日本語訳『Qiskit Textbook』勉強会 第3章 3.5節

Yuri Kobayashi
Quantum Developer Community

3.5 ベルンシュタイン・ヴァジラニアルゴリズム

ドイチ・ジョザ問題

前章3.4の振り返り

Quantum Tokyo

オラクル：$f(x)$が一定(何を入れても同じ結果）か均等（0と1が半々）を判定

$$f(x)\colon \{0,1\}^{n} \to \{0,1\}$$

オラクルに何回問合せれば、$f(x)$が一定または均等かわかるか？

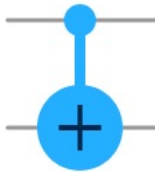
古典：ベスト　2回　ワースト　$2^{n-1}+1$　　量子：1回で判定可能

ドイチ・ジョザで使われるテクニック

オラクル：n量子ビットの制御ユニタリ

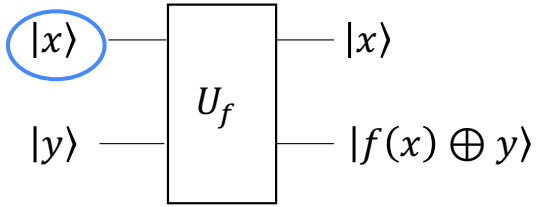
$U_f\colon |x\rangle|y\rangle \mapsto |x\rangle|f(x)\oplus y\rangle$

n=2



CNOTは制御ユニタリの特殊ケース

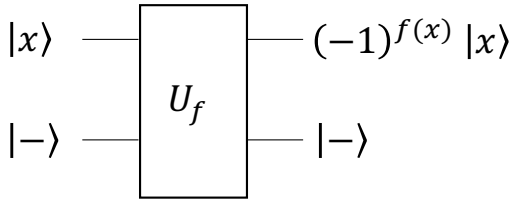
多量子ビットOK



位相キックバック

$U_f\colon |x\rangle|-\rangle \mapsto (-1)^{f(x)}|x\rangle|-\rangle$

本来ターゲット側にエンコードされる位相
情報が制御側に反映される　∴キックバック



ベルンシュタイン・ヴァジラニ問題

$$f(x_0, x_1, x_2, \dots) \rightarrow \{0,1\} \quad x_n \in \{0, 1\}$$

ベルンシュタイン・ヴァジラニ問題は、ドイチ・ジョザ(DJ)の拡張版です。DJが関数の性質を識別する問題であったのに対し、BVは関数の性質がわかっているなかで 関数内に埋め込まれた**秘密の文字列 s を求める問題**です。

関数$f(x)$はs と xのビット毎の2を法とする内積を必ず返すことがわかっています。

$$f(x) = s \cdot x \ (mod\ 2)$$

古典：順番に $|0 \dots 001\rangle, |0 \dots 010\rangle, |0 \dots 100\rangle$ を問合せて、 s の各ビットを明らかにしていく必要があります。nビットのときの **問合せ量はn回**になります。

$$f(0 \dots 001) = s_1, \cdots f(1 \dots 000) = s_n$$

量子：**問合せ量は1回**で済みます。

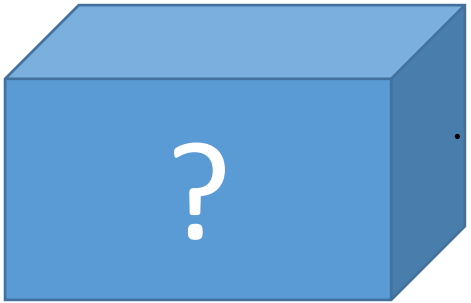
秘密の数

箱の中に秘密の数が隠されているとします。

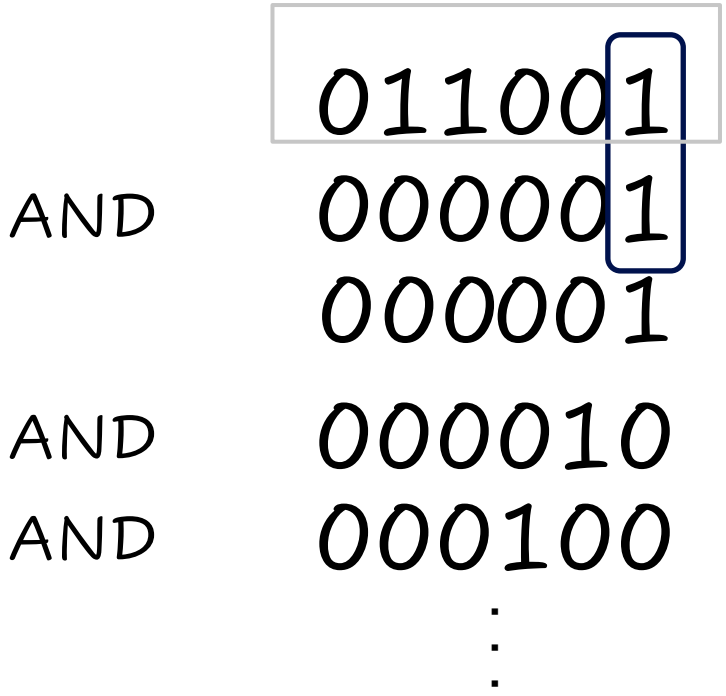
秘密の数はバイナリ文字列　(i.e. 0100110...)であることだけわかっています。

