Almost perfect nonlinear and planar functions: A survey of (not so) recent results and open problems

Alexander Pott

Otto-von-Guericke-University Magdeburg

September 3, 2015

Some connections

Geometry	Codes/Crypto

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions
	Nyberg (1994)

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions
B. Schmidt (1995)	Nyberg (1994)

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions
B. Schmidt (1995)	Nyberg (1994)
	non-weakly regular bent functions Ceşmelioğlu, McGuire, Meidl (2012)

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions
B. Schmidt (1995)	Nyberg (1994)
Davis, Jedwab (1997)	non-weakly regular bent functions Ceşmelioğlu, McGuire, Meidl (2012)

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions
B. Schmidt (1995)	Nyberg (1994)
Davis, Jedwab (1997)	non-weakly regular bent functions Ceşmelioğlu, McGuire, Meidl (2012)
relative difference set P., Zhou (2015)	degree-diameter problem

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions
B. Schmidt (1995)	Nyberg (1994)
Davis, Jedwab (1997)	non-weakly regular bent functions Ceşmelioğlu, McGuire, Meidl (2012)
relative difference set P., Zhou (2015)	degree-diameter problem
	MRD codes

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions
B. Schmidt (1995)	Nyberg (1994)
Davis, Jedwab (1997)	non-weakly regular bent functions Ceşmelioğlu, McGuire, Meidl (2012)
relative difference set P., Zhou (2015)	degree-diameter problem
Sheekey (2015), also Özbudak	MRD codes

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions
B. Schmidt (1995)	Nyberg (1994)
Davis, Jedwab (1997)	non-weakly regular bent functions Ceşmelioğlu, McGuire, Meidl (2012)
relative difference set P., Zhou (2015)	degree-diameter problem
Sheekey (2015), also Özbudak	MRD codes
symplectic spreads	

Some connections

Geometry	Codes/Crypto
planar functions	almost perfect nonlinear functions
B. Schmidt (1995)	Nyberg (1994)
Davis, Jedwab (1997)	non-weakly regular bent functions Ceşmelioğlu, McGuire, Meidl (2012)
relative difference set P., Zhou (2015)	degree-diameter problem
Sheekey (2015), also Özbudak	MRD codes
symplectic spreads	??

Definition

Let G be an Abelian group, $D \subseteq G$. Then D is a *difference set* if the list of non-zero differences $d - d'$ has some nice property, for instance

- ... every element occurs the same number λ of times.
- ... every element occurs λ or μ times.
- ... every element outside a certain subgroup occurs λ times.
- ...
- ...

Parameters: $|G|$, $|D|$, λ, ..., usually some trivial necessary conditions.

Examples with $\lambda = 1$

$$\begin{aligned} \{0,1,3\} &\subset \mathbb{Z}_7 \\ \{0,1,3,9\} &\subset \mathbb{Z}_{13} \\ \{3,6,7,12,14\} &\subset \mathbb{Z}_{21} \end{aligned}$$

Some tendencies ...

- The more cyclic a group is, the less difference sets it has.
- Small λ, less difference sets.
- If there are some examples with certain parameters, there are usually many.

Incidence structures: The geometry world

From any difference set D we construct an *incidence structure*

- Points are elements in G
- Blocks are translates $D + g$ of D

Incidence structures: The geometry world

From any difference set D we construct an *incidence structure*

- Points are elements in G
- Blocks are translates $D + g$ of D

Important observation:
$g - h$ has λ difference representations if and only if g and h are on λ blocks.

Incidence structures: The geometry world

From any difference set D we construct an *incidence structure*

- Points are elements in G
- Blocks are translates $D + g$ of D

Important observation:
$g - h$ has λ difference representations if and only if g and h are on λ blocks.
Difference sets with $\lambda = 1$ correspond to projective planes:

- $q^2 + q + 1$ points
- $q^2 + q + 1$ lines
- two different points are on exactly one line.

Prime Power Conjecture: q must be a prime power!

