数理解析研究所講究録
第1998巻 2016年 78-87

足し算と掛け算の多項式表示について

産業技術総合研究所　縫田 光司
（科学技術振興機構（JST）さきがけ研究員）
k.nuida@aist.go.jp

Koji Nuida
National Institute of Advanced Industrial Science and Technology (AIST)
(JST PRESTO Researcher)

概 要

K を位数 p の（有限）素体とするとき、K 上の任意の n 変数（対称）関数は各変数の次数が p 未満である n 変数（対称）多項式を用いて表せることはよく知られている。本稿では、p 進法の足し算と掛け算における繰り上がり関数についてその具体的な多項式表示について論じるとともに、それらと暗号理論との関連性について述べる。（本稿の内容は鍛冶静雄氏（山口大学）、前野俊昭氏（名城大学）、沼田泰英氏（信州大学）との共同研究に基づくものである。）

1 本研究について

素数位数 p の素体 $\mathbb{F}_p$ 上の n 変数関数 $(\mathbb{F}_p)^n \to \mathbb{F}_p$ は、常に $\mathbb{F}_p$ 上の n 変数多項式として表せることはよく知られている。また、この多項式は、各変数に関して $p-1$ 次以下となるように選べる。例えば、$\mathbb{F}_p$ 上の二項演算はどれも上述のような次数を持つ、従って高々 p^2 個の単項式からなる、$\mathbb{F}_p$ 上の2変数多項式として表せることが保証される。一方、具体的に与えられた関数に対するこうした多項式表示の導出は決して自明な問題ではない。本稿では、p 進法の足し算と掛け算における繰り上がり関数（ここでは、p 進法における整数の各桁の数字を $\mathbb{F}_p$ の元と同一視する）についてこの問題を論じるとともに、本研究のきっかけとなった暗号理論への応用について述べる。

本稿では、二つの数の足し算における一つ上の桁への繰り上がりだけでなく、より多くの数の足し算におけるさらに上の桁への繰り上がりも取り扱う。二進法（$p=2$）の場合には、3節の例1で触れるように、基本対称多項式を用いた綺麗な解が知られている（初出は未確認であるが、少なくとも2000年のBoyar、PeraltaおよびPochuevの論文[1]にはこの結果が記されている）。本研究では、初等整数論におけるLucasの定理[3]を用いて、一般の p の場合に足し算の繰り上がりを表す最小次数の対称多項式を導出した。ただ、p が奇素数の場合にはこの対称多項式はかなり複雑な形をしており、現時点では、例えば対称多項式の代表的な基底を用いた簡明な表示を得るには至っていない。この点は今後の研究課題である。

また、本研究では奇素数 p について、p 進法の掛け算の繰り上がりに関する最小次数の多項式表示を（完全に閉じた式ではないものの、具体的に計算可能な形で）導出した。（$p=2$ の場合には、一桁の数どうしの掛け算で繰り上がりは生じないことに注意されたい。）この多項式は高々 $(3p-1)/2$ 個の単項式からなる。これは前述した一般の関数に対する単項式の個数の上限 p^2 よりも次数が低いことから、ある意味で掛け算の繰り上がりは一般の関数よりも有意に単純な構造を持つといえよう。なお、p の選び方によっては単項式の個数は $(3p-1)/2$ よりさらに少なくなる。例えば $p=5$ の場合、単項式の個数は $(3p-1)/2=7$ よりも少ない6個である。

以下、暗号理論の観点から本研究の動機について述べる。最近の暗号理論分野における主な研究対象の一つである完全準同型暗号 [2] は、生データ（平文）に対するいかなる種類の演算も、平文を暗号化した状態のままで実行できる機能を備えた暗号技術である。例えば、本稿の著者と黒澤が最近提案した方式 [4] では、平文 $m_1, m_2 \in \mathbb{F}_p$ に関する暗号文 c_1, c_2 が与えられたとき、c_1 と c_2 だけから（m_1 や m_2 を知ることなしに）平文の和 $m_1 + m_2 \in \mathbb{F}_p$ および積 $m_1 m_2 \in \mathbb{F}_p$ に関する暗号文を新たに生成できる。そこで、もし（本稿で論じるように）p 進法の足し算や掛け算の繰り上がり関数を入力の足し算と掛け算の組合せで具体的に表せれば、p 進法の任意精度整数に対する足し算や掛け算を、各桁の数字を暗号化したままの状態で計算できるようになる。

一方、暗号化したまま足し算や掛け算を計算できる機能は、完全準同型暗号の応用に有用なだけでなく、実はこの完全準同型暗号方式 [4] 自体の構成にも一役買っている。論文 [4] の方式（に限らず、本稿執筆時点で知られている事実上全ての完全準同型暗号方式）では、暗号文がある種の「ノイズ成分」を含んでおり、このノイズ成分が大きすぎると暗号文を平文へと正しく戻せなくなる。そして、平文の足し算や掛け算を暗号文上で行う度にこのノイズ成分が増大していく。そのため、それらの演算を繰り返す場合、ノイズ成分が大きくなりすぎる前に余分なノイズ成分を除去する必要がある。このノイズ除去操作を実現する際に、暗号化された整数の足し算や掛け算が用いられているのである。従って、暗号文上での足し算や掛け算が効率化できれば、それだけこの完全準同型暗号方式自体の構成も効率化できることになる。

本稿の構成は以下の通りである。2 節では、本稿で用いる記号や用語に加え、$\mathbb{F}_p$ 上の関数の多項式表示に関する基本事項をまとめる。3 節では、p 進法の足し算における繰り上がり関数の多項式表示に関する結果を述べる。4 節では掛け算に関する同様の結果を述べる。

