Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$

By Yuyin Yu yuyuyin@163.com
Joint Work with Lilya Budaghyan, Nikolay Kaleyski and Yongqiang Li

School of Mathematics and Information Science,
Guangzhou University

Florence, Italy - June 20, 2019

$$F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_2[x].$$

$$F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_2[x].$$

- $c_{i,t} \in \{0,1\}$.

$$F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_2[x].$$

- $c_{i,t} \in \{0, 1\}$.
- No linear or constant terms.

Quadratic homogeneous APN functions in $\mathbb{F}_2[x]$

$$F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_2[x].$$

- $c_{i,t} \in \{0, 1\}$.
- No linear or constant terms.
- APN Property : When it is APN?

$$F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_2[x].$$

- $c_{i,t} \in \{0,1\}$.
- No linear or constant terms.
- APN Property : When it is APN?
- Construction : Matrix method.

$$F(x) = \sum_{1\le t<i\le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_2[x].$$

- $c_{i,t} \in \{0,1\}$.
- No linear or constant terms.
- APN Property : When it is APN?
- Construction : Matrix method.
- Classification : Coding theory , Magma.

Definition (APN)

A mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an APN (Almost perfect nonlinear) function, if the equation $F(x+a) + F(x) = b$ has at most two solutions for any $a \in \mathbb{F}_{2^n}^{\star}$ and $b \in \mathbb{F}_{2^n}$.

Definition (CCZ-equivalence)

Suppose F and T are two functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, then F and T are ***CCZ-equivalent*** *(Carlet-Charpin-Zinoviev equivalent) if there is an affine permutation which maps G_F to G_T, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ is the graph of F, and G_T is the graph of T.*

Basis

Suppose $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, such that $\alpha_{i+1} = \alpha_i^2$ for $0 \le i \le n-1$.

Define

$$M \in \mathbb{F}_{2^n}^{n \times n}$$

such that

$$M[i, u] = \alpha_u^{2^i}.$$

Rank

Definition (Rank)

Let $\eta_1, \eta_2, \ldots, \eta_m$ be m elements on $\mathbb{F}_{2^n}$ $(m, n \geq 1)$, and $B = (\eta_1, \eta_2, \ldots, \eta_m) \in \mathbb{F}_{2^n}^m$.

$$\mathrm{Span}(B) = \mathrm{Span}(\eta_1, \eta_2, \ldots, \eta_m)$$

*denotes the subspace spanned by $\{\eta_1, \eta_2, \ldots, \eta_m\}$ over $\mathbb{F}_2$. $\mathrm{Rank}_{\mathbb{F}_2}\{\eta_1, \eta_2, \ldots, \eta_m\}$ is the dimension of $\mathrm{Span}(B)$ over $\mathbb{F}_2$, which we call the **rank** of B (over $\mathbb{F}_2$).*

Definition (QAM)

Let $H = (h_{u,v})_{n\times n}$ be an $n \times n$ matrix defined on $\mathbb{F}_{2^n}$. the matrix H is called a ***QAM*** *(quadratic APN matrix) if*
1) H is symmetric and the elements in its main diagonal are all zeros.
2) Every nonzero linear combination of the n rows (or "columns" since H is symmetric) of H has rank $n-1$.

Coefficient matrix

Let $F(x) = \sum_{0 \le t < i \le n-1} c_{i,t} x^{2^i + 2^t} \in \mathbb{F}_{2^n}[x]$, define an $n \times n$ matrix C_F such that

$$C_F[t, i] = C_F[i, t] = c_{i,t}$$

for $0 \le t < i \le n-1$ and

$$C_F[i, i] = 0$$

for $0 \le i \le n-1$.

Bijection 1

[1] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions.Designs, Codes and Cryptography, vol. 73, no. 2, pp. 587-600, 2014.

