有限体上の関数が定める Cayley graph

吉荒　聡
(Satoshi Yoshiara)
東京女子大学現代教養学部数理科学科

2019 年 3 月 26 日提出

この記事は, 2018 年 12 月 13 日 (木) に京都大学数理解析研究所にて行われた筆者の講演を日本語でまとめたものである.

1　関数の定める Cayley グラフ

以下, 断らぬ限り，文字 F は標数 2 の有限体 $\mathbb{F}_{2^n}$ を, 文字 f および g は F から F 自身への関数を表す. f を $\overline{f}(x) := f(x) + f(0)$ $(x \in F)$ により定められる関数 $\overline{f}$ に取り換えて, $f(0) = 0$ と仮定する. 同様に $g(0) = 0$ とする. また V という文字で次の集合を自然に $\mathbb{F}_2$ 上の $2n+1$ 次元ベクトル空間と見なしたものを表す.

$$V = \mathbb{F}_2 \times F \times F = \{(\varepsilon; a, b) \mid \varepsilon \in \mathbb{F}_2, a, b \in F\}.$$

Cayley グラフの定義

定義 1 *F 上の関数 f に対して, 次のように定義されるグラフ $\mathcal{C}(f)$ を f の定める* **Cayley グラフ**と呼ぶ*:*

頂点 $V := \mathbb{F}_2 \times F^2 = \{(\varepsilon; x, y) \mid \varepsilon \in \mathbb{F}_2, x, y \in F\}$.

隣接関係 $u \sim v$ *iff* $u + v \in G_f := \{(1; x, f(x)) \mid x \in F\}$ *(*関数 f のグラフ*).*

Cayley グラフ $\mathcal{C}(f)$ に着目する (個人的) 理由

(1) f が quadratic APN 関数のときには, $\mathcal{C}(f)$ は f が定める DHO (dual hyperoval) $\mathcal{S}(f)$ に関連した **semibiplane** である. この semibiplane DHO と $\mathcal{S}(f)$ は, 私が quadratic APN 関数の間の同値性に関する結果を導く際に, 鍵となった幾何学的対象である. そこで一般の関数に対する Cayley グラフは, 私にはなじみ深い対象の一般化である.

(2) 同値性に関する不変量, Walsh 係数, Dillon の観察など, APN 関数に関する多くの結果が, その Cayley グラフに着目することによって，(後で解説するように) 明瞭かつ統一的に説明できる．従って, この概念は (少なくとも標数 2 の) 有限体上の関数を解析するための新しい観点を提供する.

復習–差分的一様性 (differential uniformity)

定義 2 F 上の関数 f が**差分的に** μ-**一様** *(differentially μ-uniform)* とは, すべての $a, b \in F$ ただし $a \neq 0$ について $^{\#}\{x \in F \mid f(x+a)+f(x)=b\} \leq \mu$ であること.

$F = \mathbb{F}_{2^n}$ 上のどの関数 f についても, 「f は差分的に 2^e 一様であるが, 差分的に 2^{e-1} 一様ではない」, という性質を満たすようなべき指数 2^e, $1 \leq e \leq n$, がただ一つ存在する. 例えば ($\mathbb{F}_2$-) 線形関数 f は差分的に 2^n 一様であるが, 差分的に 2^{n-1} 一様ではない. この対極的として, 差分的に 2-一様な関数のことを **APN**(almost perfect nonlinear) と呼ぶのであった.

復習–CCZ と EA-同値 (CCZ and EA-equivalence)

定義 3 F 上の関数 f と g に対して, f が g に **CCZ-同値** *(resp.* **EA-同値***)* とは, $V = \mathbb{F}_2 \oplus F^2$ 上の全単射線形変換 ρ で $\{(0; x, y) \mid x, y \in F\}$ *(resp.* および $\{(0; 0, y) \mid y \in F\}$*)* に作用し, かつ $G_f^\rho = G_g$ *(f のグラフを g のグラフに移す)* を満たすものが存在すること.

EA-変換の EA とは Extended Affine equivalence の略で, この用語は次の事実に因む.

