直交する準線形関数族について

── 多値論理極大関数族の相互関係 ──

野　崎　昭　弘

要　旨

有限集合 $X = \{0, 1, 2, \cdots, k-1\}$ 上で定義される多変数関数は，$k > 2$ のとき多値論理関数と呼ばれる。k がある素数 p のベキ（$k = p^m$, $m \geqq 1$）のときには，「準線形関数」の概念が定義できる。より正確に言えば，任意の 1 対 1 写像 $\sigma : X \to Z_p^m$ に対して，X 上の σ−準線形関数 $f : X^n \to X$ が定義でき，その全体 $L(\sigma)$ はいわゆるクローン，すなわち「合成について閉じた関数族」になる。

ここでは関数族 $L(\sigma)$, $L(\tau)$ の中に “直交する”（共通部分がほとんどない）ペアが存在するか，という問題を取り上げる。この問題は $m = 1$ の場合はすでに解けていて，直交するペア $L(\sigma)$, $L(\tau)$ は $p \geqq 7$ のとき存在し，$p < 7$ のときは存在しない。ここでは $p \geqq 5$, $m \geqq 2$ の場合について，「直交するペアが必ず存在する」ことを証明する。

$p < 5$, $m \geqq 2$ の場合は，$p = m = 2$ の場合を除いて，ほとんど未解決である。

キーワード：多値論理関数（Multi-valued logical function），合成について閉じた関数族（Clone），準線形関数（Quasi-linear function），直交（Orthogonal）

1. 多値論理関数族の研究の系譜

有限集合 $X = \{0, 1, \cdots, k-1\}$ 上で定義される多変数関数 $f : X^n \to X$ は，k が 3 以上のとき**多値論理関数**と呼ばれ，$k = 2$ の場合は**論理関数**と呼ばれる。要素 1（あるいは $k-1$），0 を真，偽と読み替えれば，論理との関係が生まれるからである。コンピュータの 2 進演算回路の入出力関係は，ある多変数の論理関数 f で表せるし，その回路をある基本的な演算素子から組み立てる問題は，その論理関数 f をある基本的な論理関数から合成する問題に帰着される。基本素子のある集合を決めて，任意の機能の回路がそれらの基本素子だけで実現できるかという問題は，ある論理関数の集合から，すべての論理関数が合成できるか，という問題と同等である。そのような関数の集合は，**完全**と呼ばれる。

多値論理関数の集合（以下，**関数族**と呼ぶ）F で，関数合成について閉じているものは，

サイバー大学 IT 総合学部・教授

原稿受付日：2009 年 9 月 25 日
原稿受理日：2010 年 1 月 13 日

クローンと呼ばれる（正確な定義は後で述べる ── 他の専門用語についても同様）。特に全体集合を除いて（集合の包含関係について）極大な関数族は**極大クローン**と呼ばれる。ある関数族 F が完全であるための必要十分条件は，「その関数族 F が，どんな極大クローンにも含まれていない」ことである。

$k = 2$ の場合については，E. ポストが可算無限個あるすべてのクローンの完全な分類に成功した（[1]）。$k \geqq 3$ の場合には，I. G. ローゼンバーグがすべての極大クローンを決定した（[2]）。しかし $k \geqq 3$ だとクローンの個数は連続濃度になるので，完全な分類は困難である。そこですべてのクローンのクラス（包含関係について束 lattice をなす）の構造を知るために，“極小クローン”（[9]）や「共通部分がほとんどない」極大クローンのペア（[4]，[5]ほか）などが注目を集め，研究されてきた。本稿では後者の系譜で，特に “直交” する極大クローンについて考察する。

この方面では，たとえば次のことが知られている。

⑴ k が素数であれば，X に加減乗除が導入でき，そこで定義される**線形関数**の全体は極大クローンになる（[2]）。そしてこの型の極大クローンの直交するペアは，k が 7 以上のときは存在し，それ以外の場合は存在しない（[5]）。

⑵ ある全順序関係についての単調増加関数族（これも極大クローンになる[2]）については，直交する極大クローンのペアは $k \geqq 4$ のときは存在し，それ以外のときは存在しない（[8]）。

⑶ “中心関係” によって定められる極大クローン（[2]）の間では，直交するペアは存在しない（[4]）。

本稿では，文献[5]でごく簡単な場合だけ扱われ，[7]で結果だけ（証明抜きで，しかも不正確な形で）述べられていた “準線形関数” の作る極大クローンについて，ある条件のもとで直交するペアが存在することを証明する。

2. 準線形関数族と直交性

以下，$X = \{0, 1, \cdots, k-1\}$ $(k \geqq 3)$ とし，X 上の n 変数関数

$$f : X^n \to X, n \geqq 1$$

を考える。**関数合成**とは，たとえば $f(x, y)$，$g(x, y, z)$，$h(x)$ から新しい 2 変数関数

$$u(x, y) = f(g(y, y, x), h(y))$$

を自由に組み立てる手続きのことで，特に問題ないと思うので，形式的な定義は省略する。

定義 1　次のような関数 $p_j^{(n)}$ を，**射影**（projection）という：

$$p_j^{(n)}(x_1, x_2, \cdots, x_n) = x_j, \ 1 \leqq j \leqq n$$

1変数の射影 $p_1^{(1)}(x_1)$ は，恒等写像にほかならない。すべての射影の集合を，記号 $\boldsymbol{P}$ で表す。

定義 2　関数族 F が**合成について閉じている**とは，F および $\boldsymbol{P}$ の中の関数から合成によって得られる関数が，すべて F に属していることである。合成について閉じている関数族は**クローン**（clone）と呼ばれる。クローンはどれも，$\boldsymbol{P}$ を含んでいる。

$\boldsymbol{P}$ の自由な使用を許すのは，回路設計においては，射影は「素子を必要とせず，配線のつなぎかえだけで実現できる」ので，自然なことである。また代数的には，それは「変数の番号は自由に付け替えてよい」ということである。

定義 3　関数値が常に a である n 変数関数（**定数関数**）を，記号 $c_a^{(n)}$ で表す：

$$c_a^{(n)}(x_1,\ x_2,\ \cdots,\ x_n) = a$$

定数関数と射影をあわせた“trivial な”関数の全体を，$\boldsymbol{T}$ で表す：

$$\boldsymbol{T} = \{c_a^{(n)} \mid n \geqq 1,\ a \in X\} \cup \boldsymbol{P}$$

定義 4　ある2つのクローン $V,\ W$ が**直交する**とは，次の条件をみたすことをいう。

$$V \cap W = \boldsymbol{T}$$

〈注意〉　最近は「直交」（orthogonal［6］）よりも「半硬直」（semi-rigid,［4］,［5］,［7］,［8］）という用語がよく使われているが，ここではイメージをもちやすい用語「直交」を用いる。