2 準備

本稿では、対象 x に関する命題 $P(x)$ について、その特性関数を $\chi[P(x)]$ で表す。すなわち、$\chi[P(x)] = 1$ は $P(x)$ が真であることを意味し、$\chi[P(x)] = 0$ は $P(x)$ が偽であることを意味する。本稿では p は素数を表す。また、p 元体 $\mathbb{F}_p$ を $\mathbb{Z}$ の部分集合 $\{0, 1, \ldots, p-1\}$ と自然に同一視するにあたり、$x \in \mathbb{F}_p$ に対応する $\{0, 1, \ldots, p-1\}$ の元を $x_{\mathbb{Z}}$ と記す。さらに、$a \in \mathbb{F}_p \setminus \{0\}$ の逆元を $\mathbb{Z}$（あるいは $\mathbb{Q}$）ではなく $\mathbb{F}_p$ で考えていることを強調するときは、a^{-1} の代わりに $\mathsf{Inv}_p(a)$ と記す。

関数 $f\colon (\mathbb{F}_p)^n \to \mathbb{F}_p$ について、あらゆる $(x_1, \ldots, x_n) \in (\mathbb{F}_p)^n$ で $\varphi(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ が成り立つような $\mathbb{F}_p$ 上の多項式 $\varphi(x_1, \ldots, x_n)$ を f の**多項式表示**と呼ぶ。以下の事実はよく知られているが、重要なので念のため証明を与えておく。

命題 1. 関数 $f\colon (\mathbb{F}_p)^n \to \mathbb{F}_p$ の各々について、その多項式表示 φ であって各変数に関する次数が $p-1$ 次以下であるものが存在する。さらにそのような多項式 φ はただ一つに定まる。

証明. 件の多項式の存在について、$a = (a_1, \ldots, a_n) \in (\mathbb{F}_p)^n$ とすると、Fermat の小定理により関数 $\chi[x = a]$（$x = (x_1, \ldots, x_n)$）の多項式表示 $\varphi_a(x) = \prod_{i=1}^{n} (1 - (x_i - a_i)^{p-1})$ が得られる。これを踏まえると、一般の関数 f の多項式表示が $\varphi(x) = \sum_{a \in (\mathbb{F}_p)^n} f(a)\varphi_a(x)$ で与えられる。

件の多項式の一意性については、零関数 $f = 0$ の場合に示せば充分である。$n = 1$ のとき、主張は多項式の剰余定理より確かに成り立つ。以下再帰的に、一つ手前の n までで主張が成り立っているとして、次数の条件を満たす零でない多項式表示 φ の存在を仮定して矛盾を導く。φ を変数 x_n に関する $\mathbb{F}_p[x_1, \ldots, x_{n-1}]$ 上の多項式とみなすと、x_n のある冪の係数は非零であるから、ある値 $(a_1, \ldots, a_{n-1})$ を代入すると値が非零となる。すると、$\varphi(a_1, \ldots, a_{n-1}, x_n)$ は x_n に関する零関数の零でない多項式表示となり、$n = 1$ の場合の結果に反する。よって命題 1 が成り立つ。 □

命題1で得られた関数 f の多項式表示を f の**最小多項式表示**と呼ぶ。命題1より、関数 f の最小多項式表示はただ一つ存在することを改めて強調しておく。また、以下が成り立つ。

命題 2. $f\colon (\mathbb{F}_p)^n \to \mathbb{F}_p$ の最小多項式表示は f のあらゆる多項式表示のうち最小の全次数を持つ。

証明. ϕ を f の多項式表示とする。もし、ある変数 x_i について ϕ が p 次以上であるとしたら、Fermat の小定理より、ϕ に現れる $x_i{}^p$ を x_i に取り替えたものも引き続き f の多項式表示である。この繰り返しで ϕ を f の（唯一の）最小多項式表示に変換できるが、この変換は全次数を増やさないので、ψ の全次数は最小多項式表示の全次数以上であることがわかる。よって命題2が成り立つ。 □

なお、対称関数の最小多項式表示について、いくつかの変数を入れ替えた結果もまたその対称関数の多項式表示であり、次数の条件も満たす。従って、最小多項式表示の一意性よりそれらの多項式は互いに等しい。これは対称関数の最小多項式表示もまた対称多項式であることを意味している。以下、混乱のない限り、$\mathbb{F}_p$ 上の関数とその最小多項式表示をしばしば同一視する。

3 足し算の繰り上がり関数

$x_1, \ldots, x_n \in \mathbb{F}_p$ として、関数 $\varphi_i\colon (\mathbb{F}_p)^n \to \mathbb{F}_p$ $(i = 0, 1, \ldots)$ の値を以下で定める。

$$\sum_{j=1}^{n} (x_j)_{\mathbb{Z}} = \sum_{i \geq 0} \varphi_i(x_1, \ldots, x_n)_{\mathbb{Z}} \cdot p^i$$

すなわち、整数 $\sum_{j=1}^{n} (x_j)_{\mathbb{Z}}$ の p 進法表示は $(\ldots, \varphi_1(x_1, \ldots, x_n)_{\mathbb{Z}}, \varphi_0(x_1, \ldots, x_n)_{\mathbb{Z}})_p$ である（$a_{\mathbb{Z}}$ のような記法の定義は2節を参照）。3.1節では、これらの関数 φ_i の最小多項式表示を導出する。それを踏まえて、3.2節では多項式を用いた p 進法整数の足し算アルゴリズムについて考察する。

