量子コンピュータ入門講座の開講へ向けて　IV

Quantum Computing for Information Science Students　IV

中島 由美*　　土屋 尚†

要旨

本学部の４年生及び大学院生に対する量子コンピュータ入門の講義内容の提案の第４回目である。今回はベルンシュタイン・ヴァジラニの問題と呼ばれている、n ビットの整数を量子コンピュータで求める問題を解説する。

1　はじめに

本学において量子コンピュータ入門講座を開講した場合の講義内容の提案を 3 回にわたり行ってきたが [1]〜[3]、本稿はその続きである。情報技術者に対する入門書であるマーミンの教科書 [4][5] を基に、それをこれ以上ないというくらいかみくだいて紹介することを目ざしている。前回の第 3 節で、量子コンピュータで解ける最も単純な問題としてドイチュ問題を解いた [3]。今回はさらにベルンシュタイン・ヴァジラニの問題と呼ばれる n ビットの整数を求める問題解くとはどういうことか解説する。

次節でベルンシュタイン・ヴァジラニの問題を示しそれを解く。これは前回のドイチュの問題より実体的ではあるが、問題という程のことはない程簡単な、問題のための問題である点にかわりはない。重要なことは古典コンピュータでは n 回の計算を要するのに対し、量子コンピュータではただ 1 回の計算で n ビットの整数が得られるということである。

2　ベルンシュタイン・ヴァジラニの問題

まず表題の問題を述べる。

a は非負の 2^n 未満の未知の整数であるとする。つまり $0 \leq a < 2^n$ である。x も同様の整数、つまり $0 \leq x < 2^n$ である。もちろん、n も非負の整数である。$f(x)$ を a と x の対応するビット毎の 2 を法とする内積をとるという関数、すなわち

$$a \bullet x = a_0 x_0 \oplus a_1 x_1 \oplus a_2 x_2 \cdots \tag{1}$$

であるとする。

$$f(x) = a \bullet x \tag{2}$$

を計算するサブルーチンがあるとして、a の値を決定するのに何回のサブルーチンを呼び出す必要があるか、というのがベルンシュタイン・ヴァジラニの問題である。

* 明星大学情報学部教授
† 明星大学名誉教授

もう少し詳しく問題自体の説明をすると、未知数 a も、それを求めるために使う数 x も共に与えられた桁数 n の 2 進数である。つまり a も x も各桁は 0 または 1 であるから、対応する桁のビット同士の積は、両方とも 1 でない限り 0 である。よって (1) 式で定義された内積は、同じ桁が共に 1 である箇所が奇数個ある場合のみ 1 という値を与え、偶数個なら $1 \oplus 1 = 0$ であるから 0 を与える。

この問題を古典コンピュータを用いて解くことを考えてみよう。2^m という数の 2 進表現は m 番目が 1 でそれ以外はすべて 0 である。よって a の 2 進表現の m 番目のビット値が知りたければ

$$a \bullet 2^m$$

を計算すればよい。なぜなら a の m 番目が 1 なら 1、0 なら 0 となるからである。従って n 個のビット列を知りたければ、m を変化させながら 2^m をかけていく操作を n 回くりかえすことになる。つまり古典コンピュータで、n ビットの 2 進数 a を知るためには、n 個の $x = 2^m (0 \leq m < n)$ をあてはめなければならない。

ところが量子コンピュータを用いれば、n がいくつあろうと、ただ 1 回のサブルーチンの呼び出しで a を完全に決めることができる。つまりこれがベルンシュタイン・ヴァジラニの問題への答ということになる訳であるが、以下で、どうしてそのようなことが可能となるのかを説明していこう。

前回 III の第 2 節で、量子コンピュータの計算過程の一般論を展開したが [3]、その (1) として n 個の入力ビットと m 個の出力ビットに対する一般的可逆変換 $\mathbf{U}_f$ を定義した。その特別な場合として n 個の入力ビットと 1 個の出力ビットを持つ系を考えよう。つまり [3] の (1) より

$$\mathbf{U}_f \left(|x\rangle_n |y\rangle_1 \right) = |x\rangle_n |y \oplus f(x)\rangle_1 \tag{3}$$

である。この 1 ビットの出力レジスタが NOT 演算子 $\mathbf{X}$ 及びアダマール演算子 $\mathbf{H}$ を用いて

$$\mathbf{HX} |0\rangle = \mathbf{H} |1\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right) \tag{4}$$