ここで，後で使う補題を一つ引用しておこう。

還元補題

X 上のすべての1変数関数の集合を $\Omega^{(1)}$ とすると，関数族 $V,\ W$ が直交するための必要十分条件は：

$$(V \cap \Omega^{(1)}) \cap (W \cap \Omega^{(1)}) \subseteq \boldsymbol{T}$$

要するに「その中の1変数関数が直交していれば，全体としても直交する」ということである（証明は，たとえば［3］にある）。

p を素数，$\boldsymbol{Z}_p = \{0,\ 1,\ \cdots,\ p-1\}$ とすると，$\boldsymbol{Z}_p$ には自然に加減乗除が導入できていわゆる体（field）になり，$\boldsymbol{Z}_p$ 上の関数 $f(x_1,\ x_2,\ \cdots,\ x_n)$ はすべて変数 $x_1,\ x_2,\ \cdots,\ x_n$ の多項式で表すことができる。

定義 5　$k = p^m$, p は素数で $m \geqq 1$ とする。以下，直積 $(\boldsymbol{Z}_p)^m$ を $\boldsymbol{Z}_p^m$ と略記する。

(1)　$\boldsymbol{Z}_p^m$ 上の n 変数関数 $\phi : (\boldsymbol{Z}_p^m)^n \to (\boldsymbol{Z}_p^m)$ が**準線形**（quasi-linear）であるとは，n 個

の m 次正方行列 $M_1, M_2, \cdots, M_n$ と，ひとつの m 次元列ベクトル $\boldsymbol{b}$ によって，ϕ が次のように表わされることをいう。

$$\phi(\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n) = M_1\boldsymbol{v}_1 + M_2\boldsymbol{v}_2 + \cdots + M_n\boldsymbol{v}_n + \boldsymbol{b}$$

ここで $\boldsymbol{v}_j$ は $\boldsymbol{Z}_p^m$ の要素を表す列ベクトルである。

⑵ X から $\boldsymbol{Z}_p^m$ への全単射 σ について，ある関数 $f: X^n \to X$ が **σ–準線形**であるとは，ある準線形関数 $\phi: (\boldsymbol{Z}_p^m)^n \to (\boldsymbol{Z}_p^m)$ によって

$$f(x_1, x_2, \cdots, x_n) = \sigma^{-1}\cdot\phi(\sigma(x_1), \sigma(x_2), \cdots, \sigma(x_n))$$

と表せることをいう。

σ–準線形関数全体の集合を $L(\sigma)$ で表し，**σ–準線形関数族**，あるいは単に**準線形関数族**と呼ぶ。準線形関数族は極大クローンである（[2]）。この型の極大クローンどうしで，直交するペアが存在するかどうかが，本稿のテーマである。

〈注意〉 文献[5]でも一般の準線形関数を（やや異なる表現で）定義しているが，実際に扱っているのは $m = 1$ の場合（普通の意味での線形関数）だけである。

還元補題によれば，$L(\sigma)$ と $L(\tau)$ とが直交するかどうかは，1 変数関数を調べればわかる。そこである 1 変数関数 $f: X \to X$ が σ–準線形でも τ–準線形でもあるとすると，その関数 f はある行列 M, M' とベクトル $\boldsymbol{b}, \boldsymbol{b}'$ によって，次のように表現できる：

$$\begin{aligned} f(\boldsymbol{x}) &= \sigma^{-1}\cdot(M\sigma(\boldsymbol{x}) + \boldsymbol{b}) \\ &= \tau^{-1}\cdot(M'\tau(\boldsymbol{x}) + \boldsymbol{b}') \end{aligned}$$

この 1 変数関数 f が $\boldsymbol{T}$ に属するとは，f が恒等写像か定数関数であることを意味しているが，f が恒等写像なら

⒜ M, M' は単位行列で $\boldsymbol{b} = \boldsymbol{b}' = \boldsymbol{0}$（ゼロベクトル）

であり，f が定数関数なら

⒝ $M = M' = 0$（ゼロ行列）

になる（それぞれ逆も成り立つ）。

さて，関数 f を表現する上の式の，第 2 の等号（恒等的に成り立つはず）

$$\sigma^{-1}\cdot(M\sigma(\boldsymbol{x}) + \boldsymbol{b}) = \tau^{-1}\cdot(M'\tau(\boldsymbol{x}) + \boldsymbol{b}')$$

に注目して，$\boldsymbol{v} = \sigma(\boldsymbol{x})$ とおくと，$\boldsymbol{v}$ は $\boldsymbol{Z}_p^m$ の要素を表す m 次元列ベクトルである。この両辺に左から τ を施し，$\boldsymbol{x}$ に $\sigma^{-1}(\boldsymbol{v})$ を代入すると

$$\tau\cdot\sigma^{-1}\cdot(M\sigma(\sigma^{-1}(\boldsymbol{v})) + \boldsymbol{b}) = \tau\cdot\tau^{-1}\cdot(M'\tau\cdot\sigma^{-1}(\boldsymbol{v}) + \boldsymbol{b}'$$

すなわち

$$\tau\cdot\sigma^{-1}(M\boldsymbol{v} + \boldsymbol{b}) = M'\tau\cdot\sigma^{-1}(\boldsymbol{v}) + \boldsymbol{b}'$$

が得られる。そこで

$$\lambda = \tau\cdot\sigma^{-1}$$

とおけば，λ は $\boldsymbol{Z}_p^m$ から $\boldsymbol{Z}_p^m$ 自身への全単射で，次の等式が導かれる。

$$\lambda(Mv+\boldsymbol{b}) = M'\lambda(\boldsymbol{v})+\boldsymbol{b}' \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(\sharp)$$

この等式 (♯) は，$L(\sigma)\cap L(\tau)$ に属する 1 変数関数についての条件式であるから，「直交するペアがある」ことを示すには，適当な全単射 λ について，