> f と g が EA-同値であることと, すべての $x \in F$ について等式 $(g(x))^\delta = f(x^\alpha) + x^\beta$ が成立するような F 上のアフィン全単射 α, δ とアフィン写像 β が存在することが同値である.

一方, CCZ-同値という用語は, この概念を初めて公表した 3 人の研究者 Carlet, Charpin, Zinoviev の頭文字を合わせたものである. 定義から, 明らかに f と g が EA-同値であれば CCZ-同値である.

復習–Walsh 係数

定義 4 F 上の関数と $(\varepsilon; a, b) \in V$ に対して, f の $(\varepsilon; a, b)$ における **Walsh 係数** とは次式で定義される整数のことである:

$$W_f(\varepsilon; a, b) := \sum_{x \in F} (-1)^{\varepsilon + \mathrm{Tr}(ax + bf(x))}.$$

V を基本可換 2-群と見て, 次式で定められる V の指標 $\chi_{(\varepsilon;a,b)}$

$$\chi_{(\varepsilon;a,b)}(\varepsilon'; x, y) := (-1)^{\varepsilon\varepsilon' + \mathrm{Tr}(ax+by)}$$

を考える. このとき Walsh 係数 $V_f(\varepsilon; a, b)$ は, グラフ G_f に対応する群環 $\mathbb{C}[V]$ の元 $[G_f] := \sum_{x \in F}(1; x, f(x))$ において指標 $\chi_{(\varepsilon;a,b)}$ が取る値である.

V の元 $(\varepsilon; a, b)$ に Walsh 係数 $W_f(\varepsilon; a, b)$ を対応させる V 上の複素数値関数を W_f と記し, f の **Walsh 関数**と呼ぶことにする. すなわち, 群環 $\mathbb{C}[V]$ (V 上の複素数値関数全体と見なす) において次の等式で定義される関数が W_f である.

$$W_f = \sum_{x \in F} \chi_{(1,x,f(x))}.$$

APN 関数 f の研究において, Walsh 係数 $W_f(0;a,b)=\sum_{x\in F}(-1)^{\mathrm{Tr}(ax+bf(x))}$ は頻繁に現れる. その理由は何か. 一つには, 与えられた $b\in F$ に対する方程式 $f(x)=b$ の解 $x\in F$ の個数が Walsh 係数を用いて次のように表示できるという事実にある [1].

$$\sum_{a\in F}W_{f+b}(0;0,a)=|F|\{x\in F\mid f(x)=b\}.$$

より根源的な理由は次の章で説明される (補題 3).

2 関数の定める Cayley グラフの基本性質

以下, 関数の定める Cayley グラフの基本的な性質について, 以上復習した概念とのかかわりを中心に述べる. この部分は, 従来主として APN 関数に関して個別によく知られた事実に関して, 明瞭で統一的な説明を与えるだけでなく, 一般の関数に関する性質への自然な拡張にもなっている.

次の事実は, 標語的に言えば「CCZ-同値は Cayley グラフの同型を誘導する」と述べられるだろう.

補題 1 *F 上の関数 f と g に対して, f が g に CCZ-同値であれば, Cayley グラフ $\mathcal{C}(f)$ は Cayley グラフ $\mathcal{C}(g)$ にグラフとして同値である.*

確認はごく易しい. f と g の CCZ-同値を与えるような V 上の全単射線形変換 ρ を取る. V の元 u,v に対して, グラフ $\mathcal{C}(f)$ において u と v が隣接する $\Leftrightarrow u+v\in G_f\Leftrightarrow u^\rho+v^\rho=(u+v)^\rho\in G_f^\rho=G_g\Leftrightarrow u^\rho\sim v^\rho$ in $\mathcal{C}(g)$.

次の事実もすぐに見て取れる.

