Memoirs of the Osaka Institute
of Technology, Series A
Vol.50,No.1(2005) pp.129～139

加算と減算を行う量子回路についてのノート

水谷　英樹・白本　長遊*・静田　　靖

情報科学部　情報科学科

〈2005年５月30日受理〉

Note on Quantum Networks Performing Addition and Subtraction

by
Hideki MIZUTANI, Takeyuki SHIRAMOTO and Yasushi SHIZUTA

Department of Information Science,
Faculty of Information Science and Technology
(Manuscript received May 30, 2005)

Abstract

We discuss the quantum networks that perform the addition and the subtraction of integers. The results obtained seem to be well-known in a sense. However, so far as we know, there is no description in the literature which discusses the matter in complete detail. We present it here in a self-contained form and it will serve as preliminaries to the forth-coming paper which is now in preparation.

* (株) ルネサス・ソリューションズ

§1 まえがき

非負整数の加算と減算はともに初等的な演算であり，それらを行う量子回路が存在することもよく知られている．にもかかわらず，加算と減算を行う量子回路についての詳しい議論はどこに述べられているかというと，筆者らが知る限り文献中では，教科書であれ論文であれ，十分に精密な形では書かれてはいないように思われる．つまり省略された部分については，すべてが読者が補うことが前提であり，それを口で言うのはたやすいが，実際に実行しようとすると意外な困難に遭遇するものである．このノートの目的は加算および減算を行う量子回路の構成について，一切の省略を行わず，すべて自己完結的に述べることであり，ほぼ目的は達成されていると思う．

§2 準備

n 桁の 2 進数で表される非負整数 a と b の加算を行う量子回路を構成するために，いくつかの準備を行う．

$$\begin{aligned} a &= 2^{n-1}a_{n-1} + \cdots + 2a_1 + a_0, \\ b &= 2^{n-1}b_{n-1} + \cdots + 2b_1 + b_0. \end{aligned}$$

とおく．ただし $a_i, b_i = \{0,1\}$，$0 \le i \le n-1$ である．$a+b=s$ と書き，

$$s = 2^n s_n + 2^{n-1}s_{n-1} + \cdots + 2s_1 + s_0$$

とおく．このとき以下の漸化式が成り立つことは明らかである．

$$\begin{aligned} s_0 &= a_0 \oplus b_0 \quad , \quad c_0 = a_0 b_0 \\ s_i &= a_i \oplus b_i \oplus c_{i-1} \quad , \quad 1 \le i \le n \\ c_i &= a_i b_i \oplus b_i c_{i-1} \oplus c_{i-1} a_i \quad , 1 \le i \le n-1 \\ a_n &= b_n = 0 \end{aligned}$$

c_{i-1} は $i-1$ 桁から i 桁への繰り上がりを表している．(但し $1 \le i \le n$)

次に補助的な量子ゲート S および C を定義する．

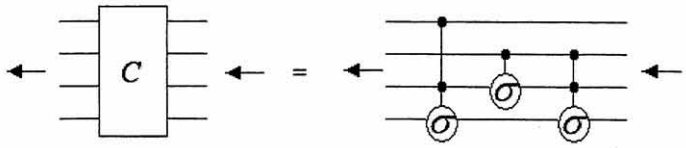
S は $(\mathbf{C}^2)^{\otimes 3}$ 上のユニタリ作用素で，次のダイアグラムで定義される．

図．1　各桁での和を求めるための量子ゲートS

ここで σ は NOT を表す記号である．S はそれぞれの桁における和を求めるための量子ゲートで

$$S|c,a,b\rangle = |c,a,a\oplus b\oplus c\rangle$$

である．$S^2 = S$ が成り立つことは，容易に確かめられるので，S の逆作用素は S 自身である．次に量子ゲート C は $(\mathbf{C}^2)^{\otimes 4}$ 上のユニタリ作用素で，次のダイアグラムで定義される．