この条件(♯)を満たす関数 f がすべて $\boldsymbol{T}$ に属していること，

いいかえれば，(♯) をみたす行列 $M,\ M'$ とベクトル $\boldsymbol{b},\ \boldsymbol{b}'$ が，

⒜ $M,\ M' = E$ 単位行列で $\boldsymbol{b} = \boldsymbol{b}' = \boldsymbol{0}$（ゼロベクトル）

かまたは

⒝ $M = M' = 0$（ゼロ行列）

の 2 つの場合に限られることを示せばよい。

ここで念のために，あとでよく使う体 $\boldsymbol{Z}_p$ の性質を列挙しておこう。

事実 1（フェルマーの小定理） $x \neq 0$ ならば $x^{p-1} = 1$

事実 2 $x^p = x$

事実 3 $(x^{p-2})^{p-2} = x$

〈証明〉 $(x^{p-2})^{p-2} = x^{p\times(p-4)+4} = (x^p)^{p-4}\times x^4 = x^{p-4+4} = x^p = x$

なお事実 2, 3 は，$x = 0$ でも成り立つ。

3. 直交するペアが存在する場合（Ⅰ）

最初に $p \geqq 5,\ m = 2$ の場合，直交する準線形関数族のペアが存在することを示す。

定理 1 $p \geqq 5,\ m = 2$ の場合，直交する準線形関数族のペアが存在する。

証　明 まず $p = 5$ の場合についての証明を述べる。うまく $\lambda : \boldsymbol{Z}_5^2 \to \boldsymbol{Z}_5^2$ を選んで，条件 (♯) をみたすどんな $M,\ M',\ \boldsymbol{b},\ \boldsymbol{b}'$ も，前節の最後に示した 2 つの場合⒜，⒝のどちらかに該当することを示せばよい。

ところで任意の全単射 $\lambda : \boldsymbol{Z}_5^2 \to \boldsymbol{Z}_5^2$ は，$\boldsymbol{Z}_5^2$ の要素を列ベクトルで示すと

$$\begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \lambda\left(\begin{bmatrix} v_1 \\ v_2 \end{bmatrix}\right),\ w_j = \lambda_j(v_1,\ v_2)$$

のように書ける。今の場合は，次の全単射 λ を使うとうまくいく。

$$w_1 = \lambda_1(v_1,\ v_2) = v_1^2+v_2^3,$$
$$w_2 = \lambda_2(v_1,\ v_2) = (v_1^2+v_2^3)^4+v_1$$

ただし加算・乗算は体 $\boldsymbol{Z}_5$ の演算である。

まずこの λ が全単射であるを確かめておこう。

$$w_1 = v_1^2 + v_2^3,$$
$$w_2 = (v_1^2 + v_2^3)^4 + v_1 = w_1^4 + v_1$$

から

$$v_1 = w_2 - w_1^4,$$
$$v_2^3 = w_1 - v_1^2 = w_1 - (w_2 - w_1^4)^2$$

となる。すると事実3から（$3 = p-2$）

$$v_2 = (v_2^3)^3 = (w_1 - (w_2 - w_1^4)^2)^3$$

であり，$(w_1,\ w_2)$ から $(v_1,\ v_2)$ が一意的に復元できる。したがって λ は単射で，$\boldsymbol{Z}_5^2$ は有限集合なので，λ は全単射である。

そこで以下，上で定めた $\lambda_1,\ \lambda_2$ について，条件（♯）のもとで，目標

Ⓐ　$M,\ M' = E$（単位行列）で $\boldsymbol{b} = \boldsymbol{b}' = \boldsymbol{0}$（ゼロベクトル）

かまたは

Ⓑ　$M = M' = 0$（ゼロ行列）

のどちらかが，必ず成り立つことを証明する。

条件式

$$\lambda(Mv + \boldsymbol{b}) = M'\lambda(\boldsymbol{v}) + \boldsymbol{b}' \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(\sharp)$$

を，行列・ベクトルの成分によって詳しく書いてみよう。そのために

$$M = \begin{bmatrix} a,\ b \\ c,\ d \end{bmatrix},\ b = \begin{bmatrix} e \\ f \end{bmatrix},\ M' = \begin{bmatrix} a',\ b' \\ c',\ d' \end{bmatrix},\ b' = \begin{bmatrix} e' \\ f' \end{bmatrix},\ v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

とおくと，等式（♯）の第1成分は次のように書ける：

$$(av_1 + bv_2 + e)^2 + (cv_1 + dv_2 + f)^3$$
$$= a'(v_1^2 + v_2^3) + b'((v_1^2 + v_2^3)^4 + v_1) + e' \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(1.1)$$

また等式（♯）の第2成分は，次のように書ける：

$$((av_1 + bv_2 + e)^2 + (cv_1 + dv_2 + f)^3)^4 + (av_1 + bv_2 + e)$$
$$= c'(v_1^2 + v_2^3) + d'((v_1^2 + dv_2^3)^4 + v_1) + f' \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(1.2)$$

〈第1段〉第1成分についての等式(1.1)の分析

等式(1.1)の左辺は $(v_1,\ v_2)$ についての3次式で，右辺の第2項

$$b'((v_1^2 + v_2^3)^4 + v_1)$$

は，$b' \neq 0$ であれば明らかに 4 次以上の項を含んでいる。したがって(1.1)の等号が成立するためには，

$$b' = 0$$

でなければならない。

以下，a' の値によって，2 つの場合を分けて考える。

(場合 1. A) $a' \neq 0$ ：

この場合は，(1.1)の右辺は v_2^3 を含むから，$d \neq 0$ でなければならない。一方，$c \neq 0$ だと「ほかにはどこにもない項」v_1^3 が現れてしまうので，$c = 0$ でなければならない。すると右辺の v_1^2 に対応するためには $a^2 = a'(\neq 0)$ でなければならないが，その上 $b \neq 0$ だと「ほかにはどこにもない項」$v_1 v_2$ が現れてしまう。したがって $b = 0$ である。$b' = 0$ とあわせて等式(1.1)を書きなおすと，次のようになる：

$$(av_1+e)^2+(dv_2+f)^3 = a'(v_1^2+v_2^3)+e'$$

右辺に 1 次の項はないから $e = f = 0$, したがって $e' = 0$ でなければならないから，等式(1.1)は次のように書きなおせる：。

$$(av_1)^2+(dv_2)^3 = a'v_1^2+a'v_2^3 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (1.1\mathrm{A})$$

