

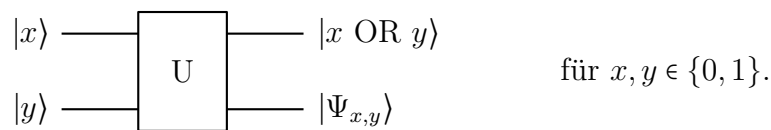
6. Übungsblatt zur Vorlesung Quanten-Computing

Aufgabe 1

Zeigen Sie, dass es keine unitäre Realisierung von OR auf einem 2-Qubit-Register gibt.

Lösung:

Angenommen, es gibt eine Realisierung von OR auf einem 2-Qubit-Register, also eine unitäre Transformation U , die zwei Qubits entgegennimmt und am Ausgang in einem Qubit – o.B.d.A. im ersten Qubit – das Resultat einer OR-Verknüpfung der Eingangs-Qubits enthält, falls diese in einem Basiszustand, also gleich $|0\rangle$ bzw. $|1\rangle$, sind. Das zweite Ausgangs-Qubit kann dabei irgendwie von den Eingangs-Qubits abhängen:



Als Formel:

$$U(|x\rangle \otimes |y\rangle) = |x \text{ OR } y\rangle \otimes |\Psi_{x,y}\rangle \quad \text{für } x, y \in \{0, 1\}.$$

Dann gilt also insbesondere

$$U|01\rangle = |1\rangle \otimes |\Psi_{00}\rangle, \quad U|10\rangle = |1\rangle \otimes |\Psi_{01}\rangle, \quad U|11\rangle = |1\rangle \otimes |\Psi_{10}\rangle.$$

Betrachtet man dies vektoriell und setzt man $|\Psi_{xy}\rangle = \alpha_{xy}|0\rangle + \beta_{xy}|1\rangle = \begin{pmatrix} \alpha_{xy} \\ \beta_{xy} \end{pmatrix}$, so erhält man als Bilder

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_{00} \\ \beta_{00} \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha_{00} \\ \beta_{00} \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_{01} \\ \beta_{01} \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha_{01} \\ \beta_{01} \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_{10} \\ \beta_{10} \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha_{10} \\ \beta_{10} \end{pmatrix}.$$

Als Bilder der hinteren drei Einheitsvektoren sind dies die hinteren drei Spalten der Abbildungsmatrix zu U . Diese Matrix hat dann also die Gestalt

$$\begin{pmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \end{pmatrix},$$

wobei * für einen beliebigen Eintrag steht.

Da die oberen beiden Zeilen Vielfache voneinander sind, kann diese Matrix nicht invertierbar, also insbesondere nicht unitär sein - Widerspruch!

Aufgabe 2

Wie lautet die Transformationsmatrix für die Toffoli-Transformation?

Lösung:

Es ist

$$\begin{aligned} |000\rangle &\mapsto |000\rangle, & |001\rangle &\mapsto |001\rangle, & |010\rangle &\mapsto |010\rangle, & |011\rangle &\mapsto |011\rangle, \\ |100\rangle &\mapsto |100\rangle, & |101\rangle &\mapsto |101\rangle, & |110\rangle &\mapsto |111\rangle, & |111\rangle &\mapsto |110\rangle. \end{aligned}$$

Die Transformationsmatrix ist also

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Aufgabe 3

Wie sehen die Ausgabe-Qubits einer Toffoli-Transformation aus, wenn alle drei Eingabe-Qubits gleich $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ sind?

Können Sie Ihre Beobachtung/Rechnung verallgemeinern?

Lösung:

Auf der Eingabe-Seite hat man dann

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2^{3/2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle). \end{aligned}$$

Bei den letzten beiden Summanden wirkt das Toffoli-Gatter:

$$|110\rangle \mapsto |111\rangle, \quad |111\rangle \mapsto |110\rangle,$$

was aber nur eine Vertauschung der Summationsreihenfolge entspricht. Der Ausgangszustand ist also gleich dem Eingangszustand.

