Quadratic zero-difference balanced functions, APN functions and strongly regular graphs

Yin Tan

Department of Electrical and Computer Engineering
University of Waterloo

(Joint work with Claude Carlet and Guang Gong)

Workshop on Mathematics of Communications, Banff
January 28, 2015

Definitions

Let F be a mapping from $\mathbb{F}_{p^n}$ to itself. For each $a, b \in \mathbb{F}_{p^n}$, the *differential function* $\Delta_F(a,b) : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{Z}$ is defined as

$$\Delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n} \mid F(x+a) - F(x) = b\}.$$

Denoting the value $\Delta = \max_{a,b \in \mathbb{F}_{p^n}, a \neq 0} \Delta_F(a,b)$. We call F a differentially Δ-uniform mapping. In particular,

- When $p = 2$, the smallest value of Δ can achieve is 2, and we call F *almost perfect nonlinear* (APN) function.
- When p is odd, the smallest value of Δ can achieve is 1, and we call F *perfect nonlinear* (PN) function.
- Particularly, if $\Delta_F(a,0) = \delta$ for all $a \neq 0$, we call F zero-difference δ-balanced (ZDB) function.

Definitions

Let F be a mapping from $\mathbb{F}_{p^n}$ to itself. For each $a, b \in \mathbb{F}_{p^n}$, the *differential function* $\Delta_F(a,b) : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{Z}$ is defined as

$$\Delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n} \mid F(x+a) - F(x) = b\}.$$

Denoting the value $\Delta = \max_{a,b \in \mathbb{F}_{p^n}, a \neq 0} \Delta_F(a,b)$. We call F a differentially Δ-uniform mapping. In particular,

- When $p = 2$, the smallest value of Δ can achieve is 2, and we call F *almost perfect nonlinear* (APN) function.
- When p is odd, the smallest value of Δ can achieve is 1, and we call F *perfect nonlinear* (PN) function.
- Particularly, if $\Delta_F(a,0) = \delta$ for all $a \neq 0$, we call F zero-difference δ-balanced (ZDB) function.
- If F is quadratic, a zero-difference δ-balanced function is differentially δ-uniform.

Quadratic PN, APN and ZDB functions

A function of the form $F(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j} + L(x)$ on $\mathbb{F}_{p^n}$ is called *quadratic*, where L is affine.

- By definition, PN functions are zero-difference 1-balanced function. Weng, Qiu, Wang, Xiang (2007); Kyureghyan, Pott (2008) proved that, up to adding an affine function, all quadratic PN functions are of the form $G(x^2)$, where G is injective on the set of squares.

Quadratic PN, APN and ZDB functions

A function of the form $F(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j} + L(x)$ on $\mathbb{F}_{p^n}$ is called *quadratic*, where L is affine.

- By definition, PN functions are zero-difference 1-balanced function. Weng, Qiu, Wang, Xiang (2007); Kyureghyan, Pott (2008) proved that, up to adding an affine function, all quadratic PN functions are of the form $G(x^2)$, where G is injective on the set of squares.
- APN functions are not zero-difference balanced in general (for example APN PP), neither for quadratic APN functions. However, there exist quadratic APN functions which are ZDB.

Quadratic PN, APN and ZDB functions

A function of the form $F(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j} + L(x)$ on $\mathbb{F}_{p^n}$ is called *quadratic*, where L is affine.

- By definition, PN functions are zero-difference 1-balanced function. Weng, Qiu, Wang, Xiang (2007); Kyureghyan, Pott (2008) proved that, up to adding an affine function, all quadratic PN functions are of the form $G(x^2)$, where G is injective on the set of squares.
- APN functions are not zero-difference balanced in general (for example APN PP), neither for quadratic APN functions. However, there exist quadratic APN functions which are ZDB.
- As a simple example, let $F(x) = x^3$ on $\mathbb{F}_{2^n}$ with n even, we have

$$\frac{1}{a^3}(F(x+a) - F(x)) = (x/a)^2 + (x/a) + 1 = 0$$

always have two solutions due to $\mathrm{Tr}(1) = 0$.

