<table>
<thead>
<tr>
<th>Title</th>
<th>On generalized quadratic APN functions (Algebraic Combinatorics and related groups and algebras)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>NAKAGAWA, Nobuo</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 1687: 84-90</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2010-05</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/141489">http://hdl.handle.net/2433/141489</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
On generalized quadratic APN functions

近畿大学理工学部理学科
中川 暢夫 (Nobuo NAKAGAWA)

1. Generalized quadratic APN functions.

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 (APN) if

$$\#\{x \in F | f(x + a) + f(x) = b\} \leq 2$$

for every $a \in F^\times$ and every $b \in R$.

We define a mapping $\Delta_a(f) : F \mapsto R$ for any $a \in F$ as

$$\Delta_a(f)(x) := f(x + a) + f(x)$$

(the difference function of $f$ w.r.t. $a$)

$f$ is APN iff $\Delta_a(f)$ is two to one map from $F$ to $\text{Im}(\Delta_a(f))$ for any $a \in F$ such that $a \neq 0$.

Strongly EA-equivalence of two functions $f$ and $g$ from $F$ to $R$ is defined as

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

where $\ell$ 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 $R$.

$$F \xrightarrow{\ell} F \xrightarrow{L} R \xrightarrow{A} R$$

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 a function $b_f$ from $F \times F$ onto $R$ as

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

It holds that $f$ is quadratic iff $b_f(x, y)$ is bilinear.
Suppose that $f$ is quadratic. Then $f$ is APN iff the equation $f(x + a) + f(x) + f(a) + f(0) = 0$ has just two solutions, namely $x = 0$ and $x = a$ for any $a \in F$ s.t. $a \neq 0$.

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

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

The following two theorems were observed by S. Yoshiara.

**Theorem 1** *(cf. [10])*

Let $\{e_1, e_2, \cdots, e_n\}$ be a basis of $F$. Then the function

$$\hat{f} : F \mapsto F \wedge F; \quad \sum_{i=1}^{n} x_i e_i \mapsto \sum_{1 \leq i < j \leq n} x_i x_j (e_i \wedge e_j)$$

is a quadratic APN function.

**Proof**) Put $x = \sum x_i e_i, y = \sum y_i e_i, z = \sum z_i e_i$, for any $i$, $(x_i + y_i + z_i)(x_j + y_j + z_j) + (x_i + y_i)(x_j + y_j) + (x_i + z_i)(x_j + z_j) + (y_i + z_i)(y_j + z_j) + x_i x_j + y_i y_j + z_i z_j = 0$. Thus

$$\hat{f}(x + y + z) + \hat{f}(x + y) + \hat{f}(y + z) + \hat{f}(z + x) + \hat{f}(x) + \hat{f}(y) + \hat{f}(z) = 0.$$

Next, suppose that $\hat{f}(x + a) + \hat{f}(x) + \hat{f}(a) = 0$ for any $a \neq 0$. We have $\hat{f}(x + a) + \hat{f}(x) + \hat{f}(a) = x \wedge a$. Hence $x \wedge a = 0$. Therefore $x = 0$ or $x = a$.

**Theorem 2** *(cf. [10])*

Let $W$ be a nonpure subspace of $F \wedge F$ and consider the following maps.

$$\hat{f} : F \mapsto F \wedge F; \quad \varphi_W : F \wedge F \mapsto (F \wedge F)/W, \quad u \mapsto u + W.$$

then the function $f_W := \varphi_W \cdot \hat{f}$ is a quadratic APN function. Conversely suppose that $f$ is a quadratic APN function from $F$ to $R$ such that $b_f$ is surjective. Then

$$f = \overline{\gamma} \cdot f_W + A$$

holds for a suitable linear mapping $\gamma$ from $F \wedge F$ onto $R$ where $W = \text{Ker}(\gamma)$ and $A$ is an affine mapping from $F$ to $R$.

We put $f := f_{\gamma,A}$ for $f$ in above theorem.