箱に1回ずつ問い合わせて正しい数字かどうかを答えてもらうことができます。

できるだけ少ない問合せ量で秘密の数字をあてるにはどうしたらよいか？



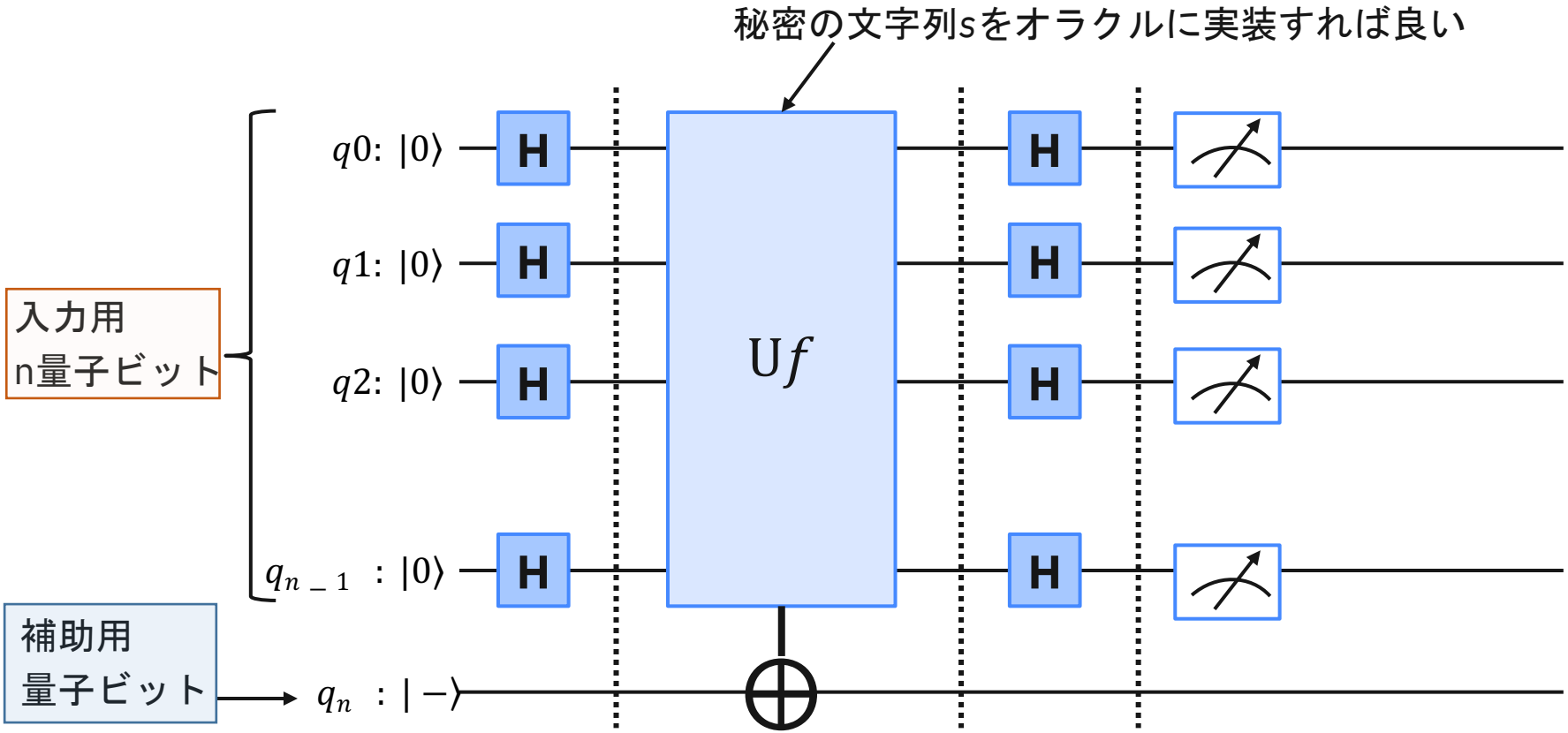
古典コンピューターの解き方



000000 ?
000001 ?
⋮
111111 ?

問合せ量は６回　　nビットの文字列だとn回!