Quadratic PN, APN and ZDB functions

A function of the form $F(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j} + L(x)$ on $\mathbb{F}_{p^n}$ is called *quadratic*, where L is affine.

- By definition, PN functions are zero-difference 1-balanced function. Weng, Qiu, Wang, Xiang (2007); Kyureghyan, Pott (2008) proved that, up to adding an affine function, all quadratic PN functions are of the form $G(x^2)$, where G is injective on the set of squares.
- APN functions are not zero-difference balanced in general (for example APN PP), neither for quadratic APN functions. However, there exist quadratic APN functions which are ZDB.
- As a simple example, let $F(x) = x^3$ on $\mathbb{F}_{2^n}$ with n even, we have

$$\frac{1}{a^3}(F(x+a) - F(x)) = (x/a)^2 + (x/a) + 1 = 0$$

  always have two solutions due to $\mathrm{Tr}(1) = 0$.
- One may verify the well-known APN function $G(x) = x^3 + \mathrm{Tr}(x^9)$ is another example of zero-difference 2-balanced functions when n is even.

Quadratic APN functions whic are ZDB

- On $\mathbb{F}_{2^6}$, 2 out of 13 pairwise inequivalent quadratic APN functions are ZDB. On $\mathbb{F}_{2^8}$, 18 out of 2,275 pairwise inequivalent quadratic APN functions are ZDB.
- What can we see from such APN functions?

Quadratic APN functions whic are ZDB

- On $\mathbb{F}_{2^6}$, 2 out of 13 pairwise inequivalent quadratic APN functions are ZDB. On $\mathbb{F}_{2^8}$, 18 out of 2,275 pairwise inequivalent quadratic APN functions are ZDB.
- What can we see from such APN functions?
  They are of the form $G(x^3)$, where $G|_{C_3}$ is injective and C_3 is the set of cubes.

Quadratic APN functions whic are ZDB

- On $\mathbb{F}_{2^6}$, 2 out of 13 pairwise inequivalent quadratic APN functions are ZDB. On $\mathbb{F}_{2^8}$, 18 out of 2,275 pairwise inequivalent quadratic APN functions are ZDB.
- What can we see from such APN functions?
  They are of the form $G(x^3)$, where $G|_{C_3}$ is injective and C_3 is the set of cubes. For example, for $F(x) = x^3 + \mathrm{Tr}(x^9)$ on $\mathbb{F}_{2^n}$ with n even, we have $G(x) = x + \mathrm{Tr}(x^3)$ which is a permutation.

Quadratic APN functions whic are ZDB

- On $\mathbb{F}_{2^6}$, 2 out of 13 pairwise inequivalent quadratic APN functions are ZDB. On $\mathbb{F}_{2^8}$, 18 out of 2,275 pairwise inequivalent quadratic APN functions are ZDB.
- What can we see from such APN functions?
  They are of the form $G(x^3)$, where $G|_{C_3}$ is injective and C_3 is the set of cubes. For example, for $F(x) = x^3 + \mathrm{Tr}(x^9)$ on $\mathbb{F}_{2^n}$ with n even, we have $G(x) = x + \mathrm{Tr}(x^3)$ which is a permutation.

Proposition

Let d be any positive integer and G a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ such that $G(x^d)$ is quadratic. Let $e = gcd(d, p^n - 1)$ and $C_d = \{x^d : x \in \mathbb{F}_{p^n}\} = C_e$. Then function $F(x) = G(x^d)$ is a differentially $(e-1)$-uniform function if and only if the restriction $G|_{C_d}$ of G to C_d is an injection.

Quadratic APN functions whic are ZDB

- On $\mathbb{F}_{2^6}$, 2 out of 13 pairwise inequivalent quadratic APN functions are ZDB. On $\mathbb{F}_{2^8}$, 18 out of 2,275 pairwise inequivalent quadratic APN functions are ZDB.
- What can we see from such APN functions?
  They are of the form $G(x^3)$, where $G|_{C_3}$ is injective and C_3 is the set of cubes. For example, for $F(x) = x^3 + \mathrm{Tr}(x^9)$ on $\mathbb{F}_{2^n}$ with n even, we have $G(x) = x + \mathrm{Tr}(x^3)$ which is a permutation.

