Grovers Suchalgorithmus

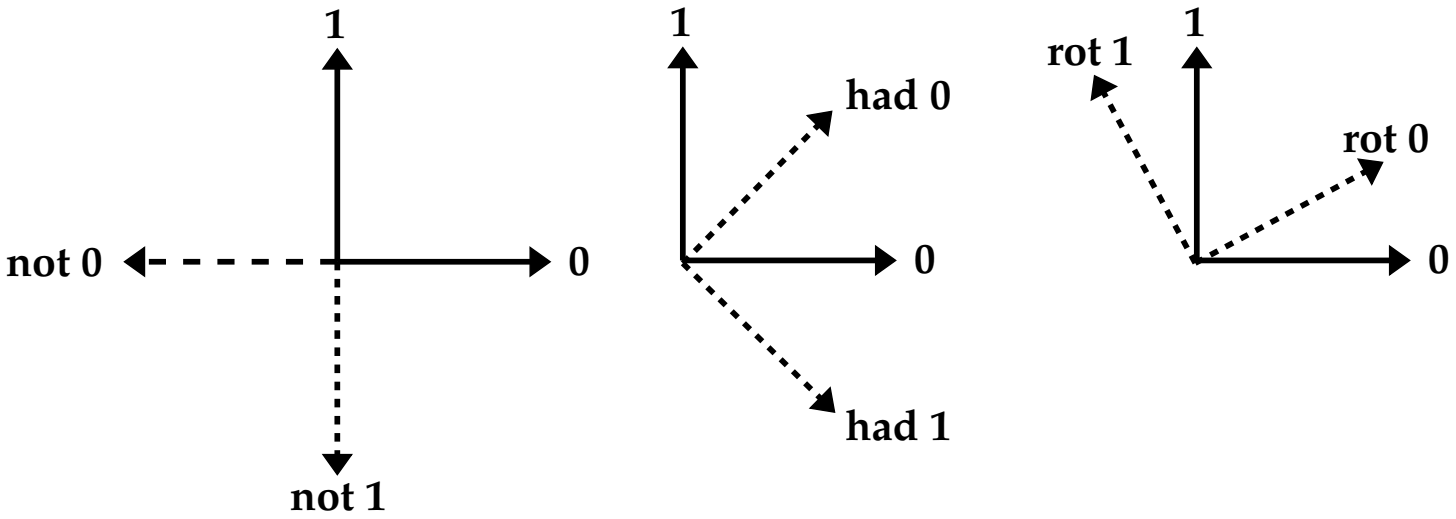
Martin Horsch

4. Dezember 2003

1-Qubit-Gates

Die grundlegenden 1-Qubit-Operationen sind die Negation $\mathfrak{not}$, die Hadamard-Transformation $\mathfrak{had}$ und die Rotation $\mathfrak{rot}_\vartheta$. Sie lassen sich als unitäre Matrizen darstellen:

$$\mathfrak{not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathfrak{had}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \mathfrak{rot}_\vartheta = \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$$



2-Qubit-Gates

Wichtige Gates mit zwei Qubits sind die kontrollierte Negation $\mathfrak{notc}$ und die kontrollierte Hadamard-Transformation $\mathfrak{hadc}$:

$$\mathfrak{notc} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \mathfrak{hadc} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 0 & 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

Die kontrollierte Negation genügt, um gemeinsam mit 1-Qubit-Gates alle in Quantenalgorithmen typischen Operationen durchzuführen. Alle Matrizen sind unitär, die Berechnungen sind also reversibel.

Der einzige irreversible Rechenschritt ist die **Messung** eines Qubits.

Grovers Suchalgorithmus

Finde die Nadel im Heuhaufen!
Suche in einer ungeordneten Menge von 2^n Elementen das passende. Dazu ist die Orakelfunktion f gegeben, die in konstanter Zeit beantwortet, ob ein Element das richtige ist.

gegeben: $f : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} : f(s) \mapsto 1 \iff s = \sigma$

gesucht: $\sigma \in \mathbb{Z}/2^n\mathbb{Z}$

Normalerweise erwartet man 2^{n-1} Aufrufe der Funktion f.
Auf Quantenrechnern ist das gleiche mit $O(\sqrt{2^n})$ Aufrufen bei einer erwarteten Rechenzeit von $O(n\sqrt{2^n})$ möglich.

Diffusionsoperator

Ein Bestandteil des Algorithmus ist der Diffusionsoperator $\mathcal{D}$:

$$\mathcal{D} \quad = \quad 2^{1-n} \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} - E_{2n} \quad = \quad \mathfrak{had}_n \begin{pmatrix} \mathbf{1} & 0 & 0 & \cdots & 0 \\ 0 & \mathbf{-1} & 0 & \cdots & 0 \\ 0 & 0 & \mathbf{-1} & & 0 \\ \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \mathbf{-1} \end{pmatrix} \mathfrak{had}_n$$

Dabei ist $\mathfrak{had}_n$ die Hadamard-Transformation für n Qubit.
Die Multiplikation mit $\mathcal{D}$ kann als Verkettung von $3n$ unitären Transformationen implementiert werden.

Die Auswirkung des Diffusionsoperators ist die Spiegelung der Amplituden um ihren Mittelwert.

Verwendet werden die Register $r1$ mit n Qubit und $r2$ mit 1 Qubit.

