多値論理関数と誤り訂正符号

Multiple-valued Logic Functions and Error-correcting Codes

松井 一 Hajime MATSUI

アブストラクト 多値論理関数とは、入出力が有限体である多変数関数であり、スイッチング回路の構成に応用がある。多値論理多項式とは、有限体係数の多変数多項式であり、多値論理関数は多値論理多項式と全体として等しいという事実がある。誤り訂正符号と多値論理多項式とは双対のような関係にあるため、誤り訂正符号の研究成果を多値論理多項式に応用できる。本稿では、「畳込み定理」と呼ばれる、多値論理関数と多値論理多項式の間の離散フーリエ変換を介して成り立つ関係を、有限体の半群と呼ばれる部分集合に対して一般化した定理について述べる。次に、この定理を多値論理多項式同士の積の高速化に応用する。最後に、多値論理関数と誤り訂正符号の関係を表すものとして、双対符号を明示的に与える一つの方法を示す。

キーワード 多値論理多項式, 有限体, 離散フーリエ変換, 畳込み定理, 双対符号

Abstract A multiple-valued logic function is a multivariable function whose input and output are in a finite field and is applied to the construction of switching circuits. A multiple-valued logic polynomial is a multivariable polynomial with coefficients in a finite field. It is known that multiple-valued logic functions are equal to multiple-valued logic polynomials. Because error-correcting codes and multiple-valued logic polynomials have a dual relationship with each other, the research results of error-correcting codes can be employed to multiple-valued logic polynomials. In this study, a generalized “convolution theorem” is described, which is a relationship between multiple-valued logic functions and polynomials through discrete Fourier transforms, and it is generalized to a subset of finite fields called a semigroup. Next, this theorem is applied to speed up the multiplication of multiple-valued logic polynomials. Finally, to show a relationship between multiple-valued logic functions and error-correcting codes, a method of explicitly obtaining dual codes is given.

Key words Multiple-valued logic polynomials, finite fields, discrete Fourier transforms, convolution theorem, dual codes

1. はじめに：多値論理関数とは？

本稿は、2018年3月8日、東京理科大学葛飾キャンパスで開催された情報理論研究会における発表⁽¹⁾の内容に加筆・修正を行ったものである。

まず、論理関数とは、 $\mathbb{F}_2$ を二元体 $\mathbb{F}_2 = \{0, 1\}$ とするとき、

$$F : (\mathbb{F}_2)^n \rightarrow \mathbb{F}_2$$

というある関数 F のこととする。ただし n は正の整数である。つまり論理関数とは、 $\mathbb{F}_2$ の n 入力 1 出力の関数のことである。
[例 1] (論理関数) $n = 2$ とする。論理関数は $F : (\mathbb{F}_2)^2 \rightarrow \mathbb{F}_2$ である F を一つ定めれば決まるから、表 1 で F を定めることができる。

表 1 論理関数の数値例 $x_1, x_2 = 0, 1$ の組合せ全てに対し $0, 1$ の値を一つずつ定める。

x_1	x_2	$F(x_1, x_2)$
0	0	1
1	0	0
0	1	1
1	1	1

このような論理関数は、3-SAT やブール代数、またデジタル論理回路理論等で用いられている^{(2)~(4)}。さて、論理関数の中には、論理多項式と呼ばれるものがある。論理多項式は $\mathbb{F}_2$ 係数の多項式で作られる論理関数の特別なものである。

[例 2] (論理多項式) 例 1 の F は、論理多項式 $f(x_1, x_2) = 1 + x_1 + x_1x_2$ と出力が同じである。実際、 $f(0, 0) = 1$, $f(1, 0) = 0$, $f(0, 1) = 1$, $f(1, 1) = 1$ を直接確かめることができる。ただし $\mathbb{F}_2$ の演算 $1 + 1 = 0$ に注意する。

例 2 では、論理関数が論理多項式で表された。実はこれは一般的に言えることで、全ての論理関数は論理多項式で表されることが知られている⁽⁵⁾。

次に、多値論理関数とは、 $\mathbb{F}_q$ を q 元体 (q はある素数の累乗)

松井 一 正員 豊田工業大学工学部
E-mail matsui@toyota-ti.ac.jp
Hajime MATSUI, Member (Undergraduate School of Engineering,
Toyota Technological Institute, Nagoya-shi, 468-8511 Japan).
電子情報通信学会 基礎・境界サイエンス
Fundamentals Review Vol.12 No.3 pp.182-190 2019 年 1 月
©電子情報通信学会 2019

とするとき、

$$F : (\mathbb{F}_q)^n \rightarrow \mathbb{F}_q$$

というある関数 F のこととする。もちろん $q = 2$ ならば多値論理関数は論理関数に一致する。多値論理関数は、論理関数を効率化・高速化するものとして期待されており、既に多数の研究成果がある^{(6), (7)}。さて、多値論理関数の中にも、多値論理多項式と呼ばれるものがある。多値論理多項式は $\mathbb{F}_q$ 係数の多項式で作られる多値論理関数の特別なものである。実は、全ての多値論理関数は多値論理多項式で表されることも知られている。

[定理 1] ⁽⁵⁾ 多値論理関数 F に対し、ある多値論理多項式

$$f = f(x_1, \dots, x_n) = \sum_{a_1=0}^{q-1} \cdots \sum_{a_n=0}^{q-1} f(a_1, \dots, a_n) x_1^{a_1} \cdots x_n^{a_n} \quad (1)$$

(ただし $f(a_1, \dots, a_n) \in \mathbb{F}_q$) があって、全ての $(\omega_1, \dots, \omega_n) \in (\mathbb{F}_q)^n$ に対し $f(\omega_1, \dots, \omega_n) = F(\omega_1, \dots, \omega_n)$ となる。

n と q を定めると、多値論理関数は q^{q^n} 個ある。一方、式 (1) のタイプの多項式も q^{q^n} 個ある。 q^{q^n} 個の多値論理多項式は全て異なる多値論理関数を定めることが示される（この事実をここでは「Vandermonde 型補題」と呼ぶことにする）ので、定理 1 が従う。

多値論理関数 F から多値論理多項式 f を求めるには、 f の係数を未知変数とする連立一次方程式を解けばよい。その際の計算量 ($\mathbb{F}_q$ における四則演算の回数) は、サイズ q^n の正方行列をベクトルに掛けるので $O(q^{2n})$ 、つまり q^{2n} のオーダーとなる。（ F が変わっても正方行列は変わらないので、逆行列を求める計算量は考慮しなかった。）実は、 F から f を求める計算量は、後で述べる手法を用いることにより、 $O(nq^{n+1})$ でできる。このように、定理 1 では単に F と f が 1 対 1 対応しているだけでなく、高速に F から f を求めることができると言ってもよい。

一般化として、多値論理関数 $F : (\mathbb{F}_q)^n \rightarrow \mathbb{F}_q$ の $(\mathbb{F}_q)^n$ を、 $(\mathbb{F}_q)^n$ の勝手な部分集合にしたときには、このような高速な F から f の構成法は知られていない。例外のケースとしては、「 $\mathbb{F}_q$ の巡回部分群の直積」と呼ぶべき部分集合については、やはり高速に F から f を構成することができる。このときの多値論理関数は $F : C_n \rightarrow \mathbb{F}_q$ である関数 F である。ただし C_n は、 $i = 1, \dots, n$ について $q-1$ の約数 d_i により

$$C_n = \{(\omega_1, \dots, \omega_n) \in (\mathbb{F}_q)^n \mid \omega_i^{d_i} = 1\} \quad (2)$$

と表される部分集合である。 $\mathbb{F}_q$ の元のうち $\omega_i^{d_i} = 1$ を満たすものは d_i 個あり、巡回群となるため、有限体上の離散フーリエ変換を用いることができ、高速に F から f を構成できる。しかし、この C_n は 0 を含まない、つまり $\omega_i = 0$ は $\omega_i^{d_i} = 1$ を満たさないで、「論理」という用途で用いるには適さないという問題がある。よって、0 を含む次の集合

$$\Omega_n = \{(\omega_1, \dots, \omega_n) \in (\mathbb{F}_q)^n \mid \omega_i^{d_i+1} = \omega_i\} \quad (3)$$

について、 $F : \Omega_n \rightarrow \mathbb{F}_q$ である関数 F から多値論理多項式 f を高速に求めたい。式 (3) の条件式 $\omega_i^{d_i+1} = \omega_i$ は、式 (2) の