ベルンシュタイン・ヴァジラニのアルゴリズム



ベルンシュタイン・ヴァジラニのアルゴリズム

Step1: 入力用n量子ビット$|0\rangle^{\otimes n}$,アンシラは$|1\rangle$に初期化

Step2: 重ね合わせをつくる　$H^{\otimes n}\,|0\rangle^{\otimes n} \otimes\ H|1\rangle = |x\rangle \otimes |-\rangle$

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x}|x\rangle|-\rangle \quad \rightarrow \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|-\rangle$$

量子状態 $|a\rangle$ にHゲートをかける

$H^{\otimes n}\,|a\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x}|x\rangle$

Step3: オラクルU_fを適用 $U_f\colon\ |x\rangle \mapsto (-1)^{s\cdot x}|x\rangle$

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{s\cdot x}|x\rangle|-\rangle$$

$s\cdot x = s_0\cdot x_0 \oplus s_1\cdot x_1 \ldots \oplus s_{n\_1}\cdot xn_{\_1}$
入力x と秘密の文字列sの各ビットの内積のXORをとることで、n番目の数字を判定する。

Step4: n量子ビット全体に再びアダマールをかける

$|s_1\rangle\cdots|s_n\rangle$　　$Recall: HH = I$　　$Recall:\ H^{\otimes n}\,|s\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{s\cdot x}|x\rangle$

Step5: n量子ビットだけを測定する

Qiskitで実装してみよう

オラクル

古典のオラクル fs は、$s{\cdot}x$mod2=1を満たす任意の入力 x に対して 1 を、それ以外のときは 0 を返します。ドイチ・ジョザでも用いた $|-\rangle$に対する位相キックバックのテクニックを利用することで、以下の変換を得られます。

$$|x\rangle \overset{fa}{\rightarrow} |x\rangle=(-1)^{a\cdot x}|x\rangle$$

隠れた文字列を明らかにするアルゴリズムは、$|0\rangle$のアダマール変換から得られた量子的な重ね合わせで、量子オラクルfaを問い合わせることで、自然に次のようになります。

$$|0\rangle \overset{H^{\otimes n}}{\rightarrow} \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle \overset{fa}{\rightarrow} \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x}|x\rangle$$

n個のアダマールゲートの逆行列は、再び n 個のアダマールゲートなので、次のようにして aを求めることができます。

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x}|x\rangle \overset{H^{\otimes n}}{\rightarrow} |a\rangle$$

n量子ビットのアダマール

1量子ビットの場合

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

$$H|a\rangle = \sum_{v\in\{0,1\}}(-1)^{a\cdot x}|x\rangle$$

2量子ビットの場合

$$\mathrm{H}^{\otimes 2}|00\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle$$
$$\mathrm{H}^{\otimes 2}|01\rangle = |00\rangle - |01\rangle + |10\rangle - |11\rangle$$
$$\mathrm{H}^{\otimes 2}|10\rangle = |00\rangle + |01\rangle - |10\rangle - |11\rangle$$
$$\mathrm{H}^{\otimes 2}|11\rangle = |00\rangle - |01\rangle - |10\rangle + |11\rangle$$

$$\mathrm{H}^{\otimes 2}|a\rangle = \sum_{v\in\{0,1\}^2}(-1)^{a\cdot x}|x\rangle$$

n量子ビットの場合

$$H^{\otimes n}|a\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x}|x\rangle$$

a=0の場合

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$$

具体例

n=2 の量子ビットと秘密の文字列 s=11 で具体的な例を見てみましょう。

2つの量子ビットのレジスタは0に初期化されています。

$$|\psi_0\rangle=|00\rangle$$

両方の量子ビットにアダマールゲートを適用します。

$$|\psi_1\rangle=\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)$$

文字列 s=11 に対して、量子オラクルは以下の演算を行います。

$$f_s$$
$$|x\rangle \rightarrow (-1)^{x\cdot 11}|x\rangle.$$

$$|\psi_2\rangle=\frac{1}{2}((-1)^{00\cdot 11}|00\rangle+(-1)^{01\cdot 11}|01\rangle+(-1)^{10\cdot 11}|10\rangle+(-1)^{11\cdot 11}|11\rangle)$$

$$|\psi_2\rangle=\frac{1}{2}(|00\rangle-|01\rangle-|10\rangle+|11\rangle$$

両方の量子ビットにアダマールゲートを適用します。 $|\psi_3\rangle=|11\rangle$  s=11

測定して秘密の文字列を得ることができる

まとめ

同じ問題を古典アルゴリズムに比べて少ない問合せ量で解くことのできる量子アルゴリズムは量子アドバンテージのあるアルゴリズムと言える。

オラクルは条件を満たすものを識別する分類機のような役割を果たしてくれる。

位相キックバックは、サイモン、ショア、グローバー、位相推定など多くの有名な量子アルゴリズムで用いられているテクニック。

ベルンシュタイン・ヴァジラニアルゴリズムは、これらのテクニックを用いることで、古典計算よりも少ない問合せ量で問題を解くことができる。

Thank you

Yuri Kobayashi
Quantum Developer Community
yurik@jp.ibm.com