3.1 多項式表示に関する結果

関数 φ_i の最小多項式表示について調べる。まず、$i = 0$ については（$\mathbb{F}_p$ 上の関係式として）$\varphi_0(x_1, \ldots, x_n) = \sum_{j=1}^{n} x_j$ が成り立つことと、$n(p-1) < p^i$ の範囲にある i については $\varphi_i = 0$ であることを注意しておく。以下の議論では、初等整数論における Lucas の定理 [3] を用いる（この定理のステートメントについては例えば [5] の Chapter 1 の Exercise 6.a にも記されている）。

命題 3 (Lucas [3]). 非負整数 a と b が $a = (a_M \ldots a_1 a_0)_p$、$b = (b_M \ldots b_1 b_0)_p$ と p 進法で表示されるとする（最高位の桁が0であってもよい）。このとき

$$\binom{a}{b} \equiv \binom{a_M}{b_M} \cdots \binom{a_1}{b_1} \binom{a_0}{b_0} \pmod{p}$$

が成り立つ。ただし $a' < b'$ のとき $\binom{a'}{b'} = 0$ と定めている。

我々の結果は以下の通りである。

定理 1. 各添字 $i \geq 0$ について、φ_i の最小多項式表示は

$$\varphi_i(x_1, \ldots, x_n) = \sum_{d_1, \ldots, d_n} \prod_{j=1}^{n} \mathrm{Inv}_p(d_j!) x_j (x_j - 1) \cdots (x_j - d_j + 1)$$

で与えられる（記法 $\mathrm{Inv}_p(a)$ については2節を参照）。ただし、上式右辺の和における添字は、$d_1 + \cdots + d_n = p^i$ を満たす $d_1, \ldots, d_n \in \{0, 1, \ldots, p-1\}$ 全てをわたるものとする。

証明. まず、命題3を $a=\sum_{j=1}^{n}(x_j)_{\mathbb{Z}}$ および $b=p^i$ に適用する（つまり、$b_i=1$ かつ、それ以外の添字 i' では $b_{i'}=0$ とする）ことで、等式

$$\varphi_i(x_1,\dots,x_n)_{\mathbb{Z}}=\binom{\varphi_i(x_1,\dots,x_n)_{\mathbb{Z}}}{1}\equiv\binom{\sum_{j=1}^{n}(x_j)_{\mathbb{Z}}}{p^i}\pmod{p}$$

が得られる。この右辺の二項係数は、$\sum_{j=1}^{n}(x_j)_{\mathbb{Z}}$ 個のものから p^i 個を選ぶ方法の総数に等しい。この $\sum_{j=1}^{n}(x_j)_{\mathbb{Z}}$ 個を、1番めが $(x_1)_{\mathbb{Z}}$ 個、2番めが $(x_2)_{\mathbb{Z}}$ 個、といった具合に n 区画に分けておき、全体から p^i 個を選んだ際に h 番めの区画から選ばれた個数を d_h と書く。するとそれらの値 $d_1,\dots,d_n$ は、上述の和に関する条件 $d_h\in\{0,1,\dots,p-1\}$ および $d_1+\cdots+d_n=p^i$ を満たし（前者については、定義より $(x_h)_{\mathbb{Z}}\leq p-1$ であることに注意されたい）、等式

$$\binom{\sum_{j=1}^{n}(x_j)_{\mathbb{Z}}}{p^i}=\sum_{d_1,\dots,d_n}\prod_{j=1}^{n}\binom{(x_j)_{\mathbb{Z}}}{d_j}$$

が得られる。さらに、これらの d_j について

$$\begin{aligned}\binom{(x_j)_{\mathbb{Z}}}{d_j}&=\frac{(x_j)_{\mathbb{Z}}((x_j)_{\mathbb{Z}}-1)\cdots((x_j)_{\mathbb{Z}}-d_j+1)}{d_j!}\\&\equiv \mathsf{Inv}_p(d_j!)_{\mathbb{Z}}(x_j)_{\mathbb{Z}}((x_j)_{\mathbb{Z}}-1)\cdots((x_j)_{\mathbb{Z}}-d_j+1)\pmod{p}\end{aligned}$$

が成り立つ。以上を合わせると、定理1の主張が導かれる。 □

例 1. $p=2$ のとき、定理1の和における添字 $d_1,\dots,d_n$ の条件は、$d_1,\dots,d_n\in\{0,1\}$ および $d_1+\cdots+d_n=p^i$ となる。すると、$S=\{j\in\{1,\dots,n\}\mid d_j=1\}$ と定めることで、定理1より

$$\varphi_i(x_1,\dots,x_n)=\sum_{S\subset\{1,\dots,n\},\,|S|=2^i}\prod_{j\in S}x_j=e_{2^i}(x_1,\dots,x_n)$$

が成り立ち、φ_i は 2^i 次の基本対称式となる。これは前述したBoyarらの結果[1]を再現している。

例 2. $p=3$ のとき、$i\leq 2$ における対称多項式 φ_i の表示を数学支援ソフトウェアSageによって計算した結果を以下に記す。ここで、m_λ、e_j および s_λ はそれぞれ単項対称多項式、基本対称多項式およびSchur多項式を表す。また計算の過程で、係数体が $\mathbb{Q}$ ではなく $\mathbb{F}_3$ であることに起因する関係をいくつか用いた。例えば、$\mathbb{F}_3$ 上では $a^3=a$ なので、$\mathbb{F}_3$ 上での値を考えると $m_{1^1 3^1}=2m_{1^2}=-m_{1^2}$ が成り立つ、といった具合である。

$$\varphi_0=m_{1^1}=e_1\ ,$$

$$\varphi_1=m_{1^3}-m_{1^1 2^1}-m_{1^2}=e_3-e_2e_1-e_2=-s_{1^1 2^1}-s_{1^2}\ ,$$

$$\begin{aligned}\varphi_2&=m_{1^9}-m_{1^8}-m_{1^7 2^1}-m_{1^6}+m_{1^5 2^2}-m_{1^5 2^1}-m_{1^5}+m_{1^4 2^2}-m_{1^4 2^1}-m_{1^3 2^3}+m_{1^2 2^3}+m_{1^1 2^4}\\&=e_9+e_8e_1-e_7e_2+e_7-e_6e_3-e_6e_1-e_6+e_5e_4+e_5e_3-e_5e_1-e_5\\&=(s_{1^9}-s_{1^5 2^2}+s_{1^1 2^4})+(s_{1^8}+s_{1^6 2^1}+s_{1^4 2^2}+s_{1^2 2^3})+(-s_{1^5 2^1})+(s_{1^6}-s_{1^4 2^1})+(-s_{1^5})\ .\end{aligned}$$

