On the number of generalized quadratic APN functions

The 9-th International Conference of Finite Fields and their applications (F_q9)

UCD,Ireland (July 13-17 2009)

The department of Math., Kinki Univ., Japan
Nobuo Nakagawa

Section 1 Introduction

Generalized quadratic APN functions was defined by S.Yoshiara.
Let F and R be vector spaces over $GF(2)$.
A function f from F to R is called almost perfect nonlinear if $\sharp\{x \in F | \ f(x+a)+f(x) = b \ \} \leq 2$ for every $a \in F^{\times}$ and every $b \in R$.
Strongly EA-equivalence of two APN functions f and g from F to R is defined as

$$g(x) = L \cdot f \cdot \ell(x) + A(x) \ \ (\forall \ x \in F)$$

where ℓ is a bijective linear mapping on F and L is a bijective linear mapping on R and A is an affine mapping from F to R.

A function f from F to R is called quadratic if

$$f(x+y+z)+f(x+y)+f(y+z)+f(z+x)+f(x)+f(y)+f(z)+f(0) = 0$$

for all elements x, y, z of F. Define as

$$b_f(x, y) = f(x + y) + f(x) + f(y) + f(0).$$

We denote the alternating tensor product of F by $F \wedge F$. A subspace W of $F \wedge F$ is called a nonpure subspace if

$$W \cap \{x \wedge y |\ x, y \in F\ \} = \{0\}.$$

Theorem 1 *(S.Yoshiara)*
Let $\{e_1, e_2, \cdots, e_m\}$ *be a basis of* F*, a map* γ *be a linear function from* $F \wedge F$ *onto* R *such that* $\mathrm{Ker}(\gamma)$ *is a nonpure subspace and a map* α *be an affine map from* F *to* R*. Then the function* $f := f_{\gamma,\alpha}$ *defined by the following formula is a quadratic APN function.*

$$f(\sum_{i=1}^{m} x_i e_i) := \sum_{0 \le i < j \le n} x_i x_j (e_i \wedge e_j)^{\gamma} + (\sum_{i=1}^{m} x_i e_i)^{\alpha}.$$

Conversely, for every quadratic APN function f *from* F *to* R *such that* b_f *is surjective, there is a uniqe pair* (γ, α) *satisfying* $f = f_{\gamma,\alpha}$ *where* γ *is a linear map from* $F \wedge F$ *to* R *such that* $\mathrm{Ker}(\gamma)$ *is a nonpure subspace and* α *is an affine map from* F *to* R*.*

An automorphism $g \in GL(F)$ induces an automorphism $\hat{g}$ of $F \wedge F$ defined as

$$\hat{g}(\sum a_{i,j} e_i \wedge e_j) := \sum a_{i,j} g(e_i) \wedge g(e_j).$$

Put $\widehat{G} := \{\ \hat{g}\ |\ g \in GL(F)\}$. For subspaces W_1, W_2 of $F \wedge F$, we define W_1 is $\widehat{G}$-equivalent to W_2 iff $W_2 = \hat{g}(W_1)$ for an automorphism $g \in GL(F)$.

Theorem 2 *(N.N.)*
Suppose that f and g are quadratic APN functions from F to R such that $f = f_{\gamma,\alpha}$ and $g = f_{\gamma',\alpha'}$ for γ, γ' are linear maps from $F \wedge F$ to R which kernels are nonpure subspaces and α, α' are affine maps from F to R. Then f is strongly EA-equivalent to g iff $\mathrm{Ker}(\gamma)$ *is $\widehat{G}$-equivalent to* $\mathrm{Ker}(\gamma')$.

Section 2 Vector spaces of alternating bilinear forms over $GF(2)$.

Let F be a m dimensional vector space over $GF(2)$ whose basis is $\{e_1, e_2, \cdots, e_m\}$
A mapping B from $F \times F$ to $GF(2)$ satisfying the following conditions is called an alternating bilinear form over F.

$$B(x + y, z) = B(x, z) + B(y, z), \quad B(x, x) = 0 \ (\forall x \in F).$$

Then note that $B(x, y) = B(y, x)$.
The set of alternating bilinear forms over F is a vector space of dimension $m(m-1)/2$ over $GF(2)$. We denote this space by $\mathbf{B}(m, 2)$, and the set of $m \times m$ alternating matrices over $GF(2)$ by $\mathbf{A}_m(2)$.

We have

$$\mathbf{B}(m, 2) \cong \mathbf{A}_m(2) \cong F \wedge F,$$

$$B \longleftrightarrow (B(e_i, e_j)) := (a_{i,j}) \longleftrightarrow \sum_{i<j} a_{i,j}(e_i \wedge e_j).$$

as vector spaces over $GF(2)$ by the above correspondences.