図．2　各桁での繰り上がりを求めるための量子ゲートC

C はそれぞれの桁での繰り上がりを求めるための量子ゲートで

$$C|c,a,b,c'\rangle = |c,a,a\oplus b,ab\oplus bc\oplus ca\oplus c'\rangle$$

である．$c' = 0$ として使うことが多いが，このときは

$$C|c,a,b,0\rangle = |c,a,a\oplus b,ab\oplus bc\oplus ca\rangle$$

となる．C の逆作用素を本論文では $\hat{C}$ で表す．即ち $\hat{C} = C^{-1} = C^*$ である．

$$\hat{C}|c,a,b,c'\rangle = |c,a,a\oplus b,a\oplus ab\oplus bc\oplus c'\rangle$$

が成り立つ．

§3 加算

n 桁の非負整数 a と b の加算を行う量子回路をつくるために，いくつかの記号を用意する．まず全空間は $Z = (\mathbf{C}^2)^{\otimes m}$ で，ここに $m = 3n+1$ である．$V_i \cong \mathbf{C}^2 (0 \le i \le 3n)$ とおくと，全空間は $Z = \prod_{i=0}^{3n}{}^{\otimes} V_i$ と書ける．$0 \le k < l \le 3n$ に対して，$X_{k,l} = \prod_{k\le i\le l}{}^{\otimes} V_i = V_k \otimes V_{k+1} \otimes \cdots \otimes V_l$ とおく．同様に $Y_{k,l} = \prod_{i<k,i>l}{}^{\otimes} V_i$ とおくと $X_{k,l} \otimes Y_{k,l} = Z$ が成り立つ．$C^{(i)} (0 \le i \le n-1)$ は $X_{3j,3j+3}$ 上で定義された量子ゲートで C に等しい．このユニタリ作用素を $Y_{3i,3i+3}$ 上では恒等作用素を与えることによって，全空間 Z 上のユニタリ作用素に拡張したものを，$C_*^{(i)} (0 \le i \le n-1)$ と書くことにする．

次に制御 NOT を $X_{3n-2,3n-1}$ 上で与え，$Y_{3n-2,3n-1}$ 上では恒等作用素を与えることによって，全空間 Z 上のユニタリ作用素に拡張したものを，$V_*^{(n)}$ と書く．更に，$S^{(j)} (0 \le j \le n-1)$ を $X_{3j,3j+2}$ 上では S に等しい量子ゲートとし，このユニタリ作用素を $Y_{3j,3j+2}$ 上では恒等作用素を与えることによって，全空間 Z 上のユニタリ作用素に拡張したものを，

$S_*^{(j)}(0 \le j \le n-1)$ と書く．同様に $\hat{C}^{(k)}(0 \le k \le n-2)$ を $X_{3k,3k+3}$ 上で $\hat{C}$ に等しい量子ゲートとし，$Y_{3k,3k+3}$ 上では恒等作用素を与えることによって，全空間 Z 上のユニタリ作用素に拡張したものを $\hat{C}_*^{(k)}(0 \le k \le n-2)$ と書く．

これらの合計 $3n$ 個のユニタリ作用素の積

$$S_*^{(0)} \otimes \hat{C}_*^{(0)} \otimes S_*^{(1)} \otimes \hat{C}_*^{(1)} \otimes \cdots \otimes S_*^{(n-2)} \otimes \hat{C}_*^{(n-1)} \otimes S_*^{(n-1)} \otimes V_*^{(n)} \otimes C_*^{(n-1)} \otimes \cdots \otimes C_*^{(0)}$$