なお、$n=2$ の場合には、定理1は以下のように少々単純化できる（$n=2$ のとき、$2(p-1)<p^2$ なので、$i\geq 2$ については $\varphi_i=0$ であることに注意されたい）。

定理 2. $n=2$ のとき、$x_1,x_2\in\mathbb{F}_p$ について以下が成り立つ。

$$\varphi_1(x_1,x_2)=\sum_{d_1=1}^{p-1}(-1)^{d_1}\mathsf{Inv}_p(d_1)x_1(x_1-1)\cdots(x_1-d_1+1)x_2(x_2-1)\cdots(x_2-(p-d_1)+1)\ .$$

証明. 定理1の添字 d_1, d_2 は $d_2 = p - d_1$ を満たし、従って $1 \leq d_1 \leq p-1$ である。すると

$$\begin{aligned} d_2! &= (p-d_1)(p-d_1-1)\cdots 2\cdot 1 \\ &\equiv (-1)^{p-d_1} d_1(d_1+1)\cdots(p-2)(p-1) \pmod p \end{aligned}$$

である。一方、$(p-1)! \equiv (-1)^p \pmod p$ である。これは、奇素数 p について集合 $\mathbb{F}_p \setminus \{-1, 0, 1\}$ が $\{\alpha, \alpha^{-1}\}$ $(\alpha \neq \alpha^{-1})$ という形の互いに交わらない部分集合たちに分けられることから導かれる。これらを用いて

$$\mathsf{Inv}_p(d_1!d_2!) = \mathsf{Inv}_p((-1)^{p-d_1} d_1 \cdot (p-1)!) = (-1)^{d_1}\mathsf{Inv}_p(d_1)$$

が得られ、従って定理1より主張が成り立つ。 □

3.2 多項式を用いた p 進法の足し算

前述した暗号分野への応用と関連して、3.1節の結果を基に、多項式を用いた p 進法による n 個の非負整数 $a_h = (a_{h,m} \ldots a_{h,1}a_{h,0})_p$ $(h = 1, \ldots, n)$ の足し算アルゴリズムを与える。その際、整数 a_h の各桁 $a_{h,i}$ を、$\mathbb{F}_p$ の元と自然に同一視することとする。まず、d を、条件 $(n+d)(p-1) < p^{d+1}$ を満たす最小の非負整数とする。このとき

$$\begin{aligned} a_1 + \cdots + a_n \leq n(p^{m+1}-1) &= n(p-1)(p^m + \cdots + p + 1) \\ &< p^{d+1}(p^m + \cdots + p + 1) < p^{d+1}\cdot p^{m+1} = p^{m+d+2} \end{aligned}$$

なので、和 $c = a_1 + \cdots + a_n$ は高々 $m+d+2$ 桁で表される。すなわち $c = (c_{m+d+1}\cdots c_1 c_0)_p$ $(c_i \in \mathbb{F}_p)$ という形となる。すると、c の各桁や、足し算の過程で生じる繰り上がり $\gamma_{j,k} \in \mathbb{F}_p$ (ただし、$0 \leq j < k \leq m+d+1$ かつ $k \leq j+d$ という範囲の j と k について、$\gamma_{j,k}$ は j 桁めの計算で生じた k 桁めへの繰り上がりを表す) は以下のように計算できる。

- $i = 0, 1, \ldots, m+d+1$ の各々について以下を行う。まず、

  $$c_i \leftarrow \varphi_0(a_{1,i}, \ldots, a_{n,i}, \gamma_{i-d,i}, \gamma_{i-(d-1),i}, \cdots, \gamma_{i-1,i})$$

  とし、次に $i+k \leq m+d+1$ を満たす範囲における $k = 1, 2, \ldots, d$ の各々について、

  $$\gamma_{i,i+k} \leftarrow \varphi_k(a_{1,i}, \ldots, a_{n,i}, \gamma_{i-d,i}, \gamma_{i-(d-1),i}, \cdots, \gamma_{i-1,i})$$

  とする。なお、$i > m$ を満たす添字 i についての入力 $a_{1,i}, \ldots, a_{n,i}$ と、$i - j < 0$ を満たす添字 i, j についての入力 $\gamma_{i-j,i}$ は無視する。

条件 $(n+d)(p-1) < p^{d+1}$ より、$k > d$ の範囲では $\varphi_k(a_{1,i}, \ldots, a_{n,i}, \gamma_{i-d,i}, \gamma_{i-(d-1),i}, \cdots, \gamma_{i-1,i}) = 0$ である。このことから、上記のアルゴリズムは $a_1, \ldots, a_n$ の和を正しく計算することがわかる。

以下、二つの整数の足し算の場合 $(n = 2)$ をさらに考察する。この場合には、$2(p-1)+1 < p^2$ が成り立つため、各桁からその直後の桁への繰り上がりだけが発生し、また繰り上がりの値は0または1となる。このとき、上記のアルゴリズムで用いた多項式を少しだけ簡略化できる。