まとめ 1. A：これで $a' \neq 0$ の場合には，次のことがわかった。

$$a^2 = d^3 = a',\ b = c = e = f = 0,$$
$$a' \neq 0,\ b' = e' = 0$$

(場合 1. B) $a' = 0$:

$b' = 0$ なので，この場合(1.1)の右辺は定数である。したがって，左辺の 3 次式

$$(cv_1+dv_2+f)^3$$

は定数 $c = d = 0$ で，残りの 2 次式

$$(av_1+bv_2+e)^2$$

も定数 $a = b = 0$ でなければならず，等式(1.1)は次のように書ける：

$$e^2+f^3 = e' \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (1.1\mathrm{B})$$

まとめ 1. B：これで $a' = 0$ の場合には，次のことがわかった：

$$a = b = c = d = 0,\ a' = b' = 0$$

〈第 2 段〉第 2 成分についての等式(1.2)の分析

(場合 2. A) $a' \neq 0$ の場合：$a^2 = d^3 = a'$（まとめ 1. A）を考慮すると，等式(1.2)は次

のように書きかえられる（$a' \neq 0$ だから $a'^4 = a'^{p-1} = 1$ に注意）：

$$\begin{aligned}
\text{左辺} &= ((av_1)^2+(dv_2)^3)^4+av_1 \\
&= (a^2v_1^2+d^3v_1^3)^4+av_1 \\
&= (a'v_1^2+a'v_1^3)^4+av_1 \\
&= a'^4(v_1^2+v_2^3)^4+av_1 \\
&= (v_1^2+v_2^3)^4+av_1 \\
\text{右辺} &= c'(v_1^2+v_2^3)+d'((v_1^2+v_2^3)^4+v_1)+f'
\end{aligned}$$

当然，$d' = 1$ でなければならない。そこで消去できる項を消すと，残りは次のようになる：

$$av_1 = c'(v_1^2+v_2^3)+v_1+f' \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(1.2')$$

ここから $a = 1$, $c' = f' = 0$ が導かれ，さらに

$$a' = a^2 = 1,\ d^3 = a' = 1$$

から，事実 3 によって

$$d = (d^{p-2})^{p-2} = (d^3)^3 = 1^3 = 1$$

となるから，けっきょく $a' \neq 0$ の場合には

$$\begin{aligned}
&a' = d' = 1,\ b' = c' = e' = f' = 0, \\
&a = d = 1,\ b = c = e = f = 0
\end{aligned}$$

でなければならない。これは目標Ⓐに一致する。

（場合 2. B）$a' = 0$：この場合はまとめ 1. B から，等式(1.2)は次のように書きなおせる：

$$(e^2+f^3)^4+e = c'(v_1^2+v_2^3)+d'((v_1^2+v_2^3)^4+v_1)+f' \quad \cdots\cdots\cdots\cdots(1.2')$$

左辺は定数だから $c' = d' = 0$ で，

$$a = b = c = d = a' = b' = c' = d' = 0$$

が得られる。これは目標Ⓑに一致する。

次に $p > 5$, $m = 2$ の場合を証明する。それには全単射 $\lambda : (\boldsymbol{Z}_p)^2 \to (\boldsymbol{Z}_p)^2$ として，次のものを使えばよい：

$$\begin{aligned}
&\lambda_1(v_1,\ v_2) = v_1^2+v_2^{p-2}, \\
&\lambda_2(v_1,\ v_2) = (v_1^2+v_2^3)^{p-1}+v_1
\end{aligned}$$

証明は，$p = 5$ に対する証明をほとんどそのまま辿ればよい（部分的には，話が簡単になるところもある）ので，省略する。

〈証明終わり〉

4. 直交するペアが存在する場合（Ⅱ）

定理 2　p が 5 以上の素数で，m が 3 以上の自然数のとき，直交する準線形関数族のペアが存在する。

証　明　全単射 $\lambda : \boldsymbol{Z}_p^m \to \boldsymbol{Z}_p^m$ を，関数値（ベクトル）の成分ごとに，次のように定める：

$$\lambda_1(v_1,\ v_2,\ \cdots,\ v_m) = v_1^2 + v_2^{p-2}$$
$$\lambda_2(v_1,\ v_2,\ \cdots,\ v_m) = (v_1^2 + v_2^{p-2})^{p-2} + v_2^2 + v_3^{p-2}$$
$$\cdots\cdots\cdots$$
$$\lambda_j(v_1,\ v_2,\ \cdots,\ v_m) = (v_{j-1}^2 + v_j^{p-2})^{p-2} + v_j^2 + v_{j+1}^{p-2}$$
$$\cdots\cdots\cdots$$
$$\lambda_{m-1}(v_1,\ v_2,\ \cdots,\ v_m) = (v_{m-2}^2 + v_{m-1}^{p-2})^{p-2} + v_{m-1}^2 + v_m^{p-2}$$
$$\lambda_m(v_1,\ v_2,\ \cdots,\ v_m) = (v_{m-1}^2 + v_m^{p-2})^{p-1} + v_1$$

〈注意〉最後の式の右辺は第 1 項の指数が $p-1$ で，そのあとが 1 次の項 v_1 である。

この λ が全単射であることは，定理 1 で用いた λ と同様に，次の手順で確かめられる。

$$w_j = \lambda_j(v_1,\ v_2,\ \cdots,\ v_m)$$

とおき，また $V_j = v_j^2 + v_{j+1}^{p-2}$ とおくと

$$w_1 = v_1^2 + v_2^{p-2} = V_1$$
$$w_2 = (v_1^2 + v_2^{p-2})^{p-2} + v_2^2 + v_3^{p-2} = V_1^{p-2} + V_2$$
$$\cdots\cdots\cdots$$
$$w_j = (v_{j-1}^2 + v_j^{p-2})^{p-2} + v_j^2 + v_{j+1}^{p-2} = V_{j-1}^{p-2} + V_j$$
$$\cdots\cdots\cdots$$
$$w_m = V_{m-1}^{p-1} + v_1$$

ここでまず次のことを注意しておく：

どの V_j も，$w_1,\ w_2,\ \cdots,\ w_m$ の多項式で表せる。

$j = 1$ の場合は第 1 式から明らかで，$j > 1$ の場合も

$$V_j = w_j - V_{j-1}^{p-2}$$

から明らかである（j についての帰納法）。すると最後の式から

$$v_1 = w_m - V_{m-1}^{p-1}$$

なので，v_1 も $w_1,\ w_2,\ \cdots,\ w_m$ の多項式で表せるし，

$$v_j = (v_j^{p-2})^{p-2} = (V_{j-1} - v_{j-1}^2)^{p-2}$$

から，v_j も同様であることがわかる（j についての帰納法）。このように（w_j）からもとの（v_j）が決まるのでλは単射で，$\boldsymbol{Z}_p^m$ は有限集合であるから，λは全単射である。

