Komplexitätstheorie

Sommersemester 2019

Mario Holldack, M. Sc.
Prof. Dr. Georg Schnitger
Hannes Seiwert, M. Sc.

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

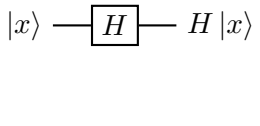
Übungsblatt 10

Ausgabe: 01.07.2019
Abgabe: 15.07.2019

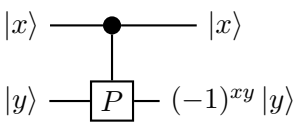
Die Bearbeitungszeit für dieses Blatt beträgt zwei Wochen, die maximal erreichbare Punktzahl beträgt 48.

Aufgabe 10.1 *Quantenschaltkreise* $(3 + 3 + 4 = 10$ Punkte$)$

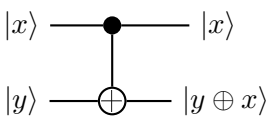
Benutzen Sie die folgenden graphischen Darstellungen der drei wichtigen Gattertypen: Hadamard, Controlled-Phasenflip (CPHASE) und Controlled-Not (CNOT). Es seien $x, y \in \{0, 1\}$.



Hadamard-Gatter



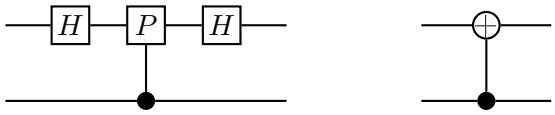
CPHASE-Gatter



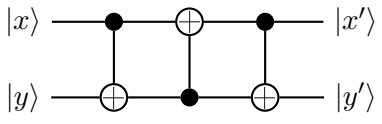
CNOT-Gatter

Beachten Sie, dass es sich bei CPHASE (bzw. CNOT) um ein Controlled-U-Gatter handelt, wobei hier U das Phasenflipgatter (bzw. das Bitflipgatter) ist.

a) Zeigen Sie, dass die folgenden beiden Quantenschaltkreise dieselbe Funktion berechnen.



b) Betrachten Sie den folgenden Quantenschaltkreis. Welche Funktion berechnet er?



c) Konstruieren Sie einen Quantenschaltkreis, der aus $|00\rangle$ den EPR-Zustand $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ erzeugt. Benutzen Sie dabei nur die Gattertypen, die in der Vorlesung behandelt wurden.

Bitte wenden!

Aufgabe 10.2 *Ein Quantenalgorithmus* (2 + 4 + 8 = 14 Punkte)

Gegeben sei eine unbekannte Funktion $f : \{0,1\}^n \to \{0,1\}$ durch eine Blackbox-Implementierung. Es sei bekannt, dass f entweder *konstant* ist, d. h. $f(x) = f(y)$ gilt für alle x, y, oder *balanciert* ist, d. h. es gibt gleich viele x mit $f(x) = 1$ bzw. $f(x) = 0$.

Die Funktion f werde durch ein $(n+1)$-Qubit-Gatter implementiert, das die unitäre Abbildung U_f berechnet, wobei für $x \in \{0,1\}^n$ und $y \in \{0,1\}$ gilt:

$$U_f\left(|x\rangle \otimes |y\rangle\right) = |x\rangle \otimes |y \oplus f(x)\rangle \ .$$

Ziel ist es, durch möglichst wenige Aufrufe von f bzw. U_f herauszufinden, ob f konstant oder balanciert ist.

a) Bestimmen Sie, wie viele Aufrufe von f ein klassischer Algorithmus im Worst Case benötigt.

b) Sei $n = 1$. Das heißt, es gilt entweder $f(0) = f(1)$ (konstant) oder $f(0) \neq f(1)$ (balanciert).

   Zeigen Sie: Der folgende Quanten-Algorithmus bestimmt mit nur einem Aufruf von U_f, ob f konstant oder balanciert ist.

   - Initialisiere den Zustand $|01\rangle$.
   - Wende ein Hadamard-Gatter auf beide Qubits an: $|\psi\rangle := (H \otimes H)|01\rangle$.
   - Wende U_f auf $|\psi\rangle$ an: $|\psi_f\rangle := U_f|\psi\rangle$.
   - Wende ein Hadamard-Gatter auf das erste Qubit von $|\psi_f\rangle$ an.
   - Miss das erste Qubit in der Standard-Basis $\{|0\rangle, |1\rangle\}$.

c) Sei nun n beliebig. Beschreiben Sie einen Quanten-Algorithmus, der mit nur einem einzigen Aufruf von U_f bestimmt, ob f konstant oder balanciert ist.

   Hinweis: Verallgemeinern Sie das Vorgehen aus Teil b).

Bitte wenden!