Theorem

Let $F(x) = \sum_{1\le t<i\le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_{2^n}[x]$, C_F *be defined as above, and* $H = M^t C_F M$. *Then,* $\delta(F) \le 2^k$ *if and only if any nonzero linear combination of the* n *rows of* H *has rank at least* $n-k$. *In particular,* F *is APN on* $\mathbb{F}_{2^n}$ *if and only if* H *is a QAM.*

Bijection 1

[1] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions.Designs, Codes and Cryptography, vol. 73, no. 2, pp. 587-600, 2014.

Theorem

Let $F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_{2^n}[x]$, C_F *be defined as above, and* $H = M^t C_F M$. *Then,* $\delta(F) \le 2^k$ *if and only if any nonzero linear combination of the* n *rows of* H *has rank at least* $n-k$. *In particular,* F *is APN on* $\mathbb{F}_{2^n}$ *if and only if* H *is a QAM.*

The correspondence between quadratic homogeneous APN functions and QAMs is one to one.

Bijection 1

[1] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions.Designs, Codes and Cryptography, vol. 73, no. 2, pp. 587-600, 2014.

Theorem

Let $F(x) = \sum_{1\le t<i\le n} c_{i,t}x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_{2^n}[x]$*,* C_F *be defined as above, and* $H = M^t C_F M$*. Then,* $\delta(F) \le 2^k$ *if and only if any nonzero linear combination of the* n *rows of* H *has rank at least* $n-k$*. In particular,* F *is APN on* $\mathbb{F}_{2^n}$ *if and only if* H *is a QAM.*

The correspondence between quadratic homogeneous APN functions and QAMs is one to one.

According to this result, constructing quadratic homogeneous APN functions is equal to construct QAMs.

Bijection 2

Theorem

Let $F(x) = \sum_{0 \le t < i \le n-1} c_{i,t} x^{2^i + 2^t}$, C_F *be defined as above. Define*

$$H = M^t C_F M.$$

Then $H[u+1, v+1] = H[u, v]^2$ *for* $0 \le v, u \le n-1$ *if and only if* $c_{i,t} \in \mathbb{F}_2$ *for* $0 \le t < i \le n-1$.

Bijection 2

Theorem

Let $F(x) = \sum_{0 \le t < i \le n-1} c_{i,t} x^{2^i + 2^t}$, C_F *be defined as above. Define*

$$H = M^t C_F M.$$

Then $H[u+1, v+1] = H[u,v]^2$ *for* $0 \le v, u \le n-1$ *if and only if* $c_{i,t} \in \mathbb{F}_2$ *for* $0 \le t < i \le n-1$.

Proposition

$F(x)$ *is a quadratic homogeneous APN function with coefficients in* $\mathbb{F}_2$ *if and only if* H *is an QAM such that* $H[i+1, j+1] = H[i,j]^2$ *for any* $0 \le i, j < n$.

Suppose $n = 6$. If $F(x) \in \mathbb{F}_{2^6}[x]$ is quadratic homogeneous APN function with coefficients in $\mathbb{F}_2$, then its corresponding matrix H must be a QAM such that

Suppose $n = 6$. If $F(x) \in \mathbb{F}_{2^6}[x]$ is quadratic homogeneous APN function with coefficients in $\mathbb{F}_2$, then its corresponding matrix H must be a QAM such that

$$H = \begin{pmatrix} 0 & a & b & c & b^{2^4} & a^{2^5} \\ a & 0 & a^2 & b^2 & c^2 & b^{2^5} \\ b & a^2 & 0 & a^{2^2} & b^{2^2} & c^{2^2} \\ c & b^2 & a^{2^2} & 0 & a^{2^3} & b^{2^3} \\ b^{2^4} & c^2 & b^{2^2} & a^{2^3} & 0 & a^{2^4} \\ a^{2^5} & b^{2^5} & c^{2^2} & b^{2^3} & a^{2^4} & 0 \end{pmatrix}.$$

Note that $H[u+1, v+1] = H[u, v]^2$ for all u, v.