Schritt 1. Initialisiere die Register auf $|r_1\rangle\,|r_2\rangle \leftarrow |0\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Schritt 2. Wende $\mathfrak{had}$ auf jedes qubit in r_1 an und erzeuge damit eine gleichverteilte Superposition aller Zahlen $0 \le k < 2^n$.

$$|r_1\rangle \leftarrow \sum_{0\le k<2^n} \frac{|k\rangle}{\sqrt{2^n}}$$

Schritt 3. Wiederhole folgende Zuweisungen $\lfloor \frac{\pi}{4}\sqrt{2^n} \rfloor$ mal:

$$|r_1\rangle\,|r_2\rangle \leftarrow \sum_{0\le k<2^n} \frac{|k\rangle}{\sqrt{2^n}}(-1)^{f(k)}\,|r_2\rangle \quad \text{und} \quad |r_1\rangle \leftarrow \mathcal{D}\,|r_1\rangle$$

Schritt 4. Messe das Register r_1 und bestimme seinen Zustand s.

Schritt 5. Falls $f(s) = 1$, gib $\sigma = s$ aus, sonst goto Schritt 1.

Was geschieht im Schritt 3?

$$|r_1\rangle\,|r_2\rangle \leftarrow \sum_{0\le k<2^n} \frac{|k\rangle}{\sqrt{2^n}}(-1)^{f(k)}\,|r_2\rangle$$

Diese Zuweisung kann als kontrollierte Negation des zweiten Registers durchgeführt werden. Sie entspricht aber auch der Multiplikation des ersten Registers mit einer $2n \times 2n$-Matrix:

$$|r_1\rangle \leftarrow I_\sigma\,|r_1\rangle = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & -1 & & \vdots \\ \vdots & \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \sum_{0\le k<2^n} \frac{(-1)^{f(k)}}{\sqrt{2^n}}\,|k\rangle$$

Die Matrix I_σ hat genau den Effekt, die Amplitude des gesuchten σ umzukehren.

Der gesamte Schritt 3 entspricht also der Multiplikation mit dem Produkt von I_σ und der Diffusionsmatrix $\mathcal{D}$.

$$|r_1\rangle \leftarrow \mathcal{D}I_\sigma|r_1\rangle = (2^{1-n}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} - E_{2n}) \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & -1 & & \vdots \\ \vdots & \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} |r_1\rangle$$

Der Diffusionsoperator behandelt alle Amplituden gleich, indem er sie um den Mittelwert aller Amplituden spiegelt. I_σ bewirkt nur die Umkehrung der Amplitude von σ.

Das Produkt $\mathcal{D}I_\sigma$ hat also auf alle $k \neq \sigma$ einen bestimmten Effekt und auf σ einen anderen.

Da alle Amplituden auf den gleichen Wert initialisiert werden, brauchen wir nur zwei Werte zu verfolgen. Den Koeffizienten a von σ und die Amplitude f aller anderen Basisvektoren.

$$\begin{pmatrix} f \\ a \end{pmatrix} \longrightarrow_{I_\sigma} \begin{pmatrix} f \\ -a \end{pmatrix} \longrightarrow_{D} \begin{pmatrix} 2^{1-n}((2^n-1)f-a) \\ 2^{1-n}((2^n-1)f-a) \end{pmatrix}$$

Man kann den Schritt 3 als Multiplikation des Wahrscheinlichkeitsvektors mit einer Rotationsmatrix schreiben:

$$\begin{pmatrix} f \\ a \end{pmatrix} \longrightarrow_{DI_\sigma} \begin{pmatrix} 1-2^{1-n} & -2^{1-n} \\ 2-2^{1-n} & 1-2^{1-n} \end{pmatrix} \begin{pmatrix} f \\ a \end{pmatrix} = \mathfrak{rot}_{\arccos(1-2^{1-n})} \begin{pmatrix} f \\ a \end{pmatrix}$$

Diese Rotation muss nur oft genug wiederholt werden, um mit hoher Wahrscheinlichkeit σ zu messen.

Wie oft muss Schritt 3 iteriert werden?

Der Zustand zu Beginn ist:

$$\begin{pmatrix} f \\ a \end{pmatrix} = \begin{pmatrix} \sqrt{1 - 1/N} \\ \sqrt{1/N} \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix}$$

Da dieser Wahrscheinlichkeitsvektor bei jeder Iteration um den Winkel θ gedreht wird, sollte m so gewählt werden, dass möglichst gilt:

$$\mathfrak{rot}_{\theta}^{m} \begin{pmatrix} f \\ a \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{bzw.} \quad m = \frac{\pi}{2\theta} - \frac{1}{2}$$

Für große n ist $\theta \approx 2^{1-n/2}$.
Das beste ganzzahlige m ist dann $m = \lfloor \frac{\pi}{4}\sqrt{2^n} \rfloor$.

Laufzeit

Mit Grovers Algorithmus kann die Nadel in einem Heuhaufen von $N = 2^n$ Elementen nach $\mathbf{O}(\sqrt{N} \cdot \log N)$ unitären Transformationen gefunden werden. Entscheidend für die Laufzeit ist Schritt 3, die anderen brauchen nur jeweils $O(\log N)$.

In jeder Iteration des Algorithmus wird Schritt 3 genau $\lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ mal ausgeführt. Jeder dieser Aufrufe braucht $O(\log N)$ unitäre Transformationen, da eine Multiplikation mit der $N \times N$-Diffusionsmatrix durchgeführt werden muss und ein Quantenrechner nur Gates für ein oder zwei Qubits kennt.

Jeder Durchlauf ist mit einer Wahrscheinlichkeit von mindestens $1 - \frac{1}{n}$ erfolgreich. Der Erwartungswert für die Anzahl der Iterationen ist damit höchstens $\sum_{k \in \mathbb{N}} \frac{1}{N^k} = \frac{1}{1 - 1/N} \in O(1)$ und fällt nicht ins Gewicht.