

Einführung in Quantenalgorithmen

Inhalt:

1. Einleitung
2. Einteilung der Quantenalgorithmen
3. Vorteile von Quantenalgorithmen
4. Funktionsweise bzw. Aufbau von Quantenalgorithmen
5. Erste Beispiele:
 - a. *Deutsch's* Algorithmus
 - b. *Deutsch – Jozsa –* Algorithmus
6. Zusammenfassung

1. Einleitung:

Die Entwicklung schreitet voran, auch die Zeit der Binärdaten ist gezählt. Seitdem nun die Möglichkeit besteht, Quantenbits als Informationsspeicher zu verwenden, ist auch die Notwendigkeit von neuen Algorithmen vorhanden, mit denen man diese Daten lesen und nach seinen Vorstellungen verändern kann.

Diese neuen Algorithmen werden Quantenalgorithmen genannt. Sie sollen die besonderen Eigenschaften der Quantenbits nutzen, um so den klassischen Algorithmen im zeitlichen Ablauf überlegen zu sein.

2. Einteilung von Quantenalgorithmen

Bekannte Quantenalgorithmen können in 3 Gruppen eingeteilt werden, abhängig davon, welche Methoden sie benutzen.

Die erste Gruppe sind Algorithmen, die darauf basieren eine globale Eigenschaft aller Funktionswerte einer Funktion zu bestimmen. Zu ihnen gehören, der *Deutsch*-Algorithmus sowie der Algorithmus von *Shor*.

Zur zweiten Gruppe werden gezählt, Algorithmen die durch Transformation des Status der Quantenbits, die Wahrscheinlichkeit erhöhen, das gewollte Ergebnis gemessen werden kann. Der Suchalgorithmus von *Grover* arbeitet nach dieser Methode.

Die dritte Gruppe sind Algorithmen, die Methoden aus den ersten beiden Gruppen kombinieren, zum Beispiel „approximate counting algorithm“ von Brassard, Hoyer und Tapp.

Weiterhin ist noch nicht bekannt, ob es weitere Typen von Algorithmen gibt, die nicht in diese Gruppen eingeteilt werden können.

3. Vorteile der Quantenalgorithmen

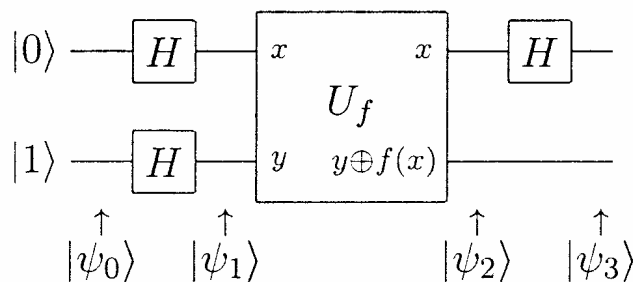
Quantenalgorithmen nutzen die Eigenschaften der Superposition und der Möglichkeit der Überlagerung von Quantenbits aus. Daraus resultiert eine sehr starke Parallelität, durch die in einem Schritt, zum Beispiel eine globale Eigenschaft einer Funktion bestimmt werden kann – die Quantenparallelität.

4. Funktionsweise bzw. Aufbau von Quantenalgorithmen

Quantenalgorithmen bestehen aus einer Kombination von:

- einem speziellen Quantenschaltkreis und
- einer genauen Auswahl der zu messenden Quantenbits.

Ein möglicher Quantenschaltkreis sieht zum Beispiel so aus:



Hier erkennt man die Hauptbestandteile eines Quantenschaltkreises:

- $|0\rangle, |1\rangle$ - Eingangszustände
- H - Hadamard-Gate
- U_f - Der „Kasten“ steht für eine Sequenz von Quantengattern, die eine Funktion f berechnet, genauer gesagt, die die eingeblendete Eingangszustände x, y umwandelt in die Form $x, y \oplus f(x)$ mit \oplus als Addition modulo 2. U_f ist eine unitäre Matrix, die die Transformation der Zustände vornimmt.

5a. Deutsch' Algorithmus

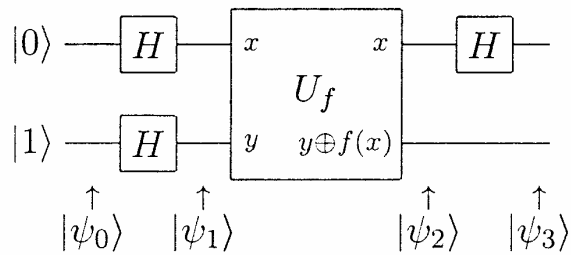
Deutsch' Problem – Wie viele Versuche benötigt man, um zu entscheiden, ob eine Münze entweder echt (Kopf und Zahl) oder unecht (auf beiden Seiten das gleiche Symbol) ist ?