という初期状態に調節されているものとする。つまり

$$|y\rangle_1 = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right)$$

となっている。このとき $\mathbf{U}_f$ が $|x\rangle_n |y\rangle_1$ に作用すれば

$$\begin{aligned}
\mathbf{U}_f |x\rangle_n |y\rangle_1 &= |x\rangle_n |y \oplus f(x)\rangle_1 \\
&= |x\rangle_n \frac{1}{\sqrt{2}} |(|0\rangle - |1\rangle) \oplus f(x)\rangle_1 \\
&= |x\rangle_n \frac{1}{\sqrt{2}} \left(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle \right) \\
&= |x\rangle_n \frac{1}{\sqrt{2}} \left(|f(x)\rangle - |1 \oplus f(x)\rangle \right)
\end{aligned}$$

$f(x)$ は (1)、(2) より 0 または 1 の値しかとらないので

$$= \begin{cases} |x\rangle_n \dfrac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right) & (f(x) = 0 \text{ のとき}) \\ |x\rangle_n \dfrac{1}{\sqrt{2}} \left(|1\rangle - |0\rangle \right) & (f(x) = 1 \text{ のとき}) \end{cases}$$

となる。これを 1 つの式にまとめて書くと

$$\mathbf{U}_f \left|x\right\rangle_n \frac{1}{\sqrt{2}} \left(\left|0\right\rangle - \left|1\right\rangle\right) = (-1)^{f(x)} \left|x\right\rangle_n \frac{1}{\sqrt{2}} \left(\left|0\right\rangle - \left|1\right\rangle\right) \tag{5}$$

である。すなわち、1 量子ビットの出力レジスタを $\frac{1}{\sqrt{2}} \left(\left|0\right\rangle - \left|1\right\rangle\right)$ という重ね合わせ状態にすることにより、我々はビットの反転を全体の符号の変化に変えることができたのである。

この事実をうまく利用していくことがベルンシュタイン・ヴァジラニの問題の解決への鍵なのである。最終的に III の (7)[3]

$$\mathbf{H}^{\otimes n} \left|0\right\rangle_n = \frac{1}{2^{\frac{n}{2}}} \sum_{0 \leq x < 2^n} \left|x\right\rangle_n \tag{6}$$

を使うことになるので、$\mathbf{H}$ の入力レジスタ $\left|x\right\rangle_n$ への影響を今得た事実で書きかえることにしよう。

まず 1 つの量子ビット $\left|x\right\rangle_1$ に対するアダマール演算子 $\mathbf{H}$ の作用は [1] の (41)、(42) より

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

であるから、$x = 0$ なら $+1$、$x = 1$ なら -1 となるからまとめて書け、

$$\mathbf{H} \left|x\right\rangle_1 = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle + (-1)^x \left|1\right\rangle\right) \tag{7}$$

となる。この (7) の右辺を見直すと

$$\begin{aligned} \frac{1}{\sqrt{2}} \left(\left|0\right\rangle + (-1)^x \left|1\right\rangle\right) &= \frac{1}{\sqrt{2}} \left(\left|y = 0\right\rangle + (-1)^x \left|y = 1\right\rangle\right) \\ &= \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{x \cdot y} \left|y\right\rangle \end{aligned}$$

と書けるから、$\mathbf{H}$ の 1 量子ビット $\left|x\right\rangle_1$ に対する効果は

$$\mathbf{H} \left|x\right\rangle_1 = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{x \cdot y} \left|y\right\rangle \tag{8}$$

となる。

では 2 個の量子ビット（$n = 2$）に対してはどうなるだろうか。

$$\begin{aligned} \mathbf{H}^{\otimes 2} \left|x\right\rangle_2 &= (\mathbf{H} \otimes \mathbf{H}) \left(\left|x_1\right\rangle \otimes \left|x_0\right\rangle\right) \\ &= \mathbf{H} \left|x_1\right\rangle \otimes \mathbf{H} \left|x_0\right\rangle \end{aligned}$$

を計算すればよいから、今得た (7) をあてはめると

$$= \frac{1}{2} \left(\left|0\right\rangle + (-1)^{x_1} \left|1\right\rangle\right) \left(\left|0\right\rangle + (-1)^{x_1} \left|0\right\rangle\right)$$