Proposition

Let d be any positive integer and G a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ such that $G(x^d)$ is quadratic. Let $e = gcd(d, p^n - 1)$ and $C_d = \{x^d : x \in \mathbb{F}_{p^n}\} = C_e$. Then function $F(x) = G(x^d)$ is a differentially $(e-1)$-uniform function if and only if the restriction $G|_{C_d}$ of G to C_d is an injection.

Therefore, to discover quadratic APN functions, we simply need to find a function G which is injective on C_3 ($e = 3$ above) and $G(x^3)$ being quadratic.

Quadratic APN functions whic are ZDB (cont.)

Indeed, any function injective on C_d coinciding with a permutation G' such that $G|_{C_d} = G'_{C_d}$.

Proposition

Let d be a positive integer, $e = gcd(d, p^n - 1)$ and G a function defined on $\mathbb{F}_{p^n}$ such that $G|_{C_d}$ is an injection. Let $h : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be the characteristic function of C_d:

$$h(x) = 1 - \left(x^{\frac{2(p^n-1)}{e}} - x^{\frac{p^n-1}{e}} \right)^{p^n-1},$$

(satisfying $h(x) = 1$ if $x \in C_d = C_e$, and $h(x) = 0$ otherwise). There exists a function $T(x)$ on $\mathbb{F}_{p^n}$ such that the function G' defined by

$$G'(x) = h(x)G(x) + (1 - h(x))T(x) \tag{1}$$

is a permutation and satisfies $G'|_{C_d} = G|_{C_d}$, that is, $G(x^d) = G'(x^d)$, for all x.

A new class of quadratic APN functions

As an application of the above proposition, consider the condition that

$$G_{\alpha,\beta,\gamma}(x) = x + \alpha \mathrm{Tr}(\beta x + \gamma x^3)$$

is a permutation on $\mathbb{F}_{2^n}$ with n even, whch leads to the APN function $G_{\alpha,\beta,\gamma}(x^3)$.

Proposition

Assume $\alpha \neq 0$. Then $G_{\alpha,\beta,\gamma}$ is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if

- *(i) $\gamma = 0$ and $\mathrm{Tr}(\beta\alpha) = 0$,*
- *(ii) $\gamma\alpha^3 = 1$ and $\mathrm{Tr}(\beta\alpha) = 0$.*

If one of these two conditions is satisfied, the function $F(x) = G_{\alpha,\beta,\gamma}(x^3) = x^3 + \alpha \mathrm{Tr}(\beta x^3 + \gamma x^9)$ is a quadratic APN function.

A new class of quadratic APN functions (cont.)

Remarks:

(1) Conditin (i) lead to APN funcions CCZ-equivalent to the Gold APN function x^3.

(2) For $\beta = 0$ and $\gamma\alpha^3 = 1$, we have $F(x) = \alpha\left(\frac{x^3}{\alpha} + \mathrm{Tr}\left(\left(\frac{x^3}{\alpha}\right)^3\right)\right)$. On $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^{10}}$, we checked that taking for α as a primitive element of $\mathbb{F}_{2^2}$ gives a function CCZ-inequivalent to $x^3 + \mathrm{Tr}(x^9)$ and x^3.

(3) On $\mathbb{F}_{2^8}$, by choosing $\alpha = w^{85}, \beta = \gamma = 1$, we obtain the No. 1.3 APN function (not in any infinite class yet) in Edel-Pott's paper, where w is a primitive element of $\mathbb{F}_{2^8}$.