The $rank(B)$ for $B \in \mathbf{B}(m, 2)$ means the $rank$ of the matrix $(B(e_i, e_j))$.

It is well known that
the value of $rank(B)$ is even for $\forall B \in \mathbf{B}(m,2)$.

nonzero pure vectors of $F \wedge F$ corespond to elements of $\mathbf{B}(m,2)$ with $rank(B) = 2$.

Under this point, we will consider $\mathbf{B}(m,2)$ instead of $F \wedge F$. Its arguments are **linear algebras over** $GF(2)$**.**

Theorem 3 *(Delsarte and Goethals)*
Let B be any element of $\mathbf{B}(m,2)$ and F be the finite field $GF(2^m)$, moreover set $m = 2r+1$. Then we have

$$B(x,y) = \mathrm{Tr}(L_B(x)y) \text{ where}$$

$$L_B(x) = \sum_{i=1}^{r} (\beta_i x^{2^i} + (\beta_i x)^{2^{2r+1-i}})$$

and $\beta_i \in F$ for $1 \leq i \leq r$.

Theorem 4 *If $m = 2r$ is enen Then we have*

$$B(x,y) = \mathrm{Tr}(L_B(x)y) \text{ where}$$

$$L_B(x) = \sum_{i=1}^{r-1} (\beta_i x^{2^i} + (\beta_i x)^{2^{2r-i}}) + \beta_r x^{2^r}$$

and $\beta_i \in F$ for $1 \leq i \leq r-1$, $\beta_r \in GF(2^r)$.

We note that $L_B \in \mathrm{End}(F)$. We write $B = B(\beta_1, \cdots, \beta_r)$ because B is determined by $\beta_1, \cdots, \beta_r$. Here we identifies $F \wedge F$ with $\mathbf{B}(m,2)$. Then a non-pure subspace of $F \wedge F$ coresponds to a subspace W of $\mathbf{B}(m,2)$ satisfying $rank(B) > 2$ for all nonzero element $B \in W$.

Let W be non-pure subspace of dimension k of $\mathbf{B}(m,2)$. Put $R := \mathbf{B}(m,2)/W$. Then $\dim(R) = (m^2 - m)/2 - k$, and the natural homomorphism φ from $\mathbf{B}(m,2)$ onto R cause a quadratic APN function f from F to R as we know by **Theorem 1**. We denote this function f by f_W.

Theorem 5 *(Delsarte and Goethals)*
Let W be a non-pure subspace of $\mathbf{B}(m,2)$. Then we have dim(W) $\leq (m^2 - 3m)/2$.

We call W is a maximal non-pure subspace if the equality in Theorem 5 holds.

Let W be a maximal non-pure subspace of $\mathbf{B}(m,2)$. Then f_W is a quadratic APN function on F because that R is isomorphic to F.
Note that $(m^2 - m)/2 - (m^2 - 3m)/2 = m$.

Theorem 6 *(Delsarte and Goethals)*
Let $m = 2r + 1$ be an odd positive integer. Then

$$W(\beta_1 = 0) := \{B(\beta_1, \beta_2, \cdots, \beta_r) \in \mathbf{B}(m,2) \mid \beta_1 = 0\}$$

is a maximal non-pure subspace of $\mathbf{B}(m,2)$.

Note that a quadratic APN function $f_{W(\beta_1=0)}$ on F is a strogly EA-equivalent to **Gold** functions.
(by S.Yoshiara)

Theorem 7 *(N.N.)*
Let $m = 2r + 1$ *be an odd positive integer. Then*

$$W(\beta_2 = 0) := \{B(\beta_1, \beta_2, \cdots, \beta_r) \in \mathbf{B}(m, 2) \mid \beta_2 = 0\}$$

is a maximal non-pure subspace of $\mathbf{B}(m, 2)$.

We note that $W(\beta_i = 0)$ contains at least a nonzero pure vector for $i > 2$.
I believe that the quadratic APN function $f_{W(\beta_2=0)}$ is strongly EA-inequivalent to $f_{W(\beta_1=0)}$ though the proof is not complete yet untill now.

Section 3 Pure vectors and the number of solutions of linear equations related to $\mathbf{B}(m, 2)$

We have a necessary and suficient conditions such that $B = B(\beta_1, \beta_2, \cdots, \beta_r)$ is puer as follows.

