Komplexitätstheorie

Sommersemester 2020

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: 29.06.2020
Abgabe: 06.07.2020

Auf diesem Blatt können Sie bis zu 8 Extrapunkte ergattern. Die Abgabe erfolgt per E-Mail an Hannes Seiwert (`seiwert@em.uni-frankfurt.de`).

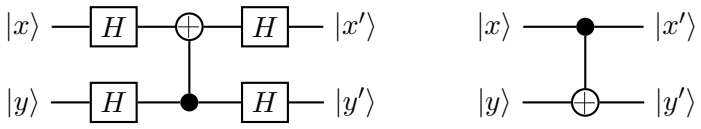
Aufgabe 10.1 *CNOT-Gatter in verschiedenen Basen* (4 + 4 = 8 Punkte)

a) Alice und Bob wollen einen Schlüssel gemäß dem Protokoll aus Aufgabe 8.1 austauschen. Diesmal versucht Dave die beiden mithilfe von Verschränkung zu belauschen. Alice schicke einen Zustand $|+\rangle := \sqrt{1/2}\,(|0\rangle + |1\rangle)$ an Bob. Dave besitzt ein eigenes Qubit $|0\rangle$. Er fängt Alice' Nachricht ab und wendet ein CNOT-Gatter an. Das System befindet sich jetzt im Zustand $\sqrt{1/2}\,(|00\rangle + |11\rangle)$. Dave sendet Alice' Qubit unverändert an Bob weiter und Bob misst es in der $\times$-Basis.

   Bestimmen Sie den Zustand von Daves Qubit nach Bobs Messung. Hat Dave Information über Bobs Messergebnis erhalten?

   Hinweis: Stellen Sie $\sqrt{1/2}(|00\rangle + |11\rangle)$ in der $\times$-Basis dar.

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



Aufgabe 10.2 *Postselektion* (4 + 4 + (2+2+2+2+3+3+2) = 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.

b) Angenommen, Sie haben 1-Qubit-Gatter zur Verfügung, die beliebige[2] lineare, invertierbare, *nicht-unitäre* Funktion $L : \mathbb{C}^2 \to \mathbb{C}^2$ berechnen können. Dadurch können auch Zustände entstehen, die nicht Norm 1 besitzen; wir nehmen an, dass ein solcher Zustand direkt vor einer Messung automatisch auf 1 normiert wird.

Zeigen Sie, dass mit einem solchen Gatter Postselektion (hochwahrscheinlich) simuliert werden kann.

Hinweis: Eine Postselektion auf ein Ereignis A entspricht einer Messung, bei der zuvor die Amplitude von A „aufgepumpt“ wurde.

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

c) Zeigen Sie: $\texttt{PostBQP} \supseteq \texttt{PP}$

Gehen Sie in folgenden Schritten vor. Nehmen Sie an, eine deterministisch 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 $\texttt{P} \subseteq \texttt{BQP}$ gilt, können wir f durch einen (in Polynomialzeit konstruierbaren) unitären Operator U_f implementieren. Ein Zustand $|0^{n+1}\rangle$ liege vor.

i) Erzeuge den $(n+1)$-Qubit-Zustand $2^{-n/2} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$.
Beschreiben Sie, wie dieser Zustand erzeugt werden kann.

ii) Wende Hadamard-Gatter auf die ersten n Qubits an und miss die ersten n Qubits in der Standardbasis.
Zeigen Sie, dass die Wahrscheinlichkeit $|0^n\rangle$ zu erhalten mindestens $1/4$ beträgt.

iii) Falls die Messung in Schritt ii) von $|0^n\rangle$ abweicht, beginne von vorn. Andernfalls sei der entstandene Zustand $|0^n\rangle|\psi\rangle$.
Bestimmen Sie $|\psi\rangle$.

iv) Ignoriere die ersten n Qubits und fahre lediglich mit dem Qubit $|\psi\rangle$ fort. Seien $\alpha, \beta \in \mathbb{R}$. Erzeuge[3] 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 $|\varphi_{\beta/\alpha}\rangle$.

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

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

vi) Angenommen, $s \geq 2^{n-1}$. Zeigen Sie, dass für alle $i \in \{-n, \ldots, n\}$ und $\beta/\alpha = 2^i$ gilt:

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

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

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

[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] Das heißt, Sie können die Funktion frei wählen.
[3] Sie müssen nicht beschreiben, wie diese Operation umgesetzt wird.