An algorithm to generate more quadratic ZDB APN functions

Proposition

Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function satisfying that $G|_{C_3}$ is an injection, and $h : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function. Let $\gamma \in \mathbb{F}_{2^n}$ be a nonzero constant. Then the function $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $H(x) = G(x) + \gamma h(x)$ has also injective restriction to C_3 if and only if

$$h(x^3) + h(y^3) = 0 \text{ holds for any } x, y \text{ satisfying } G(x^3) + G(y^3) = \gamma. \quad (2)$$

The set $S_{G,\gamma} := \{h \in \mathcal{BF}_n | G(x) + \gamma h(x)$ is an injection on $C_3\}$ is a subspace of $(\mathcal{BF}_n, +)$, where $\mathcal{BF}_n$ is the set of all Boolean functions.

Walsh spectrum of quadratic ZDB APN functions

The Walsh spectrum of a Vectorial Boolean function is the set $\{\widehat{F}(a,b) : a,b \in \mathbb{F}_{2^n}\}$.

Proposition

Let n be an even integer and $F = G(x^3)$ is a quadratic APN function on $\mathbb{F}_{2^n}$, where $G|_{C_3}$ is injective. Then the Walsh spectrum of F is $\{0, \pm 2^{n/2}, \pm 2^{n/2+1}\}$.

Zero-difference p-balanced functions

Besides the quadratic APN functions $G(x^{2+1})$ on $\mathbb{F}_{2^n}$, the following result gives construction of quadratic differentially p-uniform function with the form $F(x) = G(x^{p+1})$ on $\mathbb{F}_{p^n}$ with p odd, where $G|_{C_{p+1}}$ is injective and F is quadratic.

Proposition

Let $F(x) = x^{p+1} + \alpha \mathrm{Tr}(\beta x^{p+1} + \gamma x^{p^3+1})$ *defined on* $\mathbb{F}_{p^n}$, *where* $\alpha, \beta, \gamma \in \mathbb{F}_{p^n}$. *Then*

(i) *when* $n = 4$, *function* F *is a zero-difference p-balanced function if and only if* $\mathrm{Tr}(\alpha\beta + \gamma\alpha^{p^3}) \neq -1$.

(ii) *when* $n = 6$, *if* $\gamma^{p^3-1} = -1$ *and* $-1 - \mathrm{Tr}(\alpha\beta) \neq 0$, *then function* F *is a zero-difference p-balanced function.*

Partial difference sets and Strongly regular graphs

- Let $\mathcal{G}$ be a multiplicative group of order v. A k-subset D of $\mathcal{G}$ is called a (v,k,λ,μ) *partial difference set* (PDS) if each non-identity element in D can be represented as gh^{-1} $(g,h\in D, g\neq h)$ in exactly λ ways, and each non-identity element in $\mathcal{G}\backslash D$ can be represented as gh^{-1} $(g,h\in D, g\neq h)$ in exactly μ ways. We shall always assume that the identity element $1_{\mathcal{G}}$ of $\mathcal{G}$ is not contained in D. Particularly, D is called *regular* if, denoting $D^{(-1)}:=\{d^{-1};\, d\in D\}$, we have $D^{(-1)}=D$.
- Let Γ be the Cayley graph generated by a k-subset D of a multiplicative group $\mathcal{G}$ with order v. Then Γ is a (v,k,λ,μ) strongly regular graph (SRG) if and only if D is a (v,k,λ,μ)-PDS with $1_{\mathcal{G}}\notin D$ and $D^{(-1)}=D$.

Graphs from quadratic PN functions

The following result due to Weng, Qiu, Wang, Xiang relates quadratic PN functions (commutative semifields) to difference sets.

Theorem

Let G and H be two finite groups of the same order v. Let $f : G \to H$ be a 2-to-1 planar function and $D = f(G) \setminus \{1_H\}$. Then

(1) *If $v \equiv 3 \mod 4$, then D is a skew Hadamard difference set in H.*

(2) *If $v \equiv 1 \mod 4$, then D is a $(v, (v-1)/2, (v-5)/4, (v-1)/4)$ partial difference set in H.*

Graphs from quadratic PN functions

The following result due to Weng, Qiu, Wang, Xiang relates quadratic PN functions (commutative semifields) to difference sets.

