On the projection construction of planar and APN mappings

Jürgen Bierbrauer and Gohar M. Kyureghyan

May 12, 2010

Abstract

In the talk we present a method for constructing planar and APN mappings by a suitable choice of their coordinate functions. We expect to have more results on this subject by the dates of YACC.

Keywords: planar mapping, APN mapping, quadratic mapping

Let p be a prime number. Given a mapping $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and a nonzero element $a \in \mathbb{F}_{p^n}$, we call

$$D_{f,a} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto f(x+a) - f(x) - f(a)$$

the difference mapping of f defined by a. A mapping $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called planar (or perfect nonlinear) if all its difference mappings are bijective. Planar mappings do not exist in fields of even characteristic. Indeed, let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then the cardinality of the image set of a difference mapping $D_{f,a}$ is at most 2^{n-1}, since $D_{f,a}(x+a) = D_{f,a}(x)$ for any $x \in \mathbb{F}_{2^n}$. A mapping $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called almost perfect nonlinear (APN) if any its difference mapping has an image set of the maximal possible cardinality 2^{n-1}.

In [1] the first author introduces a method for constructing planar mappings, which meanwhile yields a unified explanation for several recent constructions of such mappings. In this note we continue study of this method.

Observe that the definition of planar and APN mappings uses only the additive group of the field, and hence such mappings can be defined in any group. The multiplicative structure of the field is beneficial in the study of planar and APN mappings, since it allows to construct explicit families of such mappings in polynomial forms. The monomial planar and APN mappings illustrate this. In this paper we show, that there are families of planar or APN mappings, which can be easier explained and better understood by studying their coordinate functions with respect to an appropriate chosen basis of $\mathbb{F}_{p^n}$ over a subfield.

In the rest of the paper we use the following notation: $n = m \cdot k$ and $\Omega := \{1, \omega_1, \ldots, \omega_{k-1}\} \subset \mathbb{F}_{p^n}$ is a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^m}$. Then, clearly, every mapping $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ can be uniquely represented by

$$F(x) = f_0(x) + \omega_1 f_1(x) + \ldots + \omega_{k-1} f_{k-1}(x),$$

where $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ for $0 \le i \le k-1$. We write $F = (f_0, \ldots, f_{k-1})$ and call the functions f_i the coordinate functions of F with respect to the basis Ω.

The following characterization of planar and APN mappings is straightforward:

Proposition 1 *The mapping $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is planar (resp. APN) if and only if for every $a \in \mathbb{F}_{p^n}^*$ and $(b_0, \ldots, b_{k-1}) \in \mathbb{F}_{p^m}^k$ the following system of equations*

$$\begin{cases} f_0(x+a) - f_0(x) &= b_0 \\ & \vdots \\ f_{k-1}(x+a) - f_{k-1}(x) &= b_{k-1} \end{cases}$$

has exactly 1 (resp. 2) solutions in $\mathbb{F}_{p^n}$.

Remark 1 *Every mapping $g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ can be represented as $g(x) = tr_{n/m}(G(x))$ where $tr_{n/m}$ is the trace mapping from $\mathbb{F}_{p^n}$ onto $\mathbb{F}_{p^m}$ and $G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.*

A mapping $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called quadratic if it is described by a polynomial of form $\sum_{i,j} \alpha_{i,j} x^{p^i+p^j}$. For quadratic mappings Proposition 1 reduces to:

Corollary 1 *Let $n = k \cdot m$ and a mapping $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be quadratic, i.e. $F(x) = \sum_{i,j} \alpha_{i,j} x^{p^i+p^j}$. Further, let $F = (f_0, \ldots, f_{k-1})$ with respect to some fixed basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^m}$. Define*

$$l_i(x,y) = f_i(x+y) - f_i(x) - f_i(y).$$

Then F is a planar (resp. APN) if and only if for every fixed $a \in \mathbb{F}_{p^n}^*$ the subspace

$$\bigcap_{i=0}^{k-1} Kernel\big(l_i(x,a)\big)$$

is trivial (resp. 1-dimensional).

Proof. It follows from Proposition 1, since for a quadratic F the mappings $l_i(x,y)$ are bilinear. ◇

Next we show that Corollary 1 allows to classify all planar mappings of the shape $x^{p^m+1} + \omega\, tr_{n/m}(\alpha x^{p^i+p^j})$ when $n = 2m$.

Theorem 1 *Let p be an odd prime number, $n = 2m$ and $\omega \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^m}$. Further, let $m, r \ge 1$, $p^m - 1 = 2^s k$ and $p^r - 1 = 2^t \ell$ with k, ℓ odd. Then the mapping $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by*

$$F(x) = x^{p^m+1} + \omega\, tr_{n/m}(\alpha x^{p^i(p^r+1)})$$

is planar if and only if

- α *is not a* (p^r+1)*th power in* $\mathbb{F}_{p^n}$*; and*

- $s \leq t$.