を A とおくと，A が求める加算を行う量子回路である．

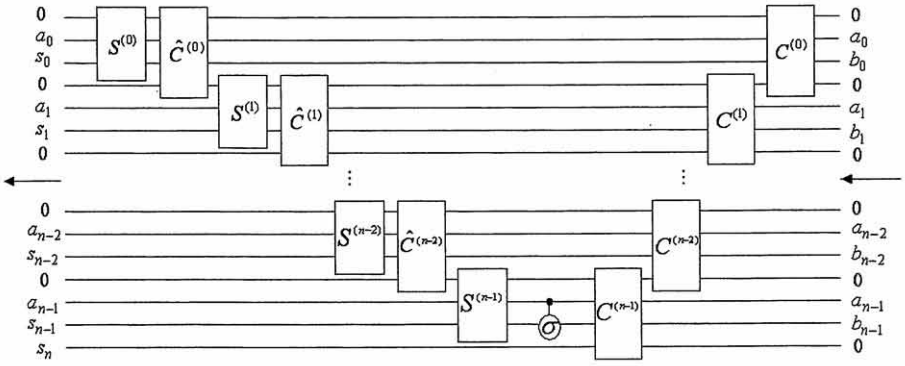


図 3　加算を行う量子回路A

命題 1

$a, b \ge 0$ を n 桁の 2 進数としたとき，$s = a + b$ は

$$A|0, a_0, b_0, 0, a_1, b_1, \cdots, 0, a_{n-1}, b_{n-1}, 0\rangle$$
$$= |0, a_0, s_0, 0, a_1, s_1, \cdots, 0, a_{n-1}, s_{n-1}, s_n\rangle$$

を満たす．

証明

$C^{(i)}$ の入出力を考える．$i = 0$ のとき，入力は $|0, a_0, b_0, 0\rangle$ であるから，

$$C^{(0)}|0, a_0, b_0, 0\rangle = |0, a_0, a_0 \oplus b_0, a_0 b_0\rangle = |0, a_0, a_0 \oplus b_0, c_0\rangle$$

となる．$1 \le i \le n-1$ のときは入力は $|c_{i-1}, a_i, b_i, 0\rangle$ なので，

$$C^{(i)}|c_{i-1}, a_i, b_i, 0\rangle = |c_{i-1}, a_i, a_i \oplus b_i, a_i b_i \oplus b_i c_{i-1} \oplus c_{i-1} a_i\rangle = |c_{i-1}, a_i, a_i \oplus b_i, c_i\rangle$$

である．次に $\hat{C}^{(i)}$ の入出力を考える．$1 \le i \le n-2$ をみたす i に対して，入力は $|c_{i-1}, a_i, a_i \oplus b_i, c_i\rangle$ であるが，ここで $c_i = a_i b_i \oplus b_i c_{i-1} \oplus c_{i-1} a_i$ である．

$$\begin{aligned}
&\hat{C}^{(i)}|c_{i-1}, a_i, a_i \oplus b_i, c_i\rangle \\
= \;& |c_{i-1}, a_i, b_i, a_i \oplus (a_i(a_i \oplus b_i)) \oplus ((a_i \oplus b_i)c_{i-1}) \oplus c_i\rangle \\
= \;& |c_{i-1}, a_i, b_i, c_i \oplus c_i\rangle = |c_{i-1}, a_i, b_i, 0\rangle
\end{aligned}$$

が成り立つ．$i=0$ のときは，

$$\begin{aligned}
&\hat{C}^{(0)}|0, a_0, a_0 \oplus b_0, a_0 b_0\rangle \\
= \;& |0, a_0, b_0, a_0 \oplus a_0(a_0 \oplus b_0) \oplus a_0 b_0\rangle \\
= \;& |0, a_0, b_0, 0\rangle
\end{aligned}$$

となる．次に $S^{(i)}$ の入出力を求める．$i=0$ のとき，入力は $|0, a_0, b_0\rangle$ であるから，

$$S^{(0)}|0, a_0, b_0\rangle = |0, a_0, a_0 \oplus b_0\rangle$$

である．$1 \leq i \leq n-1$ のときは入力は $|c_{i-1}, a_i, b_i\rangle$ なので，

$$S^{(i)}|c_{i-1}, a_i, b_i\rangle = |c_{i-1}, a_i, a_i \oplus b_i \oplus c_{i-1}\rangle$$