Example for $n = 6$

(i) According to $H[u+1, v+1] = H[u,v]^2$, we have $c = c^{2^3}$ (Let $u = 2, v = 5$, then $H[3,6] = H[6,3] = H[0,3] = c = H[2,5]^2 = c^{2^3}$);

Example for $n = 6$

(i) According to $H[u+1, v+1] = H[u,v]^2$, we have $c = c^{2^3}$ (Let $u = 2, v = 5$, then $H[3,6] = H[6,3] = H[0,3] = c = H[2,5]^2 = c^{2^3}$);

(ii) Let $\lambda = a + b + c + b^{2^4} + a^{2^4}$, then $\mathrm{Trace}(\lambda) = 0$; If H is a QAM, then $\mathrm{Rank}_{\mathbb{F}_2}\{\lambda, \lambda^2, \lambda^{2^2}, \lambda^{2^3}, \lambda^{2^4}, \lambda^{2^5}\} = 5$.

Example for $n = 6$

(i) According to $H[u+1, v+1] = H[u, v]^2$, we have $c = c^{2^3}$ (Let $u = 2, v = 5$, then $H[3,6] = H[6,3] = H[0,3] = c = H[2,5]^2 = c^{2^3}$);

(ii) Let $\lambda = a + b + c + b^{2^4} + a^{2^4}$, then $\mathrm{Trace}(\lambda) = 0$; If H is a QAM, then $\mathrm{Rank}_{\mathbb{F}_2}\{\lambda, \lambda^2, \lambda^{2^2}, \lambda^{2^3}, \lambda^{2^4}, \lambda^{2^5}\} = 5$.

(iii) Let $\{\alpha, \alpha^2, \alpha^{2^2}, \alpha^{2^3}, \alpha^{2^4}, \alpha^{2^5}\}$ be a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Suppose $a = \sum_{i=0}^{5} a_i \alpha^{2^i}$, $b = \sum_{i=0}^{5} b_i \alpha^{2^i}$, $c = \sum_{i=0}^{5} c_i \alpha^{2^i}$, with $a_i, b_i, c_i \in \mathbb{F}_2$. Let $H[i, \cdot]$ and $H[\cdot, j]$ denote the i-th row and jth column of H,respectively. Identify A_0 with $H[\cdot, 0]$ as follows:

Example for $n = 6$

$$A_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ b_0 & b_1 & b_2 & b_3 & b_4 & b_5 \\ c_0 & c_1 & c_2 & c_3 & c_4 & c_5 \\ b_2 & b_3 & b_4 & b_5 & b_0 & b_1 \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_0 \end{pmatrix} = H[\cdot, 0] = \begin{pmatrix} 0 \\ a \\ b \\ c \\ b^{2^4} \\ a^{2^5} \end{pmatrix}. \quad (1)$$

$$A_1 = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ a_5 & a_0 & a_1 & a_2 & a_3 & a_4 \\ b_5 & b_0 & b_1 & b_2 & b_3 & b_4 \\ c_5 & c_0 & c_1 & c_2 & c_3 & c_4 \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_0 \end{pmatrix} = H[\cdot, 1] = \begin{pmatrix} a \\ 0 \\ a^2 \\ b^2 \\ c^2 \\ b^{2^5} \end{pmatrix}. \quad (2)$$

Example for $n = 6$

It can be seen that

$$A_1 = PA_0P^t, \tag{3}$$

where $P = (e_1, e_2, e_3, e_4, e_5, e_0)$($e_i$ is a column vector with $e_i[i] = 1$, and $e_i[j] = 0$ for $j \neq i$), and P^t is the transpose of P.