条件式 $\omega_i^{d_i} = 1$ と比較すると、両辺に ω_i が乗じてある違いがあるだけであるが、 $\omega_i = 0$ のとき $\omega_i^{d_i} = 1$ は成り立たないが $\omega_i^{d_i+1} = \omega_i$ は成り立つため、 Ω_n には $\omega_i = 0$ となる点も含まれる。 $\mathbb{F}_q$ の半群（つまり積について閉じている $\mathbb{F}_q$ の部分集合）は 0 を含むならばこのような形に書けることが示されるから、 Ω_n は「 $\mathbb{F}_q$ の半群の直積」と呼ぶべき部分集合である。このとき定理 1 の Ω_n についての一般化は次のように述べることができる。

[定理 2] ⁽⁸⁾ 多値論理関数 $F : \Omega_n \rightarrow \mathbb{F}_q$ に対し、ある多値論理多項式

$$f = f(x_1, \dots, x_n) = \sum_{a_1=0}^{d_1} \cdots \sum_{a_n=0}^{d_n} f(a_1, \dots, a_n) x_1^{a_1} \cdots x_n^{a_n} \quad (4)$$

(ただし $f(a_1, \dots, a_n) \in \mathbb{F}_q$) があって、全ての $(\omega_1, \dots, \omega_n) \in \Omega_n$ に対し $f(\omega_1, \dots, \omega_n) = F(\omega_1, \dots, \omega_n)$ となる。

n, q, d_i を定めると、このような多値論理関数は $q^{\prod_{i=1}^n (d_i+1)}$ 個ある。一方、式 (4) のタイプの多項式も $q^{\prod_{i=1}^n (d_i+1)}$ 個あり、実際これらは全て異なる多値論理関数を定める（Vandermonde 型補題）ことが示されるので、定理 2 が従う。また、 F から f を求める際、 f の係数を未知変数とする連立一次方程式を解くと、計算量は $O(\prod_{i=1}^n (d_i+1)^2)$ となるが、後で述べる手法を用いることにより、 $O((\sum_{i=1}^n (d_i+1)) \prod_{i=1}^n (d_i+1))$ とできる。この計算量は $d_i+1 = q$ のときは $O(nq^{n+1})$ となるから、定理 1 の一般化となっている。

以下においては、この F から f の構成を、 f 同士の積の高速化に応用する。その際、基礎となるのは「畳込み定理」である。畳込み定理はフーリエ変換の理論ではよく知られており、 $\mathcal{F}$ をフーリエ変換、 f, g を実数上の性質の良い関数とすると

$$\mathcal{F}\left(\int f(\tau)g(t-\tau)d\tau\right) = \mathcal{F}(f)\mathcal{F}(g) \quad (5)$$

という等式が成り立つという定理である。式 (5) を多値論理多項式に対して示した畳込み定理を次章以降で解説する。

最後に、誤り訂正符号について、多値論理関数の観点から述べる。これまでに用意してきた道具立てを用いて、誤り訂正符号とその双対符号が多数得られ、その中には有効なものも含まれることを示す。一例として、拡大リードソロモン符号と呼ばれる誤り訂正符号の最小距離が求まる。多値論理関数と誤り訂正符号の関係が完全に分かるわけではないが、よく似た方法で両者を扱うことができる事実は興味深い。

本稿の構成は以下のようになっている。**2.** は本稿で用いる記号の準備である。**3.** は多値論理関数と多値論理多項式のそれぞれの積を定める。**4.** は離散フーリエ変換の拡張である代入写像について述べた後、畳込み定理について解説する。**5.** は代入写像のテンソル分解を用いた高速計算法について述べる。**6.** は代入写像の逆写像についてであり、多値論理関数から対応する多値論理多項式を与える写像となる。**7.** は多値論理多項式の積の計算量についてまとめる。**8.** は次章への準備として、代入写像の転置と呼ぶべき写像を導入する。**9.** は代入写像を用いて誤り

訂正符号とその双対符号を構成する。10. にまとめを述べる。

本稿を読むための予備知識としては、有限体及び線形代数の基礎を知っていればよい。代数学、特に商環を使っているところもあるが、そのところは高校で習う1変数多項式による除法の知識で読めるように書いたつもりである。9. では初歩の誤り訂正符号の知識を必要とする。研究室で学生に教えた印象では、論理関数や多値論理関数の話は、理解するために必要な予備知識が比較的少なく済むと感じる。また本稿では数値例をたくさん挙げたので、確認しながら読み進めて行くことができる。

2. 準備

多値論理関数を表す記号を準備する。

$$(\mathbb{F}_q)^{\Omega_n} = \{c = (c_\omega)_{\omega \in \Omega_n} \mid c_\omega \in \mathbb{F}_q \text{ for all } \omega \in \Omega_n\} \quad (6)$$

と置く。\$(\mathbb{F}_q)^{\Omega_n}\$ は \$\Omega_n\$ の全ての元で添え字付けられた (要するに並べられた) \$\mathbb{F}_q\$ 上の線形空間となり、次元は \$\Omega_n\$ の要素数 \$|\Omega_n| = \prod_{i=1}^n (d_i + 1)\$ に等しい。このとき、多値論理関数 \$F: \Omega_n \rightarrow \mathbb{F}_q\$ は、\$(\mathbb{F}_q)^{\Omega_n}\$ のある元と同一視できる。なぜならば、\$F\$ から \$c_\omega = F(\omega)\$ として \$(c_\omega)_{\omega \in \Omega_n} \in (\mathbb{F}_q)^{\Omega_n}\$ が定まるからである。逆に、任意に \$(c_\omega)_{\omega \in \Omega_n} \in (\mathbb{F}_q)^{\Omega_n}\$ を一つ持って来ると、全ての \$\omega \in \Omega_n\$ について \$\mathbb{F}_q\$ の値 \$c_\omega\$ が定まるので、\$F(\omega) = c_\omega\$ とすることで \$F\$ が定まる。こうして \$(\mathbb{F}_q)^{\Omega_n}\$ は、\$\Omega_n\$ 上の多値論理関数全体と一致する。

[例 3] (多値論理関数) \$n = 1, q = 7, d_1 = 3\$ とすると、\$\Omega_1 = \{0, 2, 4, 1\}\$ となり、\$(\mathbb{F}_7)^{\Omega_1}\$ の元としては例えば

$$c = (c_\omega)_{\omega \in \Omega_1} = (c_0 \ c_2 \ c_4 \ c_1) = (2 \ 5 \ 2 \ 0) \in (\mathbb{F}_7)^{\Omega_1}. \quad (7)$$

この \$c\$ の成分の並べ方、特に添え字の付け方 \$0, 2, 4, 1\$ は、文献(8)に合わせた (詳細は、後の注意 1)。

次に、\$n = 2, q = 2, d_1 = 1, d_2 = 1\$ とすると、\$\Omega_2 = \{(0, 0), (1, 0), (0, 1), (1, 1)\}\$ となり、\$(\mathbb{F}_2)^{\Omega_2}\$ の元としては例えば

$$c = (c_\omega)_{\omega \in \Omega_2} = (c_{(0,0)} \ c_{(1,0)} \ c_{(0,1)} \ c_{(1,1)}) = (1 \ 0 \ 1 \ 1) \quad (8)$$

があり、式 (8) は例 1 の \$F\$ に対応するものである。

\$n = 2, q = 7, d_1 = 2, d_2 = 3\$ とすると、\$\Omega_2 = \{(0, 0), (0, 2), \dots, (6, 0), \dots, (1, 1)\}\$ となり、\$(\mathbb{F}_7)^{\Omega_2}\$ の元としては例えば

$$c = (c_\omega)_{\omega \in \Omega_2} = \begin{pmatrix} c_{(0,0)} & c_{(0,2)} & c_{(0,4)} & c_{(0,1)} \\ c_{(6,0)} & c_{(6,2)} & c_{(6,4)} & c_{(6,1)} \\ c_{(1,0)} & c_{(1,2)} & c_{(1,4)} & c_{(1,1)} \end{pmatrix} = \begin{pmatrix} 4 & 3 & 5 & 3 \\ 6 & 3 & 5 & 6 \\ 1 & 3 & 0 & 5 \end{pmatrix}. \quad (9)$$

