Da der Abstand mit Hilfe des Skalarproduktes definiert ist, folgt die erste Aussage aus der zweiten.

2.6 Der zweite Algorithmus: Das Problem von Deutsch

In der Quantenwelt kann man zwei Seiten einer Münze gleichzeitig betrachten. Das wundert uns gar nicht mehr. Nun werden wir sehen, wie man daraus einen Vorteil ziehen kann. Nehmen wir einmal an, wir haben eine Superposition der beiden Münzseiten erzeugt. Wir *messen* diese Superposition, um etwas über die Seiten zu erfahren. Dann erhalten wir doch nur über *eine* Münzseite Informationen. Geht man geschickt vor, lässt sich dennoch etwas über beide Seiten erfahren. Das folgende Problem ist nach David Deutsch benannt, einem der Väter des Quantencomputers; der 1953 in Israel geborene wuchs in England auf und lebt in Oxford.

Ist die Münze echt?

Wir sollen herausbekommen, ob eine Münze echt oder eine plumpe Fälschung ist. Die Vorderseite der echten Münze zeigt eine Zahl, die Rückseite das Brandenburger Tor. Bei der falschen Münze sind beide Seiten gleich. Wie oft müssen wir uns die Münze ansehen, um eine echte Münze von einer Fälschung zu unterscheiden? Zweimal, da wir beide Seiten betrachten müssen. Ein Quantencomputer kann in einer ähnlichen Situation echte Vorteile bringen.

Wir sollen etwas über eine Funktion f herausfinden, die ein Bit als Eingabe bekommt und ein Bit ausgibt, $f : \{0,1\} \to \{0,1\}$. Uns wird ein Bauteil zur Verfügung gestellt, das uns zu einem Bit b den Wert $f(b)$ liefert; andere Informationen über f haben wir nicht. Man sagt, f ist uns als *Black Box* gegeben. Wir bevorzugen in der Folge das deutsche Wort *Orakel*.

Aufgabe 2.10: Geben Sie alle Funktionen $f : \{0,1\} \to \{0,1\}$ an.

Für eine solche Funktion gilt, sie ist entweder *konstant*, dann gilt $f(0) = f(1)$ oder sie ist *balanciert*: $f(0) \neq f(1)$.

Wir sollen folgende Frage beantworten: Ist die uns als Orakel vorliegende Funktion konstant oder balanciert?

Ein klassischer Computer muss die Funktion an zwei Stellen abfragen. Angenommen, wir beginnen damit, nach $f(0)$ zu fragen. Dann hilft uns die Antwort nichts, wenn wir nicht auch $f(1)$ kennen, so wie wir beide Seiten der Münze betrachten müssen. Wir betrachten nun einen Quantenalgorithmus, der dieses Problem mit nur einem Orakelaufruf löst.

Reversibles Orakel

Der Quantenalgorithmus wird ein Quantenbit in eine Superposition über beide möglichen Eingaben von f versetzen, dann auf dieses Quantenbit das Orakel anwenden und eine Superposition über beide Funktionswerte bekommen. Da aber alle Rechenschritte umkehrbar sein müssen, brauchen wir die Funktion f in einer reversiblen Version. f ist nicht umkehrbar, falls sie konstant ist. Darum verwenden wir zwei Bits $|x\rangle$ und $|y\rangle$ und folgende unitäre Form des Funktionsaufrufes

$$U_f : |x,y\rangle \mapsto |x,y \oplus f(x)\rangle.$$

Die Operation $\oplus$ ist die dem exklusiven Oder entsprechende Addition von Bits, siehe Seite 16. Es gilt $U_f^{-1} = U_f$, also ist U_f reversibel.

Aufgabe 2.11: Zeigen Sie, dass U_f unitär ist.

Nun können wir den Algorithmus angeben. Er verwendet ein Register aus zwei Quantenbits. Dem Algorithmus entspricht der Schaltkreis aus Abbildung 2.14.

Der Algorithmus für das Problem von Deutsch

1. $|x\rangle|y\rangle \leftarrow |0\rangle|1\rangle$
2. Wende die Hadamard-Transformation H auf beide Bits an:
   $|x\rangle|y\rangle \leftarrow H|x\rangle H|y\rangle$
3. Werte f aus:
   $|x\rangle|y\rangle \leftarrow U_f|x\rangle|y\rangle$
4. Wende die Hadamard-Transformation H auf beide Bits an:
   $|x\rangle|y\rangle \leftarrow H|x\rangle H|y\rangle$
5. Miss das Register:
   Hat $|x\rangle|y\rangle$ den Wert $|0\rangle|1\rangle$: Ausgabe *konstant*,
   hat $|x\rangle|y\rangle$ den Wert $|1\rangle|1\rangle$: Ausgabe *balanciert*.

Dem Algorithmus ist nicht auf den ersten Blick anzusehen, warum er unser Problem löst. Darum werden wir sein Vorgehen detailliert betrachten. Festzuhalten ist: U_f wurde nur einmal ausgeführt! Vielleicht ist noch die folgende Bemerkung zu Schritt 5 angebracht. Der Test, ob das Register einen bestimmten Wert hat, und auch die Ausgabe des Ergebnisses kann von einem klassischen Rechner übernommen werden. Dies erscheint als das praktikabelste Vorgehen. Wir werden jedoch in Kapitel 3.2 sehen, dass ein Quantencomputer theoretisch all das kann, wozu ein klassischer Rechner fähig ist.

