Aufgabe 2.6: Nach Schritt 2 ist das Bit im Zustand $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Wir erhalten $|0\rangle$ mit Wahrscheinlichkeit $(\frac{1}{\sqrt{2}})^2 = 1/2$ und $|1\rangle$ mit Wahrscheinlichkeit $(-\frac{1}{\sqrt{2}})^2 = 1/2$. Das Ergebnis ist also das gleiche.

Aufgabe 2.9: Es genügt, sich folgendes klarzumachen: Wenn A eine Permutationsmatrix ist, so tauscht A^T die Elemente gerade wieder zurück.

Aufgabe 2.10: Wir geben alle Möglichkeiten an, den Eingaben eine Ausgabe zuzuordnen:

1. $0 \to 0, 1 \to 0$,
2. $0 \to 0, 1 \to 1$,
3. $0 \to 1, 1 \to 0$,
4. $0 \to 1, 1 \to 1$

Aufgabe 2.11: wir können die Aufgabe lösen indem wir für jede Wahl von f die Matrix von U_f aufschreiben und mit U_f^* multiplizieren. Eleganter überlegen wir uns, dass U_f für jede Wahl von f eine Permutationsmatrix ist. Dann folgt die Aussage mit Übung 2.9.

Aufgabe 2.12: Wir vermeiden es, den Vektor $(-1,-1)^T$ mit der Matrix H zu multiplizieren und nutzen stattdessen die Linearität. Es gilt $H(-(|0\rangle + |1\rangle)) = -(H|0\rangle + H|1\rangle)$, da unitäre Transformationen linear sind. Wir wenden die Transformationen an und erhalten

$$-(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) = -2/\frac{1}{\sqrt{2}}|0\rangle = -\sqrt{2}|0\rangle.$$

Ein anderer Rechenweg: $H(-(|0\rangle + |1\rangle)) = -\sqrt{2}H\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = -\sqrt{2}|0\rangle$.

Aufgabe 2.14:

$$\begin{aligned}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)\end{aligned}$$

Aufgabe 2.15:

$$H \otimes I_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, I_2 \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Aufgabe 2.17: Eine Basis ist orthogonal, wenn für je zwei ihrer Elemente das Skalarprodukt 0 ist, siehe Abschnitt A.2.3 im Anhang. Wir müssen also zeigen, dass $\langle 0' \,|\, 1' \rangle = 0$ gilt. Der Zustandsvektor von $|+\rangle$ ist

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

der von $|-\rangle$ ist

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Nun genügt es, das Skalarprodukt zu berechnen.

Aufgabe 2.20: Gäbe es eine solche Zerlegung von Φ^+, so könnten wir die Gleichung

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (\alpha_0|0\rangle + \alpha_1|1\rangle) \cdot (\beta_0|0\rangle + \beta_1|1\rangle)$$

lösen. Es würde gelten:

$$\alpha_0\beta_0 = \alpha_1\beta_1 = \frac{1}{\sqrt{2}}$$

und

$$\alpha_0\beta_1 = \alpha_1\beta_0 = 0.$$

Das ist nicht möglich.

Aufgabe 2.21: Der angegebene Zustand ist in Bitschreibweise gleich $1/2(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$ und hat die Zerlegung $\Phi^+ \otimes \Phi^+$.

Aufgabe 2.22: Es gilt $z \neq 0$, wir betrachten

$$\pm\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x\cdot z}|z\rangle.$$

Seien $z_{i_1}, \ldots, z_{i_v}$ die Komponenten von z mit Wert 1. Dann gilt für die Hälfte der $x \in \{0,1\}^n$, dass eine *gerade* Anzahl der Komponenten $x_{i_1}, \ldots, x_{i_v}$ den Wert 1 hat; für diese x gilt $x \cdot z = 0$. Für die andere Hälfte gilt $x \cdot z = 1$. Also ist

$$\pm\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x\cdot z}|z\rangle = \pm\frac{1}{2^n}\left(\frac{1}{2^{n-1}} - \frac{1}{2^{n-1}}\right)|z\rangle = 0.$$

Aufgabe 2.23: Nach Schritt 4 befindet sich das Quantenregister in demselben Zustand wie nach Schritt 4 von Deutsch-Jozsa:

$$\left(\frac{1}{2^n}\sum_{z=0}^{2^n-1}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot z}|z\rangle\right) \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Nun muss nur noch die Amplitude von $|z\rangle$ für die beiden Fälle $z = a$ und $z \neq a$ berechnet werden.