Verallgemeinerung: Bei beliebigen Basiszuständen $|x\rangle, |y\rangle$ mit $x, y \in \{0, 1\}$ gilt

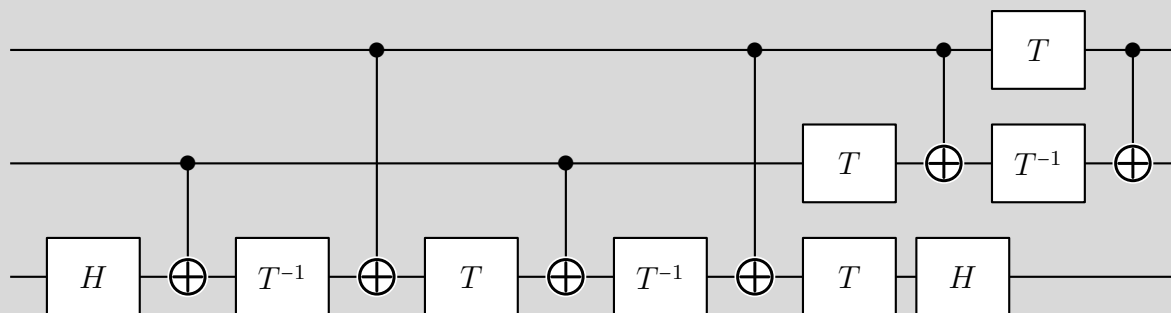
$$|x\rangle \otimes |y\rangle \otimes |+\rangle \mapsto |x\rangle \otimes |y\rangle \otimes |+\rangle,$$

denn bei $x = y = 1$ werden wie oben die beiden Summanden von $|+\rangle$ vertauscht, die Summe bleibt aber gleich, ansonsten ändert sich nichts.

Damit gilt für beliebige Zustände $|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes |+\rangle$, dass sie durch das Toffoli-Gatter unverändert bleiben.

Aufgabe 4

Verifizieren Sie, dass man mit dem 1-Qubit-Gatter $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{\pi}{4}j} \end{pmatrix}$ und entsprechend $T^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi}{4}j} \end{pmatrix}$ das Toffoli-Gatter wie folgt nachbauen kann:



Tipp:

Es reicht, sich zu überlegen, dass bei den 8 Basiszuständen das Ergebnis des Schaltkreises dem des Toffoli-Gatters entspricht.

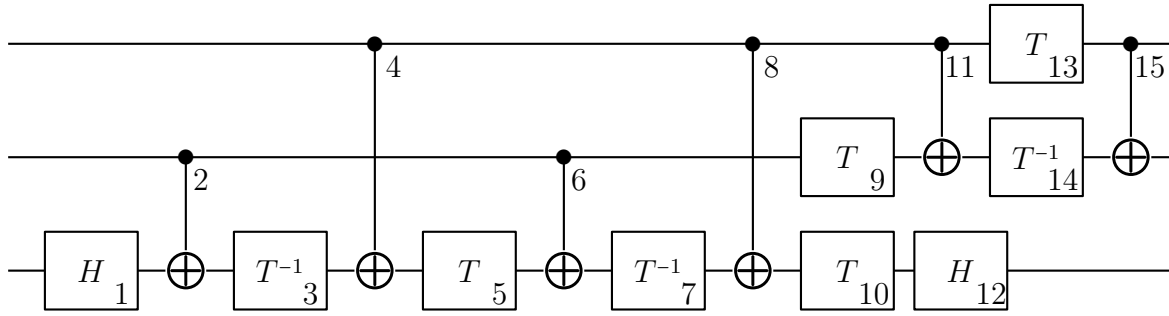
Betrachten Sie zunächst den Fall, dass das erste Qubit gleich $|0\rangle$ ist.

Betrachten Sie dann den Fall, dass das zweite Qubit gleich $|0\rangle$ ist. Was muss man sich dazu überlegen?

Es bleibt der Fall, dass die ersten beiden Qubits gleich $|1\rangle$ sind.

Lösung:

In der folgenden Darstellung sind die einzelnen Gatter nummeriert:



Betrachtet wird zunächst der Fall, dass das erste Qubit gleich $|0\rangle$ ist:

Da $T|0\rangle = |0\rangle$ ist, ist dann das erste Qubit am Ausgang weiterhin $|0\rangle$.

