数理解析研究所講究録
第81巻 1970年 126-165

多値論理関数とそのカスケード合成

原尾 政輝　鈴木 淳之　野口 正一　大泉 充郎
（東北大学電気通信研究所）

まえがき．最近多値論理回路網，特に三値論理回路網の研究が重要視されている。しかし多値論理代数に関しては若干の考察がなされているが，その複雑さのために詳しい性質はあまり知られていない。従ってそれらの回路網での合成を考える場合それに適した論理系を導びくことが必要である。一般にこれらの論理系は基本演算の定義によって種々の形をとりうるが、ここでは二値論理の環和展開系の多値への拡張としての多値論理関数を定義する。この代数系はよく知られている環の構造をもち，作用素をもつベクトル空間としてのとらえ方によって，統一的に論じることができる。又このように定義された任意の論理関数のカスケードによる合成の問題はアフィン変換の概念を用いれば自由入力端子数1の基本素子（セル）の直列接続によって常に合成可能であるという結論を得る。最後に具体的回路網合成法を示し，特に三値関数に対しては具体的合成例を与え，回路網合成に必要な基本素子は一種で充分であることを示す。

1. 多値論理関数の性質

1.1. 多値論理関数の定義

真理値定数の集合を $Z_r = \{0, 1, \cdots, r-1\}$ とし、その間に有理整数環の剰余環と同型な演算すなわち"mod r"での加法"$\oplus$"乗法"$\cdot$"を定義する。これを表1.1，表1.2 に示す。

$\oplus_r$	0	1	2	3	$\cdots$	$r-1$
0	0	1	2	3	$\cdots$	$r-1$
1	1	2	3	4	$\cdots$	0
2	2	3	4	5	$\cdots$	1
3	3	4	5	6	$\cdots$	2
$\vdots$			$\vdots$			$\vdots$
$r-1$	$r-1$	0	1	2	$\cdots$	$r-2$

（表 1.1）

$\cdot$	0	1	2	3	$\cdots$	$r-1$
0	0	0	0	0	$\cdots$	0
1	0	1	2	3		$r-1$
2	0	2	4	6		$r-2$
3	0	3	6	9		$r-3$
$\vdots$			$\vdots$		$\cdots$	$\vdots$
$r-1$	0	$r-1$	$r-2$	$r-3$	$\cdots$	1

（表1.2）

<u>定理 1</u>. 演算〈 $\oplus$, $\cdot$ 〉は可換分配系であり次の関係が成り立つ；

(1) 結合律　$x \oplus (y \oplus z) = (x \oplus y) \oplus z$,　$x(y \cdot z) = (x \cdot y) \cdot z$

(2) 交換律　$x \oplus y = y \oplus x$,　$x \cdot y = y \cdot x$

(3) 分配律　$x \cdot (y \oplus z) = (y \oplus z) x = xy \oplus yz$

(4) 零元、単位元の存在．　$0 \oplus x = x$,　$1 \cdot x = x$

又これらの分配系が体をなすための必要十分条件は r が素数なることに注意しよう。

今 n を与えられた任意の正の整数とするとき、次のようなデカルト積　$Z_r^n = Z_r \times Z_r \times \cdots \times Z_r$　—— (1.1)
を考えよう。　Z_r^n の元は r^n 個の順序ずけられた元で

$$(x_1, x_2, \cdots, x_n) \qquad \text{—— (1.2)}$$

とかける。又 Z_r^n はユークリッド空間 R^n の部分空間で (1.2) 式で表わされる成分を点とよぶ。Z_r^n を n-cube と書くこともある。これを $r=3$ について図1.1に示す。

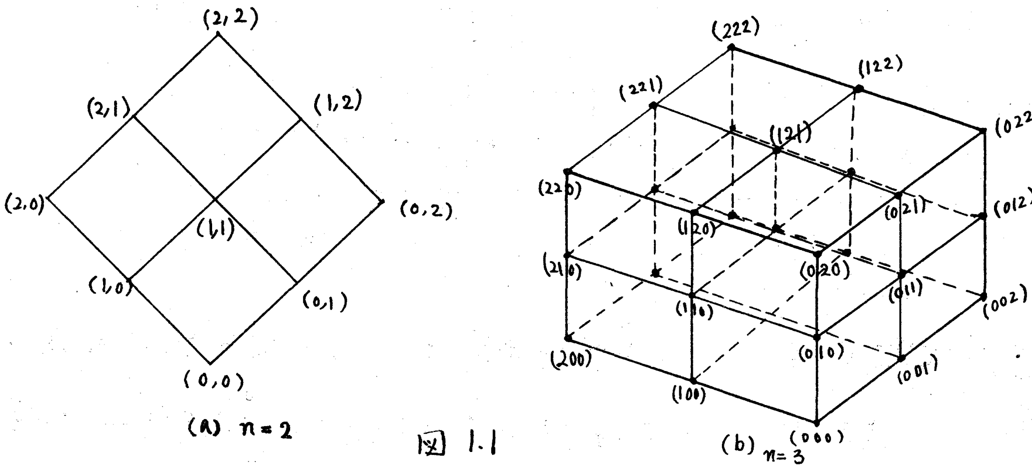

図 1.1

ここで n 変数関数　$f(x_1, x_2, \cdots, x_n)$ を写像

$$f : Z_r^n \rightarrow Z_r \qquad \text{—— (1.3)}$$

と定義する。特に n-cube のすべての点に対して1を与える単位関数を1，0を与える零関数を0で表わす。写像 f の集合を F_n とすれば、F_n の基数は r^{r^n} である。

f, g を $\mathfrak{F}_n$ の任意の二元とするとき，これらの演算を

$$f \oplus g = h \quad \Leftrightarrow \quad f(x_1, \cdots, x_n) \oplus g(x_1, \cdots, x_n) = h(x_1, \cdots, x_n)$$

$$f \cdot g = h \quad \Leftrightarrow \quad f(x_1, \cdots, x_n) \cdot g(x_1, \cdots, x_n) = h(x_1, \cdots, x_n)$$

と定義するとき，$\mathfrak{F}_n$ の部分集合 $F = \{f_i\}$ の組み合せで任意の $\mathfrak{F}_n$ の元が~~導出~~可能であるとき，この論理系 $\langle F, \oplus, \cdot \rangle$ は完備系をなすとよぶ。ここではブール環の多~~値への~~の拡張としての完備系を導びく。

今一変数関数を x とし $\overbrace{x \cdot x \cdot \cdots \cdot x}^{i} = x^i$，$\overbrace{x \oplus x \oplus \cdots \oplus x}^{i} = ix$ と書くことにする。この定義によって各々の真理値表表示は表1.3，表1.4 に表わされるように，各成分毎の積と和によって実現される。従って論理系 $\langle \oplus, \cdot \rangle$ の全ての元は単位関数 1 と一変数関数の巾 $\{x, x^2, \cdots, x^{r-1}\}$ の一次結合で表わされるが，これが完備であるための条件を求めてみる。

x	x^2	x^3	$\cdots$	x^{r-1}	1
0	0	0		0	1
1	1	1		1	1
2	2^2	2^3		2^{r-1}	1
3	3^2	3^3		3^{r-1}	1
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$r-1$	$(r-1)^2$	$(r-1)^3$		$(r-1)^{r-1}$	1

（表1.3）

x	$2x$	$3x$	$\cdots$	$(r-1)x$	$\alpha\cdot 1$
0	0	0		0	α
1	2	3		$r-1$	α
2	4	6		$r-2$	α
3	6	9		$r-3$	α
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$r-1$	$r-2$	$r-3$		1	α

(表1.4)

まず表1.5に示されるような関数

$$J_i(x) = \begin{cases} 1 & \text{if} \quad x = i \\ 0 & \text{if} \quad x \neq i \end{cases}$$

を定義し、基底関数とよぶ。

明らかにこの基底関数が導出可能なことが任意の一変数関数が合成可能なための必要十分条件である。

x	$J_0(x)$	$J_1(x)$	$\cdots$	$J_{r-1}(x)$
0	1	0		0
1	0	1		0
2	0	0	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$r-1$	0	0		1

(表1.5)

関数空間 $\mathcal{F}_n$ から Z_r の元を成分とする r^n-タップルの集合 $\mathcal{Q}_n$ への写像 χ を

$$\forall p \in Z_r^n, \quad f : p = (x_1, x_2, \cdots, x_n) \to i_p, \quad i_p \in Z_r$$

$$\Rightarrow \chi(f) = (i_0, i_1, \cdots, i_p, \cdots, i_{r^n-1}) \qquad \text{——} (1.4)$$

とすれば χ は同型である。又 $\chi^{-1}=\lambda$ とおく。

これによって

$$\forall f \cdot g \in \mathfrak{F}_n,\quad \chi \cdot f(x_1,\cdots,x_n) = (i_0, i_1, \cdots, i_{r^n-1})$$

$$\chi \cdot g(x_1,\cdots,x_n) = (j_0, j_1, \cdots, j_{r^n-1})$$

$$\Rightarrow \chi\Big(f(x_1,\cdots,x_n) \oplus g(x_1,\cdots,x_n)\Big) = (i_0 \oplus j_0,\ i_1 \oplus j_1,\ \cdots,\ i_{r^n-1} \oplus j_{r^n-1})$$

$$\chi\Big(f(x_1,\cdots,x_n) \bullet g(x_1,\cdots,x_n)\Big) = (i_0 \cdot j_0,\ i_1 \cdot j_1,\ \cdots,\ i_{r^n-1} \cdot j_{r^n-1})$$

と成分毎の加法、乗法が成立し、Z_r −加群とみなすことができる。一変数関数はそれらの部分空間をつくり、各変数に関する基底関数の積を表1.6に示す。今 $X=\{x_1, x_2, \cdots, x_n\}$ とおくと

x_n	$\cdots$	x_2	x_1	$J_0(x_1)\cdot J_0(x_2)\cdots J_0(x_n)$,	$J_1(x_1)J_0(x_2)\cdots J_0(x_n)$,	$\cdots$,	$J_{r-1}(x_1)J_{r-1}(x_2)\cdots J_{r-1}(x_n)$
0	$\cdots$	0	0	1	0		0
0		0	1	0	1		0
		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
0		0	$r-1$	0	0		0
0	$\cdots$	1	0	0	0		0
0		1	1	0	0	$\cdots$	0
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
0		1	$r-1$	0	0		0
	$\vdots$			$\vdots$	$\vdots$	$\cdots$	$\vdots$
$r-1$		$r-1$	0	0	0		0
$r-1$		$r-1$	1	0	0		0
$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$r-1$		$r-1$	$r-1$	0	0		1

(表1.6)

定理2. 論理系〈X, ⊕, ·, 1〉が完備系をなすための必要十分条件は各変数に対する基底関数が$\{1, x, \cdots, x^{r-1}\}$の一次結合として一意的に求まることである。