であり、さらに (8) より

$$= \frac{1}{2} \left(\sum_{y_1=0}^{1} (-1)^{x_1 y_1} \left|y_1\right\rangle \right) \left(\sum_{y_0=0}^{1} (-1)^{x_0 y_0} \left|y_0\right\rangle \right) \qquad (*)$$

$$
\begin{aligned}
&= \frac{1}{2}\left\{(-1)^{x_1\cdot 0}\,|0\rangle + (-1)^{x_1\cdot 1}\,|1\rangle\right\}\left\{(-1)^{x_0\cdot 0}\,|0\rangle + (-1)^{x_0\cdot 1}\,|1\rangle\right\}\\
&= \frac{1}{2}\left\{(-1)^{x_1\cdot 0}(-1)^{x_0\cdot 0}\,|0\rangle\,|0\rangle + (-1)^{x_1\cdot 0}(-1)^{x_0\cdot 1}\,|0\rangle\,|1\rangle\right.\\
&\quad \left. + (-1)^{x_1\cdot 1}(-1)^{x_0\cdot 0}\,|1\rangle\,|0\rangle + (-1)^{x_1\cdot 1}(-1)^{x_0\cdot 1}\,|1\rangle\,|1\rangle\right\}\\
&= \frac{1}{2}\left\{(-1)^{x_1\cdot 0+x_0\cdot 0}\,|0\rangle_2 + (-1)^{x_1\cdot 0+x_0\cdot 1}\,|1\rangle_2 + (-1)^{x_1\cdot 1+x_0\cdot 0}\,|2\rangle_2 + (-1)^{x_1\cdot 1+x_0\cdot 1}\,|3\rangle_2\right\}\\
&= \frac{1}{2^{\frac{2}{2}}}\sum_{y=0}^{2^2-1}(-1)^{\sum_{j=0}^{2-1}x_j y_j}\,|y\rangle_2 \qquad (9)
\end{aligned}
$$

これは、また

$$
\begin{aligned}
(-1)^{x_1\cdot 0+x_0\cdot 0} &= (-1)^{x_1\cdot 0\oplus x_0\cdot 0}\\
(-1)^{x_1\cdot 0+x_0\cdot 1} &= (-1)^{x_1\cdot 0\oplus x_0\cdot 1}\\
(-1)^{x_1\cdot 1+x_0\cdot 0} &= (-1)^{x_1\cdot 1\oplus x_0\cdot 0}\\
(-1)^{x_1\cdot 1+x_0\cdot 1} &= (-1)^{x_1\cdot 1\oplus x_0\cdot 1}
\end{aligned}
$$

であることに注意すれば

$$x \bullet y = x_1 \cdot y_1 \oplus x_0 \cdot y_0$$

を使って

$$= \frac{1}{2^{\frac{1}{2}}}\sum_{y=0}^{2^2-1}(-1)^{x\bullet y}\,|y\rangle_2 \qquad (10)$$

と書いてもよい。

一方 (*) はそのまま素直に変形すれば

$$
\begin{aligned}
&= \frac{1}{2}\sum_{y_1=0}^{1}\sum_{y_0=0}^{1}(-1)^{x_1\cdot y_1+x_0\cdot y_0}\,|y_1\rangle\,|y_0\rangle\\
&= \frac{1}{2}\sum_{y_1=0}^{1}\sum_{y_0=0}^{1}(-1)^{\sum_{j=0}^{2-1}x_j\cdot y_j}\,|y_{2-1}\rangle\,|y_0\rangle \qquad (**)
\end{aligned}
$$

つまり (10) と (**) が等しいのであるから、$|y\rangle_2 = |y_1\rangle\,|y_2\rangle$ と書いたことに留意すれば

$$\sum_{y=0}^{2^2-1}(-1)^{x\cdot y} = \sum_{y_1=0}^{1}\sum_{y_2=0}^{1}(-1)^{\sum_{j=0}^{2-1}x_j y_j} \qquad (***)$$

という関係が成り立っていることがわかる。

入力レジスタが n 個の量子ビットの場合は (**) に対応する書き方として

$$\mathbf{H}^{\otimes n}\,|x\rangle_n = \frac{1}{2^{\frac{n}{2}}}\sum_{y_{n-1}=0}^{1}\cdots\sum_{y_0=0}^{1}(-1)^{\sum_{j=0}^{n-1}x_j y_j}\,|y_{n-1}\rangle\cdots|y_0\rangle \qquad (11)$$