Sei $f: \{0,1\} \rightarrow \{0,1\}$

Über die Funktion f ist nur bekannt, dass sie entweder konstant ($f(0) = f(1)$) oder ausgeglichen ($f(0) = f(1) \oplus 1$) ist. (\oplus ist Addition modulo 2)

Um das obige Problem zu lösen, ist nun herauszufinden, welche Eigenschaft die Funktion besitzt!

Folgender Quantenschaltkreis wird erstellt, um das Problem zu lösen:



Ablauf:

1. Initialisierung der Startzustände

$$|\psi_0\rangle = |01\rangle = |0\rangle \otimes |1\rangle \quad , \text{ wobei } \otimes \text{ tensor-Produkt ist}$$

2. Der Anfangstatus wird durch eine $H^{\otimes 2}$ Hadamard-Transformation gesendet.

$$\begin{aligned} |\psi_1\rangle &= [(|0\rangle + |1\rangle) / \sqrt{2}] \otimes [(|0\rangle - |1\rangle) / \sqrt{2}] \\ &= |x\rangle \otimes [(|0\rangle - |1\rangle) / \sqrt{2}] \end{aligned}$$

3. Zwischenüberlegung:

f kann nur die Funktionswerte 0 oder 1 haben, deshalb führt die Anwendung von U_f zu folgenden Fällen:

$$\begin{aligned} |\psi_2\rangle &= \begin{aligned} &|x\rangle \otimes [(|0\rangle - |1\rangle) / \sqrt{2}] && \text{für } f(x) = f(0) \\ &|x\rangle \otimes [(|1\rangle - |0\rangle) / \sqrt{2}] && \text{für } f(x) = f(1) \end{aligned} \\ &= (-1)^{f(x)} |x\rangle \otimes [(|0\rangle - |1\rangle) / \sqrt{2}] \\ &= \begin{aligned} &+- [(|0\rangle + |1\rangle) / \sqrt{2}] \otimes [(|0\rangle - |1\rangle) / \sqrt{2}] && \text{für } f(0) = f(1) \\ &+- [(|0\rangle - |1\rangle) / \sqrt{2}] \otimes [(|0\rangle - |1\rangle) / \sqrt{2}] && \text{für } f(0) \neq f(1) \end{aligned} \end{aligned}$$

4. Das letzte Hadamard angewandt auf das 1. Qubit liefert nun:

$$\begin{aligned} |\psi_3\rangle &= \begin{aligned} &+- |0\rangle \otimes [(|0\rangle - |1\rangle) / \sqrt{2}] && \text{für } f(0) = f(1) \\ &+- |1\rangle \otimes [(|0\rangle - |1\rangle) / \sqrt{2}] && \text{für } f(0) \neq f(1) \end{aligned} \end{aligned}$$

- a. Bedenkt man das $f(0) + f(1)$ gleich 0 ist für $f(0) = f(1)$ und sonst 1 kann man $|\psi_3\rangle$ auch so darstellen:

$$|\psi_3\rangle = +- |f(0) + f(1)\rangle \otimes [(|0\rangle - |1\rangle) / \sqrt{2}]$$

Ergebnis: Das heisst, mit Messung des 1. Qubits, kann man $f(0) + f(1)$ erkennen. Mit einer **1** Ausführung von U_f haben wir die Möglichkeit eine globale Eigenschaft der Funktion U_f zu bestimmen.

Und dies ist schneller als mit einer klassischen Methode.

5b. Deutsch-Josza Algorithmus

Def.: Sei $f: \{0,1\}^n \rightarrow \{0,1\}$

f ist ausgeglichen, wenn für alle verschiedenen Funktionswerte von f gilt, das ihre Mächtigkeit gleich ist.

f ist konstant, wenn alle Funktionswerte gleich sind.

Problem:

Sei $f: \{0,1\}^n \rightarrow \{0,1\}$ eine „black box“

Aufgabe: Entscheide, welche der oben genannten Eigenschaften f besitzt!