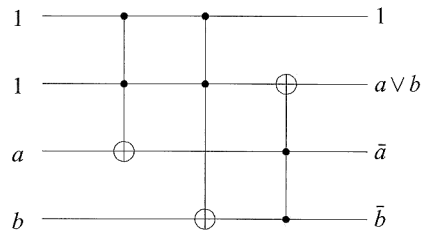

Abbildung B.1: Disjunktion aus drei Toffoligattern

Kapitel 3

Aufgabe 3.5: Um das einzusehen, benötigen wir die Regel von De Morgan:

$$\overline{a \wedge b} = \overline{a} \vee \overline{b}.$$

Damit gilt

$$a \vee b = \overline{\overline{a} \wedge \overline{b}}.$$

Wir können das Oder also durch NAND und zwei Negationen ausdrücken. Das geschieht in Abbildung B.1.

Aufgabe 3.6: Wir müssen uns dazu zwei Dinge überlegen: das Fredkin-Gatter führt eine umkehrbare Berechnung aus und ist universal, kann also zum Beispiel AND und NOT berechnen.

Man nennt das Fredkin-Gatter auch *controlled swap*, da die Belegung von c bestimmt, ob die Werte von a und b getauscht werden.

Aufgabe 3.7: Da es sich um verschränkte Zustände handelt, betrachten wir das gesamte Register:

$$\begin{aligned}
& |a\rangle|b\rangle|10101100\rangle \\
= \; & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|10101100\rangle \\
= \; & 1/2(|0010101100\rangle + |0110101100\rangle + |1010101100\rangle + |1110101100\rangle) \\
\to \; & 1/2(|0010101100\rangle + |0110101100\rangle + |1011101100\rangle + |1111101100\rangle) \\
\to \; & 1/2(|0010101100\rangle + |0110111100\rangle + |1011101100\rangle + |1111111100\rangle)
\end{aligned}$$

Das ist der Zustand nach den beiden ersten Toffoli-Gattern. Führen wir die Berechnung fort, sehen wir, dass die Ausgabebits korrekt belegt sind. Nennen wir die beiden letzten Bits o_1 und o_2, ist der Endzustand

$$|a\rangle|b\rangle|o_1\rangle|o_2\rangle = 1/2(|0000\rangle + |0110\rangle + |1010\rangle + |1101\rangle),$$

gemäß der Regel: $o_1 = a \oplus b, o_2 = a \wedge b$.

Aufgabe 3.8: Das Register aus vier Quantenbits befindet sich im Ausgangszustand

$$|1\rangle|a\rangle|b\rangle|0\rangle = 1/2\,(|1000\rangle + |1010\rangle + |1100\rangle + |1110\rangle)\,.$$

Die beiden Toffoli-Gatter überführen es in

$$1/2\,(|1000\rangle + |1010\rangle + |1110\rangle + |1101\rangle)\,.$$

Aufgabe 3.9: $|\phi_3\rangle$ und $|\psi_3\rangle$ lassen sich mit einer Messung bezüglich der Hadamard-Basis

$$\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

unterscheiden. Gleichwertig ist, $H|\phi_3\rangle$ und $H|\psi_3\rangle$ bezüglich der Standardbasis zu messen.

Aufgabe 4.1: Wir müssen zeigen: gilt für eine Eingabe G $\mathrm{HC}(G) = 1$, so lässt sich das mit Hilfe eines Zertifikats effizient verifizieren. Das Zertifikat ist der Hamilton-Kreis in dem Graphen G. Wir verifizieren, dass jeder Knoten genau einmal besucht wird, indem wir die Kanten durchlaufen. Kapitel 4

Aufgabe 6.2: Im Fall $N = 2$ können wir direkt nachrechnen, dass $-HR_2H = D_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ gilt. Für den allgemeinen Fall bietet es sich an, Multiplikation von Blockmatrizen zu verwenden und die Aussage mit vollständiger Induktion zu zeigen. Hier folgen wichtige Zwischenergebnisse: Kapitel 6

Wegen $H_{n+1} = H \otimes H_n, N = 2^n$ gilt

$$-H_{n+1}R_{2N}H_{n+1} = \frac{1}{\sqrt{2}}\begin{pmatrix} -H_n & -H_n \\ -H_n & H_n \end{pmatrix} \cdot \frac{1}{\sqrt{2}}\begin{pmatrix} R_N H_n & R_N H_n \\ H_n & -H_n \end{pmatrix}.$$

Dabei wurde verwendet, dass R_N in einer rechts multiplizierten Matrix die erste Zeile negiert und sonst nichts verändert. Ausmultiplizieren ergibt nun

$$\frac{1}{2}\begin{pmatrix} -H_nR_NH_n - I_N & -H_nR_NH_n + I_N \\ -H_nR_NH_n + I_N & -H_nR_NH_n - I_N \end{pmatrix} = \frac{1}{2}\begin{pmatrix} D_N - I_N & D_N + I_N \\ D_N + I_N & D_N - I_N \end{pmatrix} = D_{2N}.$$

Aufgabe 6.4: Wir können die Aussage formal beweisen, wenn wir die vier Basiszustände $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$ betrachten:
$|0\rangle|0\rangle \xrightarrow{X\otimes X} |1\rangle|1\rangle \xrightarrow{I_2\otimes H} |1\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{\mathrm{CNOT}} |1\rangle - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{I_2\otimes H} -|1\rangle|1\rangle$
$\xrightarrow{X\otimes X} -|0\rangle|0\rangle$.
Genauso sieht man, dass der Schaltkreis die Zustände $|0\rangle|1\rangle, |1\rangle|0\rangle$ und $|1\rangle|1\rangle$ unverändert lässt.