Remark about projective planes

- $q = p$ prime: Only one example? *open*
- $q = p^f$ with $f \geq 2$: Many, many examples. *known*

Remark about cyclic difference set with $\lambda = 1$:
Only one known example! *Supports the "tendency"*

Remark about projective planes

- $q = p$ prime: Only one example? *open*
- $q = p^f$ with $f \geq 2$: Many, many examples. *known*

Remark about cyclic difference set with $\lambda = 1$:
Only one known example! *Supports the "tendency"*

Construction: Elements of trace 0 in multiplicative group of $\mathbb{F}_{q^3}$ modulo multiplicative subgroup of order $q - 1$.

Another representation of a plane

Vector space $\mathbb{F}_p^{2f}$, collection of $p^f + 1$ subspaces of dimension f with pairwise trivial intersection. *spread*

Example

1-dimensional subspaces in $\mathbb{F}_q^2$ *with* $q = p^f$.

Corresponding projective plane:

- Points are elements in $\mathbb{F}_p^{2f}$
- lines are cosets of subspaces.

There are many, many examples (*translation planes*).

Remark: Not really a difference set construction.

Special translation planes, but p odd

Some spreads have a nice construction:

Example

$f(x) = x^2$ *on* $\mathbb{F}_{p^f}$ *then* $\mathcal{L}_a : x \mapsto f(x+a) - f(x) - f(a) = 2xa$ *generates subspaces (*spread*)*

$$\{(x, \mathcal{L}_a(x)) \ : \ x \in \mathbb{F}_{p^f}\}$$

plus $\{(0, x) \ : \ x \in \mathbb{F}_{p^f}\}$

When are the subspaces "disjoint"?

Condition:

$$\mathcal{L}_a \text{ are linear and bijective.}$$

Note: The $\mathcal{L}_a$ form a vector space of linear invertible mappings!
This is not true for general spreads.

Difference set representation, Coulter, Henderson (2008)

If f describes a spread, then

$$\{(x, f(x) \ : \ x \in \mathbb{F}_{p^f}\} \subset \mathbb{F}_{p^f} \times \mathbb{F}_{p^f}$$

is a *difference set*: Every element not in $\{0\} \times \mathbb{F}_{p^f}$ has exactly $\lambda = 1$ difference representation.

Example

$$\{(0,0),(1,1),(2,1)\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3$$

There are many examples.

Why not $p = 2$?

$$x \mapsto f(x + a) - f(x)$$

cannot be bijective if $p = 2$.
But there are spreads and also vector spaces of invertible matrices.
Actually, there are many, many, more than for p odd (Kantor 2003)

Two important definitions

A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is planar (PN), if

$$x \mapsto f(x+a) - f(x)$$

is a permutation for all $a \neq 0$.

A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is almost perfect nonlinear (APN) if

$$x \mapsto f(x+a) - f(x)$$

is 2 to 1 for all $a \neq 0$ and q is even.

Monomial APN's x^d on $\mathbb{F}_{2^n}$

	d	Condition
Gold	$2^i + 1$	$\gcd(i, n) = 1$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$
inverse function	$2^{2t} - 2$	$n = 2t + 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

Some infinite families: $q = p^n$

Example (p odd)

x^{p^k+1} *is planar on* $\mathbb{F}_{p^n}$ *if* $n/\gcd(n,k)$ *is odd.*

Example ($p = 2$)

x^{2^k+1} *is APN on* $\mathbb{F}_{2^n}$ *if* $\gcd(n,k) = 1$.

Example ($p = 3$, Coulter, Matthews 1997; Ding,Yuan 2006)

$x^{10} \pm x^6 - x^2$ *is planar on* $\mathbb{F}_{3^n}$.

Example ($p = 2$, Budaghyan, Carlet, Leander 2009)

$x^3 + tr(x^9)$ *is APN on* $\mathbb{F}_{2^n}$.

Example ($p = 2$)

$x^{(-1)}$ *is APN on* $\mathbb{F}_2^n$ *if* n *is odd.*

quadratic vs. non-quadratic

f is called a Dembowski-Ostrom polynomial or quadratic if

$$f(x+a)-f(x)$$

is affine:

$$f(x)=\sum_{i,j,i\neq j}\alpha_{i,j}x^{p^i+p^j}+\sum_j\beta_j x^{pj}+\gamma.$$

Linear and constant terms are not important!