Ferner schaltet keines der vom ersten Qubit kontrollierten CNOT-Gatter (4, 8, 11, 15).

Auf dem zweiten Qubit hebt sich daher die Wirkung von T und T^{-1} (9 und 14) auf, so dass das zweite Qubit unverändert zum Ausgang gelangt.

Auch auf dem dritten Qubit heben sich dann die Wirkungen von T und T^{-1} (3 und 5 sowie 7 und 10) auf. Damit folgen die CNOT-Gatter 2 und 6 direkt aufeinander und heben sich gegenseitig auf. Es bleiben die beiden Hadamard-Gatter 1 und 12, die sich dann auch gegenseitig aufheben, so dass das dritte Qubit am Ausgang gleich dem Eingangs-Qubit ist.

Für diesen Fall sind also die Eingangs-Qubits gleich den Ausgangs-Qubits.

Betrachtet wird nun der Fall, dass das erste Qubit gleich $|1\rangle$ und das zweite Qubit gleich $|0\rangle$ ist:

In diesem Fall schalten die CNOT-Gatter 2 und 6 nicht. Auf dem dritten Qubit hebt sich daher die Wirkung von T und T^{-1} (5 und 7) auf; damit hebt sich auch die Wirkung der CNOT-Gatter 4 und 8 auf, und damit wiederum die der T^{-1} - und T -Gatter 3 und 10. Es bleiben die beiden Hadamard-Gatter 1 und 12, die sich dann auch gegenseitig aufheben, so dass das dritte Qubit am Ausgang gleich dem Eingangs-Qubit ist.

Nun werden die beiden ersten Qubits betrachtet, die am Eingang im Zustand $|10\rangle$ sind. Das T -Gatter 9 ändert am zweiten Qubit (Zustand $|0\rangle$) nichts. Nach dem CNOT-Gatter 11 sind die beiden Qubits im Zustand $|11\rangle$. Durch die Gatter 13 und 14 wird dies zu

$$T|1\rangle \otimes T^{-1}|1\rangle = \left(e^{-\frac{\pi}{4}j} \cdot |1\rangle\right) \otimes \left(e^{\frac{\pi}{4}j} \cdot |1\rangle\right) = |1\rangle \otimes |1\rangle$$

und nach dem CNOT-Gatter 15 dann wieder zu $|10\rangle$.

Für diesen Fall sind also die Eingangs-Qubits gleich den Ausgangs-Qubits.

Es bleibt der Fall, dass die ersten beiden Qubits gleich $|11\rangle$ sind, so dass alle CNOT-Gatter schalten.

Die beiden ersten Qubits werden dann durch die Gatter 9, 11, 13, 14 und 15 folgendermaßen modifiziert:

$$\text{Nach Gatter 9: } |1\rangle \otimes (e^{-\frac{\pi}{4}j} \cdot |1\rangle).$$

$$\text{Nach Gatter 11: } |1\rangle \otimes (e^{-\frac{\pi}{4}j} \cdot |0\rangle).$$

$$\text{Nach Gatter 13 und 14: } (e^{-\frac{\pi}{4}j} \cdot |1\rangle) \otimes (e^{-\frac{\pi}{4}j} \cdot |0\rangle) = e^{-\frac{\pi}{2}j} \cdot |10\rangle.$$

$$\text{Nach Gatter 15: } e^{-\frac{\pi}{2}j} \cdot |11\rangle.$$

Falls das dritte Qubit am Eingang gleich $|0\rangle$ ist, entwickelt es sich wie folgt:

$$\text{Nach Gatter 1: } \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

$$\text{Nach Gatter 2: } \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

$$\text{Nach Gatter 3: } \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{\pi}{4}j} \cdot |1\rangle).$$

$$\text{Nach Gatter 4: } \frac{1}{\sqrt{2}}(|1\rangle + e^{\frac{\pi}{4}j} \cdot |0\rangle) = \frac{1}{\sqrt{2}}(e^{\frac{\pi}{4}j} \cdot |0\rangle + |1\rangle).$$

