P-10

平面単項式について
On the planar monomials

○中村周平 [1]
*Shuhei Nakamura[1]

Abstract: Let $p \geq 5$ be a prime. Coulter and Lazebnik proved that every planar monomial over the finite field $\mathbb{F}_{p^4}$ are only Dembowski-Ostrom polynomials. In this talk, we observe an analog of their result for the finite field $\mathbb{F}_{p^3}$.

1　導入

K, H は有限可換群とする. $f : K \to H$ が任意の $x, y \in K$ に対して $f(x+y) = f(x) + f(y)$ を満たすとき線形であるということとする. また, f が線形な写像 l と $a \in K$ で $f = l + a$ と書けているときアフィンであるいうこととする. $f : K \to H$ を線形とすれば $|f(K)| \times |\mathrm{Ker} f| = |K|$ であったから, $|K|$ が奇数, $|H|$ が 2 冪である場合は K と H の間には線形なものは自明なものに限る. ここで, K から H の写像同士の距離 d を次のように定義する.

定義 1. $d(f, g) := \sharp\{x \in K \mid f(x) \neq g(x)\}$ for $f, g : K \to H$

このとき, 写像 $f : K \to H$ に対する非線形度をアフィン写像全体からの最小距離を測るものとして定義してみる.

$$N_f := \min_{l \in \mathrm{Affin}(K,H)} d(f, l)$$

このような非線形度は $|K|$ が奇数, $|H|$ が 2 冪なときは意味をなさない. そこで, 任意の $a \in K, b \in H$ に対して記号 $D_a f(x) = f(x+a) - f(x)$ とおいて次のような非線形度を導入する.

$$P_f := \max_{a \in K^\sharp} \max_{b \in H} \Pr(D_a f(x) = b)$$

ただし, 事象 E に対して $\Pr(E)$ はその確率を表すものとする. このような非線形度 N_f, P_f はどちらも暗号理論での応用があることが知られている ([4], [7]). P_f に関して次のような不等式が成り立っている.

$$P_f \geq \frac{1}{|H|} \tag{1}$$

暗号理論や符号理論での応用から P_f が最小の値をとるような写像がどのようなものか判ることが望ましく, 本講演では特に次のような場合を扱う.

定義 2. $|K| = |H|$ で写像 $f : K \to H$ が上の式 (1) の等号を満たすとき f を平面関数であるという.

例えば p : 奇素数, $\mathbb{F}_{p^n}$ を加法群としてみると $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, f(X) = X^2$ は平面関数となる. ただし, 有限群 K, H 上に平面関数が存在すれば $|K| = |H|$ は奇数になることが判るので, 以下有限体を扱う場合など奇標数であることを仮定する. ところで, この平面関数という概念は Dembowski と Ostrom によって有限幾何の観点から研究されていた.

定義 3. $(P, L, \in)$ は次の条件を満たすとき射影平面であるという.

- $a, b \in P$ s.t. $a \neq b \ \Rightarrow\ \{a, b\} \subset {}^{\exists 1} l \in L$
- $l, l' \in L$ s.t. $l \neq l' \ \Rightarrow\ |l \cap l'| = 1$
- ${}^{\exists} a_1, a_2, a_3, a_4 \in P$ s.t. $\{a_i, a_j, a_k\} \not\subset l\ ({}^{\forall} l)$

一般に射影空間が 3 次元以上であればデザルグの定理が成り立ち, これは $\mathbb{P}^n$ と同型になるのであった. しかし, 射影平面の場合には $\mathbb{P}^2$ と同型でないような例がある. このような射影平面の構成するひとつの方法として平面関数の概念があり, 次が成り立っている ([2]).

定理 1. $f : K \to H$ が平面関数であるとする. このとき, $(P, L, \in)$ は射影平面となる. ただし, $P := (K \times H) \cup K \cup \{\infty\}, L := \{\{(x+a, f(x)+b) \mid x \in K\} \cup \{a\}\}_{(a,b) \in K \times H} \cup \{\{c\} \times H\}_{c \in K} \cup \{K \cup \{\infty\}\}$ である.