次に、多値論理多項式を表す記号を準備する。それには多項式環の商環と呼ばれるものが必要になるが、直感的な説明も加えて分かりやすく解説する。

\$\mathbb{F}_q[x_1, \dots, x_n]\$ を \$\mathbb{F}_q\$ 係数の \$n\$ 変数 \$x_1, \dots, x_n\$ の多項式全体 (つまり通常の和と積を持つ多項式環) とするとき、商環 \$R_n\$ を

$$R_n = \mathbb{F}_q[x_1, \dots, x_n] / (x_1^{d_1+1} - x_1, \dots, x_n^{d_n+1} - x_n)$$

で定める。ただし \$(x_1^{d_1+1} - x_1, \dots, x_n^{d_n+1} - x_n)\$ は、\$x_1^{d_1+1} - x_1, \dots, x_n^{d_n+1} - x_n\$ で生成されるイデアルである。つまり、このイデアルで定まる商環 \$R_n\$ を考えるということは、\$x_i^{d_i+1} - x_i\$ による除法を行った余り (剰余) を取るということなので、\$x_i\$ についての次数が \$d_i\$ 以下の多項式となり、\$R_n\$ は式 (4) で表される \$f\$ 全体となる。もっと簡潔に記述するために、次の多重添え字の集合 \$A_n\$ を用いる。\$R_n\$ の全ての単項式 \$x_1^{a_1} \dots x_n^{a_n}\$ は、

$$(a_1, \dots, a_n) \in A_n = \{a = (a_1, \dots, a_n) \mid a_i = 0, 1, \dots, d_i\}$$

と \$A_n\$ の元で一意に表すことができる。よって、式 (4) の \$f = f(x_1, \dots, x_n) \in R_n\$ は、

$$f = \sum_{a \in A_n} f_a x^a$$

と一意に表すことができる。ただし \$a = (a_1, \dots, a_n) \in A_n\$ について \$x^a = x_1^{a_1} \dots x_n^{a_n}\$ と書くことにする。

[例 4] (多値論理多項式) \$n = 1, q = 7, d_1 = 3\$ とすると、\$A_1 = \{0, 1, 2, 3\}\$ となり、\$R_1\$ の元としては例えば

$$f = \sum_{a \in A_1} f_a x^a = 2 + 1x_1 + 6x_1^2 + 5x_1^3 \in R_1. \quad (10)$$

\$n = 2, q = 2, d_1 = 1, d_2 = 1\$ とすると、\$A_2 = \{(0, 0), (1, 0), (0, 1), (1, 1)\}\$ となり、\$R_2\$ の元としては例えば

$$\begin{aligned} f &= \sum_{a \in A_2} f_a x^a = 1x^{(0,0)} + 1x^{(1,0)} + 0x^{(0,1)} + 1x^{(1,1)} \\ &= 1 + x_1 + x_1x_2 \in R_2 \end{aligned} \quad (11)$$

があり、式 (11) は例 2 の \$f\$ に対応するものである。

\$n = 2, q = 7, d_1 = 2, d_2 = 3\$ とすると、\$A_2 = \{(0, 0), (1, 0), \dots, (0, 1), \dots, (2, 3)\}\$ となり、\$R_2\$ の元としては例えば

$$\begin{aligned} f &= \sum_{a \in A_2} f_a x^a = 4 + 6x_2 + 5x_2^2 + 2x_2^3 \\ &\quad + 1x_1 + 4x_1x_2 + 0x_1x_2^2 + 5x_1x_2^3 \\ &\quad + 3x_1^2 + 5x_1^2x_2 + 1x_1^2x_2^2 + 4x_1^2x_2^3. \end{aligned} \quad (12)$$

[注意 1] 多値論理多項式はその名のとおりの多項式で表すのが普通であるが、多項式の係数を並べてベクトルで表す方法もある。多値論理関数も同様に、式 (6) のようにベクトルで表す方法と、文献(8)のように多項式で表す方法の 2 通りがある。表 2 に筆者の過去の文献において、多値論理多項式と多値論理関数をそれぞれベクトルまたは多項式のどちらで表していたかをまとめた。本稿は、文献(9)と同じく、多値論理多項式を多項式、多値論理関数をベクトルで表している。また表 2 以外の組合せ、つまり多値論理多項式をベクトル、多値論理関数を多項式で表す組合せは特にメリットがないので考えたことはない。以下、表 2 の各項目の説明を行う。この表は、多値論理多項式・多値論理関数をベクトル・多項式として考えることに加え、4. で導入する

表 2 多値論理多項式と多値論理関数の組の表現方法の比較 この表で「代入」とは 4. で導入する代入写像 $\text{ev}_n : R_n \rightarrow (\mathbb{F}_q)^{\Omega_n}$ のことである。

多値論理多項式	多値論理関数	長所	短所	文献
ベクトル	ベクトル	行列で操作可能 転置が見やすい	代入が分かりづらい 並べ方の fix 必要	文献(10)
多項式	多項式	多項式で統一 並べ方によらない	論理関数と見づらい 原始元の fix 必要	文献(8)
多項式	ベクトル	代入が分かりやすい 符号分野の標準	転置が見づらい 並べ方の fix 必要	文献(9)

代入写像の扱いやすさについてもまとめている。

第 1 に、多値論理多項式、多値論理関数共にベクトルで表す方法の長所は、変換が全て行列で表されるため、数式処理ソフトウェア等で計算が容易であること、また代入写像の転置が行列の転置に対応しているため分かりやすいこと (cf. 式 (28)) である。短所は、代入写像を記述するために Σ が必要であり分かりにくいこと (cf. 式 (27))、また式 (7) のように Ω_n の成分の並べ方を一つ決める必要があることである。ただし文献(10)は誤り訂正符号のみを扱っており、多値論理関数は扱っていない。しかし文献(10)でも代入写像を頻繁に用いているためこの表に入れることにした。

第 2 に、多値論理多項式、多値論理関数共に多項式で表す方法の長所は、多項式で全て統一され記号の定義が少なく済むこと、また並べ方によらない (例えば式 (11) であれば $1+x_1+x_1x_2$ でも $x_1x_2+x_1+1$ でも多項式としては同じ) ことである。短所は、多項式を多値論理関数と見るのは直接的ではないこと (例えば式 (8) であれば論理関数と見たものは $1+x_2+x_1x_2$ となるが多値にすると複雑になってくる)、また代入写像を定める際に有限体の原始元 (巡回生成元) を一つ決める必要があることである。文献(8)では、例えば $\mathbb{F}_7$ における 1 の原始 4 乗根 2 を一つ決めて、 $a=0,1,2,3$ に対し記号 $2^{(a)}$ を $a=0$ のとき 0, $a \neq 0$ のとき 2^a と定めた。このとき $a=0,1,2,3$ それぞれに対し $2^{(a)}=0,2,4,1$ となり、式 (7) の並びが出てくる。

第 3 に、多値論理多項式を多項式、多値論理関数をベクトルで表す方法の長所は、代入写像が多項式の代入で定義され分かりやすいこと (cf. 式 (18))、また代数的誤り訂正符号の多くの文献(11)～(13)においてこの表現方法が用いられていることである。短所は、代入写像の転置の表示がやや複雑になること (cf. 式 (29)) と、やはり Ω_n の成分の並べ方を固定しなければならないことである。

以上のとおり、どの方法も長所と短所があるが、多値論理関数と誤り訂正符号との関係を見るために、本稿では第 3 の方法を取ることにした。

本稿の数値例については、手計算や確認のしやすさから $\mathbb{F}_2$ と $\mathbb{F}_7$ の素数の要素数の有限体しか扱っていないが、例えば 16 元体や 49 元体のような一般の拡大体でも同様に扱うことができる。

3. R_n と $(\mathbb{F}_q)^{\Omega_n}$ における積

多値論理多項式と多値論理関数におけるそれぞれの積、つまり乗法について考えよう。二つの多値論理多項式の積、あるいは二

つの多値論理関数の積は、複数の多値論理多項式 (または多値論理関数) から新たな多値論理多項式 (または多値論理関数) を作る際に用いられる。多値論理関数の積、つまり $(\mathbb{F}_q)^{\Omega_n}$ における積の方が簡単なので、こちらから考えてみる。二つの多値論理関数 $(c_\omega)_{\omega \in \Omega_n}, (d_\omega)_{\omega \in \Omega_n}$ の積とは、行先における積 $(c_\omega d_\omega)_{\omega \in \Omega_n}$ 、ただし $c_\omega d_\omega \in \mathbb{F}_q$ は $\mathbb{F}_q$ における通常の積、と定める。積を開数の形で書いて、 $(c, d) \in (\mathbb{F}_q)^{\Omega_n} \times (\mathbb{F}_q)^{\Omega_n}$ について、

$$F_{\odot}(c, d) = cd = (c_\omega d_\omega)_{\omega \in \Omega_n} \in (\mathbb{F}_q)^{\Omega_n}$$