Theorem 8 *(N.N.)*
Let $m = 2r + 1$ *be an odd positive integer. Suppose that* $\beta_1 \neq 0$.
Then $rank(B := B(\beta_1, \beta_2, \cdots, \beta_r)) = 2$, *(i.e.B is pure)*
if and only if $\beta_2 \neq 0$ *and*

$$\beta_2 \beta_t^2 + \beta_1 \beta_{t-1}^4 = \beta_1^2 \beta_{t+1} \text{ for } 2 \leq t \leq r - 1$$

$$\text{and } \beta_2 \beta_r^2 + \beta_1 \beta_{r-1}^4 = \beta_1^2 \beta_r^{2^{r+1}}.$$

Theorem 9 *(N.N.)*
Let $m = 2r$ be an even positive integer. Suppose that $\beta_1 \neq 0$. Then rank$(B := B(\beta_1, \beta_2, \cdots, \beta_r)) = 2$, (i.e. B is pure) if and only if $\beta_2 \neq 0$ and

$$\beta_2 \beta_t^2 + \beta_1 \beta_{t-1}^4 = \beta_1^2 \beta_{t+1} \text{ for } \ 2 \leq t \leq r-1$$

$$\text{and } \ \beta_2 \beta_r^2 + \beta_1 \beta_{r-1}^4 = \beta_1^2 \beta_{r-1}^{2^{r+1}}.$$

Let's consider the equation $L_B(x) = 0$ for $B = B(\beta_1, \cdots, \beta_r) \in \mathbf{B}(m, 2)$. Put $X := x^2$. Then

$$\beta_1 X + \beta_2 X^2 + \cdots + \beta_r X^{2^{r-1}} + \beta_r^{2^{r+1}} X^{2^r} + \cdots + \beta_2^{2^{2r-1}} X^{2^{2r-2}} + \beta_1^{2^{2r}} X^{2^{2r-1}} = 0$$

for $m = 2r + 1$
and

$$\beta_1 X + \beta_2 X^2 + \cdots + \beta_{r-1} X^{2^{r-2}} + \beta_r X^{2^{r-1}} +$$
$$\beta_{r-1} X^{2^r} + \cdots + \beta_2^{2^{2r-2}} X^{2^{2r-3}} + \beta_1^{2^{2r-1}} X^{2^{2r-2}} = 0$$

for $m = 2r$.

We note that $\dim(Im(L_B)) = \text{rank}(B)$. Therefore the dimension of the space $\mathbf{S}$ of solutions of the above equation agree with

$$\dim(\text{Ker}(L_B)) = m - \text{rank(B)}.$$

Let $m = 2r + 1$. Then
rankB $= 2 \Longleftrightarrow \dim(\mathbf{S}) = 2r - 1$,
rankB $= 4 \Longleftrightarrow \dim(\mathbf{S}) = 2r - 3$,
$\cdots$, rankB $= 2r \Longleftrightarrow \dim(\mathbf{S}) = 1$.

Let $m = 2r$. Then
rankB $= 2 \Longleftrightarrow \dim(\mathbf{S}) = 2r - 2$,
$\cdots$,
rankB $= 2r \Longleftrightarrow \dim(\mathbf{S}) = 0$.

Examples

Let $B(x, y)$ be a alternating bilinear form over$GF(2^6) = GF(2)(\theta)$ where $\theta^6 = \theta + 1$,
and $e_1 = 1, e_2 = \theta, e_3 = \theta^2, e_4 = \theta^3, e_5 = \theta^4, e_6 = \theta^5$.
(**Remark**) At the linear eqution

$$(Eq): \quad \beta_1 X + \beta_2 X^2 + \beta_3 X^4 + \beta_2^{16} X^8 + \beta_1^{32} X^{16} = 0$$

the number of solutions of (Eq) above in $GF(2^6)$ is just 1,4 or 16.

(1):$B = B(1, \theta^9, \theta^{18})$,

$$(B(e_i, e_j)) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$(Eq(1)): \quad X + \theta^9 X^2 + \theta^{18} X^4 + \theta^{18} X^8 + X^{16} = 0$$

rank$(B) = 2$ and $\dim(S(Eq(1))) = 4$.
(All solutions of $(Eq(1))$ are contained in $GF(2^6)$).

(2):$B = B(1,1,0)$,

$$(B(e_i, e_j)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$(Eq(2)) : \quad X + X^2 + X^8 + X^{16} = 0$$

rank$(B) = 4$ and dim$(S(Eq(2))) = 2$.
(Just 4 solutions of $(Eq(2))$ are contained in $GF(2^6)$).

(3):$B = B(1,1,\theta^9)$,

$$(B(e_i, e_j)) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$(Eq(3)) : \quad X + X^2 + \theta^9 X^4 + X^8 + X^{16} = 0$$

rank$(B) = 6$ and dim$(S(Eq(3))) = 0$.
(Only one (x=0) solutions of $(Eq(2))$ are contained in $GF(2^6)$).

References

[1] P.Delsarte and J.M.Goethals, Alternating Bilinear Forms over $GF(q)$,Journal of combinatorial theory(A) 19,26-50(1975).

[2] S.Yoshiara, On dual hyperovals of splite type, preprint.