Aufgabe 2 Algorithmus von Bernstein-Vazirani

Der Algorithmus folgt demselben Ablauf wie der Algorithmus von Deutsch-Jozsa. Wir setzen mit der Analyse in Schritt 4 an (und ignorieren zur einfacheren Darstellung das Antwortqubit $|-\rangle$), also ist der Zustand der übrigen n Qubits

$$\sum_{z\in\{0,1\}^n}\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)\oplus x\cdot z}\right)|z\rangle$$

Die Funktion f ist von der speziellen Form $f(x)=s\cdot x$ für unbekanntes $s\in\{0,1\}^n$, also

$$(-1)^{f(x)\oplus x\cdot z}=(-1)^{s\cdot x\oplus x\cdot z}=(-1)^{(s\oplus z)\cdot x}$$

und es folgt

$$\sum_{z\in\{0,1\}^n}\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{(s\oplus z)\cdot x}\right)|z\rangle$$

In Schritt 5 wird gemessen und wir untersuchen die spezielle Amplitude von $|z\rangle=|s\rangle$:

Für $z=s$ ist $s\oplus z=0$ und die Amplitude von $|s\rangle$ ist

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

Damit ist die Amplitude aller anderen Zustände $|z\rangle\neq|s\rangle$ gleich 0 und die Messung ergibt mit Sicherheit $|s\rangle$. Dafür wurde genau eine Anfrage an das Quantenorakel benötigt.

Aufgabe 4

Für $f(x) = s\cdot x \oplus b$ für $b \in \{0,1\}^n$ beobachten wir in Schritt 4 (vor der Messung, wobei wir wieder das Antwortqubit $|-\rangle$ ignorieren) den Zustand

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

$$= \sum_{z\in\{0,1\}^n} \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{s\cdot x \oplus b} (-1)^{x\cdot z} \right) |z\rangle$$

$$= (-1)^b \sum_{z\in\{0,1\}^n} \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{(s\oplus z)\cdot x} \right) |z\rangle$$

Der Summand b in der Funktion f hat also keine Auswirkung bei der Analyse der Amplitude von $|s\rangle$ (vgl. Aufgabe 2) und "verschwindet" bei Messung wegen $|(-1)^b|^2 = 1$