補題 2 *F 上の関数 f の定める Cayley グラフ $\mathcal{C}(f)$ は valency $|F|=2^n$ の正則グラフで, $\{(0;x,y)\mid x,y\in F\}$ (点の集合) と $\{(1;x,y)\mid x,y\in F\}$ (ブロックの集合) を bipartite halves とする二部グラフであり, V 上正則に作用する自己同型群 $\{t_u:v\mapsto v+u\mid u\in V\}$ を持つ.*

Cayley グラフ $\mathcal{C}(f)$ を見ると, f が差分的にどの程度一様であるかが判定できる (系 1(1)). 従って, 「差分的一様性が CCZ-同値によって保たれる」という事実 (系 1(2)) が補題 1 から直ちに導かれる. (この事実自体が証明されたのも新しく (2010 年ごろの Dempwolff の論文中), 初めての証明では計算が必要であった.)

系 1 *(1) f が差分的に μ-一様 $\Leftrightarrow$ 距離 2 にある任意の二頂点 $u,v\in V$ について $^{\#}\{w\in V\mid u\sim w\sim v\}\le\mu$.*

(2) 関数 f と g が CCZ-同値とする. このとき f が差分的に μ-一様であれば, g も差分的に μ-一様である.

次の事実は, 関数 f の Walsh 係数の意味を示すものであり, 前章最後に述べた問いに答えるものである.

補題 3 *A を Cayley グラフ $\mathcal{C}(f)$ の隣接行列とする. このとき A の固有値のなす多重集合は, Walsh 係数のなす多重集合 $\{W_f(\varepsilon;a,b)\mid(\varepsilon;a,b)\in V\}$ に一致する.*

この事実は, A.Terres の本 [TBook1999] や 知念氏と平松氏の本 [平松知念 Book2003] に一般化された形で表れている. この事実自体を示すのは易しいので, 確認しておく.

[1] 講演時に提示した式は正しくなかったので, 修正した

補題 3 の証明　V によりインデックス付けられた数ベクトル空間 $\mathbb{C}^V$ において, $v \in V$ に対応する基本ベクトルを $\mathbf{e}(v)$ と記す. 自然基底 $(\mathbf{e}(v))_{v\in V}$ において次のように定義された $\mathbb{C}^V$ への写像 α を, $\mathbb{C}^V$ 上の線形変換に拡張したものを同じく α と記す.

$$\alpha(\mathbf{e}(v)) := \sum_{w\in V, w\sim v} \mathbf{e}(w).$$

このとき, 隣接行列 A は α の自然基底 $(\mathbf{e}(v))_{v\in V}$ に関する表現行列である.

V の指標 χ に対して, $\mathbf{e}(\chi) := \sum_{v\in V} \chi(v)\mathbf{e}(v)$ という $\mathbb{C}^V$ のベクトルを考える. 指標の直交関係から χ が V の指標全体を動くとき $\rceil(\chi)$ は $\mathbb{C}^V$ の基底を与える. そこで, 次の主張を確かめれば, この基底は A の固有ベクトルからなるので, 補題の主張が得られる.

主張: 指標 χ が $\chi = \chi_{(\varepsilon,a,b)}$ という形のとき, $\mathbf{e}(\chi)$ は固有値 $W_f(\varepsilon; a, b)$ に対する A の固有ベクトルである.

以下この主張を確認する. まず線形変換 α の定義から

$$\alpha(\mathbf{e}(\chi)) \;=\; \sum_{v\in V} \chi(v) \left(\sum_{w\in V, v+w\in G_f} \mathbf{e}(w) \right) = \sum_{w\in V} \left(\sum_{v\in V, v+w\in G_f} \chi(v) \right) \mathbf{e}(w).$$

ここで, 固定した F の元 w に対して

$$\sum_{v\in V, v+w\in G_f} \chi(v) \;=\; \sum_{u\in G_f} \chi(w+u) = \left(\sum_{u\in G_f} \chi(u) \right) \chi(w)$$

である. 最後の式における $\chi(w)$ の係数は, $\chi = \chi_{(\varepsilon;a,b)}$ としたから, Walsh 係数の定義より,

$$\sum_{u\in G_f} \chi(u) = \sum_{x\in F} \chi(1; x, f(x)) = W_f(\varepsilon; a, b)$$