**Proof of the first half.**) Take any $a \neq 0$. Suppose that $f_W(x + a) + f_W(x) + f_W(a) + f_W(0) = 0$. Then $x \wedge a + W = 0$.

Thus $x \wedge a \in W$ and so, $x \wedge a = 0$. Because $W$ is a nonpure subspace. Therefore $x = 0$ or $x = a$. 
An automorphism $g \in GL(F)$ induces an automorphism $\hat{g}$ of $F \wedge F$ defined as

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

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

**Theorem 3** Suppose that $f$ and $g$ are quadratic APN functions from $F$ to $R$ such that $f = f_{\gamma, A}$ and $g = f_{\gamma', A'}$ for $\gamma, \gamma'$ are linear maps from $F \wedge F$ to $R$ which kernels are nonpure subspaces and $A, A'$ are affine maps from $F \wedge F$ to $R$. Then $f$ is strongly $EA$-equivalent to $g$ if and only if $\text{Ker}(\gamma)$ is $\hat{G}$-equivalent to $\text{Ker}(\gamma')$.

In the next section we know that there are nonpure subspaces of the codimension $n$. Remark that $(F \wedge F)/W \cong F$ if $\text{codim}(W) = n$. We denote the set of nonpure subspaces of $F \wedge F$ which have the codimension $n$ by $\Omega$, then the number of orbits of a permutation group $(\hat{G}, \Omega)$ is equal to the number of inequivalent quadratic APN functions on $F$. My aim is to obtain the number of orbits of $(\hat{G}, \Omega)$.

(It seems that this is a very difficult problem!!)

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

Let $F$ be a $n$ dimensional vector space over $GF(2)$ whose basis is $\{e_1, e_2, \cdots, e_n\}$ The set of alternating bilinear forms over $F$ is a vector space of dimension $n(n-1)/2$ over $GF(2)$. We denote this space by $Alt(F)$ and the set of $n \times n$ alternating matrices over $GF(2)$ by $A_n(2)$.

We have

$$ Alt(F) \cong A_n(2) \cong F \wedge F $$

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

The $\text{rank}(B)$ for $B \in Alt(F)$ means the $\text{rank}$ of the matrix $\left(B(e_i, e_j)\right)$.

It is well known that the value of $\text{rank}(B)$ is even for $\forall B \in Alt(F)$. Nonzero pure vectors of $F \wedge F$ correspond to elements of $Alt(F)$ with $\text{rank}(B) = 2$.

From now on, we will consider $Alt(F)$ instead of $F \wedge F$.

**Theorem 4** (Delsarte and Goethals(cf.[5]))

Let $B$ be any element of $Alt(F)$ where $F$ be the finite field $GF(2^n)$. Then $B(x, y)$ is represented as

$$ B(x, y) = \text{Tr}(L_B(x)y) $$
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 \( 1 \leq i \leq r \) in the case \( m=2r+1 \).

\[ L_B(x) = \sum_{i=1}^{r-1} (\beta_i x^{2^i} + (\beta_i x)^{2^{2r-i}}) + \beta_r x^{2^r} \]
and \( \beta_i \in F \) for \( 1 \leq i \leq r-1 \) and \( \beta_r \in GF(2^r) \) in the case \( m=2r \).

\( \text{Tr} \) is the absolute trace mapping, namely \( \text{Tr}(a) = a + a^2 + a^{2^2} + \cdots + a^{2^{n-1}} \). We note that \( L_B \in \text{End}(F) \). We write \( B = B(\beta_1, \cdots, \beta_r) \) because \( B \) is determined by \( \beta_1, \cdots, \beta_r \).

The correspondence \( B(\beta_1, \cdots, \beta_r) \leftrightarrow (\beta_1, \cdots, \beta_r) \) gives an isomorphism as vector spaces between \( \text{Alt}(F) \leftrightarrow F \times \cdots \times F \) (r times) if \( n = 2r + 1 \), \( \text{Alt}(F) \leftrightarrow F \times \cdots \times F \times GF(2^r) \) (r - 1 times of F, 1 time of \( GF(2^r) \)) if \( n = 2r \).