となる．最後に $V^{(n)}$ の入出力は

$$V^{(n)}|c_{n-2}, a_{n-1}, a_{n-1} \oplus b_{n-1}, c_{n-1}\rangle = |c_{n-2}, a_{n-1}, b_{n-1}, c_{n-1}\rangle$$

である．以上の結果を組み合わせて，$s_i, i = 0, \cdots, n$ を帰納的に定義する漸化式に注意すれば証明はおわる． ■

§4 加算についての注意

前節で述べた n 桁の 2 進数 $a, b \geq 0$ の加算を本論文では第 1 種の加算と呼ぶことにする．この節では a は n 桁の非負整数であるが，b は $n+1$ 桁の非負整数である場合の加算 $a+b$ を考え，これを第 2 種の加算と呼ぶ．

$$\begin{aligned}
a &= 2^{n-1}a_{n-1} + \cdots + 2a_1 + a_0, \\
b &= 2^n b_n + 2^{n-1}b_{n-1} + \cdots + 2b_1 + b_0.
\end{aligned}$$

とする．但し $a_i = \{0,1\}, 0 \leq i \leq n-1, b_i = \{0,1\}, 0 \leq i \leq n$ である．

$$s = 2^n s_n + 2^{n-1}s_{n-1} + \cdots + 2s_1 + s_0$$

とおくと，次の漸化式

$$\begin{aligned}
s_0 &= a_0 \oplus b_0 \quad , \quad c_0 = a_0 b_0 \\
s_i &= a_i \oplus b_i \oplus c_{i-1} \quad , \quad 1 \leq i \leq n \\
c_i &= a_i b_i \oplus b_i c_{i-1} \oplus c_{i-1} a_i \quad , 1 \leq i \leq n-1 \\
a_n &= 0
\end{aligned}$$

が成り立つ．s の有効数字は $n+1$ 桁とする．従ってオーバーフローは起こりえる．即ち $a+b \geq 2^{n+1}$ の場合オーバーフローが起こり，$a+b < 2^{n+1}$ ならばオーバーフローは起こらない．そのことに注意すれば，前節で述べた加算を行う量子回路をそのまま用いても差し支えない．入力は $|0, a_0, b_0, 0, a_1, b_1, \cdots, 0, a_{n-1}, b_{n-1}, b_n\rangle$ となり，$s = a+b$ が $n+2$ 桁の2進数になった場合は 2^{n+1} は無視されて，出力は $|0, a_0, s_0, 0, a_1, s_1, \cdots, 0, a_{n-1}, s_{n-1}, s_n\rangle$ となる．$s = a+b \leq 2^{n+1}-1$ の場合，オーバーフローは起こらないので，出力は上と同じであるが意味は異なる．このような加算は以下で減算を考察する場合に現れる．

§5 2の補数

a は n 桁の正整数とする．このとき a の2の補数 a^* を $a^* = 2^{n+1} - a$ によって定義する．このとき，

$$a + a^* = 2^{n+1}$$

が成り立つ．あるいは a^* は

$$a^* \equiv -a \ (mod\ 2^{n+1})$$

が成り立つような最小の正整数と言ってもよい．ここで写像 $-a \mapsto a^*$ は全単射であることに注意する．a は $1 \leq a \leq 2^n - 1$ を満たすから，a^* は $2^n + 1 \leq a^* \leq 2^{n+1} - 1$ を満たす．よって a^* は $n+1$ 桁の正整数である．

$$a^* = 2^n a_n^* + 2^{n-1} a_{n-1}^* + \cdots + 2a_1^* + a_0^*$$

と書いたとき，定義によって $a^* = 2^{n+1} - a$ であるから，等比級数の和の公式

$$2^n + 2^{n-1} + \cdots + 1 = 2^{n+1} - 1$$

を用いると，

$$2^{n+1} - a = 2^n(1 - a_n) + 2^{n-1}(1 - a_{n-1}) + \cdots + 2(1 - a_1) + (1 - a_0) + 1$$