Theorem

Let G and H be two finite groups of the same order v. Let $f : G \to H$ be a 2-to-1 planar function and $D = f(G) \setminus \{1_H\}$. Then

(1) *If $v \equiv 3 \mod 4$, then D is a skew Hadamard difference set in H.*

(2) *If $v \equiv 1 \mod 4$, then D is a $(v, (v-1)/2, (v-5)/4, (v-1)/4)$ partial difference set in H.*

Question: Writing f in the form $G(x^2) = G(x^{p^0+1})$, where $G|_{C_2}$ is injective. Is there any similar property for quadratic functions $G(x^{p^t+1})$, where $G|_{C_{p^t+1}}$ is injective?
We start from $p = 2, t = 1$, i.e. quadratic APN functions $G(x^3)$.

Graphs from quadratic APN functions

Theorem

Let F be a quadratic APN function on $\mathbb{F}_{2^n}$ with the form $F(x) = G(x^3)$, where $G|_{C_3}$ is an injection and $n = 2k$. Let D denote the set

$$D = \{F(x) : x \in \mathbb{F}_{2^n}\} \setminus \{0\}.$$

Then D is a partial difference set with parameters

$$\left(2^n, \tfrac{2^n-1}{3}, \tfrac{1}{9}(2^k+4)(2^k-2), \tfrac{1}{9}(2^k+1)(2^k-2)\right) \quad \text{if } k \text{ is odd},$$

$$\left(2^n, \tfrac{2^n-1}{3}, \tfrac{1}{9}(2^k-4)(2^k+2), \tfrac{1}{9}(2^k-1)(2^k+2)\right) \quad \text{if } k \text{ is even}.$$

Graphs from quadratic APN functions

Theorem

Let F be a quadratic APN function on $\mathbb{F}_{2^n}$ with the form $F(x) = G(x^3)$, where $G|_{C_3}$ is an injection and $n = 2k$. Let D denote the set

$$D = \{F(x) : x \in \mathbb{F}_{2^n}\} \setminus \{0\}.$$

Then D is a partial difference set with parameters

$$\left(2^n, \tfrac{2^n-1}{3}, \tfrac{1}{9}(2^k+4)(2^k-2), \tfrac{1}{9}(2^k+1)(2^k-2)\right) \quad \text{if } k \text{ is odd},$$

$$\left(2^n, \tfrac{2^n-1}{3}, \tfrac{1}{9}(2^k-4)(2^k+2), \tfrac{1}{9}(2^k-1)(2^k+2)\right) \quad \text{if } k \text{ is even}.$$

Example

Let $F(x) = x^3 + \mathrm{Tr}(x^9)$ on $\mathbb{F}_{2^8}$, the set D defined above is a (256, 85, 24, 30)-PDS.

Graphs from quadratic ZDB functions

Theorem

Let $F(x) = G(x^d)$ be a quadratic function from $\mathbb{F}_{p^n}$ to itself, where p is any prime and $\gcd(d, p^n - 1) = p^t + 1$ for some non-negative integer t. Assume that the restriction of G to $C_d = \{x^d : x \in \mathbb{F}_{p^n}^*\} = C_{p^t+1}$ is an injection from C_d to $\mathbb{F}_{p^n}$. Define the set $D = \{F(x) : x \in \mathbb{F}_{p^n}\} \setminus \{0\}$. Then:

(i) *if $t = 0$ and p is an odd prime, then D is a*

$$\left(p^n, \tfrac{p^n-1}{2}, \tfrac{p^n-3}{4}\right) \text{ difference set}, \qquad \text{when } p^n \equiv 3 \mod 4,$$

$$\left(p^n, \tfrac{p^n-1}{2}, \tfrac{p^n-5}{4}, \tfrac{p^n-1}{4}\right) \text{ partial difference set}, \qquad \text{when } p^n \equiv 1 \mod 4.$$

(ii) *if $t > 0$ and n is divisible by $2t$, then D is a*

$$\left(p^n, \frac{p^n-1}{p^t+1}, \frac{p^n - 3p^t - 2 - \varepsilon p^{n/2+2t} + \varepsilon p^{n/2+t}}{(p^t+1)^2}, \frac{p^n - \varepsilon p^{n/2} + \varepsilon p^{n/2+t} - p^t}{(p^t+1)^2}\right)$$

partial difference set, where $n = 2kt$ and $\varepsilon = (-1)^k$.