(証明) $J_i(x)$が一意的に求まれば、表1.6に示されるように$\mathfrak{D}_n$の表現では一成分に真理値1をもつ関数である。これは最小項に相当し、$m_i(x_1, \cdots, x_n)$と記し最小関数と定義する。ここで

$$\begin{cases} \chi \cdot m_0(x_1, \cdots, x_n) = \chi(J_0(x_1) \cdot \cdots \cdot J_0(x_n)) = (1, 0, \cdots, 0) \\ \chi \cdot m_1(x_1, \cdots, x_n) = \chi(J_1(x_1) \cdot \cdots \cdot J_0(x_n)) = (0, 1, \cdots, 0) \\ \qquad \vdots \\ \chi \cdot m_{r^n-1}(x_1, \cdots, x_n) = \chi(J_{r-1}(x_1) \cdot \cdots \cdot J_{r-1}(x_n)) = (0, 0, \cdots, 1) \end{cases} \quad \text{——(1.5)}$$

と置けば$\mathfrak{F}_n$の任意の元fはこれらの一次結合として

$$f = \sum_{i=0}^{r^n-1} d_i \cdot m_i(x_1, \cdots, x_n), \quad 0 \leq d_i \leq (r-1) \quad \text{——(1.6)}$$

と一意的に表わせる。逆に完備性の定義よりこれが完備ならば一変数関数が求まらねばならないから基底関数が求まる必要がある。又変数はr個$\{1, x, \cdots, x^{r-1}\}$, 基底関数が$r$個であるから一意的に求まらねばならない。(証明終)

今後集合$\mathfrak{F}_n$と環$\mathfrak{D}_n$は同型対応をなすから、$\mathfrak{F}_n$の元と$\mathfrak{D}_n$の元とを同一視する。

$$\begin{array}{ccc} \mathfrak{F}_n & \overset{\chi}{\underset{\lambda}{\longleftrightarrow}} & \mathfrak{D}_n \\ \downarrow & & \downarrow \\ f(x_1, \cdots, x_n) & \longleftrightarrow & Z_r^{r^n} \\ \downarrow & & \downarrow \\ m_i(x_1, \cdots, x_n) & \longleftrightarrow & m_i \end{array}$$

図1.2

<u>定理3</u> 論理系 $\langle X, \oplus, \cdot, 1 \rangle$ が完備であるための必要十分条件は r が素数なることである。

(証明) 定理2より基底関数 $J_i(x)$ が一意的に求まることを示せばよい。これは $a_i \in Z_r$ とするとき次の連立一次方程式が唯一の解を持つことと同値である。

$$
\left\{
\begin{array}{l}
a_0 \cdot 1 \oplus 0 \oplus \cdots \oplus 0 = \beta_0 \\
a_0 \cdot 1 \oplus a_1 \cdot \oplus \cdots \oplus a_{r-1} = \beta_1 \\
a_0 \cdot 1 \oplus a_1 \cdot 2 \oplus \cdots \oplus a_{r-1} \cdot 2^{r-1} = \beta_2 \\
\vdots \\
a_0 \cdot 1 \oplus a_1 \cdot (r-1) \oplus \cdots \oplus a_{r-1} \cdot (r-1)^{r-1} = \beta_{r-1}
\end{array}
\right. \qquad \text{———} (1.7)
$$

行列式 A を求めると

$$
A = \begin{vmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & 2^3 & \cdots & 2^{r-1} \\ & & \vdots & & & \\ 1 & (r-1) & (r-1)^2 & (r-1)^3 & \cdots & (r-1)^{r-1} \end{vmatrix} = 2 \cdot 3 \cdot \cdots (r-1) \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{r-2} \\ 1 & 3 & 3^2 & \cdots & 3^{r-2} \\ & & \vdots & & \\ 1 & (r-1) & (r-1)^2 & \cdots & (r-1)^{r-2} \end{vmatrix} = k \cdot A_{r-1}
$$

$$
A_{r-1} = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{r-2} \\ & & \vdots & & \\ 1 & (r-1) & (r-1)^2 & \cdots & (r-1)^{r-2} \end{vmatrix} = \begin{vmatrix} 1 & 2 & \cdots & 2^{r-4} & 2^{r-3} \\ 2 & 2 \cdot 3^{r-2} & \cdots & 2 \cdot 3^{r-4} & 2 \cdot r^{r-3} \\ & & \vdots & & \\ (r-2) & (r-2)(r-1) & \cdots & (r-2)(r-1)^{r-4} & (r-2)(r-1)^{r-3} \end{vmatrix} = 2 \cdot 3 \cdots (r-1) \begin{vmatrix} 1 & 2 & \cdots & 2^{r-4} & 2^{r-3} \\ 1 & 3 & \cdots & 3^{r-4} & 3^{r-3} \\ & & \vdots & & \\ 1 & (r-1) & \cdots & (r-1)^{r-4} & (r-1)^{r-3} \end{vmatrix}
$$

$$
= k_1 \begin{vmatrix} 1 & 1 & 2 & \cdots & 2^{r-5} & 2^{r-4} \\ 1 & 2 & 2 \cdot 3 & \cdots & 2 \cdot 3^{r-5} & 2 \cdot 3^{r-4} \\ & & & \vdots & & \\ 1 & (r-2), & (r-2)(r-1), & \cdots & (r-2)(r-1)^{r-5}, & (r-2)(r-1)^{r-4} \end{vmatrix} = k_1 \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{r-4} & 2^{r-3} \\ & & \vdots & & & \\ 1 & (r-2) & (r-2)^2 & \cdots & (r-2)^{r-4}, & (r-2)^{r-3} \end{vmatrix} = k_1 \cdot A_{r-2}
$$

同様にして　$A = k \cdot k_1 \cdot \cdots \cdot k_{r-3} \cdot A_2$ をえる。

但し　$k = 2 \cdot 3 \cdot \cdots \cdot (r-1)$，　$k_i = 2 \cdot 3 \cdot \cdots \cdot (r-i-1)$

$$A_2 = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} = 1$$

ゆえに　$A = 2^{r-2} \cdot 3^{r-2} \cdot \cdots \cdot (r-2)^2 \cdot (r-1)$　——（1.8）

(i)　A は r が素数ならば $A \not\equiv 0 \pmod{r}$ を満す

(ii)　$A \not\equiv 0 \pmod{r}$ と仮定する。

(イ)　$r = 3$ なら $A = 2 \not\equiv 0 \pmod{3}$ より条件を満す

(ロ)　$r = 4$ なら $A \equiv 0 \pmod{4}$ より条件を満す。

(ハ)　$r \geq 5$ と仮定する。この時証明のためにまず次の補題を示す。

<u>補題 1.</u>　r を $r \geq 5$ なる任意の実数とすれば，$2 \leq x \leq r-2$ に対して　$(r-x)^x > r$　が成立する。

（証明）　$f(x) = (r-x)^x - r$ とおく．

$$\frac{df}{dx} = \frac{d}{dx}\left(e^{x \log_e (r-x)} - r\right) = \left(\log_e (r-x) + \frac{-x}{r-x}\right)(r-x)^x$$

仮定より　$(r-x)^x > 0$

(A)　$g(x) = \log(r-x) - \dfrac{x}{r-x}$ とおけば

$$\frac{dg(x)}{dx} = \frac{x-2r}{(r-x)^2} < 0 \quad (2 \leq x \leq r-2)$$ より $g(x)$ は単調減少

かつ $g(2) = \log(r-2) - \dfrac{2}{r-2} > 0$，$g(r-2) = \log 2 + \dfrac{2-r}{2} < 0$

より f は Fig. 1.3 のようになる。

(b) $f(2) = (r-2)^2 - r = r^2 - 5r + 4$, かつ $\dfrac{df(2)}{dr} = 2r - 5 > 0$

より r に関して単調増加, かつ $f(2)|_{r=4} = 0$. $f(2)|_{r=5} = 4$,

(c) $f(r-2) = 2^{r-2} - r$, かつ $\dfrac{df(r-2)}{dr} = (\log 2)\cdot 2^{r-2} - 1 > 0$

より r に関して単調増加, かつ $f(r-2)|_{r=4} = 0$ $f(r-2)|_{r=5} = 3$

即ち $r \geqq 5$ であれば $f > 0$ ゆえに $(r-x)^x > r$

(証明終)

従って補題1より

$$A = 2^{r-2}\cdot 3^{r-3}\cdots(r-2)^2(r-1) \not\equiv 0 \pmod r$$

で $r = 2^{\varepsilon_2}\cdot 3^{\varepsilon_3}\cdots(r-1)^{\varepsilon_{r-1}}$ と分解されたとすると, 各因子 i^{ε_i} は A の因子に含まれている。故に指数 $\varepsilon_2, \cdots, \varepsilon_{r-2}$ は全て零でなければならない。即ち r は素数でなければならない。

(証明終)

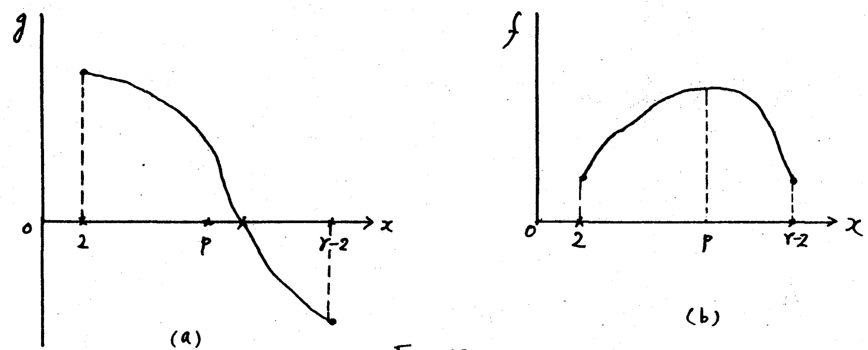

Fig. 1.3

1.2 多値論理関数の表現

一般にはここで定義した演算以外に更に独立な単項演算を定義すれば、rが素数以外でも完備系にすることが可能である。しかし実際回路網を合成する場合には演算が簡単な程、構成素子が少なくてすみ能率的である。又ここに定義した関数の構造はカスケード合成に適しており、以後rを素数に限ってこの関数の性質と合成法を述べてゆく。

<u>補題2.</u>（ウィルソンの定理）　rを素数とすれば、$(r-1)! \equiv -1\ (r)$

（証明）$GF(r^n)$ の 0と異なるすべての要素を $a_1, a_2, \cdots, a_h$ とすると

$$x^h - 1 = \prod_1^h (x - a_i)$$

が成りたつから　$a_1 \cdot a_2 \cdot \cdots \cdot a_h = -1$

特に $n = 1$ とすると rが素数だから $1, 2, \cdots, (r-1)$ が $GF(r)$ の元で　$(r-1)! \equiv -1\ (\mathrm{mod}\ r)$　（証明終）

<u>定理4.</u> 基底関数 $J_i(x)$ は次のように書ける：

$$J_i(x) = (r-1) \cdot x \cdot (x \oplus 1) \cdots\cdots (x \oplus (r-i-1)) \cdot (x \oplus (r-i+1)) \cdots (x \oplus (r-1)) \qquad (1.9)$$