が成り立つ．よって

$$\begin{aligned} a_0^* &= a_0 \quad , \quad d_0 = 1 \oplus a_0, \\ a_k^* &= a_k \oplus 1 \oplus d_{k-1} \quad , \quad 1 \leq k \leq n, \\ d_k &= (a_k \oplus 1)\, d_{k-1} \quad , \quad 1 \leq k \leq n-1. \end{aligned}$$

と書いてから，この漸化式を順に解くと $a_k^* (0 \leq k \leq n)$ が求まる．実際，

$$d_k = \prod_{i=1}^{k} (a_i \oplus 1)$$

が成り立ち，これを k を $k-1$ でおきかえて，a_k^* の式の右辺に代入すれば $a_k^* (0 \leq k \leq n)$

は，$a_k(0 \leq k \leq n)$ を用いて陽に表すことができる．結果の式はここでは省略する．

§6 減算

b を n 桁の非負整数，a を n 桁の正整数として $b-a=b+(-a)$ を求めたい．この計算は直接的に行うのでなはく，§5 で述べたように写像 $-a \mapsto a^*$ が全単射であることに注意して $-a$ を a^* でおきかえて $b+a^*$ を計算するのである．この計算は §4 で述べた第2種の加算であることに注意しよう．次の等式

$$b+(2^{n+1}-a)=2^n\bar{s}_n+2^{n-1}\bar{s}_{n-1}+\cdots+\bar{s}_0+2^{n+1}\tau(b-a) \qquad (*)$$

が成り立つ．但し $\tau(x)$ は $\mathbf{Z}$ 上の関数で，

$$\tau(x)=\begin{cases}1, & x \text{ が非負整数のとき}\\ 0, & x \text{ が負の数のとき}\end{cases}$$

で定義される．漸化式

$$\begin{aligned}
\bar{s}_0 &= a_0^* \oplus b_0 \quad , \quad \bar{c}_0 = a_0^* b_0\\
\bar{s}_i &= a_i^* \oplus b_i \oplus \bar{c}_{i-1} \quad , \quad 1 \leq i \leq n\\
\bar{c}_i &= a_i^* b_i \oplus b_i \bar{c}_{i-1} \oplus \bar{c}_{i-1} a_i^* \quad , 1 \leq i \leq n\\
b_n &= 0
\end{aligned}$$

が成り立つ．これは §4 で述べた漸化式と実質に同じである．

以下 $b-a \geq 0$ の場合と $b-a<0$ の場合に分けて考える．$b-a \geq 0$ のとき $(*)$ 式は，

$$2^{n+1}+(b-a)=2^n\bar{s}_n+2^{n-1}\bar{s}_{n-1}+\cdots+\bar{s}_0+2^{n+1}$$

となるが，2^{n+1} の項はオーバーフローによって消される．またこの場合 $\bar{s}_n=0$ が成り立つので，計算結果のレジスター表現は，

$$\bar{s}_n=b-a=2^{n-1}\bar{s}_{n-1}+2^{n-2}\bar{s}_{n-2}+\cdots+\bar{s}_0$$

である．$\bar{s}_n=0$ を示すには,$b-a$ を上から評価すればよい．即ち，

$$max_{a,b}(b-a)=(2^n-1)-1<2^n-1$$

が成り立つので，上の式の右辺は 2^n 未満の非負整数を表すからである．レジスター表現の $n+1$ 桁目は符号を表すビットなので，$b-a \geq 0$ ならば $\bar{s}_n=0$ であることは当然であるが，実はこれは必要十分条件でもある．そのことは以下の議論の過程で明らかになるであろう．次に $b-a<0$ の場合について考える．この場合オーバーフローは起こらない．また $\bar{s}_n=1$ が成り立つのでレジスター表現は，