A non-pure subspace of \( F \wedge F \) corresponds to a subspace \( W \) of \( \text{Alt}(F) \) satisfying \( \text{rank}(B) > 2 \) for all nonzero element \( B \in W \).

**Theorem 5** (Delsarte and Goethals (cf.[5]))

Let \( W \) be a non-pure subspace of \( \text{Alt}(F) \) where \( F := GF(2^n) \). Then \( \dim(W) \leq (n^2 - n)/2 - n \).

We call \( W \) is a **maximal non-pure subspace** if the equality holds in the above theorem.

Let \( W \) be a maximal non-pure subspace of \( \text{Alt}(F) \). Then \( f_W \) is a quadratic APN function on \( F \) because that \( R \) is isomorphic to \( (F \wedge F)/W \).

For a \( r \) indeterminates polynomial \( g(x_1, \cdots, x_r) \), we set
\[ W(g(\beta_1, \cdots, \beta_r) = 0) := \{ B(\beta_1, \cdots, \beta_r) | g(\beta_1, \cdots, \beta_r) = 0 \} \]
We have \( W(\beta_e = 0) \) is a maximal nonpure subspace if \( \gcd(e, n) = 1 \) as we note soon after.

Especially \( W(\beta_1 = 0) \) is a maximal nonpure subspace and \( W(\beta_2 = 0) \) and \( W(\beta_r = 0) \) are maximal nonpure subspaces if \( n \) is odd.

**3 Pure vectors of \( \text{Alt}(F) \)**

We have a necessary and sufficient conditions such that \( B := B(\beta_1, \cdots, \beta_r) \) is puer as follows.
\textbf{Theorem 6} (1) Let $m = 2r + 1$. Suppose that $\beta_1 \neq 0$. Then $\text{rank}(B) = 2$, (i.e. $B$ is pure) if and only if
\[ \beta_2 \beta_t^2 + \beta_1 \beta_{t-1}^4 = \beta_1^2 \beta_{t+1} \text{ for } 2 \leq t \leq r - 1 \]
and \[ \beta_2 \beta_r^2 + \beta_1 \beta_{r-1}^4 = \beta_1^2 \beta_r^{2^{r+1}}. \]

(2) Let $m = 2r$. Suppose that $\beta_1 \neq 0$. Then $\text{rank}(B) = 2$, (i.e. $B$ is pure) if and only if
\[ \beta_2 \beta_t^2 + \beta_1 \beta_{t-1}^4 = \beta_1^2 \beta_{t+1} \text{ for } 2 \leq t \leq r - 1, \]
\[ \beta_2 \beta_r^2 + \beta_1 \beta_{r-1}^4 = \beta_1^2 \beta_{r-1}^{2^{r+1}} \]
and \[ \beta_2 \beta_{t-1}^{2^{r-t+1}} + \beta_1 \beta_{t+1}^{2^{r-t+1}} = \beta_1^2 \beta_{t-1}^{2^{2r-1+1}} \text{ for } 2 \leq t \leq r - 1. \]

I computed the rank of vectors in maximal nonpure subspaces $W(\beta_1 = 0), W(\beta_1 + \text{Tr}(\beta_3) = 0)$ and $W(\beta_1 + \text{Tr}r(\beta_3) = 0)$ where $\text{Tr}(x) = \sum_{i=0}^{r-1} x^{2^{2i}}$ for $n = 2r$, at $F = GF(2^6), GF(2^7), GF(2^8)$ and $GF(2^9)$ by MAGMA.