命題 4. $x_1, x_2 \in \mathbb{F}_p$ と $\gamma \in \{0, 1\} \subset \mathbb{F}_p$ について、多項式 φ' を

$$\varphi'(x_1, x_2, \gamma) = \varphi_1(x_1, x_2) + \gamma \cdot (1 - (x_1 + x_2 + 1)^{p-1})$$

と定義すると、$\varphi_1(x_1, x_2, \gamma) = \varphi'(x_1, x_2, \gamma)$ が成り立つ。

証明. 和 $(x_1)_{\mathbb{Z}}+(x_2)_{\mathbb{Z}}+\gamma_{\mathbb{Z}}$ について、x_1 と x_2 を決めたとき、次の桁への繰り上がりが $\gamma=1$ のときと $\gamma=0$ のときで異なるのは $x_1+x_2=p-1$ の場合にほかならない。その場合、$\gamma=1$ のとき繰り上がりは1であり、$\gamma=0$ のとき繰り上がりは0なので、いずれにせよ繰り上がりは γ に等しい。このことと、$\gamma=0$ の場合の繰り上がりが $\varphi_1(x_1,x_2)$ に等しいことから、

$$\varphi_1(x_1,x_2,\gamma)=\varphi_1(x_1,x_2)+\gamma\cdot\chi[x_1+x_2=p-1]$$

が成り立つ。さらに、Fermat の小定理より $\chi[x_1+x_2=p-1]=1-(x_1+x_2+1)^{p-1}$ が成り立つ。以上をまとめると命題4の主張が得られる。 □

さらに、不等式 $a_1+a_2\le 2(p^{m+1}-1)\le p(p^{m+1}-1)<p^{m+2}$ に注意すると、和 $c=a_1+a_2$ は高々 $m+2$ 桁で表されることがわかる。すなわち $c=(c_{m+1}\cdots c_1c_0)_p$（$c_i\in\mathbb{F}_p$）と表せる。このとき、以下の要領で足し算を計算できる。

- まず、$c_0\leftarrow a_{1,0}+a_{2,0}$ および $\gamma_{0,1}\leftarrow\varphi_1(a_{1,0},a_{2,0})$ とする。
- 次に、各 $i=1,\ldots,m$ について、$c_i\leftarrow a_{1,i}+a_{2,i}+\gamma_{i-1,i}$ および $\gamma_{i,i+1}\leftarrow\varphi'(a_{1,i},a_{2,i},\gamma_{i-1,i})$ とする。
- 最後に、$c_{m+1}\leftarrow\gamma_{m,m+1}$ とする。

上記の結果の暗号理論への応用について述べる。論文 [4] における完全準同型暗号の構成では、1節で言及した暗号文のノイズ成分除去手続きの過程で、暗号化された $\mathbb{F}_p$ の元二つに対する足し算が繰り返し行われる。そこでは、定理1で $n=2$ としたものと本質的に同じ結果が用いられている（ただし、証明は本稿とは異なる）。一方、$n=2$ における改良された結果（定理2および命題4）に相当する結果は論文 [4] では言及されていない。これらの結果を適用することで、論文 [4] の完全準同型暗号の構成をさらに効率化できる可能性がある。この点は今後の研究課題とする。

4 掛け算の繰り上がり関数

$x,y\in\mathbb{F}_p$ として、関数 $\psi_0,\psi_1\colon(\mathbb{F}_p)^2\to\mathbb{F}_p$ の値を以下で定める。

$$x_{\mathbb{Z}}\cdot y_{\mathbb{Z}}=\psi_1(x,y)_{\mathbb{Z}}\cdot p+\psi_0(x,y)_{\mathbb{Z}}$$

すなわち、整数 $x_{\mathbb{Z}}\cdot y_{\mathbb{Z}}$ の p 進法での表示は $(\psi_1(x,y)_{\mathbb{Z}},\psi_0(x,y)_{\mathbb{Z}})_p$ である（$a_{\mathbb{Z}}$ といった記法の定義は2節を参照）。ここで、（$\mathbb{F}_p$ 上の関係式として）$\psi_0(x,y)=xy$ が成り立つ。また、$(p-1)^2<p^2$ なので、積 $x_{\mathbb{Z}}\cdot y_{\mathbb{Z}}$ は高々2桁で表示できる。さらに、$p=2$ ならば明らかに $\psi_1=0$ なので、以下では $p>2$ の場合のみを取り扱う。4.1節では、この関数 ψ_1 の最小多項式表示を導出する。それを踏まえて、4.2節では多項式を用いた p 進法の整数二つの掛け算アルゴリズムについて考察する。

4.1 多項式表示に関する結果

関数 $\psi_1(x,y)$ の最小多項式表示について調べる。我々の結果は以下の通りである。

定理 3. p を奇素数とする。また、$2\le i\le p-3$ を満たす偶数 i の各々に対し、$\mathbb{F}_p$ の非零元 ξ_i を $\xi_i^{\,i}\neq 1$ となるよう選んでおく（例えば、法 p における原始根など）。このとき、$x,y\in\mathbb{F}_p$ について

$$\psi_1(x,y)=xy(\Psi(xy)-\Psi(x)-\Psi(y)+\Psi(1))$$

が成り立つ。ただし、多項式 $\Psi(t)$ を

$$\Psi(t) = \sum_{\substack{2\le i\le p-3 \\ i;even}} \left(-\mathrm{Inv}_p(\xi_i(\xi_i{}^i - 1)) \sum_{\zeta=1}^{\xi_i-1} \sum_{k\in I_{\xi_i,\zeta}} \zeta k^{p-i-2} \right) t^i + \frac{p-1}{2} t^{p-2}$$