このλについて，条件（♯）をみたす $M,\ M',\ \boldsymbol{b},\ \boldsymbol{b}'$ が，

Ⓐ　$M,\ M' = E$ でしかも $\boldsymbol{b} = \boldsymbol{b}' = \boldsymbol{0}$

かまたは

Ⓑ　$M = M' = 0$（ゼロ行列）

のどちらかをみたすことを示せばよい。

行列 $M,\ M'$ とベクトル $\boldsymbol{v}$ を，次のように表すことにしよう。

$$M = \begin{bmatrix} a_{11},\ a_{12},\ \cdots,\ a_{1m} \\ a_{21},\ a_{22},\ \cdots,\ a_{2m} \\ \cdots\cdots\cdots\cdots \\ a_{m1},\ a_{m2},\ \cdots,\ a_{mm} \end{bmatrix},\ b = \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix},$$

$$M' = \begin{bmatrix} a'_{11},\ a'_{12},\ \cdots,\ a'_{1m} \\ a'_{21},\ a'_{22},\ \cdots,\ a'_{2m} \\ \cdots\cdots\cdots\cdots \\ a'_{m1},\ a'_{m2},\ \cdots,\ a'_{mm} \end{bmatrix},\ b' = \begin{bmatrix} e'_1 \\ e'_2 \\ \vdots \\ e'_m \end{bmatrix},\ v = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{bmatrix}$$

そして

$$W_j = a_{j1}v_1 + a_{j2}v_2 + \cdots + a_{jm}v_m + e_j,$$
$$w_j = \lambda_j(v_1,\ v_2,\ \cdots,\ v_m)$$

とおくと，条件式

$$\lambda(Mv + \boldsymbol{b}) = M'\lambda(\boldsymbol{v}) + \boldsymbol{b}' \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(\sharp)$$

は，成分ごとに分けて，次のように表せる：

$$W_1^2 + W_2^{p-2} = a'_{11}w_1 + a'_{12}w_2 + \cdots + a'_{1m}w_m + e'_1$$
$$(W_1^2 + W_2^{p-2})^{p-2} + W_2^2 + W_3^{p-2} = a'_{21}w_1 + a'_{22}w_2 + \cdots + a'_{2m}w_m + e'_2$$
$$\cdots\cdots\cdots$$
$$(W_{j-1}^2 + W_j^{p-2})^{p-2} + W_j^2 + W_{j+1}^{p-2} = a'_{j1}w_1 + a'_{j2}w_2 + \cdots + a'_{jm}w_m + e'_j$$
$$\cdots\cdots\cdots$$
$$(W_{m-1}^2 + W_m^{p-2})^{p-1} + W_1 = a'_{m1}w_1 + a'_{m2}w_2 + \cdots + a'_{mm}w_m + e'_m$$

まず準備として，次の事実に注意しておこう。

事実 4　$w_j(1<j<m)$ を表す式の第 1 項 $(v_{j-1}^2+v_j^{p-2})^{p-2}$ と，w_m の第 1 項 $(v_{m-1}^2+v_m^{p-2})^{p-1}$ を展開すると，どちらにも p 次以上の固有の（そこにしかない）項が現れる。

実際，$(v_{j-1}^2+v_j^{p-2})^{p-2}$ を展開すると $q=(p-1)/2$ として

$$ {}_{p-2}C_q(v_{j-1}^2)^q\cdot(v_j^{p-2})^{p-2-q}={}_{p-2}C_q v_{j-1}^{p-1}v_j^{(p-2)(p-2-q)}={}_{p-2}C_q v_{j-1}^{p-1}v_j^{p\times p-4p+4-pq+2q} $$

$$ ={}_{p-2}C_q v_{j-1}^{p-1}v_j^{1-4+4-q+2q}={}_{p-2}C_q v_{j-1}^{p-1}v_j^{q+1} $$

という $p+q$ 次の項 $v_{j-1}^{p-1}v_j^{q+1}$ が現れる（$x^{ph}=x^h$ に注意）が，これはほかの $w_h(h\neq j)$ には含まれていない。また $(v_{m-1}^2+v_m^{p-2})^{p-1}$ を展開すると

$$ {}_{p-1}C_{q+1}(v_{m-1}^2)^{q+1}\cdot(v_m^{p-2})^{p-1-(q+1)}={}_{p-1}C_{q+1}v_{m-1}^{p+1}(v_m^{p-2})^{p-2-q}={}_{p-1}C_{q+1}v_{m-1}^{p+1}v_m^{q+1} $$

という $p+q+2$ 次の項 $v_{m-1}^{p+1}v_m^{p+1}$ が現れるが，これは w_m にしか含まれていない。

以下，定理の証明に戻る（定理 1 の証明と，ほぼ平行に進められる）。

〈第 1 段〉第 1 成分についての条件

$$ W_1^2+W_2^{p-2}=a'_{11}w_1+a'_{12}w_2+\cdots+a'_{1m}w_m+e'_1 \quad \cdots\cdots\cdots\cdots\cdots\cdots(2.1) $$

を調べる。左辺は変数 v_j の $p-2$ 次式であるから，右辺の p 次以上の（固有の）項を含む $w_2,\cdots,w_m$ はすべて消さなければならない。すなわち

$$ a'_{12}=a'_{13}=a'_{12}=\cdots=a'_{1m}=0\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(2.1.1) $$

そこで条件式(2.1)は，次のように書きなおせる。

$$ (a_{11}v_1+a_{12}v_2+\cdots+a_{1m}v_m+e_1)^2+(a_{21}v_1+a_{22}v_2+\cdots+a_{2m}v_m+e_2)^{p-2} $$

$$ =a'_{11}(v_1^2+v_2^{p-2})+e'_1\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(2.1') $$

（場合 1. A）$a'_{11}\neq 0$ の場合：(2.1′)の右辺は v_2^{p-2} を含むので，

$$ a_{22}^{p-2}=a'_{11}(\neq 0) \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(2.1.A1) $$

