ドイチュのアルゴリズム

中央大学　香取研所属
浜本創太

量子ビット

- 量子コンピュータは2つの直交する状態を利用して量子ビットを作り量子ゲートで演算を行います。量子ビットの例としてはスピンのアップダウンを使うなどの例が考えられます。

量子ビット（1ビット）

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

量子ビット（2ビット）

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

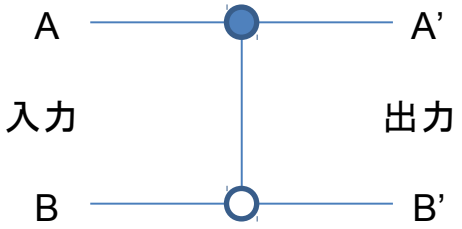
- また量子ビットは重ね合わせが可能です。

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$$

量子ゲート

- 量子ゲートは入力した量子ビットに対し出力を返します。量子ゲートは行列を使い表現されます。また量子ゲートは可逆です。

例）制御NOTゲート；U



A	B	A’	B’
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$$U|00\rangle = |00\rangle$$
$$U|01\rangle = |01\rangle$$
$$U|10\rangle = |11\rangle$$
$$U|11\rangle = |10\rangle$$

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

アダマールゲート

- 1ビットの量子ゲートに対するアダマールゲートは行列で表現すると

$$H = 1/\sqrt{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

であり、量子ビットの入力に対し以下のような出力を返します。

$$H|0\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle) \qquad H|1\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$$

アダマールゲートを実際に作る場合スピンを利用する例が考えられます。

ドイチュのアルゴリズムとは

- ドイチュ―ジョサのアルゴリズムはある関数f(z)が与えられたときその関数がどのような関数であるか判別するアルゴリズムです。

- f(z)がわかっていない時、ドイチュのアルゴリズムを使うとその関数の持つ一部の性質についてのみ真偽を判断することができます。

- 解くことのできる問題が限られていますが古典的なコンピューターで計算をする場合に比べて計算量が圧倒的に少なくなります。

ドイチュのアルゴリズムで解くことのできる問題

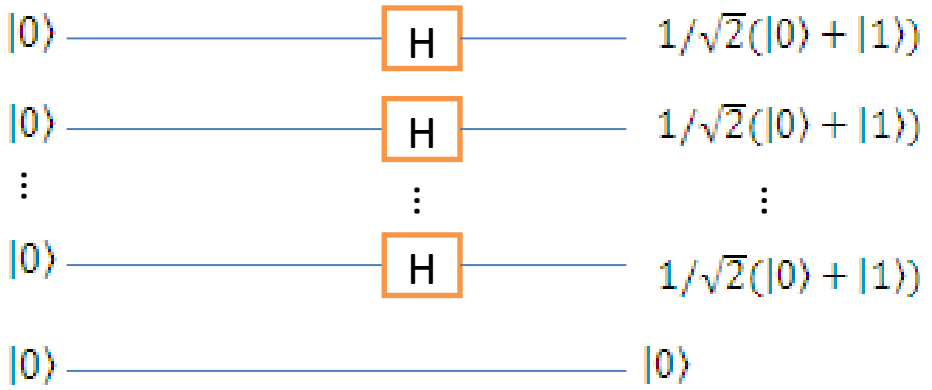
- 2^n個の整数の集合Z={0,1,…,2^n-1}からZ’={0,1}への関数fが与えられた時、次の命題が真か偽か判定せよ。

(a)fは定数関数でない

(b)集合{f(Zi)|i=0,1,…,2^n-1}の要素のうち0の個数と1の個数は同数でない

ドイチュのアルゴリズムの詳細(1)

- まずn+1個の量子ビットを用意し、値をすべて0とします。
- そのうち1つを出力ビットとし、そのほかをアダマールゲートを作用させます。



ドイチュのアルゴリズムの詳細(2)

- これにより状態は

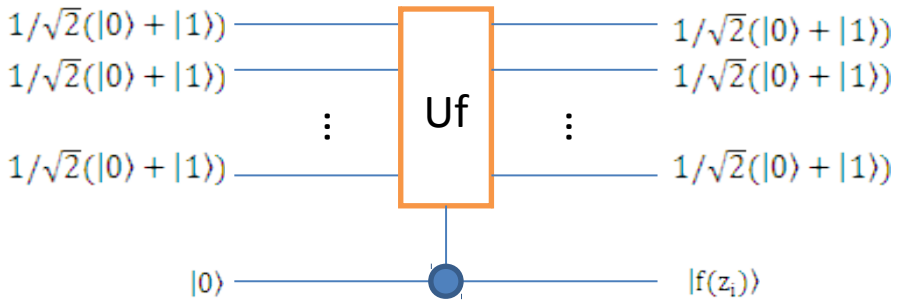
$$|\phi_i\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{z_i}^{2^n-1}|z_i, 0\rangle\right)$$