又

$$J_i(x) \cdot J_j(x) = \begin{cases} J_i(x) & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \qquad (1.10)$$

（証明）$x = i$ とおけば(1.9)式右辺は $(r-1) \cdot i \cdot (i+1) \cdot \cdots (r-1) \cdot 1 \cdot 2 \cdot \cdots (i-1) = 1 \cdot 2 \cdot \cdots (i-1) \cdot i\,(i+1) \cdot \cdots (r-2)\,(r-1)^2$

$$= (r-1) \cdot (r-1)!$$

補題２より　$(r-1)! = (r-1)$,　$\therefore$　$(r-1)(r-1)! \equiv 1 \pmod{r}$

$J_i(j)$　$(i \neq j)$ なら明らかに $J_i(j) = 0$　故に成立

$J_i^2(x)$ は $x = i$ のとき $J_i(i) = 1$ だから $J_i^2(x) = 1$ それ以外では 0 だから $J_i^2(x) = J_i(x)$，　又 $J_i(x) \cdot J_j(x)$ は同時に真理値 1 をとることはないから $J_i(x) \cdot J_j(x) = 0$　（証明終）

関数空間 $\mathfrak{F}_n$ の間に成り立つ性質を調べてみよう。

<u>定理５.</u>　$\mathfrak{F}_n$ の元の間には次の演算が成立する。

(1) $f^r = f^{tr} = f$，　$rx = r \cdot t x = 0$　$(t = 1, 2, \cdots)$

(2) $(if)(jg) = (ij) f \cdot g$，　$if \oplus jf = (i \oplus j) f$

(3) $f \oplus g = g \oplus f$，　$f \cdot g = g \cdot f$

(4) $f \cdot (g \cdot h) = (f \cdot g) \cdot h$，　$f \oplus (g \oplus h) = (f \oplus g) \oplus h$

(5) $f \cdot (g \oplus h) = (g \oplus h) \cdot f = f g \oplus f h$

（証明）　(1) r が素数であるから，Fermat の定理より $a \neq 0$ なる任意の数に対して　$a^{r-1} \equiv 1 \pmod{r}$　が成立する。

$$f = (a_1, a_2, \cdots, a_{r^n}) \quad , \quad a_i \in Z_r$$

とおくと $f^{r-1} = (a_1^{r-1}, a_2^{r-1}, \cdots, a_{r^n}^{r-1}) = (1, 1, \cdots, 1) = 1$

故に $f^r = f$，同様にこれをくり返せば　$f^{tr} = f$.

又加法に対しては　$rf = (r a_1, r a_2, \cdots, r a_{r^n}) = (0, 0, \cdots, 0) = 0$

(2) 作用素 Z_r は可換体であるから

$f = (a_1, a_2, \cdots, a_{r^n})$,　$g = (b_1, b_2, \cdots, b_{r^n})$

$\Rightarrow$ $(if)(jg) = (i a_1, i a_2, \cdots, i a_{r^n}) \cdot (j b_1, j b_2, \cdots, j b_{r^n})$

$$= \left((ia_1)(jb_1),\ (ia_2)(jb_2),\ \cdots,\ (ia_{r^n})(jb_{r^n}) \right)$$
$$= \left(ij(a_1b_1),\ (ij)(a_2b_2),\ \cdots,\ (ij)(a_{r^n}\cdot b_{r^n}) \right)$$
$$= (ij)(f\cdot g)$$

(3), (4) も同様にしてでる。

(5) $$f\cdot(g\oplus h) = (a_1, a_2, \cdots, a_{r^n})\cdot(b_1\oplus c_1,\ b_2\oplus c_2, \cdots,\ b_{r^n}\oplus c_{r^n})$$
$$= (a_1(b_1\oplus c_1),\ a_2(b_2\oplus c_2), \cdots,\ a_{r^n}(b_{r^n}\oplus c_{r^n}))$$
$$= ((b_1\oplus c_1)a_1,\ (b_2\oplus c_2)\cdot a_2, \cdots,\ (b_{r^n}\oplus c_{r^n})\cdot a_{r^n}) = (g\oplus h)f$$
$$= (a_1b_1\oplus a_1c_1,\ a_2b_2\oplus a_2c_2, \cdots,\ a_{r^n}\cdot b_{r^n}\oplus a_{r^n}\cdot c_{r^n}) = fg\oplus f\cdot h$$

（証明終）

二値の場合、ブール環は全ての元が $f^2 = f$ なる巾等元であるという定義であった。この一般化として(1)に示されるように多値環 $\mathfrak{Q}_n$ を $f^r = f$ なる元よりなる可換環として定義することができる。又任意の与えられた多値論理関数 f の点 m_j に対する真理値を t_j とすれば、関数 f は次のように最小関数の一次結合として展開される。

<u>定理 6.</u> 任意の関数は加法展開公式を用いて次のように求まる。

$$f(x_1, \cdots, x_n) = J_0(x_1)\cdot f(0, x_2, \cdots, x_n) \oplus J_1(x_1)\cdot f(1, x_2, \cdots, x_n)$$
$$\oplus \cdots \oplus J_{r-1}(x_1)\cdot f(r-1, x_2, \cdots, x_n) \qquad \text{—— (1.11)}$$
$$= \sum_{i=0}^{r^n-1} t_i\, m_i(x_1, \cdots, x_n) \qquad \text{—— (1.12)}$$

（証明）(1.11)式において 左辺 $= f(i, x_2, \cdots, x_n)$ とすると右辺は

$$J_i(i)\cdot f(i, x_2, \cdots, x_n) = f(i, x_2, \cdots, x_n)$$

故に公式が成立する。これを繰り返し使用すると，$m_i(x_1,\cdots,x_n) = J_{i_1}(x_1)\cdot J_{i_2}(x_2)\cdot\cdots\cdot J_{i_n}(x_n)$ は i 成分にのみ 1 をもつ項となるから，それに真理値 λ_i を与えれば

$$f(x_1, \cdots, x_n) = \sum_{i=0}^{r^n} \lambda_i\, m_i(x_1, \cdots, x_n)$$

が成りたつ。　　　　　　　　　　　　　　　　　　　　（証明終）

$J_0(x_1) \oplus J_1(x_1) \oplus \cdots \oplus J_{r-1}(x_1) = 1$ を用いて (1.11) 式を変形すれば次の乗法展開公式が得られる。

<u>系 1.</u>　乗法展開公式 $f(i, x_2, \cdots, x_n) = f(i)$ とおくと

$$f(x_1, \cdots, x_n) = (f(0) \oplus J_1 \oplus \cdots \oplus J_{r-1})(f(1) \oplus J_0 \oplus J_2 \oplus \cdots \oplus J_{r-1})$$
$$\cdots(f(r-1) \oplus J_0 \oplus \cdots \oplus J_{r-2})$$
$$= ((f(0)-1)J_0 \oplus 1)\cdot((f(1)-1)J_1 \oplus 1)\cdot\cdots\cdot((f(r-1)-1)J_{r-1} \oplus 1) \quad \text{-- (1.13)}$$

<u>例題 1.</u>　三値論理関数の基底関数を求め，次に与えられた真理値表表示を展開せよ。

x	y	f
0	0	1
0	1	2
0	2	1
1	0	0
1	1	2
1	2	0
2	0	1
2	1	0
2	2	2

x	x^2	$J_0(x)$	$J_1(x)$	$J_2(x)$
0	0	1	0	0
1	1	0	1	0
2	1	0	0	1

$$J_0(x) = 1 \oplus 2x^2$$

$$J_1(x) = 2x \oplus 2x^2$$

$$J_2(x) = x \oplus 2x^2$$

$$
\begin{aligned}
f = {} & J_0(y)\cdot J_0(x) \oplus 2J_1(y)\cdot J_0(x) \oplus J_2(y)\cdot J_0(x) \\
& \oplus 0\cdot J_0(y)\cdot J_1(x) \oplus 2J_1(y)\cdot J_1(x) \oplus 0\cdot J_2(y)\cdot J_1(x) \\
& \oplus J_0(y)\cdot J_2(x) \oplus 0\cdot J_1(y)\cdot J_2(x) \oplus 2\cdot J_2(y)\cdot J_2(x) \\
= {} & (1 \oplus 2x^2)(1 \oplus 2y^2) \oplus 2(2y^2 \oplus 2y)(2x^2 \oplus 1) \oplus (2y^2 \oplus y)(2x^2 \oplus 1) \\
& \oplus 2(2y^2 \oplus 2y)(2x^2 \oplus 2x) \oplus (2y^2 \oplus 1)(2x^2 \oplus x) \oplus 2(2x^2 \oplus x)(2y^2 \oplus y) \\
= {} & x^2 \oplus x^2 y \oplus xy \oplus 2xy^2 \oplus x \oplus 2y^2 \oplus 2y \oplus 1
\end{aligned}
$$

1.3. 多値論理関数の代数的構造

関数空間 $\mathfrak{D}_n$ の構造を調べてみる。前節で述べたように多値環 $\mathfrak{D}_n$ は r^n タップルの~~成分毎~~の乗法と加法に対して環をなし、$f^r = f$ を満す可換環であった。又係数体 Z_r を作用素とする多元環とみることができる。これは

$$\forall a \in Z_r, \quad f, g \in \mathfrak{D}_n$$

$$a(f\cdot g) = (af)g = f(a\cdot g)$$

が成り立つことが容易に示される。 更にこれらの基底は $m_i \ (0 \leq i \leq r^n - 1)$ であった。

$\mathfrak{D}_n$ の部分集合を B とするとき

(i) $f, g \in B \Rightarrow f - g \in B$

(ii) $f \in B,\ g \in \mathfrak{D}_n \Rightarrow f\cdot g \in B$ （又は $gf \in B$）

の条件を満すとき左(右) ideal とよばれる。ここでは可換環であるから両側 ideal である。

<u>定理7.</u> 最小関数の集合を $P_n = \{ m_0, m_1, \cdots, m_{r^n} \}$

P_n の部分集合を $\Lambda = \{ m_{i_1}, \cdots, m_{i_l} \}$ とする。このとき

Λ の元の一次結合で生成された関数 Λ^* は $\mathfrak{D}_n$ の ideal

をなす。

(証明) (i) $\forall f, g \in \Lambda^*$, $f = \sum_{m_{ij} \in \Lambda} c_j m_{ij}$, $g = \sum_{m_{ij} \in \Lambda} d_i m_{ij}$

ゆえに $f - g = \sum_{m_{ij} \in \Lambda} (c_j - d_j) m_{ij} \in \Lambda^*$

(ii) $\forall f \in \Lambda^*$, $\forall g \in \mathfrak{D}_n$; $g = \sum_{m_{ij} \in P_n} e_j \cdot m_{ij}$

ゆえに $f \cdot g = \left(\sum_{m_{ij} \in \Lambda} c_j m_{ij} \right) \left(\sum_{m_{ij} \in P_n} e_j m_{ij} \right)$

$$= \sum_{m_{ij} \in \Lambda} c_j e_j m_{ij} \in \Lambda^* \left(\because \ m_i \cdot m_j = \begin{cases} 0 & \text{if } i \neq j \\ m_i & \text{if } i = j \end{cases} \right)$$