Until 2006, only few non-quadratic APN's were known, and only the classical quadratic monomials. This changed dramatically in 2006 Edel, P., Kyureghyan; Bierbrauer; Dillon, where many new **quadratic** APN's were constructed.

The quadratic case

Let $f(x) = \sum_{i,j} \alpha_{i,j} x^{p^i+p^j}$. This gives a vector space of bilinear forms $\mathbb{F}_{p^f} \times \mathbb{F}_{p^f} \to \mathbb{F}_p$:

$$(x, y) \mapsto f(x + y) - f(x) - f(y)$$

and apply projections onto $\mathbb{F}_p$.

Theorem

f quadratic and planar exists iff there is a vector space consisting of symmetric matrices of full rank.

Geometers call these *symplectic semifield spreads*.

The geometric approach

Geometers searched for these objects and found many, and even more if $p = 2$, but the matrices are not alternating, hence cannot be constructed from a function f.

Diagonal is needed to get a vector space of symmetric invertible matrices, in this way $\mathbb{Z}_4$ enters the arena.

Functions which describe these spreads satisfy

$$x \mapsto f(x + a) + f(x) + a \cdot x$$

are bijective. (Zhou 2013, also Horadam)

APN in terms of alternating matrices

Let's do almost the best and try to find a vector space of alternating matrices of large ranks: Then they can be constructed from a mapping f:

Theorem

f quadratic and APN iff there is a vector space of alternating matrices minimizing the sum of the $2^{\text{co-rank}}$.

Problem 1

Can we use this picture to construct more quadratic APN functions?

Yu, Wang, Li 2012/2014

Change some positions of the alternating matrices carefully. Yu, Wang, Li constructed many new quadratic APN functions for $n = 7, 8$.

Problem 2

Find families in this way!

Component functions

The vector space generated here is the vector space of all component functions of f.

Component functions

The vector space generated here is the vector space of all component functions of f.

Try to build an APN function from component functions. In the quadratic case: Use alternating matrices.

Component functions

The vector space generated here is the vector space of all component functions of f.

Try to build an APN function from component functions. In the quadratic case: Use alternating matrices.

Suggestion by Claude Carlet: Plateaued functions. They have the same Walsh spectrum as quadratic functions.

Component functions

The vector space generated here is the vector space of all component functions of f.

Try to build an APN function from component functions. In the quadratic case: Use alternating matrices.

Suggestion by Claude Carlet: Plateaued functions. They have the same Walsh spectrum as quadratic functions.

Important Remark: All infinite families of APN functions so far are constructed directly, given a polynomial, although in geometry it seems easier to construct spreads!

The "trans-characteristic" construction

There are quite a few infinite families of APN functions and of planar functions, sometimes with similar proofs in even and odd characteristic:
A very interesting example:

$$x^{2^s+1} + \alpha x^{2^k+2^{2k+s}}$$

is APN on $\mathbb{F}_{2^{3n}}$ Budaghyan, Carlet, Leander, Felke (2006) and

$$x^{p^s+1} + \alpha x^{p^k+2^{2k+s}}$$

is planar on $\mathbb{F}_{p^{3n}}$. Zha, Kyureghyan, Wang (2009)
α must be choosen properly.

Question

Problem 3

Is there perhaps a better understanding of this construction in terms of the component functions and their associated symmetric matrices (in the planar case) or alternating matrices (in the APN case).

An important result by Menichetti

Theorem

A planar function on $\mathbb{F}_{p^n}$ with n prime is equivalent to x^{p^i+1} if n is a prime and p sufficiently large.

The result by Zha, Kyureghyan, Wang shows that this cannot be true for composite (odd!) numbers. If n is even, it seems easier to find APN/PN functions using bivariate methods $\mathbb{F}_{q^2} = \mathbb{F}_q^2$ (APN: Carlet (2011); planar P. Zhou (2013)).