でなければならない。また右辺は $v_j^{p-2}(j\neq 2)$ を**含まない**ので，

$$ a_{21}=a_{23}=\cdots=a_{2m}=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(2.1.A2) $$

である。一方，右辺には v_1^2 もあるので，

$$ a_{11}^2=a'_{11}(\neq 0) \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(2.1.A3) $$

でなければならず，またほかのどこにもない v_1v_2 や v_1, v_2^{p-3} などを生み出さないために，

$$a_{12} = a_{13} = \cdots = a_{1m} = 0,\ e_1 = e_2 = 0 \quad \cdots\cdots\cdots\cdots\cdots\cdots(2.1.A4)$$

でなければならない。ここから

$$e_1' = 0 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(2.1.A5)$$

もわかる。

（場合 1. B）$a_{11}' = 0$ の場合：等式(2.1′)の右辺は定数になるので，左辺の 2 つの項（2 次と $p-2$ 次）はどちらも定数でなければならない。したがって，

$$\begin{aligned} &a_{11} = a_{12} = a_{13} = \cdots = a_{1m} = 0 \\ &a_{21} = a_{22} = a_{23} = \cdots = a_{2m} = 0 \quad \cdots\cdots\cdots\cdots\cdots\cdots(2.1.B1) \end{aligned}$$

また，(2.1.1)とあわせて

$$a_{11}' = a_{12}' = a_{13}' = \cdots = a_{1m}' = 0 \quad \cdots\cdots\cdots\cdots\cdots\cdots(2.1.B2)$$

も成り立つ。

〈第 2 段〉第 2 成分についての，次の条件を調べる：

$$(W_1^2 + W_2^{p-2})^{p-2} + W_2^2 + W_3^{p-2} = a_{21}'w_1 + a_{22}'w_2 + \cdots + a_{2m}'w_m + e_2' \quad \cdots\cdots(2.2)$$

（場合 2. A）$a_{11}' \neq 0$ ：この場合は $W_1 = a_{11}v_1$, $W_2 = a_{22}v_2$ なので，左辺は v_1, v_2 についてだけ p 次以上の項を含む。そのため v_2, v_3 や v_3, v_4 について p 次以上の項を含む w_3, …, w_m はすべて消さなければならない。すなわち

$$a_{23}' = a_{24}' = \cdots = a_{2m}' = 0 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(2.2.A1)$$

そこで条件式(2.2)は，次のように書きかえられる。

$$\begin{aligned} &((a_{11}v_1)^2 + (a_{22}v_2)^{p-2})^{p-2} + (a_{22}v_2)^2 + W_3^{p-2} \\ &\quad = a_{21}'(v_1^2 + v_2^{p-2}) + a_{22}'((v_1^2 + v_2^{p-2})^{p-2} + v_2^2 + v_3^{p-2}) + e_2' \cdots\cdots\cdots\cdots(2.2.A2) \end{aligned}$$

また(2.1.A3) $a_{11}^2 = a_{11}'$, (2.1.A1) $a_{22}^{p-2} = a_{11}'$ から，この式の左辺は次のように変形できる：

$$\begin{aligned} \text{左辺} &= (a_{11}'v_1^2 + a_{11}'v_2^{p-2})^{p-2} + a_{22}^2v_2^2 + W_3^{p-2} \\ &= a_{11}'^{p-2}(v_1^2 + v_2^{p-2})^{p-2} + a_{22}^2v_2^2 + W_3^{p-2} \end{aligned}$$

$a_{11}' = 0$ であるから，両辺が一致するためには

$$a_{22}' = a_{11}'^{p-2} (\neq 0) \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(2.2.A3)$$

でなければならない。これと(2.1.A1) $a_{22}^{p-2} = a_{11}'$を合わせると，

$$a_{22} = (a_{22}^{p-2})^{p-2} = a_{11}'^{p-2} = a_{22}' (\neq 0) \quad \cdots\cdots\cdots\cdots\cdots\cdots (2.2.\mathrm{A}4)$$

が得られる。

以上の結果を合わせて，等式(2.2.A2)の一致する部分を消去すると，次の等式が残る。

$$a_{22}^2 v_2^2 + W_3^{p-2} = a_{21}' (v_1^2 + v_2^{p-2}) + a_{22}' (v_2^2 + v_3^{p-2}) + e_2' \quad \cdots\cdots\cdots\cdots (2.2.\mathrm{A}5)$$

右辺に v_3^{p-2} がある（$a_{22}' = a_{11}'^{p-2} \neq 0$）から，$W_3$ は v_3 を含まなければならない。しかし W_3 が同時に v_1 や定数項を含んでいると，v_1^{p-2} や v_3^{p-3} なども現れてしまうので，それはありえない。したがって，左辺には v_1^2 という項も定数項もなく，

$$a_{21}' = 0,\ e_2' = 0$$

でなければならない。そうなると右辺には v_2^{p-2} という項もないので，再び W_3 に戻って，これは v_2 を含まない。したがって両辺の v_2^2 の係数が一致するためには

$$a_{22}^2 = a_{22}'$$

でなければならず，(2.2.A3) $a_{22} = a_{22}'$ とあわせて

$$a_{22}'^2 = a_{22}'$$

となるが，$a_{22}' \neq 0$ だから

$$a_{22}' = 1,$$

したがって

$$a_{22} = a_{11}' = a_{22}' = 1 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (2.2.\mathrm{A}6)$$

でなければならない。ついでながら，(2.1.A3) $a_{11}^2 = a_{11}'$ と合わせると，

$$a_{11} = \pm 1 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (2.2.\mathrm{A}7)$$

もわかる。そこで(2.2.A5)から，右辺の第1項など消せる項を消すと，残りは

$$W_3^{p-2} = v_3^{p-2}$$

となる。ここから

$$W_3 = v_3 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (2.2.\mathrm{A}7)$$