Aufgabe 10.3 *Postselektion* $(4 + (4{+}4{+}4{+}4{+}4) = 24$ Punkte)

Als *Postselektion* bezeichnet man die Fähigkeit, das Ergebnis einer randomisierten Berechnung auf ein Ereignis (mit positiver Wahrscheinlichkeit) zu bedingen. Etwas genauer:
Ein randomisierter Algorithmus A berechne auf einer Eingabe w die (als Zufallsvariable zu interpretierende) Ausgabe $a = (a_1, a_2, \ldots, a_m) \in \{0,1\}^m$, der eine Wahrscheinlichkeitsverteilung $p(a) = p_a$ zugrunde liegt. Wir können nun z. B. auf das Ereignis $\{a_1 = 1\}$ postselektieren (bedingen) und erhalten damit die Zufallsvariable $a' = (1, a_2, \ldots, a_m)$ mit der Verteilung

$$p(a') = p(a \,|\, a_1{=}1) = \frac{p_{(1,a_2,\ldots,a_m)}}{\sum\limits_{(a'_2,\ldots,a'_m)\in\{0,1\}^{m-1}} p_{(1,a'_2,\ldots,a'_m)}}.$$

Beachte, dass man nur auf Ereignisse mit positiver Wahrscheinlichkeit postselektieren kann.
Wir definieren die Klasse `PostBPP` analog zu `BPP` mit der zusätzlichen Fähigkeit der Postselektion beliebig vieler Bits.

a) Zeigen Sie: `PostBPP` $\supseteq$ `NP`

Postselektion für Quantenberechnungen funktioniert analog. Sei $|\psi\rangle = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$ ein n-Qubit-Zustand.[1] Wenn wir $|\psi\rangle$ auf das Ereignis postselektieren, dass das erste Bit 1 ist, erhalten wir den Zustand $|1\rangle|\psi_1\rangle$. Eine Postselektion entspricht also einer Messung (Kollaps des Zustandes), wobei wir das Messergebnis selbst festlegen.

Wir definieren die Klasse `PostBQP` analog zu `BQP` mit der zusätzlichen Fähigkeit der Postselektion beliebig vieler Qubits.

b) Zeigen Sie: `PostBQP` $\supseteq$ `PP`

Gehen Sie in folgenden Schritten vor. Nehmen Sie an, eine in Polynomialzeit berechenbare Funktion $f : \{0,1\}^n \to \{0,1\}$ liegt vor und sei $s = |f^{-1}(1)|$. Zu entscheiden ist, ob $s < 2^{n-1}$ oder $s \geq 2^{n-1}$ gilt. O. B. d. A. gelte $s > 0$. Da `P` $\subseteq$ `BQP` gilt, können wir f durch einen (in Polynomialzeit konstruierbaren) unitären Operator U_f implementieren.

i) Nehmen Sie an, der $(n{+}1)$-Qubit-Zustand $2^{-n/2}\sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$ liege bereits vor. Wende jeweils ein Hadamard-Gatter auf die ersten n Qubits an und postselektiere auf das Ereignis, dass die ersten n Qubits 0 sind. Der so entstandene Zustand sei $|0^n\rangle|\psi\rangle$.
Bestimmen Sie $|\psi\rangle$.

ii) Wir ignorieren die ersten n Qubits und fahre lediglich mit dem Qubit $|\psi\rangle$ fort. Seien $\alpha, \beta \in \mathbb{R}$. Erzeuge[2] den 2-Qubit-Zustand $\alpha|0\rangle|\psi\rangle + \beta|1\rangle H|\psi\rangle$ und postselektiere auf das Ereignis, dass das zweite Qubit 1 ist. Der so entstandene Zustand sei $|\varphi_{\beta/\alpha}\rangle|1\rangle$.
Bestimmen Sie $|\varphi_{\beta/\alpha}\rangle$.

iii) Sei $|+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$. Angenommen, $s < 2^{n-1}$. Zeigen Sie, dass eine Zahl $i \in \{-n, \ldots, n\}$ existiert, sodass für $\beta/\alpha = 2^i$ gilt:

$$|\langle +|\varphi_{\beta/\alpha}\rangle| \geq \frac{1+\sqrt{2}}{\sqrt{6}}$$

iv) Angenommen, $s \geq 2^{n-1}$. Zeigen Sie, dass für alle $i \in \{-n, \ldots, n\}$ gilt:

$$|\langle +|\varphi_{\beta/\alpha}\rangle| \leq \frac{1}{\sqrt{2}}$$

v) Beschreiben Sie, wie mithilfe von iii) und iv) in Poynomialzeit feststellbar ist, ob $s \geq 2^{n-1}$ oder $s < 2^{n-1}$ gilt.

Kommentar: Man kann zeigen, dass auch `PostBQP` $\subseteq$ `PP` gilt. Somit folgt `PostBQP` $=$ `PP`.

[1] In dieser Aufgabe verzichten wir auf das Symbol für das Tensorprodukt und schreiben kurz $|x\rangle\,|y\rangle$ statt $|x\rangle \otimes |y\rangle$.
[2] Sie müssen nicht beschreiben, wie diese Operation umgesetzt wird.