とも書く。次に多値論理多項式の積について、こちらにも自然な積があり、それは多項式としての積である。ただし商環 R_n で考えている以上、多項式としての積の結果は $x_i^{d_i+1} - x_i$ による除法の余りを取るが、以後既に余りを取ったとして書き表すことにする。積を開数の形で書いて、 $(f, g) \in R_n \times R_n$ について、

$$F_*(f, g) = fg \in R_n$$

と定める。

[例 5] (多値論理関数の積) $n=1, q=7, d_1=3$ のとき、 $c=(2520), d=(3142) \in (\mathbb{F}_7)^{\Omega_1}$ とすると、 $cd \in (\mathbb{F}_7)^{\Omega_1}$ は

$$cd = (6510). \quad (13)$$

$n=2, q=7, d_1=2, d_2=3$ のとき、

$$c = \begin{pmatrix} 4 & 3 & 5 & 3 \\ 6 & 3 & 5 & 6 \\ 1 & 3 & 0 & 5 \end{pmatrix}, d = \begin{pmatrix} 6 & 1 & 4 & 2 \\ 5 & 0 & 2 & 6 \\ 4 & 2 & 6 & 0 \end{pmatrix} \in (\mathbb{F}_7)^{\Omega_2}$$

とすると、

$$cd = \begin{pmatrix} 3 & 3 & 6 & 6 \\ 2 & 0 & 3 & 1 \\ 4 & 6 & 0 & 0 \end{pmatrix} \in (\mathbb{F}_7)^{\Omega_2}. \quad (14)$$

[例 6] (多値論理多項式の積) $n=1, q=7, d_1=3$ のとき、 $f=2+1x_1+6x_1^2+5x_1^3, g=3+0x_1+2x_1^2+4x_1^3 \in R_1$ とすると、 $fg \in R_1$ は (1 変数多項式の積の後、 $x_1^4 - x_1$ による余りを取って)

$$fg = (fg)(x_1) = 6 + 5x_1 + 0x_1^2 + 3x_1^3 \in R_1. \quad (15)$$

$n=2, q=7, d_1=2, d_2=3$ のとき、式 (12) の $f \in R_2$ と

$$\begin{aligned} g = g(x_1, x_2) = & 6 & +0x_2 & +2x_2^2 & +1x_2^3 \\ & +3x_1 & +4x_1x_2 & +0x_1x_2^2 & +4x_1x_2^3 \\ & +2x_1^2 & +5x_1^2x_2 & +5x_1^2x_2^2 & +3x_1^2x_2^3 \end{aligned} \quad (16)$$

について、 $fg \in R_2$ は (2 変数多項式の積の後、 $x_1^3 - x_1$ と $x_2^4 - x_2$ による余りを取って)

$$\begin{aligned} fg = (fg)(x_1, x_2) = & 3 & +3x_2 & +5x_2^2 & +2x_2^3 \\ & +1x_1 & +4x_1x_2 & +1x_1x_2^2 & +4x_1x_2^3 \\ & +0x_1^2 & +1x_1^2x_2 & +5x_1^2x_2^2 & +6x_1^2x_2^3. \end{aligned} \quad (17)$$

もっと簡単な例では、例えば $f = x_1^2 x_2^2, g = x_1 x_2^3 \in R_2$ について、 $fg = x_1 x_2^5 \in R_2$ となる。

R_n と $(\mathbb{F}_q)^{\Omega_n}$ におけるこれらの積は、 R_n の元を多値論理関数と見たとき、一致するだろうか？ 実際、一致する。この事実を正確に述べたものが次章の畳込み定理である。

4. 畳込み定理

定理を述べる前に、必要な変換について解説する。この変換は、離散フーリエ変換の類似であるが、ここでは「代入写像」と呼ぶことにする（文献(1) (8) の evaluation map）。

代入写像 $\text{ev}_n : R_n \rightarrow (\mathbb{F}_q)^{\Omega_n}$ を、 $f \in R_n$ について

$$\text{ev}_n(f) = (f(\omega))_{\omega \in \Omega_n} \quad (18)$$

で定める。ただし $f(\omega)$ は多変数多項式 $f = f(x_1, \dots, x_n)$ への $\omega = (\omega_1, \dots, \omega_n) \in \Omega_n$ の代入であり、例えば $f \in R_n$ が単項式 $f = x^a = x_1^{a_1} \dots x_n^{a_n}$ のときは

$$f(\omega) = \omega_1^{a_1} \dots \omega_n^{a_n} \in \mathbb{F}_q \quad (19)$$

によって定まり、 $f \in R_n$ が一般のときは式(19)の線形結合である。式(19)における注意として、 $0^0 = 1$ と定める。代入写像は二つの線形空間の間の線形写像である。何度か出てきている「Vandermonde 型補題」により、この代入写像は同形写像、つまり全単射（1 対 1 の写像）となることが示される。この代入写像によって、多値論理多項式から多値論理関数を作ることができる。となると当然、逆の多値論理関数から多値論理多項式を作るにはどうすればよいか？ という疑問が起こるが、それが後で考える代入写像の逆写像になる。代入写像が全単射であることはそこでも示されることになる。

[例 7] (代入写像 ev_n) $n = 1, q = 7, d_1 = 3$ とし、式(10)の $f = 2 + 1x_1 + 6x_1^2 + 5x_1^3 \in R_1$ を取ると、

$$\text{ev}_1(f) = (2 \ 5 \ 2 \ 0)$$

となり、式(7)の c に一致する。この計算を行列で表すには、

$$M_1 = \begin{matrix} & & 0 & 2 & 4 & 1 \\ \begin{matrix} 1 \\ x_1 \\ x_1^2 \\ x_1^3 \end{matrix} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 4 & 1 \\ 0 & 4 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \end{matrix} \quad (20)$$

を用いて $\text{ev}_1(f) = (2 \ 1 \ 6 \ 5)M_1$ とする。ただし $1, x_1, x_1^2, x_1^3$ 及び $0, 2, 4, 1$ は、行列の成分が x_1^a ($a = 0, 1, 2, 3$) に $\omega = 0, 2, 4, 1$ を代入して得られることを示す。

$n = 2, q = 2, d_1 = 1, d_2 = 1$ とし、式(11)の $f = 1 + x_1 + x_1 x_2 \in R_2$ を取ると、

$$\text{ev}_2(f) = (1 \ 0 \ 1 \ 1)$$

となり、式(8)に一致する。

$$M = \begin{matrix} & & 0,0 & 1,0 & 0,1 & 1,1 \\ \begin{matrix} 1 \\ x_1 \\ x_2 \\ x_1 x_2 \end{matrix} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{matrix} \quad (21)$$

を用いて $\text{ev}_2(f) = (1 \ 1 \ 0 \ 1)M$ としてもよい。

$n = 2, q = 7, d_1 = 2, d_2 = 3$ とし、式(12)の $f \in R_2$ を取ると、

$$\text{ev}_2(f) = \begin{pmatrix} 4 & 3 & 5 & 3 \\ 6 & 3 & 5 & 6 \\ 1 & 3 & 0 & 5 \end{pmatrix} \quad (22)$$

となり、式(9)に一致する。この変換の行列表示は例 9 で行う。

代入写像 $\text{ev}_n(f) = (f(\omega))_{\omega \in \Omega_n}$ における $f(\omega)$ の計算量は、 ω^a の値の更新、 f_a との積、和への加算、の 3 ステップを $|A_n| = \prod_{i=1}^n (d_i + 1)$ だけ繰り返すので、 $3 \prod_{i=1}^n (d_i + 1)$ となる。よって、代入写像 $\text{ev}_n(f)$ の計算量は、 $f(\omega)$ の計算量の $|\Omega_n| = \prod_{i=1}^n (d_i + 1)$ 倍なので、 $3 \prod_{i=1}^n (d_i + 1)^2$ となる。後で計算量が $O(\prod_{i=1}^n (d_i + 1)^2)$ より小さい $\text{ev}_n(f)$ の計算方法について述べる。