が導かれる（$(x^{p-2})^{p-2} = x$ に注意）。

（場合 2. B）$a_{11}' = 0$ の場合には，W_1, W_2 は定数，W_3 は $p-2$ 次多項式なので，p 次以上の項を含む $w_j (j > 1)$ はすべて消さなければならない。したがって，条件式(2.2)は次のように書き換えられる：

$$\text{定数} + W_3^{p-2} = a_{21}' (v_1^2 + v_2^{p-2}) + e_2'$$

もし $a_{21}' \neq 0$ であるとすると，W_3 は変数 v_1 を含むことになるが，それでは W_3^{p-2} が v_1^{p-2}

を含んでしまうので，それはありえない。したがって $a'_{21}=0$ でなければならず，W_3 も定数である。

まとめ：けっきょく最初の 2 つの条件式を調べるだけで，次のことがわかった。

（2 A）$a'_{11}\neq 0$ の場合：

$$W_1=a_{11}v_1,\ a_{11}=\pm 1\ ;\ a_{12}=a_{13}=a_{12}=\cdots=a_{1m}=e_1=0,$$
$$W_2=v_2\ ;\ a_{21}=0,\ a_{22}=1,\ a_{23}=a_{24}=\cdots=a_{2m}=e_2=0$$
$$W_3=v_3\ ;\ a_{31}=a_{33}=0,\ a_{33}=1,\ a_{34}=a_{35}=\cdots=a_{3m}=e_3=0$$
$$a'_{11}=1,\ a'_{12}=a'_{13}=a'_{12}=\cdots=a'_{1m}=e'_1=0$$
$$a'_{21}=0,\ a'_{22}=1,\ a'_{23}=a'_{24}=\cdots=a'_{2m}=e'_2=0$$

（2 B）$a'_{11}=0$ の場合：

$W_1,\ W_2,\ W_3$ は定数で，すべての $1\leqq j\leqq m$ について，$a'_{1j}=a'_{2j}=0$

〈第 j 段〉第 j 成分（$2<j<m$）についての条件式

$$(W_{j-1}^2+W_j^{p-2})^{p-2}+W_j^2+W_{j+1}^{p-2}=a'_{j1}w_1+a'_{j2}w_2+\cdots+a'_{jm}w_m+e'_j\quad\cdots\cdots(2.j)$$

を調べる。この左辺は，$v_{j-1},\ v_j$ についてだけ p 次以上の項を含み，それ以外の変数の組み合わせについては $p-2$ 次以下である。したがって，右辺の「$v_{j-1},\ v_j$ 以外の変数についての高次の項」を消すために，

$$a'_{j2}=a'_{j3}=\cdots=a'_{jj-1}=a'_{jj+1}=\cdots=a'_{jm}=0\quad\cdots\cdots\cdots\cdots\cdots(2.j.1)$$

でなければならない（w_1 は高次の項を含まないので，この段階で消すわけにはゆかない）。すると残りは次のように書ける：

$$(W_{j-1}^2+W_j^{p-2})^{p-2}+W_j^2+W_{j+1}^{p-2}=a'_{j1}w_1+a'_{jj}w_j+e'_j\ \cdots\cdots\cdots\cdots\cdots(2.j')$$

（場合 j. A）$a'_{11}\neq 0$ の場合：

$$W_1=a_{11}v_1(a_{11}=\pm 1),\ W_2=v_2,\ \cdots,\ W_j=v_j$$

と

$$a'_{11}=\cdots=a'_{j-1j-1}=1,$$
$$s<j,\ 1\leqq t\leqq m,\ s\neq t\ \text{のとき}\ a'_{st}=0,$$
$$e'_j=\cdots=e'_{j-1}=0$$

を前提として（数学的帰納法の仮定），条件式(2.j')から，以下のことを導く：

$$W_{j+1}=v_{j+1},$$
$$a'_{jj}=1,$$
$$1\leqq t\leqq m,\ t\neq j\ \text{のとき}\ a'_{jt}=0,$$
$$e'_j=0$$

なお $a_{11}=1$ であることは，さらにあとのステップで証明する。

さてこの場合には，帰納法の仮定によって，条件式(2.j')は次のように書きかえられる：

$$(v_{j-1}^2+v_j^{p-2})^{p-2}+v_j^2+W_{j+1}^{p-2}$$
$$=a'_{j1}(v_1^2+v_2^{p-2})+a'_{jj}((v_{j-1}^2+v_j^{p-2})^{p-2}+v_j^2+v_{j+1}^{p-2})+e'_j \quad \cdots\cdots\cdots\cdots(2.j.\mathrm{A1})$$

右辺で p 次以上の項を含むのは $(v_{j-1}^2+v_j^{p-2})^{p-2}$ だけなので，左辺と一致するためには

$$a'_{jj}=1 \quad \cdots\cdots\cdots\cdots(2.j.\mathrm{A2})$$

でなければならない。そこで $a'_{jj}=1$ とおいて共通項を消去すると，v_j^2 も消えて

$$W_{j+1}^{p-2}=a'_{j1}(v_1^2+v_2^{p-2})+v_{j+1}^{p-2}+e'_j$$

となるが，v_1^{p-2} という項は右辺にないので，W_{j+1} は v_1 を含まない。したがって v_1 は右辺にも含まれないので，

$$a'_{j1}=0 \quad \cdots\cdots\cdots\cdots(2.j.\mathrm{A3})$$

であり，方程式はさらに簡単化できる：

$$W_{j+1}^{p-2}=v_{j+1}^{p-2}+e'_j$$

明らかに W_{j+1} は v_{j+1} を含むが，それ以外の項は（定数項も）含まない（$e'_{j+1}\neq 0$ だと，左辺に v_{j+1}^{p-3} の項が現れてしまう）。したがって

$$e'_j=0, \quad \cdots\cdots\cdots\cdots(2.j.\mathrm{A1})$$
$$W_{j+1}^{p-2}=v_{j+1}^{p-2}$$

すなわち

$$W_{j+1}=v_{j+1} \quad \cdots\cdots\cdots\cdots(2.j.\mathrm{A5})$$

が導かれる。また(2.j.1)と合わせて，

$$a'_{jj}=1,$$
$$a'_{j1}=a'_{j2}=\cdots=a'_{jj-1}=a'_{jj+1}=\cdots=a'_{jm}=e'_j=0$$

も得られた。これで目指す目標が達成された。

（場合 j. B）$a'_{11}=1$ の場合：

$W_1, W_2, \cdots, W_j$ はすべて定数である

ことを前提（数学的帰納法の仮定）として，

W_{j+1} も定数である

ことを証明する。

この場合，条件式(2.j')は次のように書ける：

$$\text{定数}+W_{j+1}^{p-2}$$
$$=a'_{j1}(v_1^2+v_2^{p-2})+a'_{jj}((v_{j-1}^2+v_j^{p-2})^{p-2}+v_j^2+v_{j+1}^{p-2})+e'_j \quad \cdots\cdots\cdots\cdots(2.j.\mathrm{B1})$$