で定義し（記法 $\mathrm{Inv}_p(a)$ については2節を参照）、また、各 $\xi,\zeta \in \mathbb{F}_p$ ごとに $I_{\xi,\zeta}$ を下記で定める。

$$I_{\xi,\zeta} := \{ z \in \mathbb{F}_p \mid p\cdot\zeta_{\mathbb{Z}} \le (z\xi)_{\mathbb{Z}} < p\cdot(\zeta_{\mathbb{Z}}+1) \} \ .$$

注意 1. 最小多項式表示の一意性より、定理3で元 ξ_i をどのように選んでも、得られる ψ_1 の表示（あるいは同じことだが、Ψ の表示）は同一となる。このことから、$2\le i\le p-3$ を満たす偶数 i の各々について、定理3での Ψ の表示における t^i の係数

$$-\mathrm{Inv}_p(\xi_i(\xi_i{}^i-1)) \sum_{\zeta=1}^{\xi_i-1} \sum_{k\in I_{\xi_i,\zeta}} \zeta k^{p-i-2}$$

は、前述した $\xi_i{}^i \neq 1$ を満たす元 $\xi_i \in \mathbb{F}_p \setminus \{0\}$ の選び方によらず一定値となることがわかる。

定理3の証明. 命題1より、関数 ψ_1 は $\psi_1(x,y) = \sum_{i,j=0}^{p-1} \alpha_{i,j} x^i y^j$ という形に一意的に表せる。掛け算の対称性より $\alpha_{i,j} = \alpha_{j,i}$ であることに注意されたい。以下、この係数 $\alpha_{i,j} \in \mathbb{F}_p$ を決定する。

まず、$y=0$ のとき $\psi_1(x,y)=0$ であるから、$\psi_1(x,0) = \sum_{i=0}^{p-1} \alpha_{i,0} x^i$ は零関数の最小多項式表示、すなわち零多項式となる。従って、各添字 i について $\alpha_{i,0} = \alpha_{0,i} = 0$ が成り立つ。

次に、各 $x,y,z \in \mathbb{F}_p$ について、

$$\begin{aligned} (x_{\mathbb{Z}}\cdot y_{\mathbb{Z}})\cdot z_{\mathbb{Z}} &= \big(\psi_1(x,y)_{\mathbb{Z}}\cdot p + (xy)_{\mathbb{Z}}\big)\cdot z_{\mathbb{Z}} \\ &= \big(\psi_1(x,y)_{\mathbb{Z}}\cdot z_{\mathbb{Z}}\big)\cdot p + (xy)_{\mathbb{Z}}\cdot z_{\mathbb{Z}} \\ &\equiv \big(\psi_1(x,y)z\big)_{\mathbb{Z}}\cdot p + \psi_1(xy,z)_{\mathbb{Z}}\cdot p + ((xy)z)_{\mathbb{Z}} \pmod{p^2} \\ &\equiv \big(\psi_1(x,y)z + \psi_1(xy,z)\big)_{\mathbb{Z}}\cdot p + (xyz)_{\mathbb{Z}} \pmod{p^2} \end{aligned} \tag{1}$$

が成り立ち、同様に

$$x_{\mathbb{Z}}\cdot(y_{\mathbb{Z}}\cdot z_{\mathbb{Z}}) \equiv \big(x\psi_1(y,z) + \psi_1(x,yz)\big)_{\mathbb{Z}}\cdot p + (xyz)_{\mathbb{Z}} \pmod{p^2} \tag{2}$$

も成り立つ。ここで、掛け算の結合法則により (1) 式と (2) 式は等しいので、それらの p^1 の桁を比較することで、各 $x,y,z\in\mathbb{F}_p$ について

$$\psi_1(x,y)z + \psi_1(xy,z) = x\psi_1(y,z) + \psi_1(x,yz)$$

が得られる。すなわち

$$\sum_{i,j=1}^{p-1} \alpha_{i,j} x^i y^j z + \sum_{i,j=1}^{p-1} \alpha_{i,j} x^i y^i z^j = \sum_{i,j=1}^{p-1} \alpha_{i,j} x y^i z^j + \sum_{i,j=1}^{p-1} \alpha_{i,j} x^i y^j z^j \tag{3}$$

である。両辺は各変数に関して $p-1$ 次以下なので、最小多項式表示の一意性より両辺は多項式として一致する。すると、まず $i\neq j$ であるような添字 $i,j\ge 2$ について、(3) 式の両辺における $x^i y^j z$ の係数を比較することで $\alpha_{i,j}=0$ が得られる。また、$i\ge 2$ のとき、両辺における $x^i y^i z$ の係

数を比較することで、$\alpha_{i,i}+\alpha_{i,1}=0$ すなわち $\alpha_{i,1}=-\alpha_{i,i}$ が得られる。対称性より、$\alpha_{1,i}=-\alpha_{i,i}$ が同様にして得られる。以上をまとめると、

$$\begin{aligned}\psi_1(x,y)&=\alpha_{1,1}xy+\sum_{i=2}^{p-1}\alpha_{i,i}\big(x^iy^i-x^iy-xy^i\big)\\&=xy\big(\Psi(xy)-\Psi(x)-\Psi(y)+\alpha_{1,1}\big)\end{aligned}\tag{4}$$

