

**Quantencomputing und Quantensimulation**  
**Wintersemester 2023/24 - Übungsblatt 4**

Ausgabe: 17.11.2023, Abgabe: 24.11.2023, Übungen: 27.11.2023

**Aufgabe 10: Messungen in verschiedenen Basen (8 Punkte)**

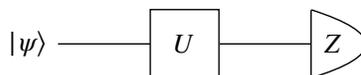
Betrachten Sie die Messung eines Qubits entlang des Vektors  $\mathbf{v} = (\sin(\theta) \cos(\varphi), \sin(\theta) \sin(\varphi), \cos(\theta))^T$ , gegeben durch

$$\langle \Psi | \mathbf{v} \cdot \boldsymbol{\sigma} | \Psi \rangle. \tag{1}$$

a) (2 Punkte) Zeigen Sie, dass sich diese Messung mithilfe der unitären Abbildung

$$U = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2)e^{-i\varphi} \\ \sin(\theta/2)e^{i\varphi} & -\cos(\theta/2) \end{pmatrix}$$

durch folgenden Schaltkreis darstellen lässt.



*Hinweis: Wie sieht der Erwartungswert für die dargestellte Schaltung aus? Vergleichen Sie diesen mit dem Erwartungswert in Gleichung (1).*

b) (2 Punkte) Jede unitäre Abbildung kann durch eine Rotation in Form von  $U = e^{i\alpha} R_{\mathbf{n}}(\beta)$  dargestellt werden. Bestimmen Sie  $\alpha$ ,  $\beta$  und  $\mathbf{n}$ , welche die unitäre Abbildung aus Teilaufgabe a) erzeugen. Drücken Sie  $\mathbf{n}$  in Kugelkoordinaten aus und vergleichen Sie das Ergebnis mit  $\mathbf{v}$ .

c) (2 Punkte) Gegeben sei ein allgemeiner Zwei-Qubit Zustand der Form

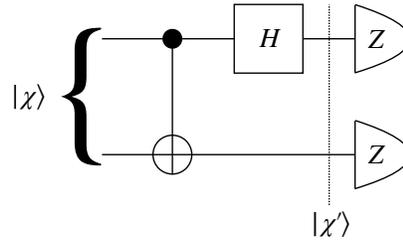
$$|\chi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle.$$

Stellen Sie  $|\chi\rangle$  in der Basis der Bell-Zustände

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle), & |\Phi^-\rangle &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle), \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle), & |\Psi^-\rangle &= \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle), \end{aligned}$$

dar. Mit welchen Wahrscheinlichkeiten werden die verschiedenen Bell-Zustände gemessen?

d) (2 Punkte) Zeigen Sie, dass sich eine Messung in der erwähnten Bell-Basis durch unten abgebildeten Schaltkreis darstellen lässt. Berechnen Sie dazu den Zustand  $|\chi'\rangle$  und vergleichen Sie diesen mit dem Ausdruck für  $|\chi\rangle$  in der Bell-Basis aus Teilaufgabe c). Mit welchen Wahrscheinlichkeiten werden bei dieser Schaltung die einzelnen Ergebnisse gemessen?



### Aufgabe 11: Bernstein-Vazirani Algorithmus (mündlich)

Gegeben sei eine Bitkette  $s$  der Länge  $n$  und eine Funktion  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  mit  $f(x) = x \cdot s$ , wobei  $x \cdot s = \sum_{i=0}^{n-1} x_i s_i \pmod{2}$  die bitweise Multiplikation beschreibt.

a) Nehmen Sie an, dass  $s$  insgesamt  $n_1$  Bits mit einer 1 und  $n_0 = n - n_1$  Bits mit einer 0 enthält. Beweisen Sie, dass  $f(x)$  ausgeglichen ist, falls  $n_1 > 0$  ist. Berechnen Sie dazu die Anzahl an Bitketten  $x$ , für die  $f(x) = 0$  gilt.

*Hinweis: Um  $x \cdot s = 0$  zu erhalten müssen entweder keine, oder eine gerade Anzahl an Bitstellen im Zustand 1 in  $x$  und  $s$  übereinstimmen. Wie viele Möglichkeiten gibt es, dass  $2k$  Bitstellen mit Zustand 1 in  $x$  und  $s$  übereinstimmen? Verwenden Sie die Formel*

$$\sum_{k=0}^{\lfloor n_1/2 \rfloor} \frac{n_1!}{(2k)!(n_1 - 2k)!} = 2^{n_1-1},$$

wobei  $\lfloor n_1/2 \rfloor$  das abgerundete Ergebnis von  $n_1/2$  beschreibt.

b) Begründen Sie, warum aus der Ausgeglichenheit von  $x \cdot s$  für  $n_1 > 0$

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{x \cdot (z \oplus s)}}{2^n} = \delta_{z,s}$$

folgt.

c) Die Identität aus Teilaufgabe b) kann auch mithilfe folgender Eigenschaft der Hadamard-Gatter hergeleitet werden:

$$H^{\otimes n} H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$$

Woraus lässt sich diese Eigenschaft der Hadamard-Gatter herleiten? Benutzen Sie diese Eigenschaft, um die Identität aus Teilaufgabe b) zu beweisen.

### Aufgabe 12: Simon-Problem (mündlich)

Betrachten Sie eine Funktion  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  für die  $f(x) = f(y)$  gilt, falls  $y = x \oplus a$ . Mithilfe eines quantenmechanischen Algorithmus erhält man Zustände  $|y\rangle$ , für welche  $y \cdot a = 0$  gilt. Misst man dann  $n - 1$  linear unabhängige  $y$ , so kann daraus ein Gleichungssystem gebildet werden, durch das sich  $a$  bestimmen lässt.

a) Wie viele verschiedene Bitketten  $y$  erfüllen die Gleichung  $y \cdot a = 0$ ?

*Hinweis: Erinnern Sie sich daran, dass die Funktion  $f(x) = a \cdot x$  für gegebene  $a$  ausgeglichen ist.*

b) Zeigen Sie, dass die Wahrscheinlichkeit  $n - 1$  linear unabhängige Bitketten  $y$  zu messen durch

$$\begin{aligned} P[n - 1 \text{ linear unabh. } y] &= \frac{2^{n-1} - 1}{2^{n-1}} \frac{2^{n-1} - 2}{2^{n-1}} \cdots \frac{2^{n-1} - 2^{n-2}}{2^{n-1}} \\ &= \prod_{k=1}^{n-1} \left(1 - \frac{1}{2^k}\right) \end{aligned}$$

gegeben ist. Der erste Multiplikator stellt hierbei die Wahrscheinlichkeit dar, das erste linear unabhängige  $y$  zu erhalten, der zweite Multiplikator das zweite linear unabhängige  $y$  zu erhalten u.s.w.

*Hinweis: Eine Bitkette  $y_3$  ist linear unabhängig von den Bitketten  $y_2$  und  $y_1$ , falls  $y_3 \neq by_2 + cy_1$  für alle  $b, c \in \{0, 1\}$ . Wenn Sie  $k$  linear unabhängige Bitketten haben, wie viele dazu linear abhängige Bitketten gibt es dann?*

c) Schätzen Sie die Wahrscheinlichkeit ab, nach  $n - 1$  Messungen  $n - 1$  linear unabhängige Gleichungen für  $a$  zu erhalten.