左辺は $p-2$ 次の多項式なので，$a'_{jj}=0$ である。またもし $a'_{j1}\neq 0$ だと，W_{j+1} は v_1 を含まなければならないが，そうすると左辺に v_1^{p-2} という項が現れてしまう。それはありえないので，$a'_{j1}=0$, したがって W_{j+1} も定数である。

〈第 m 段〉ここまでで，次のことが分かっている：

$a'_{11}\neq 0$ の場合には，

$$W_1=a_{11}v_1(a_{11}=\pm 1),\ W_2=v_2,\ \cdots,\ W_m=v_m,$$
$$\text{すべての } j \text{ に対して} a'_{jj}=1,\ e'_j=0,$$
$$\text{すべての } i\neq j \text{ に対して} a'_{ij}=0$$

また $a'_{11}=0$ の場合には，

$$W_1,\ W_2,\ \cdots,\ W_m \text{ はすべて定数である}$$

したがって，$a'_{11}=0$ の場合には，目標Ⓑがすでに達成されているので，あとは $a'_{11}=1$ の場合に

$$a_{11}=1,\ W_1=v_1$$

であることを示せばよい。そのために，第 m 成分についての条件式

$$(W_{m-1}^2+W_m^{p-2})^{p-2}+W_1=a_{m1}w_1+a_{m2}w_2+\cdots+a_{mm}w_m+e_m \quad \cdots\cdots\cdots(2.m)$$

を調べる。左辺は，すでにわかっていることから，次のように書ける：

$$(v_{m-1}^2+v_m^{p-2})^{p-2}+a_{11}v_1,\ a_{11}=\pm 1$$

したがって，右辺も v_{m-1}, v_m についてだけ p 次以上の項を含み，それ以外の変数の組み合わせについては 1 次の項 $a_{11}v_1$ だけである。したがって

$$a_{m1}=a_{m2}=a_{m3}=\cdots=a_{mm-1}=0$$

でなければならない（w_1 は v_2^{p-2} を含むので，これも消せる）。

$$(v_{m-1}^2+v_m^{p-2})^{p-2}+a_{11}v_1=a_{mm}((v_{m-1}^2+v_m^{p-2})^{p-2}+v_1)+e_m \quad \cdots\cdots\cdots(2.m')$$

だから両辺が一致するためには，$a_{mm}=1$, $e_m=0$ でなければならない。そこで $a_{mm}=1$ とおいて共通項を消去すると，

$$a_{11}v_1=v_1$$

となるので，$a_{11}=1$ が導かれる。

〈証明終わり〉

5. 未解決の場合

素数 p が 5 以上の場合は，問題は解決された____任意の $m \geqq 2$ に対して，直交する準線形関数族のペアが存在する。

$p = m = 2$ の場合については，準線形関数の極大クローンは 1 個しかないので，もちろん「直交するペア」は存在しない。それ以外の場合については，直交するペアはひじょうに構成しにくいが，存在しないという証明もできておらず，すべて今後の課題である。

参考文献

1. E. Post, 'The rwo-valued iterative systems of mathematical logic,' "Annals of Mathematical Studies," Princeton, vol. 5 (1941)
2. I. G. Rosenberg, 'La Structure des fonctions de plusieurs variables sur un ensemble fini', "Comptes-Rendus de l'Academy des Sciences," Paris, Tom 260 (1965) pp. 3817–3819
3. F. Laenger and R. Poeschel, 'Relational Systems with trivial endomorphism and polymorphism,' "Journal of Pure and Applied Algebra," Vol. 32, (1984) pp. 129–142
4. M. Miyakawa, A. Nozaki, G. Pogosyan, and I. G. Rosenberg, 'semi-rigid sets of central relations over a finite domain,' "Proceedings of 22nd International Symposium on Multiple-valued Logoc," (1992) pp. 300–307
5. A. Nozaki, G. Pogosyan, M. Miyakawa, and I. G. Rosenberg, 'Semi-rigid sets of quasi-linear clones,' "Proceedings of 23rd International Symposium of Multiple-valued Logic" (1993) pp. 105–110
6. A. Nozaki, M. Miyakawa, G. Pogosyan and I. G. Rosenberg, 'The number of Orthogonal Permutations,' "European Journal of Combinatorics," Vol. 16 (1993) pp. 71–85
7. A. Nozaki, 'On Semirigid Classes of Clones,' "多値論理研究ノート", 多値論理研究会，第 16 巻，(1993) pp. 8-1〜8-4
8. V. Lashkia, M. Miyakawa, A. Nozaki, G. Pogosyan, and I. G. Rosenberg, 'Semirigid sets of diamond orders,' "Discrete Mathmematics," No. 156, (1996) pp. 277–283
9. H. Machida and M. Pinsker, 'Some Observation on Minimal Clones,' "Proceedings of the 36th International Symposium on Multiple-Valued Logic," (2006) pp. 1–6
10. 宮川正弘，M. Pouzet, I. G. Rosenberg, 巽久行，'有限集合上の semirigid な同値関係族'，"2007 年度冬の LA シンポジウム講究録, " (2007) pp. 5-1〜5-4

Existence of Orthogonal Pairs of Clones of Quasi-linear Functions

── Relations Between Maximal Clones of Multi-valued Logical Functions ──

Akihiro Nozaki

A function defined over a finite set

$$X = \{0, 1, \cdots, k-1\}$$

is called a *multi-valued logical function* when $k > 2$. When k is a power of a prime p, $k = p^m$, we can introduce the notion of quasi-linear function. More precisely, for any one-to-one mapping σ from X to $(Z_p)^m$, we can define *σ-quasi-linear function* $f : X^n \to X$ defined over the domain X. The set $L(\sigma)$ of all σ-quasi-linear functions is a "clone", that is, a family of functions closed under the operation of composition.

We consider the existence of "orthogonal" pair of clones of the form $L(\sigma)$ and $L(\tau)$. This problem is already resolved for the case when the exponent m is equal to one: there are orthogonal pairs of such clones for $p \geqq 7$, and there is no such pair for $p < 7$.

In this paper, we show that there exist orthogonal pairs of the clones of the form $L(\sigma)$ and $L(\tau)$ for the prime $p \geqq 5$ and the exponent $m \geqq 2$.

For the case when $p < 5$ and $m \geqq 2$, the problem is still open, except the case when $p = m = 2$.

Keywords: Multi-valued logical function, Clone, Quasi-linear function, Orthogonal