(証明終)

特に一個の最小関数の結合のみよりなる部分集合も明らかに ideal をなし，これを単項 ideal とよぶ。

<u>定理8.</u> 各最小関数 m_i によって生成された単項ideal を

$\mathfrak{a}_i$ とおくと，$\mathfrak{a}_i = \mathfrak{D}_n \cdot m_i$ で

$$\mathfrak{D}_n = \mathfrak{a}_0 \oplus \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_{r^n-1}$$

と一意的に表わされる。

(証明) 単位元 $1 = m_0 \oplus m_1 \oplus \cdots \oplus m_{r^n-1}$ と分解され

$m_i \cdot m_j = 0$ (if $i \neq j$), $m_i^2 = m_i$ より $\mathfrak{D}_n$ は m_i より生成される ideal の直和であることが分る。又単項ideal $\mathfrak{a}_i$ は i 成分とのみ Z_r の元をとる関数であるから，$\mathfrak{a}_i = \mathfrak{D}_n m_i$. (証明終)

環のidealの集合や環の部分環の集合はその包含関係の下に束をなす。この多値環の束構造を調べてみる。

環 $\mathfrak{D}_n$ の任意の2元　$a=(i_0, i_1, \cdots, i_{r^n-1})$，$b=(j_0, j_1, \cdots, j_{r^n-1})$ に対し　$a \geq b \Leftrightarrow \forall p,\ i_p \geq j_p$

と関係 $\geq$ を定義する。

<u>補題3</u>　関係 $\geq$ は順序関係で，$(\mathfrak{D}_n, \geq)$ は半順序集合をなし，更に完備束である。

(証明)　Z_r は全順序集合だから　(i) $a \geq a$，(ii) $a \leq b, b \leq c \Rightarrow a \leq c$

(iii) $a \geq b,\ a \leq b \Rightarrow a = b$ が成りたつことは明らか。故に半順序集合であって

$$a \cup b = (i_0 \cup j_0, i_1 \cup j_1, \cdots, i_{r^n-1} \cup j_{r^n-1})$$

$$a \cap b = (i_0 \cap j_0, i_1 \cap j_1, \cdots, i_{r^n-1} \cap j_{r^n-1})$$

但し　$i \cup j = \max(i, j)$，　$i \cap j = \min(i, j)$

とおくと　上限 $\sup\{a, b\} = a \cup b$，下限 $\inf\{a, b\} = a \cap b$ が存在するから束をなし，有限束であるから完備束である。

(証明終)

$L_n = \langle \mathfrak{D}_n, \cup, \cap \rangle$ とおくと　L_n は $\cup, \cap$ について

(1) 巾等律　(2) 結合律　(3) 交換律　(4) 吸収律　を満す可換半群をつくっている。

<u>定理9.</u>　束 L_n は最大元，最小元を持つ分配束である。

(証明)　$I = (r-1, r-1, \cdots, r-1)$，$0 = (0, 0, \cdots, 0)$ とおけば任意の L_n の元に対して　$0 \leq f \leq I$　よりそれぞれ最大

元と最小元である。分配律 $f \cap (g \cup h) = (f \cap g) \cup (f \cap h)$

$f \cup (g \cap h) = (f \cup g) \cap (f \cap h)$ が成り立つことは Z_r が全順序集合

だから $f_i \cap (g_i \cap h_i) = \begin{cases} f_i \cap g_i & \text{if } g_i \geq h_i \\ f_i \cap h_i & \text{if } g_i \leq h_i \end{cases}$, $(f_i \cap g_i) \cup (f_i \cap h_i) = \begin{cases} f_i \cap g_i & \text{if } g_i \geq h_i \\ f_i \cap h_i & \text{if } g_i \leq h_i \end{cases}$

より示される。

(証明終)

ブール束には (i) $f \cup \bar{f} = I$ (ii) $f \cap \bar{f} = 0$ の存在が必要であったが、L_n はこの条件を満さない。この相補律の代りに次のような演算を L_n に定義する。

(1) $\tilde{f} = I \ominus f$ ($\ominus$ は $\oplus$ に対する逆元) (2) $f^{\urcorner} = f \oplus 1$

すると $L^* = \langle \cup, \cap, \sim, \urcorner \rangle$ は完備系をなし Post 代数とよばれる。今 r を素数とすれば $\mathfrak{F}_n$ と L^* は次の対応をなす (3值)

$$x \cup y = x^2y^2 \oplus x^2y \oplus xy^2 \oplus 2xy \oplus x \oplus y$$

$$x \cap y = 2x^2y^2 \oplus 2x^2y \oplus 2xy^2 \oplus xy$$

$$\tilde{x} = 2 \oplus 2x, \quad x^{\urcorner} = 1 \oplus x, \quad \tilde{x}^{\urcorner} = 1 \oplus 2x \quad \tilde{x}^{\urcorner\urcorner} = 2 \oplus x \quad \text{etc.}$$

$\mathfrak{D}_n$ の順序関係 $\geq$ に対して

(1) $a \geq b \Rightarrow b = a$ 又は $b = 0$

が成り立つとき $\mathfrak{D}_n$ の元 a は atom であるとよぶ。$\mathfrak{D}_n$ の atom は基底 m_i である。これもブール環の拡張概念である。

2. 多段論理回路網による多値論理関数の合成.

2.1. 多段論理回路網の表現.

取り扱かう回路は純組合せ的であるとする。この回路網の基本素子をセルとよび,数種のセルのカスケードよりなる回路を多段論理回路,特に一種のセルのカスケードよりなる回路を反復論理回路とよぶ。(Fig. 1).

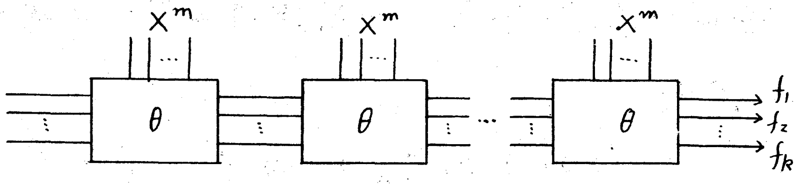

図 2.1

なお Z 端子入力を自由変数, y 入力を接続変数とよび,それぞれ r 値で r は素数とする。又 Z 端子 m, 接続端子 k のセルを (m,k)-セルと略記する。まず (m,k)-セルの接続変数を

$$(y_1, y_2, \cdots ; y_k) \leftrightarrow y_k + r\, y_{k-1} + \cdots + r^{k-1} y_1 \quad \text{—(2.1)}$$

と対応させ,この整数の集合 $N = \{0, 1, \cdots, r^k - 1\}$ を状態集合とよぶ。集合 N の上の変換を $T_N = \{t \mid N \to N\}$ とすればセル θ は入力の制御の下での写像

$$\theta : Z_r^m \to T_N \quad \text{—(2.2)}$$

とみなすことができる。特にここでは θ の値域として可換群 $H \subset T_N$ をとる。すると多値関数 $f : Z_r^n \to N$ の合成問題は変換回路網 $f : Z_r^n \to H$ の合成問題に帰着される。又前章でのべたように関数 f は r^n 次元の N を成分とするベクトル空

間と同型だから、fとそれらを同一視する。(今後変数の意味でZ_rの代りにXを用いる)

今任意の群関数を $f_i : X^m \to H$, $f_j : X^{m'} \to H$ ——(2.3)

とするとき、r^n次元空間の元として

$$f_i(X^m) = (h_0, h_1, \cdots, h_{r^n-1}) \qquad h_i \in H$$

$$f_j(X^{m'}) = (h_0', h_1', \cdots, h_{r^n-1}') \qquad h_i' \in H$$

と表わす。今 f_i と f_j のカスケードを $f_i \oplus f_j$ とすると

$$(f_i \oplus f_j)(X^m, X^{m'}) = f_i(X^m) \oplus f_j(X^m) = (h_0 \oplus h_0', h_1 \oplus h_1', \cdots, h_{r^n_{-1}} \oplus h_{r^n_{-1}}')$$

と成分毎の和、即ちカスケードはベクトル空間の加法に対応する。

一般に回路網がセル $\theta_i : X^m \to H$ のカスケードで合成される時 m 変数で合成可能とよぶが、今後1変数での合成可能性について話を限ることにする。今n変数での変換回路網(群関数)の集合を $\mathcal{H}_n$ と書く。$\mathcal{H}_n$ は群Hの元の間に乗法が定義できれば成分毎の積として環をつくる。Hを任意の可換群とすればHの自己同型の全体は単位環をつくり、その作用素の意味での演算が乗法に対応する。ここでは自己準同型 E(H) の加法 $E(\overset{+}{H})$ とHを同一視する。

<u>定理10</u> $\mathcal{H}_n$ はHの自己準同型環 E(H) が可換ならば E(H) の上の階数 r^n の多元環をなす。

(証明) 命題より $E(\dot{H})$ は単位可換環となるから

$$^{\forall} h \in E(H), \quad ^{\forall} F, G \in \mathcal{H}_n$$

$$h\cdot(F\cdot G) = h\cdot((f_1, f_2, \cdots, f_{r^n})\cdot(g_1, g_2, \cdots, g_{r^n}))$$
$$= (h(f_1\cdot g_1), h(f_2\cdot g_2), \cdots, h(f_{r^n}\cdot g_{r^n}))$$
$$= ((hf_1)\cdot g_1, (hf_2)\cdot g_2, \cdots, (h\cdot f_{r^n})\cdot g_{r^n}) = (h\cdot F)G$$
$$= (f_1(hg_1), f_2(h\cdot g_2), \cdots, f_{r^n}(h\cdot g_{r^n})) = F(h\cdot G)$$

（証明終）

このときベクトル基底の存在はHとして位数r^kの巡回群及び基本可換群C_r^kをとれば次のように示される。

<u>定理11.</u> 位数r^kの巡回群をC_{r^k}とすれば，回路網$f: X^n \to C_{r^k}$の集合$\mathcal{H}_n$は$Z/(r^k)$の上の階数r^nの多元環と同型で，基底は一意的に定まる。

（証明）$E(C_{r^k})$は$Z/(r^k)$と同型であるから，前定理より$Z/(r^k)$上の階数r^nの多元環として表わされ，基底は$\{1, x, x^2, \cdots, x^{r-1}\}$の一次結合として表現されねばならない。前章定理3の場合と同様に

$$A = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{r-1} \\ & \vdots & & & \vdots \\ 1 & (r-1) & (r-1)^2 & \cdots & (r-1)^{r-1} \end{vmatrix} = 2^{r-2}\cdot 3^{r-3}\cdot \cdots \cdot (r-2)^2(r-1) \not\equiv 0 \pmod r$$

