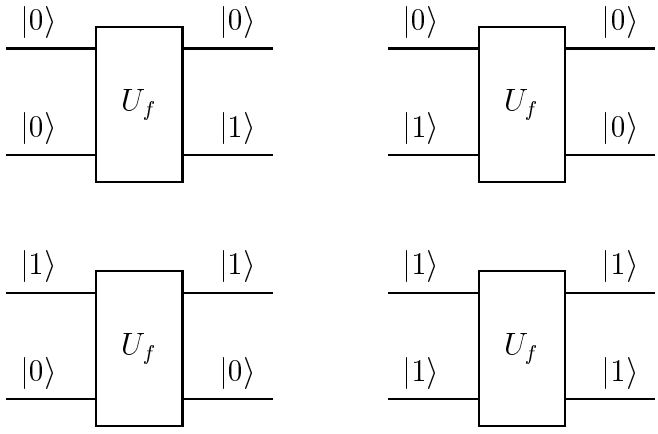
$$U_f|m\rangle|n\rangle = |m\rangle|n \oplus f(m)\rangle. \tag{2.1}$$

gegeben. Das erste (obere) Register heißt *control bit*, das zweite (untere) wird *target bit* genannt.

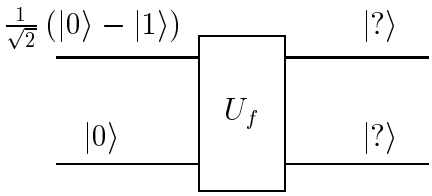
Betrachten wir zur Übung die Wirkungsweise dieses Bauteils für den Fall der Vertauschungsfunktion

$$f(0) = 1 \qquad f(1) = 0. \tag{2.2}$$

Sind beide Register in einem der Zustände der Standardbasis, so ergeben sich 4 Möglichkeiten für den Inputzustand:



Die Quantentheorie kommt ins Spiel, wenn sich ein oder zwei Register in einem *Überlagerungszustand* der Standardbasis-Vektoren befinden. Beispiel:



Wir verlangen nun, dass U_f auf eine Überlagerung wirkt, indem (2.1) auf jeden ihrer Bestandteile angewandt wird[2] (das ist genau jene Eigenschaft, die ein klassisches Gatter von einem Quantengatter unterscheidet), und berechnen den Output-Zustand:

$$\begin{aligned} U_f\left(\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)|0\rangle\right) &= U_f\left(\frac{1}{\sqrt{2}}|0\rangle|0\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle\right) \\ &= \frac{1}{\sqrt{2}}\big(U_f|0\rangle|0\rangle - U_f|1\rangle|0\rangle\big) \qquad (2.3) \\ &= \\ &\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

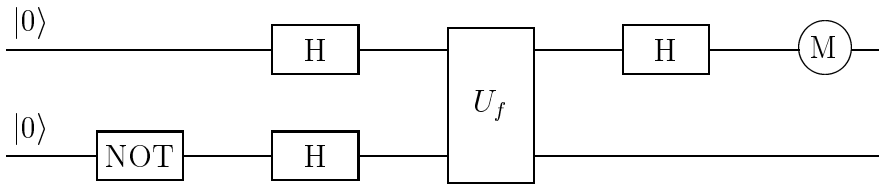
Lösung: Der Output ist genau der EPR-Zustand. Den beiden Output-Registern können nun keine individuellen Zustandsvektoren mehr zugeordnet werden! (Ein solcher Zustand des Gesamtsystems heißt *verschränkt*). Man beachte weiters, dass zum Output-Zustand *sowohl* $f(0)$ *als auch* $f(1)$ beitragen, obwohl die Funktion nur *ein einziges Mal* aufgerufen wurde! Hier wird bereits die Idee des "Quanten-Parallelrechnens" sichtbar.

3 Quantencomputer

Nun stellen wir uns vor, eine solche Datenbank zu bekommen. Wir wissen nicht, welche der vier möglichen Funktionen f sie darstellt, und wollen mit einer minimalen

[2]Die Frage, wie das experimentell zu realisieren ist, klammern wir hier aus. Mathematisch gesehen, wird U_f durch diese Vorschrift zu einer *linearen* Transformation des Zustandsvektors für das Gesamtsystem fortgesetzt, $U_f(|\psi\rangle + c\,|\phi\rangle) = U_f|\psi\rangle + c\,U_f|\phi\rangle$, von der sich leicht zeigen lässt, dass sie *unitär* ist.

Zahl an Abfragen herausfinden, ob f konstant ist. Dazu bauen wir sie in einen Versuchsaufbau gemäß dem folgenden Schaltplan ein:



Hier haben wir das einfachste Konzept eines Quantencomputers vor uns. Er legt einen konkreten Ablauf (einen Quanten-Algorithmus) von Transformationen fest: Zu Beginn wird das System im Zustand $|0\rangle|0\rangle$ präpariert. Danach durchläuft es die vorbereitete Anordnung. Zuletzt wird im ersten Register eine Messung in der Standardbasis durchgeführt.

Frage: Was lässt sich über den Ausgang der Messung (in Abhängigkeit von der Funktion f) sagen? Wenden Sie das bisher Besprochene an, um diese Frage zu beantworten! Rechtfertigen Sie folgende

Schlussfolgerung: Mit einer einzigen Datenbankabfrage lässt sich feststellen, ob die beiden Einträge (d.h. $f(0)$ und $f(1)$) gleich sind!

Dieser bescheidene Vorsprung des Quantencomputer gegenüber dem klassischen lässt sich (vorerst nur auf der Ebene theoretischer Konzepte) stark verbessern, wenn komplexere Probleme betrachtet werden. Beispiele für solche Quanten-Algorithmen sind

- der Algorithmus von Peter Shor zur Faktorisierung großer Primzahlen in polynomialer Zeit (1994) und
- der Algorithmus von Lov Grover, der es gestattet, in einer ungeordneten Datenbank mit n Einträgen einen bestimmten Eintrag nach nur $O(\sqrt{n})$ Abfragen zu finden (1996).

Links und Literatur
zu diesem Workshop finden Sie am Web unter

http://www.ap.univie.ac.at/users/fe/Quantentheorie/Fortbildungswoche2004/