My favorite problem

Finding new examples of quadratic planar or APN functions seems to be less interesting now.

Problem 4

Show that

- *there is no polynomial g_p such that the number of (quadratic) planar or APN functions on $\mathbb{F}_p^n$ is smaller than $g_p(n)$ for all n.*
- *Show that the number of APN functions grows exponentially in n (no Menichetti bound).*

Construction method: Switching or Projection

Theorem (Budaghyan, Carlet, Leander (2009))

$$x^3 + tr(x^9)$$

is APN.

Theorem (Göloglu (2015))

$$x^{2^k+1} + [tr_m^n(x)]^{2^k+1}$$

is APN on $\mathbb{F}_{2^{2m}}$ *if* $\gcd k, 2m = 1$ *and* m *is even.*

The BIG open problem

Brwoning, Dillon, McQuistan, Wolfe (2009) found an APN permutation in $\mathbb{F}_{2^6}$. They used the APN $x \mapsto x^3 + x^{10} + \alpha x^{24}$.

Problem 5

Are there other examples of APN permutations in $\mathbb{F}_{2^n}$ if n is even? It is easy to find APN permutations if n is odd.

Recently, many constructions of "almost APN" permutations with n even (differentially 4-uniform) have been constructed.

Walsh spectrum

In the quadratic case, the ranks of $x \mapsto f(x+y) - f(x) - f(y)$ determine the Walsh spectrum of f. Which rank distributions are possible?

More generally (including non-quadratic case): Determine

$$\{* \sum_{x,y} (-1)^{\mathrm{tr}(\alpha x + \beta f(x))} : \alpha, \beta \in \mathbb{F}_{2^n}, \beta \neq 0 *\}.$$

Result

- *f quadratic and n odd: Walsh spectrum is known (almost bent functions).*
- *n even: Walsh spectrum is not known, even for quadratic APN.*

If n is even, only one quadratic APN is known with n even and not 5-valued spectrum.

Which Walsh spectra

Problem 6

Determine the possible Walsh spectra of APN functions

Composing two functions

Theorem (Weng, Zeng (2012))

If $\pi : \mathbb{F}_q \to \mathbb{F}_q$ is injective on squares and $\pi(0) = 0$, then $f(x) = \pi(x^2)$ is planar provided that it is Dembowski-Ostrom (quadratic).

Proof.

x^2 is planar, $\pi((x+a)^2) - \pi(x^2) = 0$ has at most one solution, which is sufficient since $\pi(x^2)$ is quadratic (which means $\pi((x+a)^2) - \pi(x^2)$ is affine). □

Example

$x^5 \pm x^3 - x$ is permutation on $\mathbb{F}_{3^n}$ if $n = 2$ or n odd. Hence $x^{10} \pm x^6 - x^2$ is planar.

The APN analogue, 2014

Theorem (Carlet, Gong, Tan (2015))

If $\pi : \mathbb{F}_q \to \mathbb{F}_q$ is injective on cubes and $\pi(0) = 0$, then $f(x) = \pi(x^3)$ is APN provided that it is Dembowski-Ostrom (quadratic).

Example

$x + tr(x^3)$ is permutation on $\mathbb{F}_{2^n}$ if n is even. Hence $x^3 + tr(x^9)$ is planar.

Problem 7

Exploit this: Composing permutation polynomial with x^2 or x^3.

One sporadic non-quadratic APN

Edel, P. 2009 found some u such that

$$x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \\ u^{14}(\mathrm{tr}(u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) + \\ \mathrm{tr}_2^8((u^2x)^9) + \mathrm{tr}_2^4(x^{21}))$$

in $\mathbb{F}_{2^6}$ is APN, where

$$x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24})$$

is APN (switching)

One family of non-quadratic planar functions

Theorem (Coulter, Matthews 1997)

In $\mathbb{F}_{3^n}$, the mapping

$$x^{(3^a+1)/2}$$

with $\gcd(a, n) = 1$, a odd, is planar.

Problem 8

Find more non-quadratic planar or APN mappings.