であるから，$A \not\equiv 0 \pmod{r^k}$である。従って基底関数

$J_0(x)$, $J_0(x)$, $\cdots$, $J_{r-1}(x)$が一意的に求まる。又基底はこれらの積として一意的に定まる。　　　　（証明終）

ベクトル基底を最小関数とよび，$m_i(x_1, x_2, \cdots, x_n)$ とおくと $\mathcal{H}_n$ の元はこれらの一次結合として一意的に次のように展開される；

$$f(X^n) = \sum_{i=0}^{r^n-1} d_i\, m_i(x_1, x_2, \cdots, x_n) \qquad \text{—— (2.4)}$$

$$m_i \cdot m_j = \begin{cases} 0 & \text{if } i \neq j \\ m_i & \text{if } i = j \end{cases}, \quad \sum_{i=0}^{r^n-1} m_i = 1 \qquad \text{—— (2.5)}$$

$$d_i \in Z/(r^k)$$

(2.5) 式より，$m_i(x_1, \cdots, x_n)$ は atom で

$$\mathcal{H}_n = \mathcal{H}_n \cdot m_0 \oplus \mathcal{H}_n \cdot m_1 \oplus \cdots \oplus \mathcal{H}_n \cdot m_{r^k-1} \qquad \text{—— (2.6)}$$

と単項 ideal の直和に分解される。

同様に群 H として基本可換群 C_r^k をとると，$Z/(r)$ 上の k 次元ベクトルと同型であるから次の結果を得る。

<u>定理 12.</u> 回路網 $f: X^n \to C_r^k$ の集合 $\mathcal{H}_n$ は $GF(r^k)$ の上の階数 r^k の多元環と同型で，$\mathcal{H}_n$ の任意の元は一意的に定まるベクトル基底を $m_i(x_1, x_2, \cdots, x_n)$ とすれば次のように展開される；

$$f(X^n) = \sum_{i=0}^{r^n-1} v_i\, m_i(x_1, x_2, \cdots, x_n) \qquad \text{—— (2.7)}$$

$$= \sum_{i=0}^{r^n-1} (v_{j0} m_j,\ v_{j1} \cdot m_j,\ \cdots,\ v_{j\,k-1} \cdot m_j) \qquad \text{—— (2.8)}$$

$$= (\mathcal{X}_0,\ \mathcal{X}_1,\ \cdots,\ \mathcal{X}_{k-1})$$

但し $v_i = (v_{i0}, v_{i1}, \cdots, v_{i\,k-1}) \in (Z/(r))^k$.

基本可換群を用いた群関数は図2.2に示すように各端子毎の関数の表現を与え，x_i は i 端子の出力関数を示している。又回路網では C_r^k の生成元に対応する k 種のセルが必要である。更にこの時の基底関数は r 値論理関数のものと同様である。

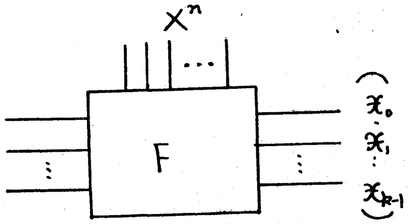

図2.2

これらの(2.4), (2.7)式は多値論理関数の加法展開の一般化であり，これを最小関数表示とよぶ。最小関数表示の項を $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$ とするとき長さを $l_n(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n})$ と定義し，0でない ε_i の個数とする。このとき最小関数表示の各項の長さは，セルへの入力の数を又係数はその所要個数を示す。従ってこの表示の最大長が l ならば，この回路網は l 変数で合成可能である。故に $(1,k)$-セルで合成するには何らかの他の方法が必要である。

<u>例題2.</u> 次の真理値表表示された回路網 $f: X^n \to C_3^2$ を最小関数表示せよ。

$$
\begin{aligned}
F = {} & (0,1)\, J_0(x_1)\cdot J_0(x_2) \oplus (2,0)\, J_1(x_1)\cdot J_0(x_2) \oplus (1,1)\, J_2(x_1)\cdot J_0(x_2) \\
& \oplus (1,0)\, J_0(x_1)\cdot J_1(x_2) \oplus (0,2)\, J_1(x_1)\cdot J_2(x_2) \oplus (0,1)\, J_2(x_1)\cdot J_1(x_2) \\
& \oplus (1,2)\, J_0(x_1)\cdot J_2(x_2) \oplus (0,0)\, J_1(x_1)\cdot J_2(x_2) \oplus (2,1)\, J_2(x_1)\cdot J_2(x_2)
\end{aligned}
$$

$$J_0 = 1 \oplus 2x^2, \quad J_1 = 2x \oplus 2x^2, \quad J_2 = 2x^2 \oplus x$$

を代入すれば

$$F = (2x_1,\ 1 \oplus x_1 \oplus x_1^2) \oplus (2x_1 \oplus x_1^2,\ 2x_1 \oplus 2)\, x_2$$
$$\oplus\ (2x_1 \oplus 1 \oplus x_1^2,\ 2x_1 \oplus 2x_1^2)\, x_2^2$$
$$= (2x_1 \oplus 2x_1x_2 \oplus x_1^2x_2 \oplus 2x_1x_2^2 \oplus x_2^2 \oplus x_1^2x_2^2,$$
$$1 \oplus x_1 \oplus x_1^2 \oplus 2x_1x_2 \oplus 2x_2 \oplus 2x_1x_2^2 \oplus 2x_1^2x_2^2)$$

x_2	x_1	f_2	f_1	$2x_1$,	$2x_1x_2$,	$x_1^2x_2$,	$2x_1x_2^2$,	x_2^2,	$x_1^2x_2^2$	1,	x_1,	x_1^2,	$2x_1x_2$,	$2x_2$,	$2x_1x_2^2$	$2x_1^2x_2$
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	1	2	0	2	0	0	0	0	0	1	1	1	0	0	0	0
0	2	1	1	1	0	0	0	0	0	1	2	1	0	0	0	0
1	0	1	0	0	0	0	0	1	0	1	0	0	0	2	0	0
1	1	0	2	2	2	1	2	1	1	1	1	1	2	2	2	2
1	2	0	1	1	1	1	1	1	1	1	2	1	1	2	1	2
2	0	1	2	0	0	0	0	1	0	1	0	0	0	1	0	0
2	1	0	0	2	1	2	2	1	1	1	1	1	1	1	2	2
2	2	2	1	1	2	2	1	1	1	1	2	1	2	1	1	2

表2.1

2.2 環論的回路網の合成

回路網の表現としての $\mathfrak{M}_n$ は多元環をなし、$\mathfrak{M}_n$ の加法に対しては回路網のカスケードが対応し、各項の変数が入力を示すのであった。これに対し $\mathfrak{M}_n$ には更に乗法が定義されており、$\mathfrak{M}_n$ の元を r^n-次元ベクトルとみなした時これはこの空間の一次変換に対応し回路網では一定のセルの配列に相当する。従って非線形変換をその複雑さより考察の対称より除外すれば回路網合成の問題はアフィン変換の概念を用いて解くことができる。又各入力はベクトルの点を指定するだけであるから、本質的には係数の上の一次変換の性質を調べればよい。

ここでは巡回群 C_{r^k} と基本可換群 C_r^k の群関数としての回路網について論じる。

定理13. r を2と異なる素数とするとき、C_{r^k} の生成元 a に対して、作用素 φ_i を $\varphi_i \cdot a = g^{-1} a \cdot g = a^i$ とすれば、i が r の巾と異なるとき単位元を単位元に移す自己同型作用素である。
又 Euler 関数を $\phi(r^k)$ とすれば、この自己同型作用素の全体 $A(C_{r^k})$ は $\phi(r^k)$ 又はその約数を位数とする巡回群をなす。
ここで

$$g = \begin{pmatrix} 0 & 1 & 2 & \cdots & r^k-1 \\ 0 & i & 2i & \cdots & (r^k-1)i \end{pmatrix}$$

(証明) $g.c.d(i, r^k) = 1$ であるから、$\exists p, q \in \mathbb{Z}/(r^k)$

$pi + q \cdot r^k = 1 \quad \therefore \quad pi \equiv 1 \pmod{r^k}$. 故に φ_i は自己同型

更に $i^{\phi(r^k)} \equiv 1 \pmod{r^k}$ より $\mathcal{G}_i^{\phi(r^k)}\cdot a = a^{\phi(r^k)\cdot i} = a = \mathcal{G}_i\cdot a$

∴ $\mathcal{G}_i^{\phi(r^k)} = \mathcal{G}_i$ すなわち $\mathcal{G}_i$ は $\phi(r^k)$ 又はその約数を位数とする巡回群をなす。

又 $a = \begin{pmatrix} 0 & 1 & 2 & \cdots & r^k-1 \\ 1 & 2 & 3 & \cdots & 0 \end{pmatrix}$ とおくと $\mathcal{G}_i\cdot a = g^{-1}\cdot a\cdot g = \begin{pmatrix} g(0),\ g(1),\ \cdots,\ g(r^k-1) \\ g(1),\ g(2),\ \cdots,\ g(0) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & \cdots & r^k-1 \\ i & i+1 & i+2 & \cdots & i+r^k-1 \end{pmatrix} = a^i$

かつ $g(0) = 0$ より $g = \begin{pmatrix} 0 & 1 & 2 & \cdots & r^k-1 \\ 0 & i & 2i & \cdots & (r^k-1)i \end{pmatrix}$ （証明終）

図2.3に示されるようにセル入力 x_n の下で $n-1$ 変数関数に作用素 $\mathcal{G}_i$ を用いることを $\mathcal{G}_i^{x_n}$ と表わす。これは空間 $\mathcal{S}_n$ では x_n の指定するベクトル成分に作用素 $\mathcal{G}_i$ を施すことを意味する。真理値表での作用素の働きを表2.2に示す。各点は作用素の有無によって

$$i J_l(x_n)\cdot f_{n-1} \quad \text{又は} \quad J_l(x_n)\cdot f_{n-1}$$

となり

$$\mathcal{G}_i^{x_n} f_{n-1} = J_0(x_n)\cdot f_{n-1} \oplus i J_1(x_n)\cdot f_{n-1} \oplus \cdots \oplus i J_{r-1}(x_n)\cdot f_{n-1}$$

と変形される。一般に任意の n 変数関数が与えられたとき、その最小関数表示より $n-1$

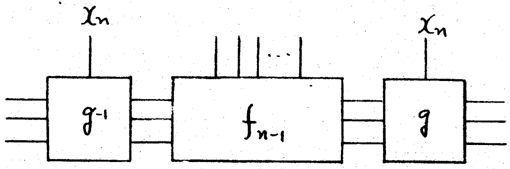

図2.3

x_n	$\mathcal{G}_i^{x_n} f_{n-1}$	
0	$e\ a_0\ e$ $e\ a_1\ e$ $\vdots$ $e\ a_{r^{n-1}-1}\ e$	$J_0(x_n)\cdot f_{n-1}$
1	$g^{-1}\ a_0\ g$ $g^{-1}\ a_1\ g$ $\vdots$ $g^{-1}\ a_{r^{n-1}-1}\ g$	$i\cdot J_1(x_n)\cdot f_{n-1}$
$\vdots$	$\vdots$	
$r-1$	$g^{-1}\ a_0\ g$ $g^{-1}\ a_1\ g$ $\vdots$ $g^{-1}\ a_{r^{n-1}-1}\ g$	$i\cdot J_{r-1}(x_n)\cdot f_{n-1}$