次の定理が畳込み定理と呼んでいるものである。

[定理 3] ⁽⁸⁾ 合成写像の等式 $\text{ev} \circ F_* = F_{\odot} \circ (\text{ev} \times \text{ev})$ が成り立つ。言い換えると、次の可換図式が成り立つ。

$$\begin{array}{ccc} R_n \times R_n & \xrightarrow{\text{ev} \times \text{ev}} & (\mathbb{F}_q)^{\Omega_n} \times (\mathbb{F}_q)^{\Omega_n} \\ F_* \downarrow & & \downarrow F_{\odot} \\ R_n & \xrightarrow{\text{ev}} & (\mathbb{F}_q)^{\Omega_n} \end{array}$$

定理 3 の証明はここではしないが、扱っている写像は全て線形写像だから、基底である単項式についてだけ定理を証明すればよく、易しい。定理 3 は代数学の言葉では、 ev_n が二つの可換環（あるいは $\mathbb{F}_q$ 代数） R_n から $(\mathbb{F}_q)^{\Omega_n}$ への準同形写像（後で分かるように、同形写像）であることを示す。

[例 8] (畳込み定理) $n = 1, q = 7, d_1 = 3$ のとき、式(15)の $F_*(f, g) = fg \in R_1$ について

$$\text{ev}_1(fg) = (6 \ 5 \ 1 \ 0)$$

となり、式(13)と一致する。

$n = 2, q = 7, d_1 = 2, d_2 = 3$ のとき、式(17)の $F_*(f, g) = fg \in R_2$ について

$$\text{ev}_2(fg) = \begin{pmatrix} 3 & 3 & 6 & 6 \\ 2 & 0 & 3 & 1 \\ 4 & 6 & 0 & 0 \end{pmatrix}$$

となり、式(14)と一致する。

5. 代入写像の高速計算法

代入写像 ev_n の計算量を減らすために、 ev_n の分解を行う。この分解は、一言で言えばテンソル分解である。現に、式(21)の行列は、テンソル積の間の線形写像を表す行列のクロネッカー積

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ に等しい. ここで $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ は, $d_1 = 1$ としたときの $\text{ev}_1 : R_1 \rightarrow (\mathbb{F}_2)^{\Omega_1}$ の行列表示である. 更に言えば高速フーリエ変換 (FFT) の類似とも言える.

非負の整数 l, m は $l+m = n$ を満たすとする. R_n と $(\mathbb{F}_q)^{\Omega_n}$ の中間的なものとして,

$$(R_l)^{\Omega_m} = \{ (f_\omega)_{\omega \in \Omega_m} \mid f_\omega \in R_l \text{ for all } \omega \in \Omega_m \}$$

を定める. ただし $(R_n)^{\Omega_0} = R_n$, $(R_0)^{\Omega_n} = (\mathbb{F}_q)^{\Omega_n}$ とする. このとき $\text{ev}_{n,l} : (R_l)^{\Omega_m} \rightarrow (R_{l-1})^{\Omega_{m+1}}$ を,

$$\text{ev}_{n,l}((f_\omega)_{\omega \in \Omega_m}) = (f_\omega(x_1, \dots, x_{l-1}, \omega_l))_{(\omega_l, \omega) \in \Omega_{m+1}} \quad (23)$$

によって定める. こうして $\text{ev}_n : R_n \rightarrow (\mathbb{F}_q)^{\Omega_n}$ は,

$$R_n = (R_n)^{\Omega_0} \rightarrow (R_{n-1})^{\Omega_1} \rightarrow \dots \rightarrow (R_0)^{\Omega_n} = (\mathbb{F}_q)^{\Omega_n}$$

と n 個の $\text{ev}_{n,l}$ ($l = n, n-1, \dots, 1$) に分解される. つまり $\text{ev}_n = \text{ev}_{n,1} \circ \text{ev}_{n,2} \circ \dots \circ \text{ev}_{n,n}$ と合成写像で表される. $n = 2$ のとき $\text{ev}_{n,1} \circ \text{ev}_{n,2}$ をやってみると

$$\begin{aligned} & \text{ev}_{2,1}(\text{ev}_{2,2}(f(x_1, x_2))) \\ &= \text{ev}_{2,1} \left(\text{ev}_{2,2} \left(\sum_{a_1=0}^{d_1} f_{a_1}(x_2) x_1^{a_1} \right) \right) \\ &= \text{ev}_{2,1} \left(\left(\sum_{a_1=0}^{d_1} f_{a_1}(\omega_2) x_1^{a_1} \right)_{\omega_2 \in \Omega_1} \right) \quad (24) \\ &= \text{ev}_{2,1}((f(x_1, \omega_2))_{\omega_2 \in \Omega_1}) \\ &= (f(\omega_1, \omega_2))_{(\omega_1, \omega_2) \in \Omega_2} = \text{ev}_2(f). \end{aligned}$$

このように $\text{ev}_{n,l}$ は, x_l に ω_l を代入するので, ev_1 と似ている. ただし, 例えば $\text{ev}_{2,2}$ の計算量は, 式 (24) を見ると分かるように, ev_1 の計算量 $3(d_2 + 1)^2$ が $|A_1| = d_1 + 1$ だけ必要なので, $3(d_2 + 1) \prod_{i=1}^2 (d_i + 1)$ となる. 一般には, 式 (23) における $f_\omega(x_1, \dots, x_{l-1}, \omega_l)$ の計算量は, 以前説明したとおり 3 ステップの計算を $d_l + 1$ 回行ったものが $|A_{l-1}| = \prod_{i=1}^{l-1} (d_i + 1)$ だけあるので, $3 \prod_{i=1}^l (d_i + 1)$ となる. 式 (23) には $f_\omega(x_1, \dots, x_{l-1}, \omega_l)$ が $|\Omega_{m+1}| = \prod_{i=l}^n (d_i + 1)$ だけあるから, $\text{ev}_{n,l}$ の計算量は $3(d_l + 1) \prod_{i=1}^n (d_i + 1)$ となる. $\text{ev}_{n,l}$ を $l = n, n-1, \dots, 1$ について行うので, 最終的に $\text{ev}_n = \text{ev}_{n,1} \circ \text{ev}_{n,2} \circ \dots \circ \text{ev}_{n,n}$ の計算量は

$$3 \sum_{l=1}^n \left((d_l + 1) \prod_{i=1}^n (d_i + 1) \right) = 3 \left(\sum_{l=1}^n (d_l + 1) \right) \prod_{i=1}^n (d_i + 1)$$

となり, この分解により ev_n の計算量は, $3 \prod_{i=1}^n (d_i + 1)^2$ から $3 \left(\sum_{l=1}^n (d_l + 1) \right) \prod_{i=1}^n (d_i + 1)$ まで削減された.

[例 9] (代入写像の分解 $\text{ev}_{n,l}$) $n = 1, q = 7, d_1 = 2$ とし, 例 7 でやったように, ev_1 の計算を行列で表すと,

$$M_2 = \begin{matrix} & 0 & 6 & 1 \\ x_1 & \begin{pmatrix} 1 & 1 & 1 \\ 0 & 6 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{matrix} \quad (25)$$

を用いて $\text{ev}_1(\sum_{a=0}^2 f_a x^a) = (f_0 \ f_1 \ f_2 \ f_3) M_2$ となる. 式 (12) の $f \in R_2$ に $\text{ev}_{2,2}$ を行うことは, 式 (20) の M_1 を右から掛けることに相当する.

$$f = \begin{matrix} & 4 & +6x_2 & +5x_2^2 & +2x_2^3 \\ & +1x_1 & +4x_1x_2 & +0x_1x_2^2 & +5x_1x_2^3 \\ & +3x_1^2 & +5x_1^2x_2 & +1x_1^2x_2^2 & +4x_1^2x_2^3 \end{matrix} \curvearrowright M_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 4 & 1 \\ 0 & 4 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

次に $\text{ev}_{2,1}$ を行うことは, 式 (25) の M_2 の転置 $M_2^\top$ を左から掛けることに相当する.

$$M_2^\top = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 6 & 1 \\ 1 & 1 & 1 \end{pmatrix} \curvearrowright \text{ev}_{2,2}(f) = \begin{pmatrix} 4 & +3 & +5 & +3 \\ +1x_1 & +0x_1 & +1x_1 & +3x_1 \\ +3x_1^2 & +0x_1^2 & +1x_1^2 & +6x_1^2 \end{pmatrix}$$