On $GF(2^6)$,
\begin{center}
\begin{tabular}{|c|c|c|}
\hline
 & rank 2 & rank 4 & rank 6 \\
\hline
$W(\beta_1 = 0)$ & 0 & 315 & 196 \\
$W(\beta_1 + \text{Tr}(\beta_3) = 0)$ & 0 & 315 & 196 \\
$W(\beta_1 + \text{Tr}r(\beta_3) = 0)$ & 10 & 297 & 204 \\
\hline
\end{tabular}
\end{center}

On $GF(2^7)$,
\begin{center}
\begin{tabular}{|c|c|c|c|}
\hline
 & rank 2 & rank 4 & rank 6 & rank 8 \\
\hline
$W(\beta_1 = 0)$ & 0 & 2667 & 13716 \\
$W(\beta_1 + \text{Tr}(\beta_3) = 0)$ & 0 & 2667 & 13716 \\
\hline
\end{tabular}
\end{center}

On $GF(2^8)$,
\begin{center}
\begin{tabular}{|c|c|c|c|c|}
\hline
 & rank 2 & rank 4 & rank 6 & rank 8 \\
\hline
$W(\beta_1 = 0)$ & 0 & 22491 & 583780 & 442304 \\
$W(\beta_1 + \text{Tr}(\beta_3) = 0)$ & 0 & 22491 & 583780 & 442304 \\
$W(\beta_1 + \text{Tr}r(\beta_3) = 0)$ & 24 & 22499 & 583236 & 442816 \\
\hline
\end{tabular}
\end{center}

On $GF(2^9)$,
\begin{center}
\begin{tabular}{|c|c|c|c|c|}
\hline
 & rank 2 & rank 4 & rank 6 & rank 8 \\
\hline
$W(\beta_1 = 0)$ & 0 & 182427 & 21370020 & 112665280 \\
$W(\beta_1 = \text{Tr}(\beta_3))$ & 0 & 182427 & 21370020 & 112665280 \\
\hline
\end{tabular}
\end{center}

The following nice observation was done by Yoshiara using dual basis of $\{e_1, \cdots, e_n\}$ with respect to the trace mapping.
Any pure vector $x \wedge y$ in $F \wedge F$ corresponds to $(\beta_1, \cdots, \beta_r) = (xy^{2^k} + x^{2^k}y)_{k=1}^r$.

$x \wedge y \leftrightarrow (xy^2 + x^2y, xy^4 + x^4y, xy^8 + x^8y, xy^{16} + x^{16}y, \cdots)$.

Hence if $u \in W(\beta_k = 0) \cap \{x \wedge y \mid x, y \in F\}$ then $u = x^{2^k+1}(a^{2^k} + a) = 0$ where $a = y/x$, and $a^{2^k-1} = 1$ if $x \neq 0$, $y \neq 0$. Then clearly $a = 1$ iff $\gcd(2^k - 1, 2^n - 1) = 1$. Therefore $a = 1$ iff $\gcd(n, k) = 1$. It implies that $W(\beta_k = 0)$ is a maximal nonpure subspace if and only if $\gcd(n, k) = 1$.

Then clearly $a = 1$ iff $\gcd(2^k - 1, 2^{n} - 1) = 1$. Therefore $a = 1$ iff $\gcd(k, n) = 1$.

It implies that $W(\beta_k = 0)$ is a maximal nonpure subspace if and only if $\gcd(n, k) = 1$.

Lastly we consider the following statement. Take a positive integer $r$ such that $r > 3$.

(\nabla) $Tr((u + u^2)^{-1}) = Tr(u)$ holds for any $u \in GF(2^r)$ such that $u \neq 0, u \neq 1$.

If the statement (\nabla) is true for some $r$, then $W(\beta_1 + Tr(\beta_3) = 0)$ is a maximal subspace and the corresponding function $f(x) = x^3 + Tr(x^9)$ is a APN function on $GF(2^{2r})$. Anyhow it seems that the cardinality of $W(\beta_1 + Tr(\beta_3) = 0) \cap PV(Alt(GF(2^{2r})))$ is relative small where $PV(Alt(F))$ is the set of pure vectors of $Alt(F)$.

References