$$\bar{s}_n=2^{n+1}-(a-b)=2^n+2^{n-1}\bar{s}_{n-1}+\cdots+\bar{s}_0$$

が得られる．$\bar{s}_n=1$ を示すには左辺の下からの評価を行えばよい．即ち，

$min_{a,b}\{2^{n+1}-(a-b)\}=2^n+1$

であるから，$\bar{s}_n=0$ とすれば矛盾が生じる．よって $b-a<0$ のときは $\bar{s}_n=1$ が必要条件として得られ，符号のビットは 1 となる．先に得た結果と組み合わせれば $b-a\geq 0$ と $\bar{s}_n=0$ は同値であり，また $b-a<0$ と $\bar{s}_n=1$ は同値であることが分かる．

§7 減算を行う量子回路

§3 で構成した加算を行う量子回路 A の逆作用素を $\hat{A}$ と書くことにする．$\hat{A}$ は $(\mathbf{C}^2)^{\otimes m}(m=3n+1)$ 上のユニタリ作用素で，$\hat{A}=A^{-1}=A^*$ である．

命題 2

a を n 桁の正整数，b を n 桁の非負整数とする．

$$\begin{aligned}&\hat{A}|0,a_0,b_0,0,a_1,b_1,\cdots,0,a_{n-1},b_{n-1},0\rangle\\ =\ &|0,a_0,\bar{s}_0,0,a_1,\bar{s}_1,\cdots,0,a_{n-1},\bar{s}_{n-1},\bar{s}_n\rangle\end{aligned}$$

が成り立つ．ここで $\bar{s}=2^n\bar{s}_n+2^{n-1}\bar{s}_{n-1}+\cdots+\bar{s}_0$ は減算 $b-a$ (実は第 2 種の加算 a^*+b) の結果のレジスター表示である．

証明

$$\begin{aligned}&A|0,a_0,\bar{s}_0,0,a_1,\bar{s}_1,\cdots,0,a_{n-1},\bar{s}_{n-1},\bar{s}_n\rangle\\ =\ &|0,a_0,b_0,0,a_1,b_1,\cdots,0,a_{n-1},b_{n-1},0\rangle \qquad (**)\end{aligned}$$

を示せばよい．$m=3n+1$ 本あるワイヤーの上から順に $0,1,2,\cdots,3n$ と名づける．そして $\{1,4,7,\cdots,3n-2\}$ を A グループ，$\{2,5,\cdots,3n-1\}\cup\{3n\}$ を B グループとする．また $\{0,3,\cdots,3n-3\}$ を C グループとする．A の出力は a と $\bar{s}$ の加算の結果を示すから，それがどうなるかを見ればよい．まず $\bar{s}_n=0$ の場合と $\bar{s}_n=1$ の場合に分けて考える．$\bar{s}_n=0$ は $b-a\geq 0$ と同値であるから，この場合 $\bar{s}=b-a$ なので $\bar{s}+a=(b-a)+a=b$ となる．この場合の加算は第 1 種の加算である．次に $\bar{s}_n=1$ は $b-a<0$ と同値であるから，$\bar{s}=2^{n+1}-(a-b)$ である．よって $\bar{s}$ に a を加えれば $\bar{s}+a=2^{n+1}+b$ であるが，ここで $b\geq 0$ であるから 2^{n+1} はオーバーフローによって消される．したがってこの場合も結果のレジスター表示は $\bar{s}=b$ となる．このときの加算は第 2 種の加算であるからオーバーフローを生じたのである．以上をまとめると，量子回路 A によって加算 $\bar{s}+a$ を行うと，結果のレジスター表現は常に b に等しい．即ち (**) 式が成り立つことが示された．A はユニタリ作用素であるから可逆である．よって (**) 式の両辺に A の逆作用素 $\hat{A}$ を施せば，

$$\begin{aligned}&\hat{A}|0,a_0,b_0,0,a_1,b_1,\cdots,0,a_{n-1},b_{n-1},0\rangle\\ =\ &|0,a_0,\bar{s}_0,0,a_1,\bar{s}_1,\cdots,0,a_{n-1},\bar{s}_{n-1},\bar{s}_n\rangle\end{aligned}$$