となります。これを始状態とします。

- 次に、f(z)を計算しその値を出力ビットに与えるサブルーチンUfを作用させます。その結果量子状態は

$$|\phi_1\rangle = U_f|\phi_i\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{z_i}^{2^n-1}|z_i, f(z_i)\rangle\right)$$

となります。



ドイチュのアルゴリズムの詳細(3)

- 次に出力ビットの位相を計算するサブルーチンを作用させ量子状態は

$$|\phi_2\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{z_i}^{2^n-1}(-1)^{f(z_i)}|z_i, f(z_i)\rangle\right)$$

となります。

- さらにこの状態にUfの逆演算を作用させ

$$|\phi_f\rangle = U_f{}^{-1}|\phi_2\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{z_i}^{2^n-1}(-1)^{f(z_i)}|z_i, 0\rangle\right)$$

を得ます。これが求める終状態です。

ドイチュのアルゴリズムの詳細(4)

- この値が求める終状態であり、これと始状態の重なりをとると

$$P = \left|\left\langle \phi_f \middle| \phi_i \right\rangle\right|^2 = \left(\frac{1}{2^n}\right)^2 \left|\sum_{z_i}^{2^n-1} (-1)^{f(z_i)}\right|^2$$

という結果を得ます。

ドイチュのアルゴリズムの詳細(5)
命題の真偽の判定

- 観測によりPの値が求まるとその値により命題の真偽を

$$P = \begin{cases} 1 & \text{(a)が偽かつ(b)が真} \\ 0 & \text{(a)が真かつ(b)が偽} \\ 0 < P < 1 & \text{(a)が真かつ(b)が真} \end{cases}$$

と判定することができます。

ドイチュのアルゴリズムが命題の真偽を判定できる理由(1)

- 命題(a)が偽の場合zの各値に対するf(z)は常に0あるいは1であり絶対値の中の値は2^nまたは-2^nとなります。

$$\left|\sum_{z_i}^{2^n-1}(-1)^{f(z_i)}\right|^2 = (2^n)^2$$

従ってP=1の時(a)は偽(b)は真となります。

ドイチュのアルゴリズムが命題の真偽を判定できる理由(2)

- 命題(b)が偽の場合絶対値の中の値は0となります。

$$\left| \sum_{z_i}^{2^n-1} (-1)^{f(z_i)} \right|^2 = 0$$

従ってP=0の時(b)は偽(a)は真となります。

ドイチュのアルゴリズムが命題の真偽を判定できる理由(3)

- 命題(a),(b)がともに真の場合は絶対値の中の値は

$$-1 < \sum_{z_i}^{2^n-1} (-1)^{f(z_i)} < 0,0 < \sum_{z_i}^{2^n-1} (-1)^{f(z_i)} < 1$$

でありPの値は0<P<1となります。

古典的な計算の場合と量子コンピューターの利点

- 命題の真偽を判断するためには与えられた関数fに整数Zを入れた場合の結果をすべて調べるしかありません。

- そのためある数値に対して関数fの結果を計算する過程を2^n回行う必要があります。

- それに対しドイチュのアルゴリズムではnがいくつになっても関数fの計算とその逆演算、位相の計算の3つのステップで命題の真偽を判断できます。

まとめ、課題

- 量子コンピューターによりドイチュのアルゴリズムを使うと重ね合わせ、位相の操作により異なる数値を同時に計算し計算結果を判断することができます。
- そのため古典的な計算では同じ操作の繰り返しが必要なサブルーチンが不要になります。
- 量子ウォークを用いる場合、アマダールウォークを利用することにより、アマダールゲートは実現することが可能であるがそのほかの量子ゲートについては実現方法が分からなかった。今後はそのほかの量子ゲートの実現方法について検討を重ねたい。

参考文献

- SPRINGER UNIVERSITY TEXTBOOKS　量子情報理論　第2版　佐川弘幸,吉田宣章著
- 数理科学　量子コンピューターの基礎第2版　細谷暁夫