

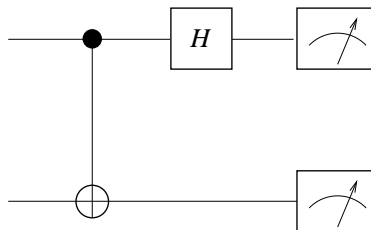
Übungen zur Vorlesung  
**Quantenrechner: Algorithmen und Komplexität**  
 Wintersemester 2004/2005  
 Blatt 3

**Aufgabe 3.1**

Die in der Vorlesung definierten Quantenschaltkreise erlauben nur Messungen bezüglich der Basis  $\{|0\rangle, |1\rangle\}$ . Um uns davon zu überzeugen, dass damit auch Messungen bezüglich anderer Basen möglich sind, betrachten wir den unten abgebildeten Quantenschaltkreis. Zeige, dass der Quantenschaltkreis eine Messung bezüglich der Basis realisiert, die aus den vier Bell-Zuständen

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

gebildet wird.

**Aufgabe 3.2**

Der Deutsch-Jozsa-Algorithmus ist ein Quantenschaltkreis für das folgende Promise-Problem:

**Deutsch-Jozsa-Problem**

**Gegeben:** Ein Schaltkreis oder Quantenschaltkreis  $G$  für  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ .

**Promise:**  $f$  ist konstant oder balanciert.

**Problem:** Ist  $f$  konstant oder balanciert?

Um das Problem zu lösen, ist es nur erlaubt, den Schaltkreis/Quantenschaltkreis auszuwerten, nicht aber, die Struktur des Schaltkreises auszunutzen. Wir interessieren uns dabei nur für die Anzahl der Auswertungen des Schaltkreises.

In der Vorlesung haben wir überlegt, dass ein deterministischer klassischer Algorithmus den Schaltkreis mindestens  $(2^{n-1} + 1)$ -mal auswerten muss, um das Problem zu lösen. Wir wollen in dieser Aufgabe untersuchen, ob dies mit randomisierten (klassischen) Algorithmen verbessert werden kann. Wir unterscheiden zwei Typen von randomisierten Algorithmen:

- a) Algorithmen, die auf Zufallsbits zugreifen dürfen, aber immer das richtige Ergebnis oder die Ausgabe „weiß nicht“ liefern (sog. Las-Vegas-Algorithmen). Formal: Für alle Eingaben  $x$  ist die Wahrscheinlichkeit, dass der Algorithmus das richtige Ergebnis liefert, mindestens  $2/3$ , und der Algorithmus liefert niemals ein falsches Ergebnis.
- b) Algorithmen, die auf Zufallsbits zugreifen dürfen und mit begrenzter Wahrscheinlichkeit auch ein falsches Ergebnis liefern dürfen (sog. Monte-Carlo-Algorithmen). Formaler: Für alle Eingaben  $x$  ist die Wahrscheinlichkeit, dass der Algorithmus das richtige Ergebnis liefert, mindestens  $2/3$ .

Beachte, dass alle Wahrscheinlichkeiten über die Wahl der Zufallsbits gebildet werden, dass also nicht die Eingaben zufällig gewählt werden.

- Überlege, ob es Las-Vegas-Algorithmen für das Deutsch-Jozsa-Problem gibt, die mit weniger als  $2^{n-1} + 1$  Auswertungen auskommen. Falls nein, beweise dies. Falls ja, entwirf einen solchen Algorithmus, der mit möglichst wenigen Auswertungen auskommt.
- Überlege, ob es Monte-Carlo-Algorithmen für das Deutsch-Jozsa-Problem gibt, die mit weniger als  $2^{n-1} + 1$  Auswertungen auskommen. Falls nein, beweise dies. Falls ja, entwirf einen solchen Algorithmus, der mit möglichst wenigen Auswertungen auskommt.

### Aufgabe 3.3

Wir wollen zeigen, dass der Deutsch-Jozsa-Algorithmus auch für andere Probleme benutzt werden kann.

#### Parity-Problem

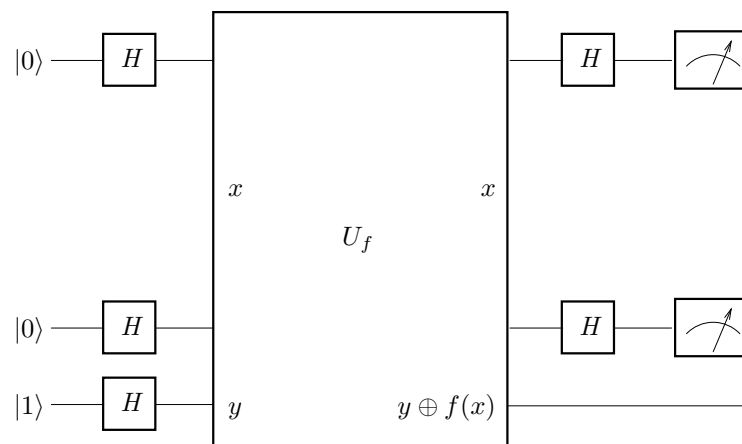
**Gegeben:** Ein Schaltkreis oder Quantenschaltkreis  $G$  für  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ .

**Promise:**  $f$  ist von der Form  $f(x) = \langle x, a \rangle$  für ein (unbekanntes)  $a \in \{0, 1\}^n$ .

**Problem:** Berechne  $a$ .

Dabei ist  $\langle x, a \rangle = \bigoplus_i x_i a_i$ , mit anderen Worten,  $f(x)$  berechnet das Parity der Bits  $x_i$ , für die  $a_i = 1$  ist.

Wir verwenden denselben Quantenschaltkreis wie für das Deutsch-Jozsa-Problem:



Zeige: Mit Wahrscheinlichkeit 1 ist das Ergebnis der Messung in dem Quantenschaltkreis gleich  $a$ .

### Aufgabe 3.4

- Sei  $A$  ein  $n \times m$ -Matrix und  $B$  eine  $m \times n$ -Matrix. Zeige, dass  $\text{tr}(AB) = \text{tr}(BA)$  gilt.
- Zeige, dass eine Matrix  $A$  genau dann unitär ist, wenn ihre Zeilen eine orthonormale Basis bilden, was wiederum genau dann gilt, wenn ihre Spalten eine orthonormale Basis bilden.