こうして $\text{ev}_{2,1}(\text{ev}_{2,2}(f))$ が得られ, 式 (22) の $\text{ev}_2(f)$ に一致する.

$$\text{ev}_{2,1}(\text{ev}_{2,2}(f)) = \begin{pmatrix} 4 & 3 & 5 & 3 \\ 6 & 3 & 5 & 6 \\ 1 & 3 & 0 & 5 \end{pmatrix}$$

6. 代入写像の逆写像

代入写像の分解 $\text{ev}_n = \text{ev}_{n,1} \circ \text{ev}_{n,2} \circ \dots \circ \text{ev}_{n,n}$ により, 逆写像は $\text{ev}_n^{-1} = \text{ev}_{n,n}^{-1} \circ \text{ev}_{n,n-1}^{-1} \circ \dots \circ \text{ev}_{n,1}^{-1}$ と各分解の逆写像の合成となる. 各 $\text{ev}_{n,l}$ は, ω_l の x_l への代入と言う意味で本質的には ev_1 である. よって ev_1 の逆写像 ev_1^{-1} が分かれば,あとは各成分に ev_1^{-1} を行いまた合成写像により ev_n^{-1} が得られるので, 以下において ev_1^{-1} を求める.

ev_1^{-1} はもちろん逆行列を用いて表示できる. しかし, 逆離散フーリエ変換が離散フーリエ変換で記述できるように, ev_1^{-1} にも公式があるので以下に紹介する.

[定理 4] ^{(8), (9)} $\text{ev}_1 : R_1 \rightarrow (\mathbb{F}_q)^{\Omega_1}$ の逆写像 $\text{ev}_1^{-1} : (\mathbb{F}_q)^{\Omega_1} \rightarrow R_1$ は, 以下のように記述される. $(c_\omega)_{\omega \in \Omega_1} \in (\mathbb{F}_q)^{\Omega_1}$ について,

$$\begin{aligned} & \text{ev}_1^{-1}((c_\omega)_{\omega \in \Omega_1}) \\ &= c_0(1 - x^{d_1}) + \frac{1}{d_1} \sum_{a=1}^{d_1} \left(\sum_{\omega \in \Omega_1 \setminus \{0\}} c_\omega \omega^{-a} \right) x^a. \quad (26) \end{aligned}$$

証明は文献 (1), (8), (9) を参照とするが, 文献 (8) では直接計算, 文献 (1), (9) では中国剰余定理により示している.

[例 10] (代入写像の逆写像 ev_1^{-1}) $n = 1, q = 7, d_1 = 3$ とする. $(c_\omega)_{\omega \in \Omega_1} = (c_0 \ c_2 \ c_4 \ c_1)$ に対し, 逆写像 ev_1^{-1} は次で与えられる. $\text{ev}_1^{-1}((c_\omega)_{\omega \in \Omega_1}) = \sum_{a=0}^3 f_a x^a$ とすると,

$$(f_0 \ f_1 \ f_2 \ f_3) = (c_0 \ c_2 \ c_4 \ c_1) \begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & 6 & 3 & 5 \\ 0 & 3 & 6 & 5 \\ 0 & 5 & 5 & 5 \end{pmatrix}.$$

この行列は式 (20) の行列の逆行列である。一方、この行列の第 1 行は式 (26) の $c_0 (1 - x^{d_1})$ に対応している。また、この行列の $\begin{pmatrix} 6 & 3 & 5 \\ 3 & 6 & 5 \\ 5 & 5 & 5 \end{pmatrix}$ の部分は、式 (26) の第 2 項に対応していることが

$$3 \begin{pmatrix} 6 & 3 & 5 \\ 3 & 6 & 5 \\ 5 & 5 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 1 \\ 2 & 4 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 2^{-1} & 2^{-2} & 2^{-3} \\ 4^{-1} & 4^{-2} & 4^{-3} \\ 1^{-1} & 1^{-2} & 1^{-3} \end{pmatrix}$$

という計算から分かる。

逆行列である $(d_1 + 1)$ 次正方行列を $(d_1 + 1)$ 次元ベクトルに掛ける計算量は $O((d_1 + 1)^2)$ である。(ただし逆行列を求める計算量は $O((d_1 + 1)^3)$ 程度であるが、固定して考えるので通常は考慮しない。) 一方、式 (26) を用いて ev_1^{-1} を求める際、計算量はやはり $O((d_1 + 1)^2)$ となる。よって、オーダは同じであり、式 (26) の公式が計算量的に特に優れているというわけではない。しかし、逆写像が簡潔に書ける、また、先に述べたように幾つか示す方法があるという意味では注目される。

7. 積の計算量の比較

以上により、多値論理多項式の積について二つの方法が得られたことになる。一つは R_n における通常の積であり、 F_* と表していた。もう一つは畳込み定理を用いて一見う回路を取る方法であり、これまでに用いた写像の合成で書けば $\text{ev}_n^{-1} \circ F_{\odot} \circ (\text{ev}_n \times \text{ev}_n)$ となる。可換図式をもう一度書くと

$$\begin{array}{ccc} R_n \times R_n & \xrightarrow{\text{ev}_n \times \text{ev}_n} & R_n \times R_n \\ F_* \downarrow & & \downarrow F_{\odot} \\ R_n & \xleftarrow{\text{ev}_n^{-1}} & R_n. \end{array}$$

となり、写像として等しく $F_* = \text{ev}_n^{-1} \circ F_{\odot} \circ (\text{ev}_n \times \text{ev}_n)$ であるが、計算量は異なる。

F_* については、 $f = \sum_{a \in A_n} f_a x^a$, $g = \sum_{a \in A_n} g_a x^a \in R_n$ の係数はそれぞれ $|A_n| = \prod_{i=1}^n (d_i + 1)$ 個あるから、 $F_*(f, g)$ の計算量は $O(\prod_{i=1}^n (d_i + 1)^2)$ となりそうである。実際には、 $x_i^{d_i+1} - x_i$ による除法も考慮する必要があるが、正確に計算量を求めると $2 \prod_{i=1}^n (d_i + 1)^2$ となる⁽⁸⁾。一方、 $\text{ev}_n^{-1} \circ F_{\odot} \circ (\text{ev}_n \times \text{ev}_n)$ については、写像 ev_n^{-1} , $F_{\odot}$, $\text{ev}_n \times \text{ev}_n$ の計算量が全て $O((\sum_{i=1}^n (d_i + 1)) \prod_{i=1}^n (d_i + 1))$ と同じかそれ以下であることから、合成写像も同じオーダの計算量となる。以下の表 3 に積の計算量についてまとめる。

F_* から $\text{ev}_n^{-1} \circ F_{\odot} \circ (\text{ev}_n \times \text{ev}_n)$ とするとどのくらいの計算量の削減かを見るために、例えば $d_i + 1 = q$, つまり半群として有限体全体を取った場合を考えると、 $O(q^{2n})$ から

表 3 多値論理多項式の積についての二つの方法の計算量の比較

方法	F_*	$\text{ev}_n^{-1} \circ F_{\odot} \circ (\text{ev}_n \times \text{ev}_n)$
計算量	$O\left(\prod_{i=1}^n (d_i + 1)^2\right)$	$O\left(\left(\sum_{i=1}^n (d_i + 1)\right) \prod_{i=1}^n (d_i + 1)\right)$

$O(nq^{n+1})$ への削減となる。 $N = q^n$ と置くと、 $O(N^2)$ から $O(qN \log_q N)$ への削減となる。特に $q = 2$ とすると、オーダが N^2 から $N \log_2 N$ に削減されたことになり、この場合は高速フーリエ変換 (FFT) と同じ削減量となる。こうして半群の直積上の多値論理多項式同士の積について、畳込み定理を用いた高速化が確認できた。

8. 代入写像の転置

次章の準備のために、代入写像の転置について記述しておこう。そのためには、文献 (10) でやっていたように、 R_n も $(\mathbb{F}_q)^{\Omega_n}$ のようにベクトルで書いた方がよいので、 R_n を $(\mathbb{F}_q)^{A_n}$ と書き換えておく。多項式とベクトルの対応は

$$R_n \ni \sum_{a \in A_n} f_a x^a \mapsto (f_a)_{a \in A_n} \in (\mathbb{F}_q)^{A_n}.$$