表2.2

変数関数がある手順で求まれば、この作用素の概念を用いて合成できる。

即ち r 種の $n\text{-}1$ 変数関数を $f_{n-1}^{0}, f_{n-1}^{1}, \dots, f_{n-1}^{r-1}$ とおくと

$$\begin{cases} {}^{0}\varphi_i^{x_n}\cdot f_{n-1}^{0} = (\alpha_0 J_0 \oplus \alpha_1 J_1 \oplus \cdots \oplus \alpha_{r-1}\cdot J_{r-1})\cdot f_{n-1}^{0} \\ {}^{1}\varphi_i^{x_n}\cdot f_{n-1}^{1} = (\beta_0 J_0 \oplus \beta_1 J_1 \oplus \cdots \oplus \beta_{r-1}\cdot J_{r-1})\cdot f_{n-1}^{1} \\ \qquad\vdots \\ {}^{r-1}\varphi_i^{x_n}\cdot f_{n-1}^{r-1} = (\gamma_0 J_0 \oplus \gamma_1 J_1 \oplus \cdots \oplus \gamma_{r-1}\cdot J_{r-1})\cdot f_{n-1}^{r-1} \end{cases} \quad \text{———} (2.9)$$

各基底関数を代入すると次の連立方程式が求まり標準方程式とよぶ。

$$\begin{cases} (\text{定数項}) = (p_0 f_{n-1}^{0} \oplus p_1 f_{n-1}^{1} \oplus \cdots \oplus p_{r-1}\cdot f_{n-1}^{r-1}) \\ (x_n \text{の項}) = (q_0 f_{n-1}^{0} \oplus q_1 f_{n-1}^{1} \oplus \cdots \oplus q_{r-1}\cdot f_{n-1}^{r-1}) \\ \qquad\vdots \\ (x_n^{r-1}\text{の項}) = (\gamma_0 f_{n-1}^{0} \oplus \gamma_1 f_{n-1}^{1} \oplus \cdots \oplus \gamma_{r-1} f_{n-1}^{r-1}) \end{cases} \quad \text{———} (2.10)$$

故に各 $n\text{-}1$ 変数関数がこれより一意的に求まるには各作用素 ${}^{i}\varphi_i^{x_n}$ が独立であればよい。これらを満す作用素は種々あるが計算の簡単さと能率を考えて次の作用素を用いる。

$${}^{0}\varphi_i^{x} = \varphi_\phi , \qquad {}^{j}\varphi_i^{x}\cdot a = \begin{cases} g^{-1}\cdot a\cdot g & \text{if } x = j \\ e\cdot a\cdot e & \text{if } x \neq j \end{cases} \quad \text{———} (2.11)$$

これを用いた一回路網構成を図2.4に示す。

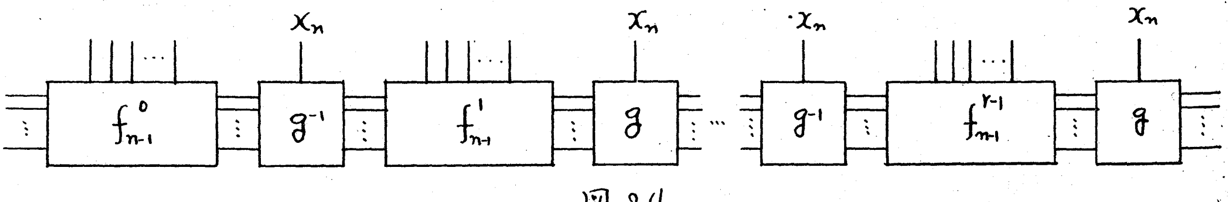

図2.4

補題 2.(i) r を任意の素数とすると $(i-1)^{r-1} \equiv 1 \pmod r$

(ii) $a \equiv 1 \pmod r \Rightarrow g.c.d(a, r^k) = 1$

(iii) $g.c.d(a, r^k) = 1 \Rightarrow \exists p \in \mathbb{Z}/(r^k),\ \frac{1}{a} = p$

(証明) (i) $(i-1)^{r-1} = \frac{(i-1)^r}{(i-1)} = \frac{i^r - 1}{(i-1)} = \frac{i \cdot i^{r-1} - 1}{i-1} = \frac{i-1}{i-1} = 1$

(ii) $a \equiv 1 \pmod r \Rightarrow a = dr + 1$ とおくと $g.c.d(a, r^k) = (d \cdot r + 1, r^k) = 1$

(iii) $g.c.d(a, r^k) = 1 \Rightarrow \exists p, q \in \mathbb{Z}/(r^k),\ ap + r^k q = 1$

$\therefore ap \equiv 1 \pmod{r^k}$ すなわち $\frac{1}{a} \equiv \frac{ap}{a} \equiv p \pmod{r^k}$ (証明終)

定理 14. k 出力回路網 $f : X^n \to C_{r^k}$ は $2r-1$ 種の $(1,k)$-セルを用いて常に合成可能で、所要セル数は

$$L_n \leq (r^{k+1} - r + 2) \cdot r^{n-1} - 2 \qquad (r \geq 3)$$

(証明) 表2.3 の作用素と図2.4 の構成法を用いる。この作用素が独立であることを示せばよい。

x	${}^{0}\varphi_i^{x}$	${}^{1}\varphi_i^{x}$	$\cdots$	${}^{r-1}\varphi_i^{x}$
0	1	1		1
1	1	i		1
2	1	1	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$r-1$	1	1		i

表2.3

$$\alpha = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & i & \cdots & 1 \\ & \vdots & & \vdots \\ 1 & 1 & \cdots & i \end{vmatrix} = (i-1)^{r-1}$$

補題より $\alpha = (i-1)^{r-1} \not\equiv 0 \pmod{r^k}$ 故に一次独立である。かつ $\mathbb{Z}/(r^k)$ の閉じた系で解ける。

所要セル数は $L_n = r \cdot L_{n-1} + 2(r-1)$

$$= r^2 L_{n-2} + 2r(r-1) + 2(r-1)$$

$$= \cdots = r^{n-1} L_1 + 2 \cdot r^{n-1} - 2 = (L_1 + 2) \cdot r^{n-1} - 2$$

$L_1 \leq r(r^k - 1)$ より $L_n \leq (r^{k+1} - r + 2) \cdot r^{n-1} - 2$ （証明終）

系.1. rを2と異なる任意の素数とすると、任意の回路網 $f : X^n \to G_r$ は (1,1)-セルのカスケードで合成することができる。所要セル数は $L_n \leq (r^2 - r + 2) \cdot r^{n-1} - 2$

同様に基本可換群 G_r^k の自己同型作用素を T で表わし、xの制御の下での i 成分のみに変換 T をもつ作用素を T_i^x と書く。これを表2.4に示す。

各自己同型作用素は $Z(r)$ の元を成分とする $k \times k$ の行列で表わすことができる。

I_k は $k \times k$ の単位行列とする。

x	T_0^x	T_1^x	$\cdots$	T_{r-1}^x
0	I_k	I_k		I_k
1	I_k	T		I_k
2	I_k	I_k	$\cdots$	I_k
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$r-1$	I_k	I_k		T

表2.4

r個の $(n-1)$-変数関数を $F_{n-1}^0, F_{n-1}^1, \cdots, F_{n-1}^{r-1}$ とする。

$$\begin{cases} T_0^{x_n} \cdot F_{n-1}^0 = J_0 \cdot F_{n-1}^0 \oplus J_1 \cdot F_{n-1}^0 \oplus \cdots \oplus J_{r-1} \cdot F_{n-1}^0 \\ T_1^{x_n} \cdot F_{n-1}^1 = J_0 \cdot F_{n-1}^1 \oplus J_1 \cdot (F_{n-1}^1 \cdot T) \oplus \cdots \oplus J_{r-1} \cdot F_{n-1}^1 \\ \vdots \\ T_{r-1}^{x_n} \cdot F_{n-1}^{r-1} = J_0 \cdot F_{n-1}^{r-1} \oplus J_1 \cdot F_{n-1}^{r-1} \oplus \cdots \oplus J_{r-1} \cdot (F_{n-1}^{r-1} \cdot T) \end{cases} \qquad (2.12)$$

故に図2.4の構成法を用いれば

$$F_n = T_0^{x_n} \cdot F_{n-1}^0 \oplus T_1^{x_n} \cdot F_{n-1}^1 \oplus \cdots \oplus T_{r-1}^{x_n} \cdot F_{n-1}^{r-1}$$

$$= J_0 (F_{n-1}^0 \oplus F_{n-1}^1 \oplus \cdots \oplus F_{n-1}^{r-1}) \oplus J_1 (F_{n-1}^0 \oplus F_{n-1}^1 \cdot T \oplus \cdots \oplus F_{n-1}^{r-1}) \oplus \cdots$$

$$\cdots \oplus J_{r-1}\,(F^0_{n-1} \oplus F^1_{n-1} \oplus \cdots \oplus F^{r-1}_{n-1}\cdot T) \qquad \text{——}(2.13)$$

$J_0, J_1, \cdots, J_{r-1}$ を代入すれば

$$\left\{\begin{array}{l} M_{00}\,F^0_{n-1} \oplus M_{01}\,F^1_{n-1} \oplus \cdots \oplus M_{0r-1}\,F^{r-1}_{n-1} = (\text{定数項}) \\ M_{10}\,F^0_{n-1} \oplus M_{11}\,F^1_{n-1} \oplus \cdots \oplus M_{1r-1}\,F^{r-1}_{n-1} = (x\text{ の項}) \\ \qquad\vdots \\ M_{r-1,0}\,F^0_{n-1} \oplus M_{r-1,1}\,F^1_{n-1} \oplus \cdots \oplus M_{r-1,r-1}\,F^{r-1}_{n-1} = (x^{r-1}\text{の項}) \end{array}\right. \qquad \text{——}(2.14)$$

が求まる。この式を基本可換群の標準方程式とよぶ。ここで M_{ij} は $k\times k$ の行列で自己同型作用素 T と単位行列 I_k との組み合せよりなる。従って体をつくっている。次に表2.4の作用素が一次独立なための条件を求める。

$$\Sigma = \begin{vmatrix} I_k & I_k & \cdots & I_k \\ I_k & T & \cdots & I_k \\ \vdots & & & \vdots \\ I_k & I_k & \cdots & T \end{vmatrix} = \left|(T \ominus I_k)^{r-1}\right| \neq 0 \pmod r$$

が成り立てばよいから、T は固有値1を持たない自己同型作用素であればよい。

$GF(r)$ の次の k 次方程式を

$$f(x) = x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_1 x + \alpha_0$$

とすると、この随伴行列（Companion matrix）はベクトル空間の線形変換に対応し、自明でない自己同型作用素を示している。

$$T_c = \begin{vmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ & \vdots & & & & \\ 0 & 0 & & \cdots & & 0\ 1 \\ -\alpha_0 & -\alpha_1 & & \cdots & & -\alpha_{k-1}\ -\alpha_k \end{vmatrix}.$$