が得られる．これが示すべきことであった． ■

§8 あとがき

現在準備中の論文「$\mathbf{Z}_N$ 上の指数関数を計算する量子回路」のあらすじを以下に述べる．そのことによって，本研究ノートのねらいと方向性を，はっきりさせることができると思われるからである．主な目的は命題１，命題２，および命題３を示すことで，それぞれの命題の内容は次の通りである．

まず第１の命題では $\mathbf{Z}_N$ における加算を行う量子回路を構成する．$\mathbf{Z}_N$ の完全代表系としては $\{0,1,\cdots,N-1\}$ をとる．N は与えられた正整数である．いいかえれば $a,b \in \{0,1,\cdots,N-1\}$ に対して，$a+b$ を N で整除したときの剰余，即ち $a+b(\mathrm{mod}N)$ を計算することが目的である．このとき，本研究ノートで述べた加算器 A を３個，そして減算器 A^{-1} を２個，その他に制御 NOT などを何個か用いる．構成された量子回路をここでは A_{mod} で表すことにする．

第２の命題では $\mathbf{Z}_N$ における乗算の計算をする量子回路を構成する．乗算は２項演算なので $(a,x) \mapsto ax(\mathrm{mod}N)$ と書いてもよいが，実質的には a をパラメータと見ている．この時，先に構成した A_{mod} を数個と補助的な量子ゲート（制御 NOT など）を数個用いる．構成された回路をここでは M_{mod} で表すことにする．

最後に第３の命題では，$\mathbf{Z}_N$ 上の指数関数を計算する量子回路を構成する．この回路は，M_{mod} とその類似物である $\widetilde{M}_{mod}$ を何個か組み合わせて作ることができる．構成された量子回路をここでは $U_{a,N}$ と書くことにすると，$U_{a,N} : x \mapsto a^x(\mathrm{mod}N)$ である．但し $a \in 0,1,\cdots,N-1$ で a と N は互いに素であると仮定する．

N は素因数分解すべき正整数で，奇数の合成数であると仮定しても一般性を失わない．この問題を解く量子アルゴリズムは，Shor のアルゴリズムとして著名なものである（文献[4][5]）．このアルゴリズムはいくつかのステップから成り立っているが，その中には例えばランダムに選んだ a と N の最大公約数を求めるなど，古典的な方法で容易に解くことができるものもある．しかし，Shor のアルゴリズムの中で核心をなす部分は，a の位数を求めるステップである．この計算を行うための量子回路は，上に述べた $\mathbf{Z}_N$ 上の指数関数を計算する量子回路と，離散フーリエ変換を組み合わせて構成される．離散フーリエ変換を U_{QFT} と書くことにすると，$(U_{QFT} \otimes I)U_{a,N}(U_{QFT} \otimes I)$ が位数を求める量子回路である（I は恒等作用素である）．これを U_{SHOR} で表すことにする．

この量子回路は $V = (\mathbf{C}^2)^{\otimes L}$，$\lceil L = 2\log N \rceil$ としたとき，$V \otimes V$ で働くユニタリ作用素である．$q = 2^L$ とおくと，

$$N^2 \leq q < 2N^2$$

が成り立ち，$V \otimes V$ は q^2 次元の複素線形空間である．この程度のサイズの空間が，計算にある程度の余裕を持たせるため必要なものと考えられる．入力として $|0\rangle \otimes |0\rangle \in V \otimes V$ をとった