$$\text{Nach Gatter 5: } \frac{1}{\sqrt{2}}(e^{\frac{\pi}{4}j} \cdot |0\rangle + e^{-\frac{\pi}{4}j} \cdot |1\rangle).$$

$$\text{Nach Gatter 6: } \frac{1}{\sqrt{2}}(e^{\frac{\pi}{4}j} \cdot |1\rangle + e^{-\frac{\pi}{4}j} \cdot |0\rangle) = \frac{1}{\sqrt{2}}(e^{-\frac{\pi}{4}j} \cdot |0\rangle + e^{\frac{\pi}{4}j} \cdot |1\rangle).$$

$$\text{Nach Gatter 7: } \frac{1}{\sqrt{2}}(e^{-\frac{\pi}{4}j} \cdot |0\rangle + e^{\frac{\pi}{4}j} \cdot e^{\frac{\pi}{4}j} \cdot |1\rangle) = \frac{1}{\sqrt{2}}(e^{-\frac{\pi}{4}j} \cdot |0\rangle + e^{\frac{\pi}{2}j} \cdot |1\rangle).$$

$$\text{Nach Gatter 8: } \frac{1}{\sqrt{2}}(e^{-\frac{\pi}{4}j} \cdot |1\rangle + e^{\frac{\pi}{2}j} \cdot |0\rangle) = \frac{1}{\sqrt{2}}(e^{\frac{\pi}{2}j} \cdot |0\rangle + e^{-\frac{\pi}{4}j} \cdot |1\rangle).$$

$$\text{Nach Gatter 10: } \frac{1}{\sqrt{2}}(e^{\frac{\pi}{2}j} \cdot |0\rangle + e^{-\frac{\pi}{4}j} \cdot e^{-\frac{\pi}{4}j} \cdot |1\rangle) = e^{\frac{\pi}{2}j} \cdot \frac{1}{\sqrt{2}}(|0\rangle + e^{-\pi j} \cdot |1\rangle)$$

$$\text{Wegen } e^{-\pi j} = -1 \text{ ist dieser Zustand gleich } e^{\frac{\pi}{2}j} \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = e^{\frac{\pi}{2}j} \cdot |-\rangle.$$

$$\text{Nach Gatter 12: } e^{\frac{\pi}{2}j} \cdot |1\rangle.$$

Die drei Qubits befinden sich also am Ende im Zustand

$$e^{-\frac{\pi}{2}j} \cdot |11\rangle \otimes e^{\frac{\pi}{2}j} \cdot |1\rangle = |111\rangle.$$

Falls das dritte Qubit am Eingang gleich $|1\rangle$ ist, ist die Analyse ähnlich: Bei den Zuständen nach Gatter 1 bis 10 hat man in der Mitte jeweils ein „-“ statt des „+“ und durch die CNOT-Gatter – also die Vertauschung von $|0\rangle$ und $|1\rangle$ – zieht sich ein „-“ nach vorne. Wegen der insgesamt vier CNOT-Gatter heben diese Vorzeichen sich insgesamt auf. Nach Gatter 10 ist das Qubit also im Zustand

$$e^{\frac{\pi}{2}j} \cdot \frac{1}{\sqrt{2}}(|0\rangle - e^{-\pi j} \cdot |1\rangle) = e^{\frac{\pi}{2}j} \cdot \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = e^{\frac{\pi}{2}j} \cdot |+\rangle$$

und nach Gatter 11 daher im Zustand $e^{\frac{\pi}{2}j} \cdot |0\rangle$. Die drei Qubits befinden sich also am Ende im Zustand

$$e^{-\frac{\pi}{2}j} \cdot |11\rangle \otimes e^{\frac{\pi}{2}j} \cdot |0\rangle = |110\rangle.$$

Damit sieht man, dass der Schaltkreis für die Basiszustände und damit für alle Zustände die gleiche Wirkung hat wie ein Toffoli-Gatter.