が得られる。ここで、$\Psi(t)=\sum_{i=1}^{p-2}\beta_it^i$ かつ各添字 i について $\beta_i:=\alpha_{i+1,i+1}$ と定めている。この Ψ は定数項を持たない高々 $p-2$ 次の多項式であることを注意しておく。さて、

$$0=\psi_1(1,1)=\Psi(1)-\Psi(1)-\Psi(1)+\alpha_{1,1}=\alpha_{1,1}-\Psi(1)$$

であるから、$\alpha_{1,1}=\Psi(1)$ が成り立つ。ここまでの議論により、示すべきことの残りは Ψ が定理の主張にあるような形であることのみである。

まず、$x\in\mathbb{F}_p\setminus\{0\}$ について

$$x-1=\psi_1(x,p-1)=-x\big(\Psi(-x)-\Psi(x)-\Psi(-1)+\Psi(1)\big)$$

が成り立つ。ここで Fermat の小定理より $x^{p-1}=1$ であることを用いると、

$$\Psi(x)-\Psi(-x)+\Psi(-1)-\Psi(1)=x^{p-2}(x-1)=x^{p-1}-x^{p-2}$$

が $x\in\mathbb{F}_p\setminus\{0\}$ の各々について成り立つことが導かれる。そして、残りの $x=0$ については、上式の左辺は $\Psi(-1)-\Psi(1)$、右辺は 0 となる。ここで、全ての $x\in\mathbb{F}_p$ について $\chi[x=0]=1-x^{p-1}$ が成り立つことを用いると、上式の両辺の差を補正することができて、全ての $x\in\mathbb{F}_p$ について

$$\Psi(x)-\Psi(-x)+\Psi(-1)-\Psi(1)=x^{p-1}-x^{p-2}+(1-x^{p-1})(\Psi(-1)-\Psi(1))$$

すなわち

$$\Psi(x)-\Psi(-x)=(1-\Psi(-1)+\Psi(1))x^{p-1}-x^{p-2}$$

が導かれる。最小多項式表示の一意性より、これらは多項式として等しくなる。特に、Ψ は $p-2$ 次以下なので、$1-\Psi(-1)+\Psi(1)=0$ であり、従って $\Psi(x)-\Psi(-x)=-x^{p-2}$ となる。今、p は奇数であり、また $1\le k\le p-2$ の範囲で $\Psi(x)-\Psi(-x)$ における x^k の係数は、k が偶数ならば 0、k が奇数ならば $2\beta_k$ である。このことから、$\beta_{p-2}=\mathsf{Inv}_p(-2)=(p-1)/2$ および、$k\le p-4$ の範囲で奇数の k について $\beta_k=0$ が導かれる。

次に、$2\le i\le p-3$ の範囲で偶数の i について、定理の主張のように $\xi_i\in\mathbb{F}_p$ を選ぶと、$\psi_1(x,\xi_i)=\xi_ix(\Psi(\xi_ix)-\Psi(x)-\Psi(\xi_i)+\Psi(1))$ における x^{i+1} の係数は $\beta_i\xi_i(\xi_i{}^i-1)$ となる。一方、各 $\zeta\in\{0,1,\dots,\xi_i-1\}$ について、集合 $I_{\xi_i,\zeta}$ を定理の主張にあるように定めると、全ての $x\in I_{\xi_i,\zeta}$ について $\psi_1(x,\xi_i)=\zeta$ が成り立つ。このことから、

$$\psi_1(x,\xi_i)=\sum_{\zeta=1}^{\xi_i-1}\sum_{k\in I_{\xi_i,\zeta}}\zeta\cdot\chi[x=k]=\sum_{\zeta=1}^{\xi_i-1}\sum_{k\in I_{\xi_i,\zeta}}\zeta(1-(x-k)^{p-1})$$

が導かれる。右辺における x^{i+1} の係数は

$$-\sum_{\zeta=1}^{\xi-1}\sum_{k\in I_{\xi,\zeta}}\zeta\binom{p-1}{i+1}(-k)^{p-i-2}=\binom{p-1}{i+1}\sum_{\zeta=1}^{\xi-1}\sum_{k\in I_{\xi,\zeta}}\zeta k^{p-i-2}$$

である（iは偶数でありpは奇数であることに注意されたい）。さらに、$\mathbb{F}_p$において

$$\binom{p-1}{i+1} = \frac{(p-1)(p-2)\cdots(p-i-1)}{(i+1)i\cdots 1} = \frac{(-1)(-2)\cdots(-(i+1))}{(i+1)i\cdots 1} = (-1)^{i+1} = -1$$

が成り立つ（今、$i+1$は奇数であることに注意されたい）。以上を合わせると、

$$\beta_i \xi_i({\xi_i}^i - 1) = -\sum_{\zeta=1}^{\xi-1} \sum_{k \in I_{\xi,\zeta}} \zeta k^{p-i-2}$$

すなわち（ξ_iの選び方から${\xi_i}^i - 1 \neq 0$なので）

$$\beta_i = -\mathrm{Inv}_p(\xi_i({\xi_i}^i - 1)) \sum_{\zeta=1}^{\xi_i-1} \sum_{k \in I_{\xi_i,\zeta}} \zeta k^{p-i-2}$$

が導かれる。よって定理3が成り立つ。 □

一般の関数$(\mathbb{F}_p)^2 \to \mathbb{F}_p$を考えると、その最小多項式表示は最大で$p^2$個の単項式からなる。それと比べて、上述した$\psi_1$の多項式表示はそれよりかなり少ない$(3p-1)/2$個の単項式からなる。この意味では、掛け算の繰り上がり関数は一般の関数よりも比較的単純であるといえよう。