[1] 日大理工・院 (後)・数学

2　有限体上の平面関数

有限体の間の関数は多項式で書くことができ, 平面関数に関しては次のような形の多項式が重要である.

定義 4. $\mathbb{F}_{p^e}$ 上で次の形をしている多項式を Dembowski-Ostrom(以下 $D.O.$) 多項式と呼ぶ.

$$\sum_{i,j} a_{i,j} X^{p^i+p^j}$$

例えば X^2 もこの形をしているが, $D.O.$ 多項式は次のようにして特徴づけられる.

命題 1. $D.O.$ 多項式 F は次の条件を満たす.

$$B(x,y) := F(x+y) - F(y) - F(x) + F(0) \text{ は双線形である}$$

平面関数となる $D.O.$ 多項式が構成する射影平面は可移平面となるが, $D.O.$ 多項式が平面関数となる条件に関しては次のようなものがある ([8]).

命題 2. f が $D.O.$ 多項式であるとする. このとき, f が平面関数であることと f が 2 対 1 写像であることは同値である.

Dembowski と Ostrom は次のようなことを予想した ([2]).

予想 1. 有限体上の平面関数は $D.O.$ 多項式の形をしている.

この予想は単項式に限れば $\mathbb{F}_p, \mathbb{F}_{p^2}$ 上に対して正しいことが知られているが, 次のような反例がある.

反例 1. X^{14} は $\mathbb{F}_{3^4}$ 上で平面関数となる.

この反例は [5] の中で系列として一般化されている. 現在, 平面関数の系列が活発に構成されている ([6]) が予想 1 にアフィン項を加えた場合の予想での反例は多項式を含めて [5] の中の系列のみであり, $p \geq 5$ の場合には発見されていない. このことに関連して次のような結果がある.

定理 2 (Coulter and Lazebnik[1])**.** $p \geq 5$ とすると $\mathbb{F}_{p^4}$ 上での平面関数 X^n は $D.O.$ 多項式の形に限られる.

ある有限体上で平面関数となる単項式はその部分体でも平面関数となるので, この結果は $\mathbb{F}_{p^4}$ が部分体として $\mathbb{F}_{p^2}$ を含み冪指数 n の形が強く限定されていることが影響している. すなわち, $\mathbb{F}_{p^e}$ で e が素数な場合難しい. 講演では $e = 3$ のときに関してこのような類似に対しての考察を述べその一般化についても触れる.

参考文献

[1] R.S. Coulter and F. Lazebink : “ On the classification of planar monomials over fields of square order ”, Finite Fields Appl. **18**, 316-336 (2012).

[2] P. Dembowski and T.G. Ostrom : “ Planes of order n with collineation groups of order n^2 ”, Math. Z. **103**, 239-258 (1968).

[3] C. Carlet and C. Ding : “ Highly nonlinear mappings ”, J. Complexity, **20** 205-244 (2004),

[4] M. Matsui : “ Linear cryptanalysis method for DES cipher ”, in: Advances in Cryptology, EUROCRYPT ’93, Lecture Notes in Computer Science, **765**, Springer, Berlin, 386-397 (1994).

[5] R.S. Coulter and R.W. Matthews: “ Planar functions and planes of Lenz- Barlotti class II ”, Des. Codes Cryptogr. **10**, 167-184 (1997).

[6] L. Budaghyan and T. Helleseth : “ New commutative semifields defined by new PN multinomials ” . Cryptogr. Commun. **3**, 1-16 (2011).

[7] K. Nyberg :“ Perfect non-linear S-boxes ”, in: Advances in Cryptology, EUROCRYPT ’91, Lecture Notes in Computer Science, **547**, Springer, Berlin, 378-386 (1992).

[8] G.Weng , W. Qiu, Z. Wang and Q. Xiang : “ Pseudo-Paley graphs and skew Hadamard difference sets from presemifields ”, Des. Codes Cryptogr. (2007) 44:49-62 .