となる. 以上合わせて

$$\alpha(\mathbf{e}(\chi)) = W_f(\varepsilon; a, b) \sum_{w\in V} \chi(w)\mathbf{e}(w) = W_f(\varepsilon; a, b)\mathbf{e}(\chi)$$

であり, 確かに $\mathbf{e}(\chi)$ は固有値 $W_f(\varepsilon; a, b)$ に対する A の固有ベクトルである. □

次の系は補題 3 からすぐに得られるが, 重要な結果である. 系 2(1) は正則グラフの一般論と補題 3 から得られる. 系 2(2) に相当する事実は Edel-Pott により群環を通じた議論で初めて示された [EdelPott2009] が, そこでは符号の扱いにやや不自然な点がある.

系 2　*(1)* 隣接行列 A の固有値としての $|F|$ の重複度は *Cayley* グラフ $\mathcal{C}(f)$ の連結成分の個数と一致し, $|F|$ の約数である.

(2) 関数 f が g に *CCZ*-同値であれば, 多重集合として
$\{W_f(\varepsilon; a, b) \mid (\varepsilon; a, b) \in V\} = \{W_g(\varepsilon; a, b) \mid (\varepsilon; a, b) \in V\}$ である.

次も形式的な計算で示される事実である.

補題 4 $a,b \in F$ と非負整数 m に対して, *Cayley* グラフ $\mathcal{C}(f)$ において頂点 $(0;0,0)$ と $(m \bmod 2;a,b)$ を結ぶ長さ m の *walk* の個数とする.

$$w_m(a,b) = {}^{\#}\{(x_1,\ldots,x_m) \in F^m \mid \sum_{i=1}^{m} x_i = a, \sum_{i=1}^{m} f(x_i) = b\}.$$

このとき

$$(W_f)^m = \sum_{(a,b)\in F^2} w_m(a,b)\chi_{(m;a,b)}.$$

この式は $\mathcal{C}(f)$ の正則性が高いときに有効に使える. また, 最後に見るように f が $F = \mathbb{F}_{2^n}$ (n 奇数) 上の逆数関数 $f(x) = x^{2^n-2}$ のとき, Kloosterman 和に関する和公式を与える.

3 Cayley グラフの連結性と直径

この章では, 関数の定める Cayley グラフについて, その連結性と (連結な場合には) 直径について考察する. 連結性は関数のクラス分けに関して重要な示唆を与えるが, 直径に関しては APN 関数というクラス (このとき Cayley グラフは連結) に限っても未解決な部分がある.

次は新しい結果である.

補題 5 $x,y \in F$ に対する $B_f(x,y) := f(x+y)+f(x)+f(y)$ の全体が生成する F の部分空間を S と記すとき, 関数 f の定めるグラフ $\mathcal{C}(f)$ の連結成分の個数は $|F|/|S|$ に等しい.

S は $x,y,z \in F$ に対する $f(x)+f(y)+f(z)+f(x+y+z)$ の全体が生成する F の部分空間にも一致する.

次の事実は, Carlet, Charpin, Zinoviev の論文 [CCZ1998] で内在的に示されている.

補題 6 $\mathrm{Map}(F,\mathbb{F}_2)$ *(*F から二元体への写像全体のなす空間*)* から V への次に与える線形写像 ρ を考えるとき, その像 $\mathrm{Im}(\rho)$ は $(0;0,0)$ を含む $\mathcal{C}$ の連結成分に等しい.

$$\rho(\alpha) := (\sum_{x\in F}\alpha(x); \sum_{x\in F}\alpha(x)x, \sum_{x\in F}\alpha(x)f(x)).$$

以上の補題 5,6 に正則グラフの一般論を組み合わせると, Cayley グラフ $\mathcal{C}(f)$ の連結性に対する次の判定条件を得る. (iii) が新しく加わった.

系 3 $F = \mathbb{F}_{2^n}$ 上の関数 f に対して, 次は同値である.

(i) *Cayley* グラフ $\mathcal{C}(f)$ は連結である.