Example for $n = 6$

Similar as (1) and (2), we define A_2, A_3, A_4 and A_5. Therefore, similar as (3) we can get

$$\begin{aligned} A_2 &= PA_1P^t = P^2A_0(P^2)^t, \\ A_3 &= PA_2P^t = P^3A_0(P^3)^t, \\ A_4 &= PA_3P^t = P^4A_0(P^5)^t, \\ A_5 &= PA_4P^t = P^5A_0(P^5)^t. \end{aligned} \tag{4}$$

Example for $n = 6$

Similar as (1) and (2), we define A_2, A_3, A_4 and A_5. Therefore, similar as (3) we can get

$$\begin{aligned} A_2 &= PA_1P^t = P^2A_0(P^2)^t, \\ A_3 &= PA_2P^t = P^3A_0(P^3)^t, \\ A_4 &= PA_3P^t = P^4A_0(P^5)^t, \\ A_5 &= PA_4P^t = P^5A_0(P^5)^t. \end{aligned} \tag{4}$$

Based on Eq (3) and Eq (4), we have H is a QAM if and only if the rank of $\sum_{i=0}^{5} \mu_i P^i A_0 (P^i)^t$ is 5 for all $(\mu_0, \mu_1, \cdots, \mu_5) \neq 0 \in \mathbb{F}_2^5$.

Theorem

Suppose $H \in GF(2^n)^{n\times n}$, $H[0,0] = 0$, $H[u,v] = H[v,u]$ *for* $0 \leq v < u \leq n-1$, *and* $H[u+1, v+1] = H[u,v]^2$ *for* $0 \leq v, u \leq n-1$. *Let* $P = (e_1, e_2, \cdots, e_{n-2}, e_{n-1}, e_0)$, *where* e_i *is a column vector with* $e_i[i] = 1$, *and* $e_i[j] = 0$ *for* $j \neq i$. *Define a matrix* $A_0 \in \mathbb{F}_2^{n\times n}$ *such that* $H[i,0] = \sum_{k=0}^{n-1} A_0[i,k]\alpha^{2^k}$. *Then* H *is a QAM if and only if the rank of* $\sum_{i=0}^{n-1} \mu_i P^i A_0 (P^i)^t$ *is* $n-1$ *for all* $(\mu_0, \mu_1, \cdots, \mu_{n-1}) \neq 0 \in \mathrm{GF}(2)^n$. *(*$P^t$ *is the transpose of* P*).*

As a matter of fact, the condition $H[u+1, v+1] = H[u, v]^2$ for $0 \leq v, u \leq n-1$ has assured that there is only one half elements of $H[\cdot, 0]$ is uncertain, and it can be divided into two cases:

- i) when $n = 2m$, then $H[0,0] = 0$, $H[i,0] \in \mathbb{F}_{2^n}$ for $0 < i < m$, $H[m,0] = H[m,0]^{2^m}$, and $H[i,0] = H[n-i,0]^{2^i}$ for $m < i < n$.
- ii) when $n = 2m+1$,then $H[0,0] = 0$, $H[i,0] \in \mathbb{F}_{2^n}$ for $0 < i \leq m$, and $H[i,0] = H[n-i,0]^{2^i}$ for $m < i < n$.

Equivalence

Proposition

Suppose $f_1 \in \mathbb{F}_{2^n}[x]$, *with coefficients in* $\mathbb{F}_2$, *and its corresponding QAM is* H. *Define a new matrix* H' *such that* $H'[i,j] = H[i,j]^2$ *for any* $0 \le i, j < n$. *Then* H' *is also a QAM, and its corresponding function* $f_2 \in \mathbb{F}_2[x]$, *and* f_1 *is EA-equivalent to* f_2.

List for $n = 4, 5, 6$

n	Functions
4	x^3
5	x^3, x^5
6	x^3

List for $n = 7$

x^3
x^9
x^5
$x^3 + x^9 + x^{10} + x^{66}$
$x^5 + x^{18} + x^{34}$
$x^3 + x^6 + x^{20}$
$x^3 + x^{17} + x^{20} + x^{34} + x^{66}$
$x^3 + x^{17} + x^{33} + x^{34}$
$x^3 + x^5 + x^{10} + x^{33} + x^{34}$
$x^3 + x^9 + x^{18} + x^{66}$
$x^3 + x^{12} + x^{17} + x^{33}$
$x^3 + x^{20} + x^{34} + x^{66}$
$x^3 + x^{12} + x^{40} + x^{72}$
$x^3 + x^6 + x^{34} + x^{40} + x^{72}$
$x^3 + x^5 + x^6 + x^{12} + x^{33} + x^{34}$