例 3. 2がpを法とする原始元である場合、定理3に現れる元ξ_iとして常に$\xi_i = 2$を用いることで、ψ_1の表示を簡略化できる。すなわち、$I_{2,1} = \{(p+1)/2, \ldots, p-1\}$が成り立つことから、

$$\begin{aligned}\Psi(t) &= \sum_{\substack{2 \le i \le p-3 \\ i:\text{even}}} \left(-\mathrm{Inv}_p(2(2^i-1)) \sum_{k=(p+1)/2}^{p-1} k^{p-i-2} \right) t^i + \frac{p-1}{2} t^{p-2} \\ &= \sum_{\substack{2 \le i \le p-3 \\ i:\text{even}}} \left(\mathrm{Inv}_p(2(2^i-1)) \sum_{k=1}^{(p-1)/2} k^{p-i-2} \right) t^i + \frac{p-1}{2} t^{p-2}\end{aligned}$$

が得られる（pが奇数なので、偶数iについて$-k^{p-i-2} \equiv (-k)^{p-i-2} \pmod p$であることに注意されたい）。例えば$p=3$のとき、$\Psi(t) = t$となり、従って以下が成り立つ。

$$\psi_1(x,y) = xy(xy - x - y + 1) = x(x-1)y(y-1) \ .$$

である。また、$p=5$のとき、$\Psi(t) = 2t^3 + 3t^2$となり、従って以下が成り立つ。

$$\psi_1(x,y) = xy(2x^3y^3 + 3x^2y^2 - 2x^3 - 3x^2 - 2y^3 - 3y^2) \ .$$

4.2 多項式を用いたp進法の掛け算

ここでは、4.1節の結果を基に、p進法による二つの非負整数$a_1 = (a_{1,m_1} \cdots a_{1,1}a_{1,0})_p$と$a_2 = (a_{2,m_2} \cdots a_{2,1}a_{2,0})_p$の掛け算アルゴリズムについて考察する。その際、整数a_hの各桁$a_{h,i}$を、$\mathbb{F}_p$の元と自然に同一視する。なお、4.1節と同様に$p > 2$の場合のみを取り扱う。

まず、積$c = a_1a_2$は高々$m_1 + m_2 + 2$桁で表せる。すなわち$c = (c_{m_1+m_2+1} \cdots c_1c_0)_p$（$c_i \in \mathbb{F}_p$）という形となる。すると、$c$の各桁は以下のように計算できる。ここで$\gamma$は、各桁から次の桁への繰り上がりを表す補助的な変数である。

- まず、以下の計算を行う。
  - $c_0 \leftarrow a_{1,0}a_{2,0}$（積は$\mathbb{F}_p$上で考える）および$\gamma \leftarrow \psi_1(a_{1,0}, a_{2,0})$とする。
  - $i = 1, \ldots, m_1$の各々に対し、$c_i \leftarrow a_{1,i}a_{2,0} + \gamma$とし、また$\gamma$を以下のように更新する。

$$\gamma \leftarrow \psi_1(a_{1,i}, a_{2,0}) + \varphi_1(a_{1,i}a_{2,0}, \gamma) \ .$$

  - そして、$c_{1,m_1+1} \leftarrow \gamma$とする。
- $j = 1, \ldots, m_2$の各々について、以下の計算を行う。
  - c_jとγを、$(c_j, \gamma) \leftarrow \big(a_{1,0}a_{2,j} + c_j, \psi_1(a_{1,0}, a_{2,j}) + \varphi_1(a_{1,0}a_{2,j}, c_j)\big)$と更新する。
  - $i = 1, \ldots, m_1 - 1$の各々に対し、c_{i+j}とγを以下のように更新する。

$$(c_{i+j}, \gamma) \leftarrow \big(a_{1,i}a_{2,j} + c_{i+j} + \gamma, \psi_1(a_{1,i}, a_{2,j}) + \varphi_1(a_{1,i}a_{2,j}, c_{i+j}, \gamma)\big) \ .$$

  - 最後に、c_{m_1+j}を$c_{m_1+j} \leftarrow a_{1,m_1}a_{2,j} + c_{m_1+j} + \gamma$で更新し、$c_{m_1+j+1}$を以下で更新する。

$$c_{m_1+j+1} \leftarrow \psi_1(a_{1,m_1}, a_{2,j}) + \varphi_1(a_{1,m_1}a_{2,j}, c_{m_1+j}, \gamma) \ .$$

上記のアルゴリズムにおいて、添字i, jの各々について

$$a_{1,i}a_{2,j} + c_{i+j} + \gamma \leq (p-1)^2 + 2(p-1) = p^2 - 1$$

が成り立つことから、$i+j$桁めの更新で現れる数は高々2桁で表され、従って$k \geq 2$に対するφ_kは不要である。このことから、このアルゴリズムが積$c = a_1a_2$を正しく計算することがわかる。

謝辞 本研究に際して、黒澤馨氏および、山田翔太氏、江村恵太氏、花岡悟一郎氏をはじめとする新明るい暗号勉強会の参加者諸氏よりコメントをいただいたので深く感謝する。

参考文献

[1] J. Boyar, R. Peralta, and D. Pochuev. On the multiplicative complexity of Boolean functions over the basis (cap, +, 1). Theor. Comput. Sci. vol.235, no.1, 43–57 (2000)

[2] C. Gentry. Fully homomorphic encryption using ideal lattices. in: Proceedings of STOC 2009, 169–178 (2009)

[3] E. Lucas. Théorie des fonctions numériques simplement périodiques. Amer. J. Math. vol.1, no.3, 197–240 (1878)

[4] K. Nuida, and K. Kurosawa. (Batch) fully homomorphic encryption over integers for non-binary message spaces. EUROCRYPT 2015, to appear. Preprint available at IACR Cryptology ePrint Archive 2014/777 (2014), `http://eprint.iacr.org/2014/777`

[5] R. P. Stanley. Enumerative Combinatorics, Volume I (first edition). Cambridge University Press (1997)