Alternative Herleitung für das dritte Qubit für den Fall, dass die ersten beiden Qubits gleich $|11\rangle$ sind:

Da alle CNOT-Gatter schalten, wirken sie auf das dritte Qubit wie $P_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Die Wirkung der Gatter 2, 3, 4 und 5 lässt sich also beschreiben durch

$$\begin{aligned} U &= T \cdot P_X \cdot T^{-1} \cdot P_X = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{\pi}{4}j} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi}{4}j} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ e^{-\frac{\pi}{4}j} & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ e^{\frac{\pi}{4}j} & 0 \end{pmatrix} = \begin{pmatrix} e^{\frac{\pi}{4}j} & 0 \\ 0 & e^{-\frac{\pi}{4}j} \end{pmatrix}. \end{aligned}$$

Die Gatter 6, 7, 8 und 10 sind die gleichen wie 2, 3, 4 und 5, so dass die Wirkung der Gatter 2 bis 10 beschrieben wird durch

$$\begin{aligned} U \cdot U &= \begin{pmatrix} e^{\frac{\pi}{4}j} & 0 \\ 0 & e^{-\frac{\pi}{4}j} \end{pmatrix} \cdot \begin{pmatrix} e^{\frac{\pi}{4}j} & 0 \\ 0 & e^{-\frac{\pi}{4}j} \end{pmatrix} \\ &= \begin{pmatrix} e^{\frac{\pi}{2}j} & 0 \\ 0 & e^{-\frac{\pi}{2}j} \end{pmatrix} = \begin{pmatrix} j & 0 \\ 0 & -j \end{pmatrix} = j \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

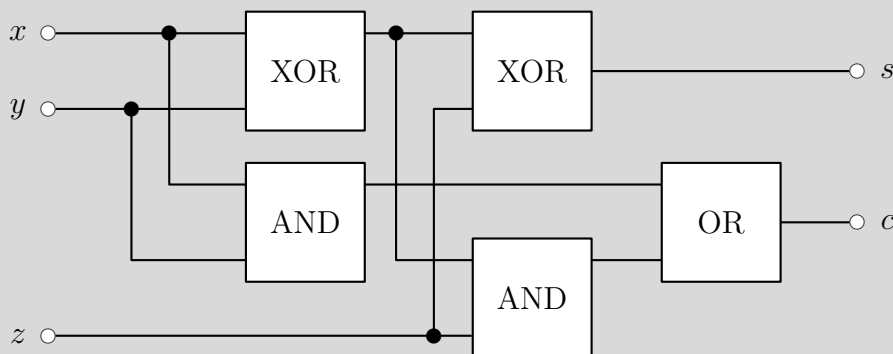
Mit den äußeren Hadamard-Gattern erhält man als Wirkung insgesamt

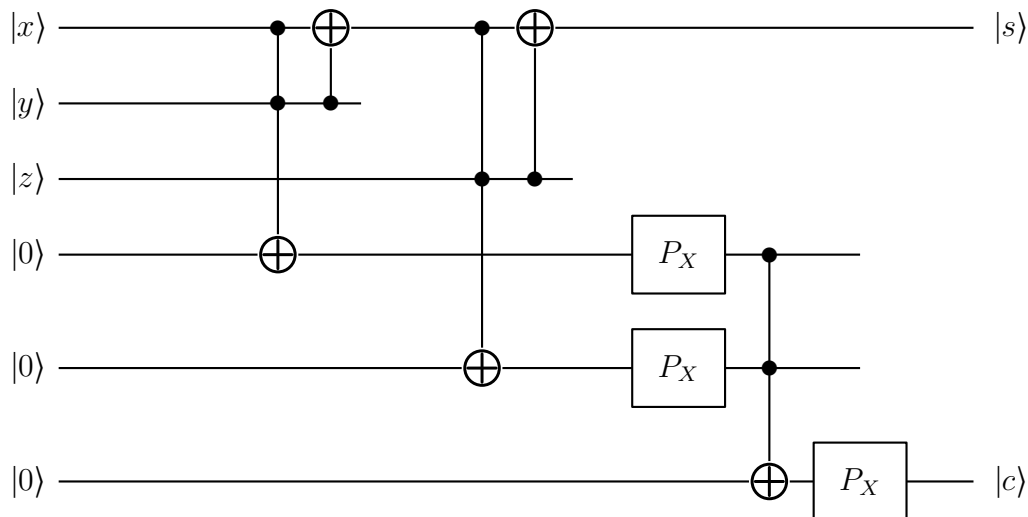
$$\begin{aligned} H \cdot j \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot H &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot j \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= j \cdot \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = j \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

Der Faktor „j“ wird durch den Faktor $e^{-\frac{\pi}{2}j} = -j$, der bei den ersten beiden Qubits nach Gatter 15 entsteht, aufgehoben, und so sieht man, dass beim dritten Qubit $|0\rangle$ und $|1\rangle$ vertauscht werden.