(ii) *Cayley* グラフ $\mathcal{C}(f)$ の最大固有値 $|F|$ の重複度は 1.

(iii) 補題 *5* で定義した F の部分空間は F に一致する.

(iv) 補題 *6* で定義した $\mathbb{F}_2$-線形写像 ρ は V 上への全射である.

次の結果は APN 関数が持つ最も重要な性質であると考えられる．この事実に相当する命題は，上記の判定条件 3 の判定条件 (iv) に基づいて, 長さ 2^n $(n \geq 3)$, 次元 $2^n - 2n$, 最小重さ 6 の二元線形符号の非存在に帰着される形で, 1990 年 [CCZ1998] において初めて証明された．しかし, この符号の非存在証明には非常に複雑な組合せ論的議論が必要であった. 後に，判定条件 (ii) に基づいて, Carlet 氏の本 [CarletBook2010B] において指標理論のみを用いた別証明が与えられている.

定理 1 *f が APN (差分的 2-一様) であれば, その Cayley グラフ $\mathcal{C}(f)$ は連結である.*

一般の関数についてその Cayley グラフの連結成分について調べたところ, 上の結果は次の形に一般化出来た.

定理 2 *$F = \mathbb{F}_{2^n}$, $n \geq 2e+1$, 上で定義された, 差分的に 2^e-一様な関数 f に対し, その Cayley グラフ $\mathcal{C}(f)$ の連結成分は高々 2^{e-1} 個である.*

$e = 1$ のとき, この結果は APN 関数 f に対する Cayley グラフ $\mathcal{C}(f)$ の連結性を示す. この定理の証明は, APN 関数 f に対する Cayley グラフ $\mathcal{C}(f)$ の連結性の新しい証明を, 適宜修正して得られる.

非連結な Cayley グラフを持つ関数は非常に多い．それらを構成するために, 次の補題が使われる.

補題 7 *f を F 上の差分 μ-一様な関数とし, F の元 α, β を $\mathrm{Tr}(\alpha\beta) = 1$ を満たすように選ぶ (Tr は F 上の絶対トレース関数). 関数 $f_{(\alpha,\beta)}$ を*

$$f_{(\alpha,\beta)}(x) := f(x) + \alpha\mathrm{Tr}(\beta f(x))$$

(従って, 任意の $x \in F$ において $f_{(\alpha,\beta)}(x) = f(x)$ または $f(x)+\alpha$) により定めると, 次が成立する.

(1) $f_{(\alpha,\beta)}$ *は差分的に 2μ-一様.*

(2) *もし $\alpha \notin \{f(x)+f(y)+f(z)+f(x+y+z) \mid x, y, z \in F\}$ であれば, $f_{(\alpha,\beta)}$ は差分的に μ-一様である.*

(3) $\mathcal{C}(f_{(\alpha,\beta)})$ *は非連結.*

補題 7(3) の証明　β に直交する部分空間上への射影を考える. 簡単のため, $g(x) = f_{(\alpha,\beta)}(x)$ と略記する. 任意の $x \in F$ に対して

$$\begin{aligned}
\mathrm{Tr}(\beta g(x)) &= \mathrm{Tr}(\beta(f(x) + \alpha\mathrm{Tr}(\beta f(x)))) \\
&= \mathrm{Tr}(\beta f(x)) + \mathrm{Tr}(\beta\alpha\mathrm{Tr}(\beta f(x))) \\
&= \mathrm{Tr}(\beta f(x)) + \mathrm{Tr}(\beta f(x))\mathrm{Tr}(\beta\alpha) \\
&= \mathrm{Tr}(\beta f(x)) + \mathrm{Tr}(\beta f(x)) = 0.
\end{aligned}$$

を得る. (下から二番目の等式においては $\mathrm{Tr}(\beta f(x))$ が二元体の元であることが効いている.) そこで部分空間 $S = \langle g(x+y)+g(x)+g(y) \mid x, y \in F\rangle$ は β の直交空間 $\beta^{\perp} = \{z \in F \mid \mathrm{Tr}(\beta z) = 0\}$ に含まれる. 系 3 の判定条件 (iii) から $\mathcal{C}(g)$ は非連結である. □

APN 関数に対する定理 1 と上の補題 7 から次が結論できる. 系 4(1) は **Dillon の観察** として知られている結果である. 系 4(2) は新しい結果であり, Cayley グラフの連結性という性質が APN 関数のクラスを特徴づけることを示す.

