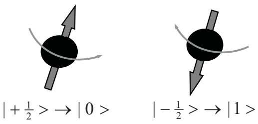
ERATO セミナ 2010 - No. 08

Introduction to Grover Algorithm

山下茂
立命館大学 情報理工学部 情報システム学科

2010/8/3

量子状態



- スピン1/2粒子系など 2状態系で実現する

・光の偏光 （０° と ９０° ）
・電子のスピンの向き （↑ と↓）
・量子ドットのエネルギー準位（基底と励起）
・etc.

量子状態 $1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$ 　公理１

↓

重ね合わせ状態 　公理2

もし、観測すると、0と1が1/2の確率で得られる。

0　0

量子計算のモデル

量子ビット　$\alpha|0\rangle + \beta|1\rangle$　（α, β: 確率振幅）

"区別"可能な2つの状態の任意の量ね合わせ

確率$|\alpha|^2$で$|0\rangle$， 確率$|\beta|^2$で $|1\rangle$

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

量子ゲート　*ユニタリ変換*

量子ビットへの"ある種の"操作

1

Hadmard変換

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \quad H = 1/\sqrt{2}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$$

とすると

$$H\begin{pmatrix}1\\0\end{pmatrix} = 1/\sqrt{2}\begin{pmatrix}1\\0\end{pmatrix} + 1/\sqrt{2}\begin{pmatrix}0\\1\end{pmatrix}$$

つまり、

$|0\rangle$ —$\boxed{H}$— $\boxed{1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle)}$

$|0\rangle$と$|1\rangle$が，1/2の確率で重ね合わされた状態

2

量子量ね合わせ Walsh-Hadamard変換

$|0\rangle$ —$\boxed{H}$— $1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$
$|0\rangle$ —$\boxed{H}$— $1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$
$|0\rangle$ —$\boxed{H}$— $1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$
⋮
$|0\rangle$ —$\boxed{H}$— $1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$

nビット

全体で見ると…

$|0\rangle|0\rangle|0\rangle\ldots|0\rangle$ から$|1\rangle|1\rangle|1\rangle\ldots|1\rangle$までの 2^n個の状態の量ね合わせ

3

nビットの量子状態の表現方法

$|0\rangle|0\rangle|0\rangle\ldots|0\rangle$　　$|0\rangle$

⇔　　$|\,i\,\rangle$

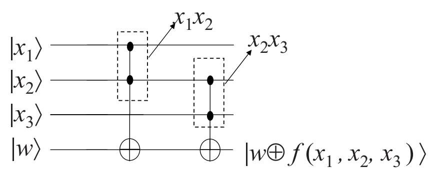
$|1\rangle|1\rangle|1\rangle\ldots|1\rangle$　　$|2^n\rangle$

$1/\sqrt{2^n}\,(\,\Sigma|i\rangle\,)$　（i= 000…0 ~ 111…1 ）

2^n列ベクトル， 2^n 行2^n列の遷移行列

4

ブール関数を計算する量子回路



$f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3$

•入力は重ね合わせ O.K.
$|w\rangle = |0\rangle$ → 量子並列で $f(x_1, x_2, x_3)$ を計算

$|w\rangle = 1/\sqrt{2}\,(|0\rangle - |1\rangle)$ → $1/\sqrt{2}\,(|1\rangle - |0\rangle)$ ($f(x_1, x_2, x_3)$=1の時)
→$f(x_1, x_2, x_3)$=1となる状態の確率振幅のみ正負反転

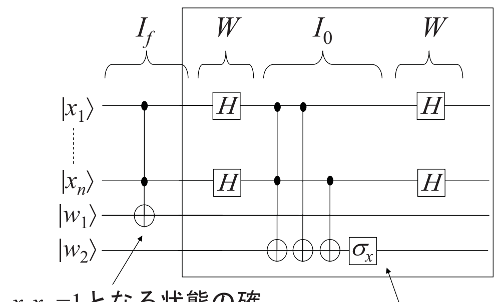
5

Groverのアルゴリズム

- n変数ブール関数
$f(x) = (x_1 + x'_2 + x_3)\,(x'_4 + x_5 + x_6)\,\dots\,(x_n + x'_{n-2} + x_1)$
が，１となる割り当てを見つける
- 2^n個の中から答えを一つ見つける
- “古典”では，$O(2^n)$ の計算コスト
- Groverでは，$\Theta(2^{n/2})$ の計算コスト

6

Grover　Iterationの量子回路



$x_1 x_n$=1となる状態の確率振幅のみ正負反転
$|1\rangle\dots|1\rangle$

“平均値に関しての折り返し“

7

行列 I_f

$$\begin{pmatrix} a_{0\cdots 0} \\ \vdots \\ a_i \\ \vdots \\ a_{1\cdots 1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & -1 & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} b_{0\cdots 0} \\ \vdots \\ b_i \\ \vdots \\ b_{1\cdots 1} \end{pmatrix}$$

$|i\rangle$ の振幅のみの正負を反転
$(f(i)=1)$

8

行列 W

$$W = \otimes H = \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

⇩

$$\begin{pmatrix} a_{0\cdots 0} \\ \vdots \\ a_i \\ \vdots \\ a_{1\cdots 1} \end{pmatrix} = \frac{1}{\sqrt{2^n}} \begin{pmatrix} 1 & 1 & \cdots & & 1 \\ 1 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & (-1)^{i \cdot j} & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 1 & \cdots & \cdots & & \ddots \end{pmatrix} \begin{pmatrix} b_{0\cdots 0} \\ \vdots \\ b_i \\ \vdots \\ b_{1\cdots 1} \end{pmatrix}$$