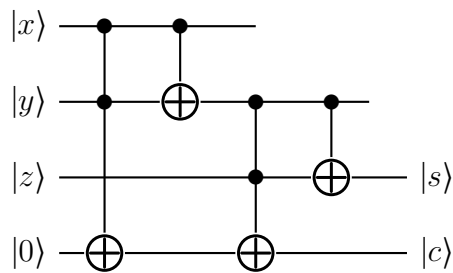
Aufgabe 5

Betrachtet wird ein klassischer Volladdierer, d.h., der Output stellt in der Form cs die zweistellig binär dargestellte Summe von x, y und z , $x, y, z \in \{0, 1\}$, dar:





Tatsächlich kann man sogar mit nur einem Hilf-Qubit und vier Gattern den Volladdierer realisieren:



Aufgabe 6 (mit Qiskit, 5 Punkte)

Erstellen Sie in Qiskit einen Schaltkreis, der auf $|0\rangle/|1\rangle$ -Eingaben wie ein Volladdierer funktioniert.

Welche Ausgaben erhält man bei anderen Eingaben, z.B. $|+\rangle$?

Aufgabe 7

Betrachtet wird das sogenannte *Fredkin-* oder kontrolliertes Swap-Gatter F auf einem 3-Qubit-Register. Für Basiszustände $|xyz\rangle$ mit $x, y, z \in \{0, 1\}$ wirkt es wie folgt:

$$F(x, y, 0) = (x, y, 0) \quad \text{und} \quad F(x, y, 1) = (y, x, 1).$$

Wie kann man mit dem Fredkin-Gatter eine AND-Verknüpfung realisieren?

Lösung:

Bei $F(0, x, y)$ ist das erste Ausgabe-Bit gleich x AND y :

Bei $y = 0$ ist $F(0, x, y) = F(0, x, 0) = (0, x, 0)$.

Bei $y = 1$ ist $F(0, x, y) = F(0, x, 1) = (x, 0, 1)$.

Bei $y = 1$ und $x = 0$ ist also $F(0, x, y) = (0, 0, 1)$ und bei $x = y = 1$ ist $F(0, x, y) = (1, 0, 1)$.

Aufgabe 8

Betrachtet wird ein Zufallsexperiment mit den Ausgabewerten „A“ und „B“, wobei bekannt ist, dass

1. entweder immer „A“ geliefert wird, oder
2. mit Wahrscheinlichkeit $p > 0$ „B“ und mit Wahrscheinlichkeit $1 - p$ „A“ geliefert wird.

Das Zufallsexperiment wird k mal wiederholt. Erhält man dabei mindestens ein Mal „B“, so gilt 2.; erhält man immer „A“, entscheidet man, dass 1. gilt.

Wie oft müssen Sie das Zufallsexperiment durchführen, damit die Wahrscheinlichkeit für eine Fehlentscheidung kleiner als 10^{-n} ist?

Wie groß ist k konkret bei $n = 100$ und

- a) $p = 0.6$, b) $p = 0.2$?

Lösung:

Eine Fehlentscheidung erfolgt, wenn 2. gilt, aber k mal „A“ geliefert wird. Die Wahrscheinlichkeit dafür ist $(1 - p)^k$. Es muss also gelten

$$(1 - p)^k \leq 10^{-n} \quad \Leftrightarrow \quad k \geq \log_{1-p}(10^{-n}) = n \cdot (-\log_{1-p} 10).$$

Bei $p = 0.6$ und $n = 100$ erhält man $k \geq 251,3$.

Bei $p = 0.2$ und $n = 100$ erhält man $k \geq 1031,8$.