Aufwandsabschätzung für klassische Algorithmen:

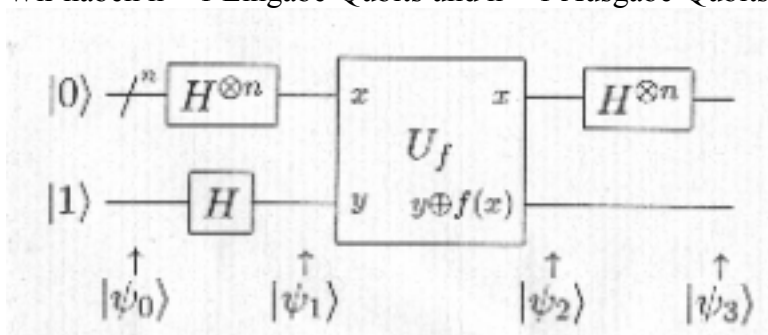
Alle $2^n - 1$ Möglichkeiten müssten durchlaufen werden, um zu entscheiden, ob die Funktion konstant ist.

→ exponentielle Laufzeit

Aber mit Quantencomputern ist es möglich das Deutsch-Problem zu lösen mit nur einer Anwendung von U_f .

Aufbau:

Wir haben $n + 1$ Eingabe-Qubits und $n + 1$ Ausgabe-Qubits



Ablauf:

1. $|\varphi_0\rangle = |0\rangle \otimes^n |1\rangle$

- Die n Eingabe-Qubits werden durch eine $H^{\otimes n}$ (Hadamard-Transformation) gesendet.
- Das $n+1$. Eingabe-Qubit wird ebenfalls durch ein Hadamard-Gatter geschickt.

2. $|\varphi_1\rangle = [\sum_x (|x\rangle / \sqrt{2^n})] \otimes [(|0\rangle - |1\rangle) / \sqrt{2}]$

→ die ersten n -Qubits sind nun in einer Superposition über alle 2^n Zustände, das $n+1$. Qubit in einer Superposition zw. 0 und 1.

- U_f angewendet auf den Zustand $|\varphi_1\rangle$

3. $|\varphi_2\rangle = [\sum_x ((-1)^{f(x)} |x\rangle) / \sqrt{2^n}] \otimes [(|0\rangle - |1\rangle) / \sqrt{2}]$

→ in diesem Status sind nun alle Funktionswerte von f , enthalten.

Interessant ist, dass diese in den ersten n Qubits stecken, obwohl ein Blick auf U_f vermuten lässt, dass das $n+1$. Qubit die Verknüpfung der Funktionswerte enthält.

- Durch eine weitere Hadamard-Transformation auf die Superposition der ersten n Qubits werden die Zustände nun überlagert.

4. Zwischenüberlegung:

Hadamard-Transformation für einen Status $|x\rangle$ führt zu:

$$H |x\rangle = \sum_z (-1)^{xz} |z\rangle / \sqrt{2} \quad , \text{ wobei } xz \text{ das bitweise innere Produkt von } x \text{ und } z \text{ modulo 2 ist}$$

Daraus folgt:

$$H^{*n} |x_1, \dots, x_n\rangle = \sum_{z_1, \dots, z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1, \dots, z_n\rangle / \sqrt{2^n}$$

Das Ergebnis der Hadarmard-Transformation auf den Status $|\varphi_2\rangle$ ist:

$$|\varphi_3\rangle = \sum_z \sum_x ((-1)^{xz + f(x)} |z\rangle / 2^n) * [(|0\rangle - |1\rangle) / \sqrt{2}]$$

Auswertung:

1. Fall: f konstant

die Amplitude für $|0\rangle^{*n}$ ist entweder 1 oder -1 je nachdem, welchen Funktionswert, die Funktion besitzt.

Weil der Zustand $|\varphi_3\rangle$ Einheitslänge besitzt, müssen alle anderen Amplituden 0 sein. Ein Messen der ersten n Eingangs-Qubits ergibt für alle 0.

2. Fall: f ausgeglichen

die positiven und negativen Einflüsse heben sich auf sich und die Amplitude für $|0\rangle^{*n}$ bleibt 0.

Das Messen der ersten n Eingangs-Qubits ergibt bei mindestens einem einen Wert ungleich 0.

Das heißt, werden nur 0en gemessen, ist die Funktion konstant, sonst ist sie ausgeglichen.

Folgerung: Mit nur einem Funktionsaufruf konnte entschieden werden, ob f konstant oder ausgeglichen ist, statt im klassischen Fall: mind. $2^n/2 + 1!$

6. Zusammenfassung

Es ist also mit Hilfe der Quantenalgorithmien möglich, klassische Algorithmen in ihre Schranken zu weisen und zeigt, damit dass die bisher gesetzten Grenzen überschritten werden können.