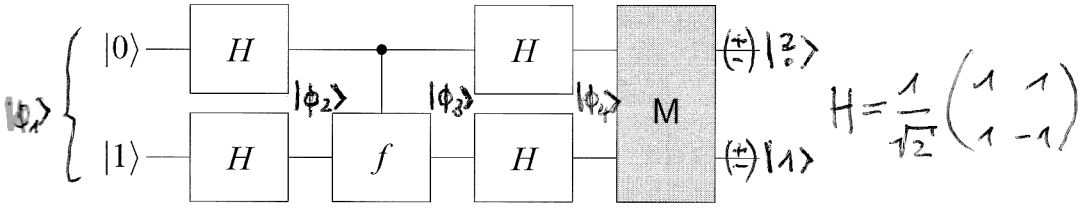

Abbildung 2.14: Schaltkreis für das Problem von Deutsch

(es reicht, $|x\rangle$ zu messen)

Analyse

In Schritt 2 wird unser Zwei-Bit Quantenregister $|x\rangle|y\rangle$ durch die Hadamard-Transformation von dem Zustand $|0\rangle|1\rangle$ in den Zustand Schritt 2

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

überführt. Der erste Faktor entspricht dem Zustand von Bit $|x\rangle$, der zweite dem von Bit $|y\rangle$. Ausmultiplizieren ergibt

$$|\phi_2\rangle = \frac{1}{2}\big(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\big).$$

Nun haben wir eine Superposition über alle Basiszustände unseres Registers, wobei die Vorzeichen eine wichtige Rolle spielen. Schritt 3 wendet U_f an. Der Inhalt des ersten Registers dient als Eingabe der Funktion f, der Funktionswert wird auf das zweite Register addiert. Schritt 3

$$\begin{aligned}
|\phi_2\rangle &= \frac{1}{2}\big(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\big) \\
&\xrightarrow{U_f} \frac{1}{2}\big(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle\big) \\
&= \frac{1}{2}\Big(|0\rangle \cdot \big(|f(0)\rangle - |1 \oplus f(0)\rangle\big) + |1\rangle \cdot \big(|f(1)\rangle - |1 \oplus f(1)\rangle\big)\Big) \\
&= |\phi_3\rangle.
\end{aligned}$$

Wir haben unseren ursprünglichen Plan ausgeführt und eine Superposition über die Funktionswerte erhalten. Würden wir nun messen, bekämen wir mit einer Wahrscheinlichkeit von jeweils $1/4$ einen der Werte $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle$ oder $|1\rangle|1\rangle$ geliefert, was uns keine Informationen für unser Problem liefert. Darum wenden wir die Hadamard-Transformation ein zweites Mal an. Zuvor stellen wir fest, dass für die beiden Bitwerte x gleich $0, 1$

$$|f(x)\rangle - |1 \oplus f(x)\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$$

gilt. Wir können den Registerzustand umformen in

$$\begin{aligned}
|\phi_3\rangle &= \frac{1}{2}\Big((-1)^{f(0)}|0\rangle \cdot \big(|0\rangle - |1\rangle\big) + (-1)^{f(1)}|1\rangle \cdot \big(|0\rangle - |1\rangle\big)\Big) \\
&= \frac{1}{2}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big) \cdot \big(|0\rangle - |1\rangle\big).
\end{aligned}$$

Der Funktionswert ist in das Vorzeichen der Amplitude verlagert worden. Das erste Bit in $|\phi_3\rangle$ befindet sich im Zustand

$$\frac{1}{\sqrt{2}}\big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\big).$$

Schritt 4

Nun betrachten wir den vierten Schritt für beide der möglichen Eigenschaften der Funktion separat.

Fall: konstant

Wir nehmen zunächst an, f sei konstant. In diesem Fall gilt $(-1)^{f(0)} = (-1)^{f(1)}$, und der Zustand von Bit $|x\rangle$ ist entweder $1/\sqrt{2}\cdot(|0\rangle+|1\rangle)$ oder $-1/\sqrt{2}\cdot(|0\rangle+|1\rangle)$. Die Hadamard-Transformation bildet $1/\sqrt{2}\cdot(|0\rangle+|1\rangle)$ auf $|0\rangle$ und $-1/\sqrt{2}\cdot(|0\rangle+|1\rangle)$ auf $-|0\rangle$ ab. Denn unitäre Transformationen sind linear, siehe Abschnitt A.3.

$|y\rangle$ befindet sich vor Schritt 4 im Zustand $1/\sqrt{2}\cdot(|0\rangle-|1\rangle)$ und wird auf $|1\rangle$ abgebildet. Schritt 4 überführt das ganze Register somit in den Zustand

$$|\phi_4^k\rangle = \pm|0\rangle|1\rangle.$$

Dabei bedeutet $a = \pm b$, dass einer der Fälle $a = b$ oder $a = -b$ zutrifft.