このとき、式 (18) の代入写像は、次のように書き換えられるが、それも再び $\text{ev}_n : (\mathbb{F}_q)^{A_n} \rightarrow (\mathbb{F}_q)^{\Omega_n}$ と書くことにすれば、 $(f_a)_{a \in A_n} \in (\mathbb{F}_q)^{A_n}$ について

$$\text{ev}_n((f_a)_{a \in A_n}) = \left(\sum_{a \in A_n} f_a \omega^a \right)_{\omega \in \Omega_n}. \quad (27)$$

このとき、写像 $\text{ev}_n^{\top} : (\mathbb{F}_q)^{\Omega_n} \rightarrow (\mathbb{F}_q)^{A_n}$ を、 $(c_{\omega})_{\omega \in \Omega_n} \in (\mathbb{F}_q)^{\Omega_n}$ について

$$\text{ev}_n^{\top}((c_{\omega})_{\omega \in \Omega_n}) = \left(\sum_{\omega \in \Omega_n} c_{\omega} \omega^a \right)_{a \in A_n} \quad (28)$$

で定める。このように、 ev_n と $\text{ev}_n^{\top}$ では A_n と Ω_n の役割が入れ替わっている。なぜ式 (28) を転置と呼ぶべきかと言えば、実は適当に線形空間の基底を定めて行列表示すると、行列が転置の関係になっているからである。後の数値例で基底として標準基底を取ったとき、確かに転置となっていることを確かめよう。勝手な基底では一般には転置の関係にはならないが、正規直交基底に取ったときにはやはり転置の関係になっていることが示される⁽¹⁰⁾。

代入写像の転置写像が得られたところで、 $(\mathbb{F}_q)^{A_n}$ ではなく R_n による表示を求めておこう。要は、式 (28) の右辺の $\sum_{\omega \in \Omega_n} c_{\omega} \omega^a$ を x^a の係数に持つ多項式となる。 R_n による表示もやはり $\text{ev}_n^{\top}$ を用いて $\text{ev}_n^{\top} : (\mathbb{F}_q)^{\Omega_n} \rightarrow R_n$ と書くことにすると、 $(c_{\omega})_{\omega \in \Omega_n} \in (\mathbb{F}_q)^{\Omega_n}$ について

$$\text{ev}_n^\top((c_\omega)_{\omega \in \Omega_n}) = \sum_{a \in A_n} \left(\sum_{\omega \in \Omega_n} c_\omega \omega^a \right) x^a. \quad (29)$$

[例 11] (代入写像の転置 $\text{ev}_n^\top$) $n = 1, q = 7, d_1 = 3$ とする. まずは $\text{ev}_1 : R_1 \rightarrow (\mathbb{F}_q)^{\Omega_1}$ について, $R_1 = \mathbb{F}_q[x]/(x^{d_1+1} - x)$ の標準基底 $1, x, x^2, x^3$ の行先は, $x = 0, 2, 4, 1$ とするので,

$$\begin{aligned} 1 &\mapsto (1111) \\ x &\mapsto (0241) \\ x^2 &\mapsto (0421) \\ x^3 &\mapsto (0111). \end{aligned}$$

よって, $(\mathbb{F}_q)^{\Omega_1}$ の標準基底 $(1000), \dots, (0001)$ を取るとき, $\sum_{a=0}^3 f_a x^a \mapsto (c_0 c_2 c_4 c_1)$ のとき, ev_1 の行列表示は

$$(c_0 c_2 c_4 c_1) = (f_0 f_1 f_2 f_3) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 4 & 1 \\ 0 & 4 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \quad (30)$$

となり, 式 (20) の M_1 と一致する.

次に $\text{ev}_1^\top : (\mathbb{F}_q)^{\Omega_1} \rightarrow R_1$ の行列表示を求める. $\sum_{\omega \in \Omega_1} c_\omega \omega^a = c_0 0^a + c_2 2^a + c_4 4^a + c_1 1^a$ だから,

$$\begin{aligned} (1000) &\mapsto \sum_{a \in A_1} 0^a x^a = 1 \\ (0100) &\mapsto \sum_{a \in A_1} 2^a x^a = 1 + 2x + 4x^2 + 1x^3 \\ (0010) &\mapsto \sum_{a \in A_1} 4^a x^a = 1 + 4x + 2x^2 + 1x^3 \\ (0001) &\mapsto \sum_{a \in A_1} 1^a x^a = 1 + 1x + 1x^2 + 1x^3. \end{aligned}$$

よって, $(c_0 c_2 c_4 c_1) \mapsto \sum_{a=0}^3 f_a x^a$ のとき, $\text{ev}_1^\top$ の行列表示は

$$(f_0 f_1 f_2 f_3) = (c_0 c_2 c_4 c_1) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 4 & 1 \\ 1 & 4 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad (31)$$

となり, $M_1^\top$ と一致する.

式 (30) と (31) の行列を見ると, 行列の第 1 行目と第 1 列目以外は等しいことが分かる. 等しい理由は, $a = 0$ や $\omega = 0$ に関係するところ以外の行列は転置行列になっているからである. 更に転置行列になる理由は, 一言で言えば, $a, b \neq 0$ かつ $\omega \neq 0$ ならば, x^a で $x = \omega^b$ とした値と x^b で $x = \omega^a$ とした値が等しいからである. このように, 転置の関係は, $\omega = 0$ を考慮して初めて現れるものであり, 通常の離散フーリエ変換では転置と言うより等しいという関係だったため見えていなかった関係である. 1. で述べたとおり, 多値論理関数の話で 0 の入力を考える理由は, 論理を扱う際 0 が重要だからであった. 一方, 誤

り訂正符号ではこの「0 の入力」が出てくる場面は比較的少なかった. 例えばリードソロモン符号では, 0 の入力を行って符号化を行ったものは拡大符号や伸長符号と呼ばれているが, 符号長の観点からは 1 長くなるだけであり, 実用的にはそれほど影響はなかった. 次章では, 代入写像と誤り訂正符号との関係について解説するが, その際にはこの転置は注目すべき関係となる.

9. 誤り訂正符号との関係

誤り訂正符号のうち, 通常用いられる線形符号とは, $\mathbb{F}_q$ 上の線形空間の部分空間のことである. 以下では, 線形符号を単に符号と言う. 実際には, 勝手な部分空間ではなく, 高い誤り訂正能力を高速に処理できるようにするために, 様々な構造を持った部分空間を構成し実用化されている. また符号の直交補空間を双対符号と言うが, 双対符号の基底を並べた行列はパリティ検査行列と呼ばれ, 符号を扱う際にはよく用いられている. 本章では, 今まで出てきた様々な写像の応用として, 符号とその双対符号を構成する一つの方法を示す.

[定理 5] ⁽¹⁰⁾ $U \subset (\mathbb{F}_q)^{A_n}$ を部分空間, $U^\perp \subset (\mathbb{F}_q)^{A_n}$ を U の直交補空間, つまり $u \in U, v \in U^\perp$ のとき必ず $uv^\top = 0$ となる部分空間, とする. このとき, $\text{ev}_n(U)$ の直交補空間は $(\text{ev}_n^\top)^{-1}(U^\perp)$ である, つまり符号 $\text{ev}_n(U)$ の双対符号は $(\text{ev}_n^\top)^{-1}(U^\perp)$ である.

この定理の証明は易しい. $u \in U, v \in U^\perp$ について, ある行列によって $\text{ev}_n(u) = uM$ とすると, $(\text{ev}_n^\top)^{-1}(v) = v(M^\top)^{-1} = v(M^{-1})^\top$ から

$$\text{ev}_n(u) \left((\text{ev}_n^\top)^{-1}(v) \right)^\top = uMM^{-1}v^\top = uv^\top = 0$$

だからである.

こうして $U \subset (\mathbb{F}_q)^{A_n}$ を取ってくれば, 定理 5 を用いて, 符号 $\text{ev}_n(U)$ とその双対符号 $(\text{ev}_n^\top)^{-1}(U^\perp)$ が得られる. 実際, エルミート曲線符号や代数曲線符号, 代数幾何符号と呼ばれる符号^{(13)~(15)}は, Ω_n として代数曲線等の零点集合 (一般には半群の直積ではない) を取ったものである.