Aufgabe 6.6: Es ist die Operation V_f! Sie invertiert die Amplitude jedes von f auf 1 abgebildeten Elements - rechnen Sie das nach! Nun betrachten wir die Ebene, die vom Startzustand $|s\rangle$ und von $|\hat{x}_d\rangle$ aufgespannt wird. In dieser Ebene entspricht das Kippen der Komponenten aller gesuchten Elemente der Spiegelung an der Achse längs $|\tilde{x}^{\perp}\rangle$. Das kann man sich durch eine Skizze veranschaulichen.

Aufgabe 6.8: Wir führen den Algorithmus k-mal aus. Angenommen, wir haben die Elemente $\hat{x}_1,\ldots,\hat{x}_l$ schon gefunden. Dann Kippen wir nach der Anwendung von V_f die Amplituden von $\hat{x}_1,\ldots,\hat{x}_l$ wieder zurück. Das lässt sich wie auf Seite 145 realisieren. Wir führen die Groveriteration $G(N,k-l)$-mal aus und erhalten eine Superposition über $\hat{x}_{l+1},\ldots,\hat{x}_k$.

Wenn k groß ist (Größenordnung $\Omega\left(\sqrt{N}\right)$), bietet es sich an, für jedes Element x den Funktionswert zu bestimmen.

Kapitel 7

Aufgabe 7.3: Wir nehmen an, dass $a'=0$ und $e'=1$ gilt: Messen wir ein Bit im Zustand $|0\rangle$ oder $|1\rangle$ in der falschen Basis B', befindet sich $|x\rangle$ anschließend im Zustand $|+\rangle$ oder $|-\rangle$. Misst Bob nun in B, erhält er nur in der Hälfte der Fälle das korrekte Ergebnis.

Der Fall $a'=1$ und $e'=0$ ergibt sich analog.

Aufgabe 7.5: An der Argumentation ist bis zu dem letzten Satz nichts auszusetzen. Jedoch bietet sich für Eve folgende Möglichkeit an: Alice hat ihr Soll erfüllt, die Quantenbits verschickt und verwahrt $a_1,\ldots,a_m$ in einem Panzerschrank. Diesen kann Eve knacken. Nun wartet sie, bis Bob misst, belauscht den Austausch der Basen und erfährt, welche der von ihr gestohlenen Bits den Schlüssel bilden. Kann sie den Panzerschrank wieder verschließen, bleibt ihr Tun unbemerkt.

Wichtig ist: Theoretisch kann ihr Eindringen in den Panzerschrank unbemerkt bleiben. Ihr Hantieren am Quantenkanal wird aus theoretischen Gründen bemerkt, wenn sie wesentliche Teile des Schlüssels erlauschen will.

Kapitel 8

Aufgabe 8.1: Wäre $a^{p/2}-1$ ein Vielfaches von n, hieße das $a^{p/2}-1\equiv 0 \bmod n$ und also $a^{p/2}\equiv 1 \bmod n$. Das ist aber ausgeschlossen, weil in diesem Fall die Periode kleiner gleich $p/2$ wäre. Diese ist jedoch gleich p.

Aufgabe 8.2: Wenn eine Zahl m sowohl x als auch n teilt, dann teilt sie für jedes k die Differenz $x-kn$. Darauf beruht der Euklidische Algorithmus.

Aufgabe 8.6: Der formale Beweis lautet wie folgt:

$$\begin{aligned}\sum_{i=0}^{N-1}\left(\omega_N^k\right)^i &= \frac{(\omega_N^k)^N-1}{\omega_N^k-1}\\ &= \frac{(\omega_N^N)^k-1}{\omega_N^k-1}=0\end{aligned}$$

Ist k ein Vielfaches von N, gilt $\omega_N^k=1$ und die Summe ist N.

Aufgabe 8.8: $R_4\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)=\frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle)$. Die komplexe Zahl $-1=e^{\pi i}$ wurde um den Winkel $\pi/2$ gedreht: auf $e^{3/2\pi i}=-i$.

Aufgabe 8.10: Wir betrachten als Beispiel Bit y_0. x_2 wird von H in $|\phi_1\rangle=\frac{1}{\sqrt{2}}(|0\rangle+\omega_2^{x_2}|1\rangle)$ überführt. R_4 multipliziert den $|1\rangle$-Anteil in $|\phi_1\rangle$ mit