ときの，この量子回路の出力に対して観測を行う．このとき用いる観測量は，$0,1,2,\cdots,q-1$ をすべて多重度 q の固有値としてもつようなエルミート作用素である．レジスターの内容の観測を行うことによって，波束の収縮が起こり，状態はひとつの純粋な状態に遷移する．そして観測値として，$0,1,2,\cdots,q-1$ の中からひとつの値 c が得られる．この c を入力データとして短い計算を行う．このアルゴリズムは古典的な連分数近似の計算を行うもので，古典コンピュータで十分である．この計算の出力として a の位数 r らしきものが得られる．ここまでが位数を求めるためのステップであるが，実はこのステップの計算結果として a の位数が得られる場合もあれば，また別の値が得られる場合もあるといわねばならない．いずれの場合が起きるかは，観測値 c の値によりけりである．

そこで，どれくらいの頻度で正しい位数が求まるかという確率を下から評価することが，重要な問題になる．Shor の計算によれば，この確率は下から $const./\log\log N$ でおさえられる．ここで $const.$ は N によらない正の定数である．この不等式によれば，粗くいって $O(n)$ 回反復計算すれば，1 に十分近い確率で a の位数の値を知ることができる．ここで $n=\log_2 N$ は N を 2 進数で表した場合の桁数なので，入力のサイズを表す．

これまで位数の定義を述べてなかったので，ここで定義を与える．$\mathbf{Z}_N$ の元の中で N と互いに素なものを全部集めて $\mathbf{Z}_N^*$ と書くことにする．$\mathbf{Z}_N^*$ の元は乗法に関して必ず逆元をもつことになる．$a\in\mathbf{Z}_N^*$ に対して，$a^x=1$ であるような正整数 x の中で最小のものを a の位数と呼び，r で表すことにする．この位数 r を求めることが，古典コンピュータでは極めて困難な問題として知られている．そのことが巨大な正整数の素因数分解が実際上できないことの原因であった（文献 [2]）．また，そのことを逆手にとって RSA 暗号系などが考案され，実用に供されてきた．

Shor の素因数分解に対する量子アルゴリズムの計算論的な意義は，入力サイズ n について多項式オーダー時間で，位数の計算ができること，したがって素因数分解を効率的に行うことが可能であることを示したという点にあった（無論，理論的にはという話である）．そのからくりは量子並列計算が，計算全体の効率を劇的に改善したことにあった．アルゴリズム全体の評価は，例えば文献 [1] にゆずるとして，ここでは U_{QFT} の計算量は $O(n^2)$，$U_{a,N}$ の計算量も n の多項式オーダー時間であることを注意しておく．以上のような解説が，読者にとって本研究ノートを読む上で何らかの参考になれば幸いである．

謝辞

投稿原稿の校閲結果として，無名氏から，この研究ノートで構成されている加減算回路は，古典計算における可逆計算のための回路であるというのが適切であろうとのご注意を頂きました．ひとつの見方としてもっともなご指摘であり，ここに感謝の意を表したいと思います．§8 はその後，最初の原稿の説明不足と思われる部分（例えば，本研究ノートの目的と方向性）を補うために書き加えたものです．

参考文献

1. 上坂　吉則：量子コンピュータの基礎数理，コロナ社, 2000.
2. 今井 浩：20 世紀の名著名論, 情報処理, **45**, 1 , pp.79, 情報処理学会, 2004.
3. A.N.Al-Rabadi : Reversible Logic Synthesis, Springer, 2004.
4. P.W.Shor : *Algorithms for quantum computation:discrete logarithms and factoring*, Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, IEEE Press, pp.124-134, 1994.
5. P.W.Shor : Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing, **26**, 5 , pp.1484-1509, 1997.
6. Vedral,V. , Barenco,A. , and Ekert,A. : Quantum Networks for Elementary Arithmetic Opeartions , Physical Rev , **A** , **54** , 1 , pp.147-153, 1996.
7. Mizutani,H. , Shiramoto,T. , and Shizuta,Y. : $\mathbf{Z}_N$ 上の指数関数を計算する量子回路 (準備中) .