(10) に対応する書き方としては

$$\mathbf{H}^{\otimes n}\left|x\right\rangle_n = \frac{1}{2^{\frac{n}{2}}}\sum_{y=0}^{2^n-1}(-1)^{x\bullet y}\left|y\right\rangle_n \tag{12}$$

である。

標準的初期状態 $\mathbf{H}^{\otimes n}\left|0\right\rangle$ （[3] の第 2 節で説明した）にある n 量子ビットの入力レジスタと、1 量子ビットの出力レジスタを状態 $\mathbf{H}\left|1\right\rangle$ として出発し、$\mathbf{U}_f$ を作用させ、そして再び入力レジスタに $\mathbf{H}^{\otimes n}$ を施すと、以下のようになる。

$$\begin{aligned}&\left(\mathbf{H}^{\otimes n}\otimes\mathbf{1}\right)\mathbf{U}_f\left(\mathbf{H}^{\otimes n}\otimes\mathbf{H}\right)\left|0\right\rangle_n\left|1\right\rangle_1\\ =&\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{f(x)+x\cdot y}\left|y\right\rangle_n\frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)\end{aligned} \tag{13}$$

なぜこうなるかを順に説明していこう。

$$\begin{aligned}&\left(\mathbf{H}^{\otimes n}\otimes\mathbf{1}\right)\mathbf{U}_f\left(\mathbf{H}^{\otimes n}\otimes\mathbf{H}\right)\left|0\right\rangle_n\left|1\right\rangle_1\\ =&\left(\mathbf{H}^{\otimes n}\otimes\mathbf{1}\right)\mathbf{U}_f\left(\mathbf{H}^{\otimes n}\otimes\mathbf{H}\right)\left|0\right\rangle_n\otimes\left|1\right\rangle_1\end{aligned}$$

であるから、この後半に II の (38) で示した公式

$$(\mathbf{a}\otimes\mathbf{b})(\left|x\right\rangle\otimes\left|y\right\rangle)=\mathbf{a}\left|x\right\rangle\otimes\mathbf{b}\left|y\right\rangle \tag{14}$$

を使えば

$$\begin{aligned}&=\left(\mathbf{H}^{\otimes n}\otimes\mathbf{1}\right)\mathbf{U}_f\left(\mathbf{H}^{\otimes n}\left|0\right\rangle_n\right)\otimes\left(\mathbf{H}\left|1\right\rangle_1\right)\\ &=\left(\mathbf{H}^{\otimes n}\otimes\mathbf{1}\right)\mathbf{U}_f\left(\mathbf{H}^{\otimes n}\left|0\right\rangle_n\right)\otimes\frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)\end{aligned}$$

となる。一方、

$$\begin{aligned}\mathbf{H}^{\otimes n}\left|0\right\rangle_n&=\left(\frac{1}{\sqrt{2}}(\left|0\right\rangle+\left|1\right\rangle)\right)^n\\ &=\frac{1}{2^{\frac{n}{2}}}(\left|0\right\rangle+\left|1\right\rangle)^n\\ &=\frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1}\left|x\right\rangle_n\end{aligned}$$

であるから

$$=\left(\mathbf{H}^{\otimes n}\otimes\mathbf{1}\right)\mathbf{U}_f\left(\frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{x^n-1}\left|x\right\rangle\right)\frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)$$

となる。さらに

$$=\left(\mathbf{H}^{\otimes n}\otimes\mathbf{1}\right)\left(\frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1}\mathbf{U}_f\left|x\right\rangle_n\right)\frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)$$

となり、(5) を使えば

$$=\left(\mathbf{H}^{\otimes n}\otimes\mathbf{1}\right)\frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\left|x\right\rangle_n\frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)$$

となる。これは係数をつけたままで書くため見にくいが

$$= \left(\mathbf{H}^{\otimes n} \otimes \mathbf{1}\right) \left\{ \left(\frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle_n \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right\}$$

のことであるから、再び公式 (14) を使うことができ

$$\begin{aligned}
&= \frac{1}{2^{\frac{n}{2}}} \left(\mathbf{H}^{\otimes n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle_n \right) \otimes \left\{ \mathbf{1} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right\} \\
&= \frac{1}{2^{\frac{n}{2}}} \left(\mathbf{H}^{\otimes n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle_n \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
&= \frac{1}{2^{\frac{n}{2}}} \left(\mathbf{H}^{\otimes n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle_n \right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \mathbf{H}^{\otimes n} |x\rangle_n \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
\end{aligned}$$