Proof. Note that $\{1, \omega\}$ is a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^m}$. Further, $F = (f_0, f_1)$ with $f_0(x) = x^{p^m+1}$ and $f_1(x) = tr_{n/m}(\alpha x^{p^i(p^r+1)})$. Since F is quadratic we apply Corollary 1. Here we have

$$l_0(x,y) = x^{p^m}y + xy^{p^m}$$

and

$$l_1(x,y) = tr_{n/m}\left(\alpha(xy^{p^r} + x^{p^r}y)^{p^i}\right).$$

Let $a \in \mathbb{F}_{p^n}^*$. Then

$$l_0(x,a) = a^{p^m+1}\left(\left(\frac{x}{a}\right)^{p^m} + \frac{x}{a}\right)$$

and thus $l_0(x,a) = 0$ if and only if $x/a \in \delta\,\mathbb{F}_{p^m}$, where u is a primitive element of $\mathbb{F}_{p^n}$ and $\delta = u^{(p^m+1)/2}$. Note that

$$\begin{aligned} l_1(x,a) &= tr_{n/m}\left(\alpha a^{p^i(p^r+1)}\left(\frac{x}{a} + \left(\frac{x}{a}\right)^{p^r}\right)^{p^i}\right) \\ &= tr_{n/m}\left(\beta\left(\frac{x}{a} + \left(\frac{x}{a}\right)^{p^r}\right)\right)^{p^i}, \end{aligned}$$

where we set $\beta = \left(\alpha a^{p^i(p^r+1)}\right)^{p^{n-i}}$.

Let $y = x/a \in \delta\,\mathbb{F}_{p^m}$. So $y = \delta z$ with $z \in \mathbb{F}_{p^m}$. Then $l_1(y,a) = 0$ if and only if

$$(\beta\delta + (\beta\delta)^{p^m})z + (\beta\delta^{p^r} + (\beta\delta^{p^r})^{p^m})z^{p^r} = 0.$$

By the choice of δ we have $\delta^{p^m} = -\delta$. So the last equality can be written as

$$(\beta - \beta^{p^m})\delta z + (\beta - \beta^{p^m})(\delta z)^{p^r} = (\beta - \beta^{p^m})(\delta z + (\delta z)^{p^r}) = 0. \tag{1}$$

Hence (1) holds if and only if one of the following conditions is satisfied

$$\beta^{p^m-1} = 1 \tag{2}$$

or

$$(\delta z)^{p^r} + \delta z = 0. \tag{3}$$

From the definition of β it follows that (2) is equivalent to

$$\alpha^{p^m-1}a^{p^i(p^r+1)(p^m-1)} = 1,$$

the latter equality holds for some $a \in \mathbb{F}_{p^n}$ if and only if α is a (p^r+1)th power in $\mathbb{F}_{p^n}$. Finally, using the definition of δ, condition (3) can be reduced to

$$u^{(p^m+1)\frac{p^r-1}{2}}z^{p^r-1} = -1 = u^{(p^m+1)\frac{p^m-1}{2}},$$

or equivalently

$$z^{p^r-1} = u^{(p^m+1)p^r \frac{p^{m-r}-1}{2}}.$$

The latter equation has a solution in $\mathbb{F}_{p^m}$ if and only if $\gcd(p^r-1, p^m-1) = 2^{\min(s,t)}\gcd(k,\ell)$ divides $\gcd((p^{m-r}-1)/2, p^m-1) = \gcd((p^r-1)/2, p^m-1) = 2^{\min(s-1,t)}\gcd(k,\ell)$.

$\diamond$

Remark 2 *Corollary 1 implies the classification of all APN mappings of the shape* $x^{p^m+1} + \omega\, tr_{n/m}(\alpha x^{p^i+p^j})$ *when* $n = 2m$ *as well.*

The following result follows from Theorem 1 and extends the construction of planar mappings given in [3, Main Theorem] based on the APN trinomials from [2, Corollary 1].

Corollary 2 *Let* $n = 2m$, $m, r \geq 1$, $p^m - 1 = 2^s u$ *and* $p^r - 1 = 2^t v$ *with* u, v *odd. Further, let* $c \in \mathbb{F}_{p^n}$ *be of multiplicative order* k *with* $\gcd(k, p^m-1) = 1$. *Define* ℓ *to satisfy* $\ell(p^m-1) \equiv 1 \pmod{k}$. *Then the mapping*

$$F(x) = bx^{p^m+1} + x^{p^i(p^r+1)} + cx^{p^{m+i}(p^r+1)}$$

is planar if and only if all of the following conditions are fulfilled:

- $c^\ell b$ *does not belong to* $\mathbb{F}_{p^m}$;
- c^ℓ *is not a* (p^r+1)*th power in* $\mathbb{F}_{p^n}$; *and*
- $s \leq t$.

Proof. Note that

$$\begin{aligned} c^\ell F(x) &= c^\ell b x^{p^m+1} + c^\ell x^{p^i(p^r+1)} + c^{\ell+1} x^{p^{m+i}(p^r+1)} \\ &= c^\ell b x^{p^m+1} + tr_{n/m}(c^\ell x^{p^i(p^r+1)}), \end{aligned}$$

since by choice of ℓ it holds $c^{\ell+1} = c^{\ell p^m}$. Hence Theorem 1 completes the proof. $\diamond$

More results on planar and APN mappings obtained via Corollary 1 will be presented in the extended version of this note.

References

[1] J. Bierbrauer: *New commutative semifields from projection mappings,* submitted to *Designs, Codes and Cryptography.*

[2] L. Budaghyan and C. Carlet, *Classes of quadratic APN trinomials and hexanomials and related structures*, *IEEE Trans. Inf. Theory*, 54(5) (2008) pp. 2354–2357.

[3] Z. Zha and X. Wang: *New families of perfect nonlinear polynomial functions, Journal of Algebra* (2009), doi:10.1016/j.algebra.2009.04.042.