系 4 *(1) f が APN* 関数ならば, 任意の $c \in F$ に対して $c = f(x)+f(y)+f(z)+f(x+y+z)$ を満たす $x, y, z \in F$ が存在する.

(2) 任意の 2 べき $2^e \geq 4$ に対して, 差分的 2^e-一様な関数 f で, その *Cayley* グラフ $\mathcal{C}(f)$ が非連結なものが存在する.

以下, 関数が定める Cayley グラフの (連結成分の) 直径について考える. 関数が明示的に与えられたとしても, この直径を決めるのは関数の値の分布と関連して以外に難しい問題である.

基本的な補題 4 から $0 \neq c \in F$ が $\{f(x)+f(y)+f(z)+f(x+y+z) \mid x, y, z \in F\}$ に入ることと, 頂点 $(0;0,c)$ と $(0;0,0)$ のグラフ $\mathcal{C}(f)$ における距離が 4 であることは同値である. 従って Dillon の観察 (系 4(1)) から

APN 関数 f に対して, その Cayley グラフ $\mathcal{C}(f)$ の直径は高々 6 である.

また, 基本的な補題 4 から次も言える.

(1) $diam\mathcal{C}(f) \leq 5 \Leftrightarrow$ 任意の $(a,b) \in F^2$ に対して $f(x)+f(y)+f(z)+f(x+y+z+a) = b$ を満たす $x, y, z \in F$ が存在する.

(2) $diam\mathcal{C}(f) = 4 \Leftrightarrow$ 任意の $(a,b) \in F^2$ に対して $f(x)+f(y)+f(x+y+a) = b$ を満たす $x, y, z \in F$ が存在する.

今まで知られている APN 関数 f を調べると, 次が確かめられた.

Quadratic APN 関数 f に対して, $\mathrm{diam}\mathcal{C}(f) = 4$.
知られている 単項 APN function f に対して, $\mathrm{diam}\mathcal{C}(f) = 4$ または 5.

私は今のところ, $\mathcal{C}(f)$ の直径が 5 または 6 であるような APN 関数 f の例を知らない.

問題

(1) 任意の APN 関数 f について $\mathrm{diam}\mathcal{C}(f) = 4$ であることを示すか, または $\mathrm{diam}\mathcal{C}(f) = 5$ or 6 を満たす APN 関数 f の例を構成せよ.

(2) 一般の関数 f に対して, $\mathcal{C}(f)$ の連結成分の直径の上限はあるか?

4　距離正則性と Walk の数え上げ

APN 関数 f に対する Cayley グラフ $\mathcal{C}(f)$ が距離正則グラフとなるための必要十分な条件を求めることが出来た. 下の定理における **AB 関数**とは, APN 関数の重要なクラスをなす. 形式的には, 任意の $(\varepsilon;a,b)\in V$ に対して $W_f(\varepsilon;a,b)$ が $\pm|F|$, 0 または $\pm\sqrt{2|F|}$ のいずれかとなるような $F=\mathbb{F}_{2^n}$ 上の関数, と定義される. Wlash 係数は整数なので, AB 関数が存在するのは n が奇数の体 $F=\mathbb{F}_{2^n}$ 上のみである.

AB 関数が定める Cayley グラフが距離正則であることは [Yo2010] で示されているが, 今回はその逆を示した.