Can new graphs arise?

Recall that there are 18 APN functions of the form $F(x) = G(x^3)$ on $\mathbb{F}_{2^8}$, where $G|_{C_3}$ is injective. By the above theorem, the image set of F (exclude 0) is a (256, 85, 24, 30)-PDS, which generates (256, 85, 24, 30)-SRG (negative Latin square type).
(256, 85, 24, 30)-SRGs can be constructed via the

- Projective binary [85, 8] two-weight codes with weights 40, 48. Checking the database maintained by Eric Chen, SRGs from known such codes are isomorphic to the one generated by x^3x^9, x^{57};

Can new graphs arise?

Recall that there are 18 APN functions of the form $F(x) = G(x^3)$ on $\mathbb{F}_{2^8}$, where $G|_{C_3}$ is injective. By the above theorem, the image set of F (exclude 0) is a (256, 85, 24, 30)-PDS, which generates (256, 85, 24, 30)-SRG (negative Latin square type).
(256, 85, 24, 30)-SRGs can be constructed via the

- Projective binary [85, 8] two-weight codes with weights 40, 48. Checking the database maintained by Eric Chen, SRGs from known such codes are isomorphic to the one generated by $x^3 x^9, x^{57}$;
- Cyclotomic construction by Calderbank and Kantor (1986). The corresponding SRGs from this construction are isomorphic to those from x^3, x^9, x^{57} (they are CCZ-inequivalent but the corresponding graphs are isomorphic).

Can new graphs arise?

Recall that there are 18 APN functions of the form $F(x) = G(x^3)$ on $\mathbb{F}_{2^8}$, where $G|_{C_3}$ is injective. By the above theorem, the image set of F (exclude 0) is a (256, 85, 24, 30)-PDS, which generates (256, 85, 24, 30)-SRG (negative Latin square type).
(256, 85, 24, 30)-SRGs can be constructed via the

- Projective binary [85, 8] two-weight codes with weights 40, 48. Checking the database maintained by Eric Chen, SRGs from known such codes are isomorphic to the one generated by x^3x^9, x^{57};
- Cyclotomic construction by Calderbank and Kantor (1986). The corresponding SRGs from this construction are isomorphic to those from x^3, x^9, x^{57} (they are CCZ-inequivalent but the corresponding graphs are isomorphic).
- Cyclotomic construction by Brouwer, Wilson and Xiang (1999). The corresponding graph is isomorphic to the one from x^3x^9, x^{57}. Indeed, to obtainan SRGwith the above parameter, we need to require (using the same notation as in [4, Theorem 2]) $u/e = 1/3$, where $e \mid 255$ and there exists $l > 0$ such that $2l \equiv 1 mode$ and $1 \leq u \leq e-1$. Only $e = 3, u = 1$ satisfy the above conditions, which generated from the cyclotomic set C_3.

Can new graphs arise? (cont.)

Let $\mathbb{G}$ be the $(256, 85, 24, 30)$-SRG, M be its adjacent matrix, and Rank(M) the 2-rank of M.

Table : New Negative Latin square type $(256, 85, 24, 30)$-SRGs from APN functions

No.	$\lvert\mathrm{Aut}(\mathbb{G})\rvert$	Rank(M)	Remark	No.	$\lvert\mathrm{Aut}(\mathbb{G})\rvert$	Rank(M)	Remark
1	2^9	256	new	2, 6	2^{11}	256	new
3	2^8	256	new	4	2^{10}	256	new
5	2^9	256	new	6	2^{11}	256	new
7	2^{10}	256	new	8	2^{10}	256	new
9	2^9	256	new	10	2^{10}	256	new
11	2^8	256	new	12	2^{10}	256	new
13, 14, 17	$2^{11} \cdot 5 \cdot 17$	256		15	2^{10}	256	new
16	2^9	256	new	18	2^{10}	256	new