となる。(12) を使えば、さらに

$$\begin{aligned}
&= \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \left(\frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} (-1)^{x \bullet y} |y\rangle_n \right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
&= \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)+x \bullet y} |y\rangle_n \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
\end{aligned}$$

となり、今考えているのは (2) すなわち $f(x) = a \bullet x$ であるから

$$= \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{a \bullet x + x \bullet y} |y\rangle_n \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \tag{15}$$

となる。この (15) の中の x についての和

$$\sum_{x=0}^{2^n-1} (-1)^{a \bullet x + x \bullet y}$$

についてさらに変形していこう。

$$\sum_{x=0}^{(a \bullet x + x \bullet y)} = \sum_{x=0}^{2^n-1} (-1)^{a \bullet x} (-1)^{x \bullet y}$$

は $\bullet$ がビット毎の内積であるから問題ない。さらに

$$= \sum_{x=0}^{2^n-1} (-1)^{a \bullet x} (-1)^{y \bullet x}$$

としてもよい。このように変形すれば

$$= \sum_{x=0}^{2^n-1} (-1)^{(a+y) \bullet x}$$

とすることができることが表 1 よりわかる。

表 1　$a \bullet x + y \bullet x = (a+y) \bullet x$ を示す表。$\oplus$ はビットごとの 2 を法とする和である。

a	y	x	$a \bullet x$	$y \bullet x$	左辺	$a \oplus y$	右辺
0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	1	0	0	0	0	1	0
0	1	1	0	1	1	1	1
1	0	0	0	0	0	1	0
1	0	1	1	0	1	1	1
1	1	0	0	0	0	0	0
1	1	1	1	1	0	0	0

表式 (11) と (12) を比べれば

$$\sum_{y_{n-1}=0}^{1} \cdots \sum_{y_0=0}^{1} (-1)^{\sum_{j=0}^{n-1} x_j y_j} = \sum_{y=0}^{2^n-1} (-1)^{x \bullet y}$$

であるから、これを使ってさらに変形すると

$$= \sum_{x_{n-1}=0}^{1} \cdots \sum_{x_{n-1}=0}^{1} (-1)^{\sum_{j=0}^{n-1} (a_j+y_j) x_j}$$

となる。n 体にわたる和であれば $\sum_{j=0}^{n-1}$ も $\sum_{j=1}^{n}$ も同じことであるから

$$\begin{aligned}
&= \sum_{x_n=0}^{1} \cdots \sum_{x_1=0}^{1} (-1)^{\sum_{j=1}^{n} (a_j+y_j) x_j} \\
&= \sum_{x_n=0}^{1} \cdots \sum_{x_2=0}^{1} \left((-1)^{(a_1+y_1)\cdot 0} + (-1)^{(a_1+y_1)\cdot 1} \right) (-1)^{\sum_{j=2}^{n} (a_j+y_j) x_j} \\
&= \sum_{x_n=0}^{1} \cdots \sum_{x_3=0}^{1} \left((-1)^{(a_1+y_1)\cdot 0} + (-1)^{(a_1+y_1)\cdot 1} \right) \\
&\quad \times \left((-1)^{(a_2+y_2)\cdot 0} + (-1)^{(a_2+y_2)\cdot 1} \right) (-1)^{\sum_{j=3}^{n} (a_j+y_j) x_j} \\
&= \left((-1)^{(a_1+y_1)\cdot 0} + (-1)^{(a_1+y_1)\cdot 1} \right) \left((-1)^{(a_2+y_2)\cdot 0} + (-1)^{(a_2+y_2)\cdot 1} \right) \\
&\quad \times \cdots \times \left((-1)^{(a_n+y_n)\cdot 0} + (-1)^{(a_n+y_n)\cdot 1} \right) \\
&= \prod_{j=1}^{n} \sum_{x_j=0}^{1} (-1)^{(a_j+y_j)\cdot x_j}
\end{aligned}$$

つまり

$$\sum_{x=0}^{2^n-1} (-1)^{a \bullet x + x \bullet y} = \prod_{j=1}^{n} \sum_{x_j=0}^{1} (-1)^{(a_j+y_j) x_j} \tag{16}$$