定理 3 *f を $F=\mathbb{F}_q$, $q=2^n$ 上の APN 関数とする. このとき $\mathcal{C}(f)$ が距離正則であることと f が* **AB** *(almost bent) 関数であることは同値である. また, このときの array は次の形である.*

$$\begin{pmatrix} q & q-1 & q-2 & (q/2)+1 & * \\ * & 1 & 2 & (q/2)-1 & q \end{pmatrix}.$$

特に APN 関数 f に対して $\mathcal{C}(f)$ が距離正則ならば, $\mathrm{diam}\mathcal{C}(f)=4$ である.

f が APN 関数でなくとも, $\mathcal{C}(f)$ が距離正則となる場合がある. 次の例は, [BCN1989] に記述されている.

例　$n=em$, $(m,k)=1$ とする.　このとき, 関数 $f(x)=x^{1+2^{ek}}$ は差分的に $\mu=2^e$-一様で, $\mathcal{C}(f)$ は距離正則で次の array を持つ:

$$\begin{pmatrix} q & q-1 & q-\mu & q-(q/\mu)+1 & * \\ * & 1 & \mu & (q/\mu)-1 & q \end{pmatrix},\quad q=2^n.$$

APN とは限らない一般の関数については, 今のところ次の部分的な結果しか得られていない.

補題 8 *Cayley グラフ $\mathcal{C}(f)$ が直径 4 の距離正則グラフであれば, その array はある μ に対する上の形である. ここで μ は q の約数で μq は平方数である.*

問題

(1) 一般の関数 f についても, その Cayley グラフ $\mathcal{C}(f)$ が距離正則であれば $\mathrm{diam}\mathcal{C}(f)=4$ となることを示せ.

(2) Cayley グラフ $\mathcal{C}(f)$ が距離正則となるような差分的に μ-一様な関数 f の族を Walsh 係数の言葉で特徴づけ出来るか?

上の定理 3 や補題 8 の証明には, 補題 4 が重要な手段となる.

補題 4 を用いて示せる他の事実の例として Kloosterman 和について触れる. $c \in F = \mathbb{F}_{2^n}$ に対して Kloosterman 和 $K(c)$ は

$$K(c) \ := \ \sum_{x \in F^\times} (-1)^{\mathrm{Tr}(cx+x^{-1})},$$

と定義され, これは F 上の逆数関数 $f(x) = x^{2^n-2}$ の Walsh 係数である. 逆数関数は n が奇数のとき APN 関数であり, n が偶数ならば 差分的に 4-一様である. Kloosterman 和の取る値や重複度については数論により決定されている. ここでは, 基本的な補題 4 から Kloosterman 和に関する次の公式が直ちに示せることに注意したい. 最後の式以外は良く知られている.

$\sum_{\gamma \in F^\times}(1+K(\gamma)) = |F|$, $\sum_{\gamma \in F^\times}(1+K(\gamma))^2 = |F|^2$.
n が奇数のときにはさらに $\sum_{\gamma \in F^\times}(1+K(\gamma))^3 = 2|F|^2$,
すべての $(a,b) \in F^2$ に対して $-|F|^3 \neq \sum_{\gamma \in F^\times}(1+K(\gamma))^3 K(ab\gamma)$.

References

[BCN1989] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance regular graphs, Springer, Berlin-Heidelberg, 1989.

[CarletBook2010B] C. Carlet, Vectorial boolean functions for cryptography, Chapter 9 (pp.398–470) of the volume "Boolean Methods and Models in Mathematics, Computer Science, and Engineering", Y. Crema and P. Hammer eds, Cambridge University Press.

[CCZ1998] C. Carlet, P. Charpin and V. Zinoviev, Codes, bent Functions and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography, 15 (1998), 125–156.

[EdelPott2009] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, Advances in Mathematics of Communications, 3 (2009), 59–81.

[平松知念 Book2003] 平松 豊・知念 宏司, 有限数学入門-有限上半平面とラマヌジャングラフ, 牧野書店, 2003.

[TBook1999] A. Terras, Fourier Analysis on Finite Groups and Applications, London Math. Soc. Student Texts 43, Cambridge University Press, 1999.

[Yo2010] S. Yoshiara, Notes on APN functions, semibiplanes and dimensional dual hyperovals, Designs, Codes and Cryptography **56**, 197–218 (2010).