9 - Algorytm Groovera

Saturday, 22 June 2024 19:16

Model Obliczeń

Qbit: $\begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \alpha|1\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C}$

$\alpha^2 + \beta^2 = 1$ - prawdopodobieństwa na 0 lub 1.

Dla układu N q-bitów rozpatrujemy prawdopodobieństwo na konkretną maskę

Bramka Hadamarda

$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

$H\left(\begin{bmatrix}\alpha \\ \beta\end{bmatrix}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix}\alpha+\beta \\ \alpha-\beta\end{bmatrix}$

$H = \begin{bmatrix}1 & 1 \\ 1 & -1\end{bmatrix}$

Będziemy budować obwód z bramek (przekształceń liniowych)

Załóżmy, że mamy bramkę dla funkcji której własności chcemy poznać.

Algorytm Groovera

Mamy N pudełek. Chcemy znaleźć (jedyne) wyróżnione z $p > \frac{2}{3}$

$f: N \to \{0,1\}$ dla dokładnie jednego x^*: $f(x^*) = 1$

Niech $N = 2^n$. Wejście do funkcji to n-elementowe ciągi 0 i 1.

Możemy stworzyć następującą bramkę O_f:

$f(|\bar{x}\rangle) = |x\rangle$

$f(|\bar{x}^*\rangle) = -|\bar{x}^*\rangle$

Do naszego obwodu wpuszczamy Q-bity $|\bar{0}\rangle$.

Przepuszczamy przez bramkę H.

Każda kombinacja tak samo prawdopodobna.

Chcemy aby po każdej iteracji $|\bar{x}^*\rangle$ się (istotnie) zwiększyło.

$\delta_{\bar{x}}$ - współczynnik dla układu $\bar{x}$.

Będziemy utrzymywać $\delta_{\bar{x}} \in \mathbb{R}$. $\delta'_{\bar{x}^*} > \delta_{\bar{x}^*} + \frac{1}{\alpha\sqrt{N}}$

Wtedy po $O(\sqrt{N})$ iteracjach z istotną szansą zmierzymy x^*.

Wykorzystamy do tego dwie bramki: O_f i D:

$D: (\delta_0, \dots, \delta_{N-1}) \to (2\mathfrak{s} - \delta_0, \dots, 2\mathfrak{s} - \delta_{N-1})$

gdzie $\mathfrak{s} = \frac{1}{N}(\delta_0 + \dots + \delta_{N-1})$

$\bar{x} \neq \bar{x}^*$ po każdej operacji równe, a $\bar{x}^*$ rośnie

$D = \frac{2}{N}\begin{bmatrix}1 & 1 & \cdots & 1 \\ 1 & \ddots & & \vdots \\ \vdots & & & \vdots \\ 1 & \cdots & & 1\end{bmatrix} - \underline{I} = 2vv^T - \underline{I} \quad v = \frac{1}{\sqrt{N}}\begin{bmatrix}1 \\ 1 \\ \vdots \\ 1\end{bmatrix}$

$D \stackrel{\sim}{=} H_n \cdot Z_0 \cdot H_n$ gdzie H_n to macierz H dla każdego q-bitu.

$Z_0 = \begin{bmatrix}-1 & & 0 \\ & 1 & \\ 0 & & \ddots \\ & & & 1\end{bmatrix}$ - „prawie" NOR

$H_n = \frac{1}{\sqrt{2}}\begin{bmatrix}H_n & H_n \\ H_n & -H_n\end{bmatrix}, \quad H_0 = [1]$