ということがわかり和が積に変換されるのである。積の形に表されれば

$$\prod_{j=1}^{n}(-1)^{(a_j+y_j)x_j} = \prod_{j=1}^{n}\left((-1)^{(a_j+y_j)\cdot 0} + (-1)^{(a_j+y_j)\cdot 1}\right)$$
$$= \prod_{j=1}^{n}\left(1 + (-1)^{(a_j+y_j)}\right)$$

において

$$1 + (-1)^{a_j+y_j} = \begin{cases} 1+1=2 & (a_j = y_j) \\ 1+(-1)=0 & (a_j \neq y_j) \end{cases}$$

であるから、どの y_j も a_j に等しくなっていないと、すなわち $y = a$ でない限り、0 が積の中に生じて全体が 0 となってしまう。$y = a$ ならば積は

$$\prod_{j=1}^{n}\left(1 + (-1)^{a_j+y_j}\right) = \prod_{j=1}^{n}\left(1 + (-1)^{2a_j}\right)$$
$$= \prod_{j=1}^{n}\left(1 + 1^{a_j}\right)$$

となり、a_j が 0 であっても 1 であっても

$$= \prod_{j=1}^{n}(1+1) = 2^n$$

となる。(15) の x についての和に関する部分のみに着目して展開してきて明らかになったのは、$y = a$ でなければ消えてしまい、残る項の寄与は 2^n となるということであるから

$$(15)\text{ の右辺} = \frac{1}{2^n}\cdot 2^n \left|a\right\rangle_n \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)$$
$$= \left|a\right\rangle_n \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)$$

ということである。(15) の右辺は (13) の左辺であったから結局全体としていえるのは

$$\left(\mathbf{H}^{\otimes n}\otimes \mathbf{1}\right)\mathbf{U}_f\left(\mathbf{H}^{\otimes n}\otimes \mathbf{H}\right)\left|0\right\rangle_n\left|1\right\rangle_1 = \left|a\right\rangle_n \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)$$

ということである。最後に 1 ビットの出力レジスタに $\mathbf{H}$ を施せば

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

であるから

$$\mathbf{H}\otimes\left(\mathbf{H}^{\otimes n}\otimes \mathbf{1}\right)\mathbf{U}_f\left(\mathbf{H}^{\otimes n}\otimes \mathbf{H}\right)\left|0\right\rangle_n\left|1\right\rangle_1 = \mathbf{H}^{\otimes(n+1)}\mathbf{U}_f\mathbf{H}^{\otimes(n+1)}\left|0\right\rangle_n\left|1\right\rangle_1$$

という対称性のよい形にかくことができる。つまりベルンシュタイン・ヴァジラニの問題に対しては

$$\mathbf{H}^{\otimes(n+1)}\mathbf{U}_f\mathbf{H}^{\otimes(n+1)}\left|0\right\rangle_n\left|1\right\rangle_1 = \left|a\right\rangle_n\left|1\right\rangle_1$$

となり、入力ビットに求める a が現れて解決ということになるのである。

3 おわりに

ベルンシュタイン・ヴァジラニの問題と呼ばれる、n ビットの整数 a を求める問題を、量子コンピュータで解くにはどうすればよいかを詳しく解説した。重要なのは $\mathbf{U}_f$ という演算子はただ 1 度しか作用していないにもかかわらず結果が得られるという点である。古典コンピュータでは n 回の演算が必要であるから、その有利さは明らかである。しかし $2(n+1)$ 個のアダマール演算子をあらかじめ用意しておかなくてはならないことや、入力ビットと呼んでいる量子ビット列に結果が現れること等、入門者にとっては少しも解法が簡単になったようには感じられない点も多く残される。

参考文献

[1] 中島由美, 土屋尚, 量子コンピュータ入門講座の開講へ向けて, 明星大学情報学部研究紀要第 19 号, pp.21-39 (2011)
[2] 中島由美, 土屋尚, 量子コンピュータ入門講座の開講へ向けて II, 明星大学情報学部研究紀要第 20 号, pp.75-88 (2012)
[3] 中島由美, 土屋尚, 量子コンピュータ入門講座の開講へ向けて III, 明星大学情報学部研究紀要第 21 号, pp.59-66 (2013)
[4] D. Mermin, Quantum Computer Science - An Introduction , Cambridge UP (2007)
[5] マーミン著, 木村元訳, 量子コンピュータ科学の基礎, 丸善株式会社 (2009)