Fall: balanciert

Ist f balanciert, ist $|x\rangle$ vor Schritt 4 im Zustand $1/\sqrt{2}\cdot(|0\rangle-|1\rangle)$ oder im Zustand $-1/\sqrt{2}\cdot(|0\rangle-|1\rangle)$. Die Hadamard-Transformation bildet $1/\sqrt{2}\cdot(|0\rangle-|1\rangle)$ auf $|1\rangle$ ab, und analog zum anderen Fall bekommen wir als Folge von Schritt 4

$$|\phi_4^b\rangle = \pm|1\rangle|1\rangle.$$

Schritt 5

Messen liefert also für eine balancierte Funktion $|1\rangle|1\rangle$ und für eine konstante Funktion $|0\rangle|1\rangle$. ◇

Der erste Quantenalgorithmus für dieses Problem wurde 1985 von Deutsch veröffentlicht.

Aufgabe 2.12: Wenden Sie die Hadamard-Transformation auf $-(|0\rangle+|1\rangle)$ an.

Beispielrechnung

Falls noch Unklarheiten bestehen, ist das folgende Beispiel vielleicht hilfreich. Danach sollte man dann die Analyse noch einmal durchgehen. Uns sei die Funktion f mit $f(0) = 1$ und $f(1) = 0$ gegeben, f ist also die Negation. Die Schritte 1 und 2 sind von der Funktion unabhängig, und wir verweisen auf die Analyse. Schritt 3 überführt unser Register aus zwei Bits dann aus dem Zustand

$$|\phi_2\rangle = \frac{1}{2}\big(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\big)$$

in

$$\begin{aligned}|\phi_3\rangle &= \frac{1}{2}\big(|0\rangle|0\oplus f(0)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|0\oplus f(1)\rangle - |1\rangle|1\oplus f(1)\rangle\big)\\ &= \frac{1}{2}\big(|0\rangle|1\rangle - |0\rangle|0\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\big).\end{aligned}$$

Um die Wirkung von H auf das erste Bit zu untersuchen, klammern wir es aus:

$$\begin{aligned}|\phi_3\rangle &= \frac{1}{2}\Big(-|0\rangle\cdot(|0\rangle-|1\rangle)+|1\rangle\cdot(|0\rangle-|1\rangle)\Big)\\ &= \frac{1}{2}(|1\rangle-|0\rangle)\cdot(|0\rangle-|1\rangle).\end{aligned}$$

H bildet $|1\rangle-|0\rangle$ auf $-\sqrt{2}|1\rangle$ ab und $|0\rangle-|1\rangle$ auf $\sqrt{2}|1\rangle$. Schritt 4 erzeugt also den Registerzustand

$$|\phi_4\rangle = \frac{1}{2}(-\sqrt{2}|1\rangle\cdot\sqrt{2}|1\rangle) = -|1\rangle|1\rangle.$$

Messen liefert $|1\rangle|1\rangle$ mit Wahrscheinlichkeit $(-1)^2 = 1$. Der Algorithmus gibt *balanciert* aus.

Aufgabe 2.13: Rechnen Sie den Algorithmus für die 1-Funktion mit $f(0) = f(1) = 1$ durch. Betrachten Sie alle fünf Schritte.

Interferenz

Die meisten Quantenalgorithmen nutzen ein Phänomen namens *Interferenz*: Amplituden können sich zu einem größeren Wert addieren, das nennt man konstruktive Interferenz, aber auch gegenseitig auslöschen; man spricht von destruktiver Interferenz. Wir untersuchen dahingehend unseren Algorithmus für das Problem von Deutsch. In der Analyse ist erwähnt, dass wir aus einer Messung nach Schritt 3 nicht erfahren, ob die Funktion f konstant oder balanciert ist. Wie gelingt es nun, mit der zweiten Hadamardtransformation diese Information aus der Superposition $|\phi_3\rangle$ zu extrahieren? Dazu betrachten wir die Wirkung auf das erste Bit im Fall, dass f konstant ist:

$$\pm\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \xrightarrow{H} \pm\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)).$$

Im Resultat dieser Transformation addieren sich für $|0\rangle$ und $|1\rangle$ je zwei Amplituden. Die von $|0\rangle$ ist $1/2+1/2=1$, die von $|1\rangle$ ist $1/2-1/2=0$. Ist f hingegen balanciert, lässt die Anwendung von H die Amplitude von $|0\rangle$ durch destruktive Interferenz verschwinden und vergrößert die von $|1\rangle$. Wir kommen in den Abschnitten 4.4 und 9.3 darauf zurück.

Die Analyse des Algorithmus hat gezeigt, dass er das gestellte Problem löst. Vielleicht ist beim Leser noch kein intuitives Verständnis seines Vorgehens entstanden. Darum werden wir noch einmal auf das Problem von Deutsch zurückkommen, und zwar in Abschnitt 2.9.

2.7 Die Rolle des Tensorprodukts

Im vorletzten Abschnitt haben wir mehrere Bits zusammengesteckt und sind so zum Register gelangt. Nun tun wir das gleiche mit den Rechenschritten.