15 CCZ-inequivalent classes.

List for $n = 8$

x^3
x^9
$x^3 + x^6 + x^{72}$
$x^3 + x^6 + x^{144}$
$x^3 + x^6 + x^{68} + x^{80} + x^{132} + x^{160}$
$x^3 + x^5 + x^{18} + x^{40} + x^{66}$
$x^3 + x^{12} + x^{40} + x^{66} + x^{130}$

7 CCZ-inequivalent classes.

List for $n = 9$

x^3
x^5
x^{17}
$x^{257} + x^{144} + x^{130} + x^{72} + x^{65} + x^{18} + x^9$
$x^{144} + x^{130} + x^{72} + x^{65} + x^{18} + x^9 + x^3$
$x^{136} + x^{132} + x^{96} + x^{80} + x^{36} + x^{34} + x^{18} + x^{17} + x^{12}$
$x^{264} + x^{160} + x^{144} + x^{132} + x^{80} + x^{72} + x^{66} + x^{40} + x^{17}$
$x^{288} + x^{272} + x^{264} + x^{160} + x^{144} + x^{130} + x^{48} + x^{34}$

8 CCZ-inequivalent classes.

List for $n = 9$

x^3
x^5
x^{17}
$x^{257}+x^{144}+x^{130}+x^{72}+x^{65}+x^{18}+x^9$
$x^{144}+x^{130}+x^{72}+x^{65}+x^{18}+x^9+x^3$
$x^{136}+x^{132}+x^{96}+x^{80}+x^{36}+x^{34}+x^{18}+x^{17}+x^{12}$
$x^{264}+x^{160}+x^{144}+x^{132}+x^{80}+x^{72}+x^{66}+x^{40}+x^{17}$
$x^{288}+x^{272}+x^{264}+x^{160}+x^{144}+x^{130}+x^{48}+x^{34}$

8 CCZ-inequivalent classes.

Not finished!

List for $n = 9$

x^3
x^5
x^{17}
$x^{257} + x^{144} + x^{130} + x^{72} + x^{65} + x^{18} + x^9$
$x^{144} + x^{130} + x^{72} + x^{65} + x^{18} + x^9 + x^3$
$x^{136} + x^{132} + x^{96} + x^{80} + x^{36} + x^{34} + x^{18} + x^{17} + x^{12}$
$x^{264} + x^{160} + x^{144} + x^{132} + x^{80} + x^{72} + x^{66} + x^{40} + x^{17}$
$x^{288} + x^{272} + x^{264} + x^{160} + x^{144} + x^{130} + x^{48} + x^{34}$

8 CCZ-inequivalent classes.

Not finished!

Nothing new for $n \leq 8$.

[2] Yves Edel, Alexander Pott. A new almost perfect nonlinear function which is not quadratic. Advances in Mathematics of Communications, 2009, 3 (1) : 59-81

Open problems

Conjecture

Given a quadratic APN function $f_1 \in \mathbb{F}_{2^n}[x]$, with coefficients in $\mathbb{F}_2$, then it is CCZ-equivalent to another quadratic APN function $f_2 \in \mathbb{F}_{2^n}[x]$, with coefficients in $\mathbb{F}_2$ and has at most n nonzero terms.

Open problems

Conjecture

Given a quadratic APN function $f_1 \in \mathbb{F}_{2^n}[x]$*, with coefficients in* $\mathbb{F}_2$*, then it is CCZ-equivalent to another quadratic APN function* $f_2 \in \mathbb{F}_{2^n}[x]$*, with coefficients in* $\mathbb{F}_2$ *and has at most* n *nonzero terms.*

Problem

Constructing quadratic APN functions $f(x) \in \mathbb{F}_2[x]$ *in* $\mathbb{F}_{2^n}$ *for infinite* n*.*

Thanks

Wisdom in the mind
is better than money in the hand.