9

拡散行列

$$D = W I_0 W$$

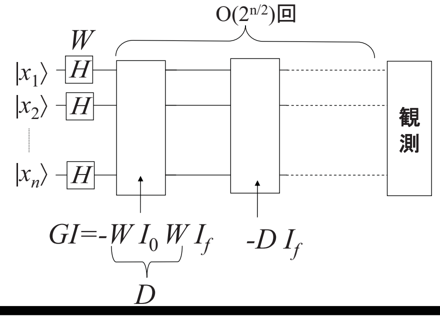
$$\begin{pmatrix} -1 + \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1 + \frac{2}{2^n} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \frac{2}{2^n} \\ \frac{2}{2^n} & \cdots & \frac{2}{2^n} & -1 + \frac{2}{2^n} \end{pmatrix} \begin{pmatrix} \alpha_{0\cdots 0} \\ \\ \alpha_i \\ \\ \alpha_{1\cdots 0} \\ \alpha_{1\cdots 1} \end{pmatrix}$$

$\alpha_i \rightarrow 2\frac{\Sigma \alpha_i}{2^n} - \alpha_i$　（α_i を平均に関して折り返す）

10

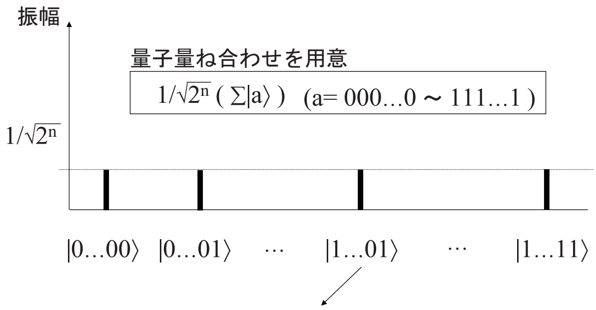
Groverのアルゴリズム

n変数ブール関数fの2^n個の変数割り当ての中から関数fを１とする割り当てを探す



11

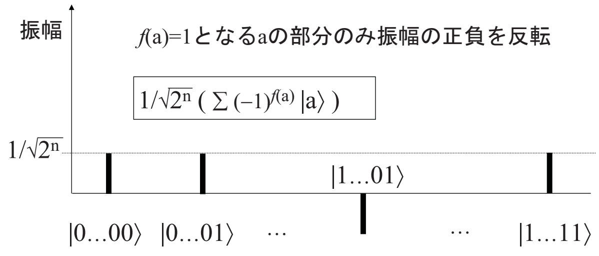
Groverのアルゴリズムのイメージ



Walsh-Hadamard変換により可能

12

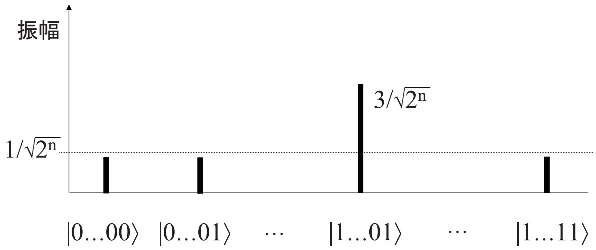
Groverのアルゴリズムのイメージ



I_fの量子回路により可能

13

Groverのアルゴリズムのイメージ



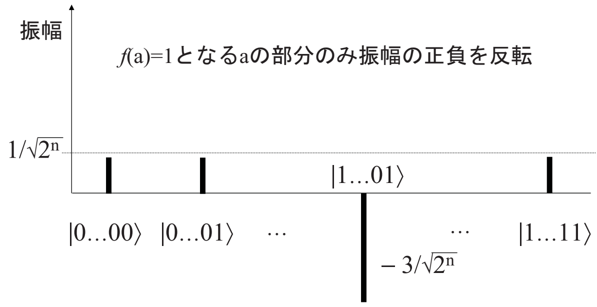
(ステップ3)
振幅全体の平均に関して各振幅の正負を反転

$\boxed{1/\sqrt{2^n}\ (\sum |a\rangle) + 2/\sqrt{2^n}\ |c\rangle}$　　$(f(c) = 1)$

拡散行列により可能

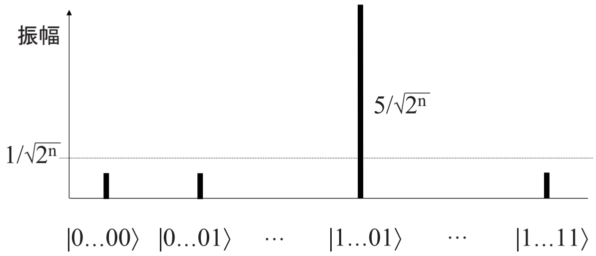
14

Groverのアルゴリズムのイメージ



15

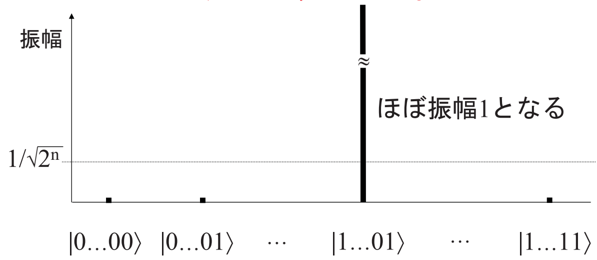
Groverのアルゴリズムのイメージ



振幅全体の平均に関して各振幅の正負を反転

16

Groverのアルゴリズムのイメージ



$O(2^{n/2})$繰り返したあと，量子ビットを観測すると
ほぼ確率1で，$|1\ldots01\rangle$ が観測される

$f(x) = 1$の解

17