定理 15. k出力回路網 $f: X^n \to C_r^k$ は $(2r+k-2)$種の$(1,k)$-セル
を用いて常に合成可能であり所要セル数は

$$L_n \leq k(r^{n+1} - r^n) + 2\cdot r^{n-1} - 2$$

（証明）半前は明らか。所要セル数は図2.4と同じ構成を用いれば

$$L_n = (L_1 + 2)r^{n-1} - 2.$$

$$L_1 \leq (r-1)\cdot r\cdot k \qquad \therefore\ L_n \leq \{k(r^2 - r) + 2\}\cdot r^{n-1} - 2.$$

$$= k(r^{n+1} - r^n) + 2\cdot r^{n-1} - 2$$

又セルの種類はC_r^kの生成元k個，作用セル$2r-2$個より
$(2r+k-2)$-種のセルが必要．　　　　　　（証明終）

2.3. 三値論理関数とその合成

実際の回路網の合成を考えると、多値論理関数のうちでも、三値論理関数が重要である。又三値の場合が状態に冗長度なしにカスケード合成できる最小の状態数である。三値論理関数の合成について例題を中心に考察する。

<u>補題 3.</u> 位数3の巡回群C_3の単位元を単位元に移す自己同型作用素で自明でないものは $\varphi_2\cdot a = g^{-1}a\cdot g = a^2$ だけで、$g^{-1} = g$

<u>定理 16.</u> 任意の三値一出力回路網は三種の(1,1)-セルを用いて所要セル数 $L_n \leq 8\cdot 3^{n-1} - 2$ で合成可能である。

(証明略)

例題3. 次の与えられた関数を合成せよ.

						f_0		f_1				f_2		f_0			f_1			f_2	
x	y	f	x	x	x	2	x	2	y^2	$2y$	x	y^2	x	$2y^2$	2	x	$2y^2$	$2y$	x	y^2	x
0	0	1	e	e	e	a^2	e	a^2	e	e	e	e	e	e	a^2	e	e	e	e	e	e
0	1	2	e	e	e	a^2	e	a^2	a	a^2	e	a	e	a^2	a^2	e	a^2	a	e	a	e
0	2	1	e	e	e	a^2	e	a^2	a	a	e	a	e	a^2	a^2	e	a^2	a^2	e	a	e
1	0	0	g^{-1}	e	g^{-1}	a^2	g	a^2	e	e	e	e	g	e	a^2	e	e	e	e	e	g
1	1	2	g^{-1}	e	g^{-1}	a^2	g	a^2	a	a^2	e	a	g	a^2	a^2	e	a^2	a	e	a	g
1	2	0	g^{-1}	e	g^{-1}	a^2	g	a^2	a	a	e	a	g	a^2	a^2	e	a^2	a^2	e	a	g
2	0	1	g^{-1}	g^{-1}	e	a^2	e	a^2	e	e	g	e	g	e	a^2	g^{-1}	e	e	g	e	e
2	1	0	g^{-1}	g^{-1}	e	a^2	e	a^2	a	a^2	g	a	g	a^2	a^2	g^{-1}	a^2	a	g	a	e
2	2	2	g^{-1}	g^{-1}	e	a^2	e	a^2	a	a	g	a	g	a^2	a^2	g^{-1}	a^2	a^2	g	a	e

表 2.5

真理値表表示を展開すると

$$f = x^2 \oplus x^2 y \oplus xy \oplus 2xy^2 \oplus x \oplus 2y^2 \oplus 2y \oplus 1$$

(i) 図2.5のような構成法を用いると

$$f = [\{(J_0 \oplus 2J_1 \oplus J_2) f_0 \oplus f_1\}(J_0 \oplus J_1 \oplus 2J_2) \oplus f_2](J_0 \oplus 2J_1 \oplus J_2)$$

より標準方程式は

$$\begin{cases} (\text{定数項}) = f_0 \oplus f_1 \oplus f_2 = 2y^2 \oplus 2y \oplus 1 \\ (x\text{の項}) = 2f_1 = y \oplus 2y^2 \oplus 1 \\ (x^2\text{の項}) = 2f_1 \oplus f_2 = y \oplus 1 \end{cases}$$

故に $f_0 = 2$, $f_1 = y^2 \oplus 2y \oplus 2$, $f_2 = y^2$

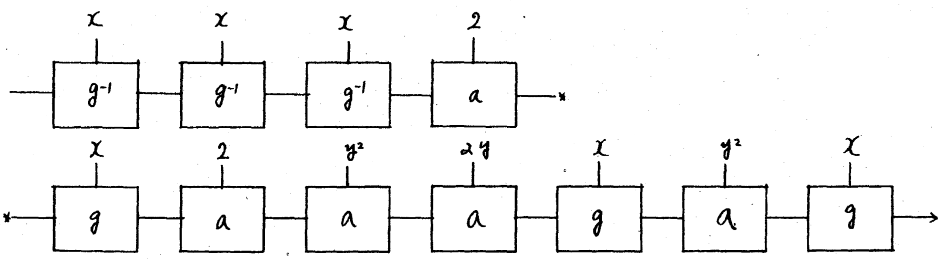

図2.5

(ii) 図2.6の構成法を用いる。

$$f = (J_0 \oplus J_1 \oplus J_2) f_0 \oplus (J_0 \oplus 2J_1 \oplus J_2) f_1 \oplus (J_0 \oplus J_1 \oplus 2J_2) f_2$$

標準方程式は

$$\begin{cases} (\text{定数項}) = f_0 \oplus f_1 \oplus f_2 = 2y^2 \oplus 2y \oplus 1 \\ (x\text{の項}) = 2f_1 \oplus f_2 = 2y^2 \oplus y \oplus 1 \\ (x^2\text{の項}) = 2f_1 \oplus 2f_2 = y \oplus 1 \end{cases}$$

故に $f_0 = 2y^2 \oplus 2$, $f_1 = 2y^2 \oplus 2y \oplus 2$, $f_2 = y^2$

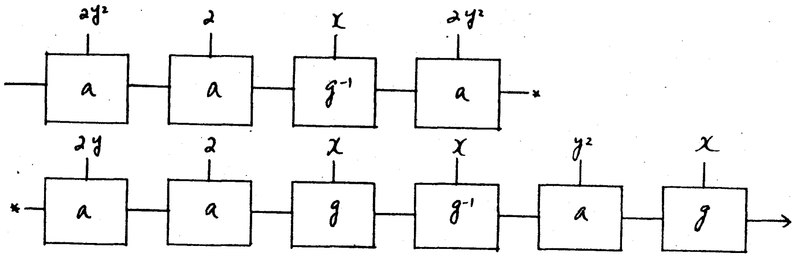

図2.6

次に多出力回路網の合成についてのべる。まず巡回群 C_{3^k} の変換回路網は最小関数表示が mod 3^k での演算であるから表2.7より次の結果を得る。

x	x^2	1	$(3^k-1)x^2$	$(3^k-1)x$	$2x^2$
0	0	1	0	0	0
1	1	1	3^k-1	3^k-1	2
2	1	1	3^k-1	3^k-2	2

表2.7

定理17. 回路網 $f: X^n \to C_{3^k}$ の基底関数は次のように与えられる。

$$\begin{cases} J_0(x) = 1 \oplus (3^k-1)x^2 \\ J_1(x) = (3^k-1)x \oplus 2x^2 \\ J_2(x) = x \oplus (3^k-1)x^2 \end{cases} \qquad (2.15)$$

このとき作用素としてはいろいろあるが、二面体群作用素

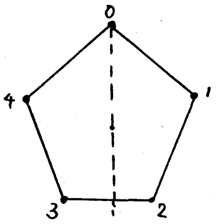

図2.7

が 3^k が奇数であるので条件を満し

$$g_{r^k-1}\cdot a = a^{r^k-1} = g^{-1}\cdot a\cdot g$$

かつ $g^{-1}=g$ である。

定理18 任意の3値k出力回路網は二面体群セルを用いて3種のセルで常に合成可能。所要セル数は

$$L_n \le (3^{k+1}-1)\,3^{n-1}-2$$

(証明略)

基本可換群による合成法も同様に成り立つが、巡回群の場合に比してセルの種類が増え所要個数が減っている。

例題4. 次の関数を回路網 $f: X^2 \to C_3^2$ として実現せよ。

x_2	x_1	f_2	f_1	x_2	($2x_1$,	$2x_1^2$,	2,	x_1,	$2x_1^2$)	x_2,	x_2	(1,	$2x_1$,	1,	$2x_1$)	x_2,	x_2	(2,	x_1,	x_1^2,	1,	x_1,	$2x_1^2$)	x_2
0	0	0	1	e	e	e	a_3^2	e	e	e	e	a_1	e	a_3	a_3	e	e	a_1^2	e	e	a_3	e	e	e
0	1	2	0	e	a_1^2	a_1^2	a_3^2	a_3	a_3^2	e	e	a_1	a_1^2	a_3	a_3^2	e	e	a_1^2	a_1	a_1	a_3	a_3	a_3^2	e
0	2	1	1	e	a_1	a_1^2	a_3^2	a_3^2	a_3^2	e	e	a_1	a_1	a_3	a_3	e	e	a_1^2	a_1^2	a_1	a_3	a_3^2	a_3	e
1	0	1	0	g^{-1}	e	e	a_3^2	e	e	g	e	a_1	e	a_3	e	e	g^{-1}	a_1^2	e	e	a_3	e	e	g
1	1	0	2	g^{-1}	a_1^2	a_1^2	a_3^2	a_3	a_3^2	g	e	a_1	a_1^2	a_3	a_3^2	e	g^{-1}	a_1^2	a_1	a_1	a_3	a_3	a_3^2	g
1	2	0	1	g^{-1}	a_1	a_1^2	a_3^2	a_3^2	a_3^2	g	e	a_1	a_1	a_3	a_3	e	g^{-1}	a_1^2	a_1^2	a_1	a_3	a_3^2	a_3	g
2	0	1	2	e	e	e	a_3^2	e	e	e	g^{-1}	a_1	e	a_3	e	g	g^{-1}	a_1^2	e	e	a_3	e	e	g
2	1	0	0	e	a_1^2	a_1^2	a_3^2	a_3	a_3^2	e	g^{-1}	a_1	a_1^2	a_3	a_3^2	g	g^{-1}	a_1^2	a_1	a_1	a_3	a_3	a_3^2	g
2	2	2	1	e	a_1	a_1^2	a_3^2	a_3^2	a_3^2	e	g^{-1}	a_1	a_1	a_3	a_3	g	g^{-1}	a_1^2	a_1^2	a_1	a_3	a_3^2	a_3	g