Ω_n の選び方だけでなく, U の選び方もまた符号の性能に強く影響する. 勝手に U を選んでも, 良い符号が得られるとは限らない. 次の例は $\Omega_1 = \mathbb{F}_q$ としたとき, 良い符号が得られる U の選び方の例である.

[例 12] (拡大リードソロモン符号) $n = 1, q = 7, d_1 = 6$ とする. $1 \leq l \leq 6$ について, $U_l, U_l^\perp \subset (\mathbb{F}_7)^{A_1}$ を次で定める.

$$\begin{aligned} U_l &= \{(f_0, \dots, f_6) \in (\mathbb{F}_7)^{A_1} \mid f_i = 0, l \leq i \leq 6\} \\ U_l^\perp &= \{(f_0, \dots, f_6) \in (\mathbb{F}_7)^{A_1} \mid f_i = 0, 0 \leq i < l\} \end{aligned}$$

このとき $(U_l)^\perp = U_l^\perp$, つまり $U_l, U_l^\perp$ は互いに他の直交補空間であり, 次元はそれぞれ $l, 7-l$ である. 定理 5 から, $\text{ev}_1(U_l)$ と $(\text{ev}_1^\top)^{-1}(U_l^\perp)$ は互いに他の双対符号となる. 後で示すように, $(\text{ev}_1^\top)^{-1}(U_l^\perp) = \text{ev}_1(U_{7-l})$ となる⁽¹¹⁾. $\text{ev}_1(U_l)$ は拡大リードソロモン符号⁽¹¹⁾と呼ばれる符号の例である. ここでも「Vandermonde 型補題」により, $\text{ev}_1(U_l)$ の最小距離は $8-l$, $(\text{ev}_1^\top)^{-1}(U_l^\perp)$ の最小距離は $l+1$ となり, シングルトン限

界⁽¹²⁾の意味で最良である。

[例 13] (例 12 の続き) ev_1 と $(\text{ev}_1^\top)^{-1}$ を行列表示しておく。 $f = \sum_{a=0}^6 f_a x^a \in R_1$, $\text{ev}_1(f) = (c_0 \ c_3 \ c_2 \ c_6 \ c_4 \ c_5 \ c_1) \in (\mathbb{F}_7)^{\Omega_1}$ とすると,

$$(c_0 \ c_3 \ c_2 \ c_6 \ c_4 \ c_5 \ c_1) = (f_0 \ f_1 \ f_2 \ f_3 \ f_4 \ f_5 \ f_6)M,$$

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 2 & 6 & 4 & 5 & 1 \\ 0 & 2 & 4 & 1 & 2 & 4 & 1 \\ 0 & 6 & 1 & 6 & 1 & 6 & 1 \\ 0 & 4 & 2 & 1 & 4 & 2 & 1 \\ 0 & 5 & 4 & 6 & 2 & 3 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

また, $(\text{ev}_1^\top)^{-1}(f) = (d_0 \ d_3 \ d_2 \ d_6 \ d_4 \ d_5 \ d_1) \in (\mathbb{F}_7)^{\Omega_1}$ とすると,

$$(d_0 \ d_3 \ d_2 \ d_6 \ d_4 \ d_5 \ d_1) = (f_0 \ f_1 \ f_2 \ f_3 \ f_4 \ f_5 \ f_6)N,$$

$$N = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 3 & 1 & 5 & 4 & 6 \\ 0 & 3 & 5 & 6 & 3 & 5 & 6 \\ 0 & 1 & 6 & 1 & 6 & 1 & 6 \\ 0 & 5 & 3 & 6 & 5 & 3 & 6 \\ 0 & 4 & 5 & 1 & 3 & 2 & 6 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 \end{pmatrix}.$$

$l = 4$ とすると, 例えば

$$u = (5 \ 3 \ 6 \ 1 \ 0 \ 0 \ 0) \in U_4, \quad \text{ev}_1(u) = (5 \ 4 \ 1 \ 0 \ 2 \ 1 \ 1)$$

$$v = (0 \ 0 \ 0 \ 0 \ 2 \ 4 \ 3) \in U_4^\perp, \quad (\text{ev}_1^\top)^{-1}(v) = (4 \ 2 \ 2 \ 6 \ 5 \ 4 \ 5)$$

となり, $\text{ev}_1(u)$ と $(\text{ev}_1^\top)^{-1}(v)$ は確かに直交する。

また, $-N$ の下から $7-l$ 行が, M の上から $7-l$ 行と一致するから, $(\text{ev}_1^\top)^{-1}(U_l^\perp) = \text{ev}_1(U_{7-l})$ が成り立つ。

10. む す び

本稿では, 多値論理関数, 特に有限体の半群の直積を入力とするものを扱い, 多値論理多項式との対応や畳込み定理について解説し, 多値論理多項式の積の高速化に応用した。また多値論理多項式と誤り訂正符号との関係として, 代入写像とその転置の逆写像を用いて, 誤り訂正符号とその双対符号が得られることを解説した。今後も, 多値論理関数及び誤り訂正符号について, 一方の研究成果を他方の研究に応用するなど, 相互に良い影響を与えることが期待される。

謝辞 原稿を読み有益なコメントをして頂いた読者の方々, また藤沢編集委員に感謝します。

文 献

- (1) 松井 一, “多値論理多項式に対する離散フーリエ変換の応用と積の高速化,” 信学技報, IT2017-116, ISEC2017-104, WBS2017-97, p. 71, March 2018. 発表資料: <http://www.>

ieice.org/ess/sita/forum/article/2018/201804091900.pdf

- (2) D.E. Knuth, “Zeros and ones,” The Art of Computer Programming, vol. 4, Fascicle 0, Section 7.1, pp. 47–133, Addison-Wesley, 2008.
- (3) 湊 真一, “論理代数と論理関数,” 知識ベース 知識の森, 1 群 (信号・システム), 8 編 (論理回路), 1 章, 電子情報通信学会, 2010.
- (4) 笹尾 勤, 論理設計—スイッチング回路理論—, 近代科学社, 東京, 1995. (T. Sasao, Switching Theory for Logic Synthesis, Springer US, 1999.)
- (5) 高橋磐郎, 組合せ理論とその応用, 岩波全書 316, 岩波書店, 東京, 1979.
- (6) M.G. Karpovsky, R.S. Stanković, and J.T. Astola, Spectral Logic and Its Applications for the Design of Digital Devices, Wiley-Interscience, May 2008.
- (7) Proc. 2018 IEEE 48th International Symposium on Multiple-Valued Logic (ISMVL).
- (8) H. Matsui, “A convolution theorem for multiple-valued logic polynomials of a semigroup type and their fast multiplication,” IEICE Trans. Fundamentals, vol. E99-A, no. 6, pp. 1025–1033, June 2016.
- (9) H. Matsui, “On multiple-valued logic polynomials of a subset type,” Recent Results Posters at ISITA2016, p. 547, Monterey, USA, Oct.–Nov. 2016.
- (10) H. Matsui, “Lemma for linear feedback shift registers and DFTs applied to affine variety codes,” IEEE Trans. Inf. Theory, vol. 60, no. 5, pp. 2751–2769, May 2014.
- (11) 今井秀樹, 符号理論, 電子情報通信学会, 東京, 1990.
- (12) J. Justesen and T. Høholdt, A Course In Error-Correcting Codes, European Mathematical Society, 2004. (ユステセン, ホーホルト, 誤り訂正符号入門, 阪田省二郎, 栗原正純, 松井 一, 藤沢匡哉 (共訳), 森北出版, 東京, 2005.)
- (13) 阪田省二郎, “代数的符号理論,” IEICE Fundamentals Review, vol. 1, no. 3, pp. 44–57, Jan. 2008.
- (14) 松井 一, “線形帰還シフトレジスタ理論とその発展,” 信学技報, IT2013-41, pp. 1–9, Nov. 2013.
- (15) 松井 一, “符号理論における代数的手法,” IEICE Fundamentals Review, vol. 8, no. 3, pp. 151–161, Jan. 2015.

(IT 研究会提案, 平成 30 年 9 月 24 日受付,

平成 30 年 10 月 22 日再受付)

松井 一 (正員)

1999 名大大学院多元数理論科学研究科博士課程了。博士 (数理学)。1999 豊田工大・工・ポストドクトラル研究員。2002 同大学助手。2006 同大学助教授 (2007 から准教授), 現在に至る。2016 本会論文賞受賞。情報工学, 符号理論, 多値論理の研究に従事。