

Übungen zur Vorlesung
Quantenrechner: Algorithmen und Komplexität
Wintersemester 2004/2005
Blatt 8

Aufgabe 8.1

- a) Der Algorithmus zum Zählen der Lösungen des allgemeinen Suchproblems benutzt gesteuerte G -Bausteine. Überlege, wie man gesteuerte G -Bausteine realisieren kann, wenn G -Bausteine gegeben sind und man die innere Struktur dieser G -Bausteine nicht ausnutzen möchte.
- b) Der in der Vorlesung vorgestellte Algorithmus für das allgemeine Suchproblem besteht aus den Unterprozeduren für das Zählen der Lösungen und dem Grover-Algorithmus, wobei sich die Anzahl der Grover-Iterationen aus dem Ergebnis des ersten Unterprogramms ergibt. Zeige, dass sich der gesamte Algorithmus auch als Quantenschaltkreis darstellen lässt. Beachte dabei, dass sich in Quantenschaltkreisen Schleifen mit einer variablen Anzahl von Iterationen nicht direkt realisieren lassen.

Aufgabe 8.2

Wir betrachten das Problem der Berechnung des Minimums, wobei auf die Eingabe über ein Orakel zugegriffen wird, das zu einem Index i den Wert x_i liefert. Beweise eine möglichst gute untere Schranke für die Anzahl der Orakelaufrufe von klassischen randomisierten Algorithmen.

Aufgabe 8.3

Das Majoritätsproblem erhält als Eingabe eine boolesche Funktion $f : \{0, 1\}^n \rightarrow \{0, 1\}$, die durch ein Orakel/eine Blackbox realisiert ist. Es ist zu entscheiden, ob $|f^{-1}(1)| \geq 2^n/2$ ist. Wir betrachten den folgenden Algorithmus: Sei p ein Polynom. Wähle $p(n)$ viele zufällig gewählte Eingaben aus. Gib den Wert 1 aus, wenn für mindestens die Hälfte der Eingaben der Funktionswert 1 ist.

Schätze die Fehlerwahrscheinlichkeit dieses Algorithmus möglichst genau ab.

Aufgabe 8.4

Der Suchalgorithmus aus der Vorlesung benötigt den Wert $M = |f^{-1}(1)|$, um die Anzahl der Iterationen wählen zu können. Daher wurde in der Vorlesung ein Algorithmus für die (approximative) Bestimmung von M vorgestellt. In dieser Aufgabe wollen wir einen alternativen Ansatz diskutieren, der durch Ausprobieren eine geeignete Anzahl von Iterationen findet. Im Folgenden sei $M \geq 1$, d. h., das Suchproblem habe eine Lösung.

Die Idee ist die Folgende: Der Bereich, in dem der Rotationswinkel ϑ liegen kann, wird in aufeinanderfolgende Intervalle der Form $[\varphi, (1 + \delta)\varphi]$ zerlegt. Für die Situation, dass ϑ im Intervall $[\varphi, (1 + \delta)\varphi]$ liegt, wählen wir für die Anzahl der Iterationen $\lfloor \pi / (2\varphi(1 + \delta)) \rfloor$. Dies ist eine gute Schätzung, wenn δ klein genug ist. Wenn andererseits δ groß genug ist, ist die Anzahl der Intervalle klein, so dass nicht zu viele Aufrufe des Suchalgorithmus nötig sind. Es ergibt sich folgender Algorithmus:

$\varphi := \varphi_{min}$.

while $\varphi \leq \varphi_{max}$ **do**

$T := \lfloor \pi / (2\varphi(1 + \delta)) \rfloor$.

 Führe den Suchalgorithmus mit T Iterationen aus.

 Bei Erfolg gib das Ergebnis aus, Stop.

$\varphi := (1 + \delta) \cdot \varphi$.

end

Ausgabe: Misserfolg.

Was sind φ_{min} und φ_{max} ? Finde eine geeignete Wahl für δ . Schätze für diese Wahl von δ die Erfolgswahrscheinlichkeit des Algorithmus, sowie die Anzahl der Durchläufe der **while**-Schleife und die Gesamtanzahl von Grover-Iterationen ab.