表2.6

表2.6. 図2.7に示すような構成を用いると標準方程式は

$$
\begin{cases}
F^1_{n-1} \oplus F^2_{n-1} \oplus F^3_{n-1} = (\text{定数}) \\
F^1_{n-1}(I_k \oplus 2T) \oplus F^2_{n-1}(2I_k \oplus T) = (x\text{の項}) \\
F^1_{n-1}(I_k \oplus 2T) \oplus F^2_{n-1}(I_k \oplus 2T) \oplus F^3_{n-1}(2I_k \oplus T) = (x^2\text{の項})
\end{cases}
$$

として求まる。

まず真理値表表示を展開すると

$$
F = (2x_1, 1 \oplus x_1 \oplus x_1^2) \oplus (2x_1 \oplus x_1^2, 2x_1 \oplus 2)x_2 \oplus (2x_1 \oplus x_1^2, 2x_1 \oplus 2x_1^2)x_2^2
$$

故に
$$
\begin{cases}
F^1 \oplus F^2 \oplus F^3 = (2x_1, 1 \oplus x_1 \oplus x_1^2) = g_1 \\
F^1(I_k \oplus 2T) \oplus F^2(2I_k \oplus T) = (2x_1 \oplus x_1^2, 2x_1 \oplus 2) = g_2 \\
F^1(I_k \oplus 2T) \oplus F^2(I_k \oplus 2T) \oplus F^3(2I_k \oplus T) = (2x_1 \oplus 1 \oplus x_1^2, 2x_1 \oplus 2x_1^2) = g_3
\end{cases}
$$

これより
$$\begin{cases} F^1 = g_1 \oplus (g_3 \oplus 2g_2)(T \oplus 2I_k)^{-1} \\ F^2 = g_1 \oplus 2(g_2 \oplus g_3)(T \oplus 2I_k)^{-1} \\ F^3 = g_1 \oplus g_3 (T \oplus 2I_k)^{-1} \end{cases}$$

自己同型作用素として

$$T = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \quad T \cong \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 2 & 5 & 7 & 1 & 4 & 7 & \end{pmatrix}$$
$$= (1\,3\,2\,6)(4\,5\,7\,8)$$

をとると

$$\begin{cases} F^1 = (2x_1 \oplus 2x_1^2,\ 2 \oplus 2x_1^2) \\ F^2 = (1 \oplus 2x_1,\ 1 \oplus 2x_1) \\ F^3 = (2 \oplus x_1 \oplus x_1^2,\ 1 \oplus x_1 \oplus 2x_1^2) \end{cases}$$

故に次の回路網を得る。

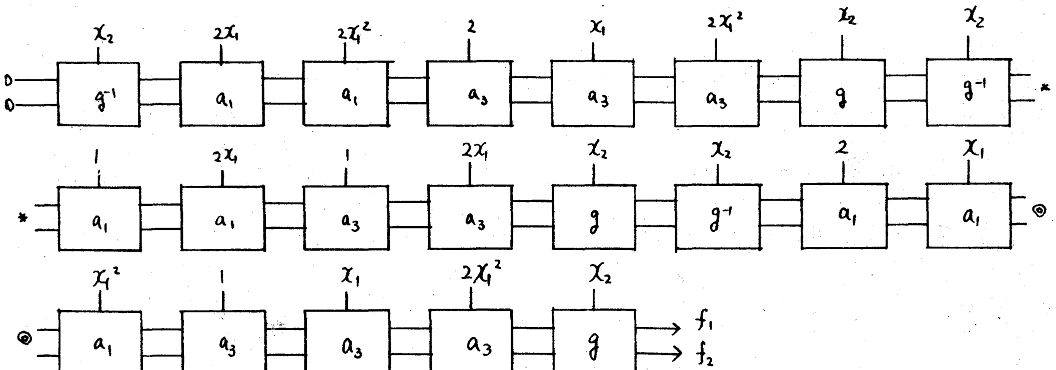

図2.7

回路網の集積化等を考慮すれば、セルの個数の増加をある程度許してもセルの種類が少ない方が有利なこともある。二値の場合は全ての群セルは一種のもので置き換えることができた。三値について次に述べる。

S_p を p 次の対称群とする，$\forall a, b \in S_p$，$G = \{a, b\}$ とおくとき．$G^{(2)} = \{a^2, ab, ba, b^2\}$，$G^{(i)} = G^{(i-1)} \cdot G$ と定義する。

$$\langle \{G\} \rangle = \{G, G^{(2)}, \cdots, G^{(k)}\}$$

を G より生成された巡回群とよび，$G^{(p+r)} = G^{(r)}$ なる r を $\langle \{G\} \rangle$ の周期とよぶ。回路網 $f(x) = (g_1, g_2, g_3)$ がセル $\theta(x) = (a_1, a_2, a_3)$ の l 段のカスケードで実現されるには $G = \{a_1, a_2, a_3\}$ とすると $G^{(l)} \ni g_1, g_2, g_3$ が必要である。

<u>定理 19</u>　p 次の対称群 S_p は二種の生成元

$$a_1 = (1\,2) \text{ と } a_2 = (1\,2 \cdots p)\text{，又は } a_3 = (2\,3 \cdots p)$$

で生成される。即ち $\langle \{a_1, a_2\} \rangle = \langle \{a_1, a_3\} \rangle = S_p$

(証明)　$a_2 = a_1 a_3$ より $\langle \{a_1, a_2\} \rangle = \langle \{a_1, a_3\} \rangle$

従って $\langle \{a_1, a_2\} \rangle = S_p$ を示そう。

$\forall s \in S_p$，$s = (i_1, i_2, \cdots, i_l) = (i_1, i_2)(i_2, i_3) \cdots (i_{l-1}\, i_l)$

かつ $(i_l\, i_m) = (i_1\, i_l)(i_1\, i_m)(i_1\, i_l)$ より任意の元は次の互換の積として書ける

$$(i_1, i_2), (i_1, i_3), \cdots, (i_1, i_l)$$

更に $a_3^{-k}(1, r-k+1) = (1\,2)\, a_3^{k}$ より

$$(1,\ r-k+1) = a_3^{-k}\,(12)\,a_3^{k}$$

$\therefore\ \langle \{a_1,\ a_2\} \rangle = S_p$ （証明終）

定理20. 三値多出力回路網は一種のセルで合成することができる。即ち反復論理回路網で実現できる。

(証明) 入力変数集合 $\{0,\ 1,\ 2,\ x,\ x^2\}$ に対して

セル θ を $\theta(x) = (a_2, a_1, a_2^{i})$, $(i, p) = 1$ とおくと

(1) $\theta(0) = (a_2,\ a_2,\ a_2)$ (2) $\theta(1) = (a_1,\ a_1,\ a_1)$

(3) $\theta(2) = (a_2^{i},\ a_2^{i},\ a_2^{i})$ (4) $\theta(x) = (a_2,\ a_1,\ a_2^{i})$

(5) $\theta(x^2) = (a_2,\ a_1,\ a_1)$

$a_1,\ a_2$ の位数はそれぞれ 2 と $p=3^k$ である。特に $i=2$ とする

(4) より $(a_2,\ a_1,\ a_2^{2})^{p} = (a_2^{p},\ a_1^{p},\ a_2^{2p}) = (e,\ a_1,\ e)$ —(6)

$(a_2,\ a_1,\ a_2^{2})^{p+1} = (a_2,\ e,\ a_2^{2})$ —(7)

(5) より $(a_2,\ a_1,\ a_1)^{p} = (e,\ a_1,\ a_1)$ —(8)

(6),(8) より $(e,\ a_1,\ e)\cdot(e,\ a_1,\ a_1) = (e,\ e,\ a_1)$ —(9)

(2),(8) より $(a_1,\ a_1,\ a_1)(e,\ a_1,\ a_1) = (a_1,\ e,\ e)$ —(10)

(5) より $(a_2,\ a_1,\ a_1)$ に対して $\exists\, r_1,\ r_2,\ -pr_1 + 2\cdot r_2 = 1$

$\therefore\ (a_2,\ a_1,\ a_1)^{2r_2} = (a_2^{pr_1+1},\ e,\ e) = (a_2,\ e,\ e)$ —(11)

$\therefore$ (7),(11) より $(a_2,\ e,\ e)^{p-1}\cdot(a_2,\ e,\ a_2^{2}) = (e,\ e,\ a_2^{2})$ —(12)

(3),(11),(12) より $(a_2^{2},\ a_2^{2},\ a_2^{2})\cdot(a_2,\ e,\ e)^{p-2}\cdot(e,\ e,\ a_2^{2})^{p-1} = (e,\ a_2^{2},\ e)$ —(13)

故に
$$\left\{\begin{array}{ll} (a_1,\ e,\ e) & (a_2,\ e,\ e) \\ (e,\ a_1,\ e) & (e,\ a_2^{2},\ e) \\ (e,\ e,\ a_1) & (e,\ e,\ a_2^{2}) \end{array}\right\}$$

が求まり，$(2, p)=1$ より $\exists r_1, r_2,\ 2r_1 - pr_2 = 1$

$$\therefore\ (e, a_2^2, e)^{2r_1} = (e, a_2, e).$$

同様に $(e, e, a_2^2)^{2r_1} = (e, e, a_2)$

故に $\langle \theta(x) = (a_2, a_1, a_2^2) \rangle = S_p \times S_p \times S_p$

(証明終)

結言．ある種の完備な論理系を定義し，それらの論理系の代数的構造とそれらの性質について述べ，更に多段論理回路網での合成に関して純代数的に考察した。この多段論理回路網は可換環の上の多元環として表示され，線形変換の概念を用いれば与えられたn変数関数の展開式上の変形を見い出すことによって合成可能であった。その結果任意の多出力回路網は巡回群又は基本可換群セルを用いればその作用素セルが存在して合成可能である。ここで述べた性質は回路網合成の可能性の判定のみならず，論理関数の性質を調べるのにも重要であると思われる。最後にいろいろ討論いただいた研究室の皆様に深謝致します。

文献

(1) M. H. Stone : Boolean algebras Harvard Uni 1936

(2) R. L. Herrmann : Selection and Implementation of Ternary Switching Algebra.. Spring Joint Comp. Conf. 1968

(3) Yoeli : A group-theoretical approach to two-rail Cascades, IEEE. EC-14. 1965

(4) Elspas & Stone : Decomposition of group functions and the synthesis of multi-rail cascades. IEEE. 8-th annual symp. on Switching & Automata theory 1967

(5) 厚尾.鈴木.野口.大泉: 多出力多段論理回路網に関する基礎的考察. オートマトン.インフォメーション研究会資料 1968

(6) 〃 : 多段論理回路網の多元環表示とその合成法. 電子通信学会全国大会 1968

(7) 〃 : A fundamental consideration on the multi-staged logical network. The 2-nd Hawaii International Conference on system sciences 1969

(8) 鈴木.野口.大泉: 多段論理回路網の構造に関する一考察 電通学会誌 vol. 51-C, No. 7. 1968

(9) 厚尾.鈴木.野口.大泉: 多出力多段論理回路網の合成 電通学会誌 vol 52-C, No. 9. 1969