Partially almost perfect nonlinear permutations

Alexander Pott

Otto-von-Guericke-University Magdeburg

July 9, 2019

One example ...

$$F(x) = x^2$$

defined on $\mathbb{F}_q$ with q odd:

$$F(x+a) - F(x) = 2xa + a^2$$

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

Problem

Find functions F such that $F(x+a) - F(x)$ are permutations for all $a \neq 0$.

Not possible if q even: $F(x+a) + F(x) = F(y+a) + F(y)$ with $y = x + a$.

... one more example ...

$$F(x) = x^3$$

defined on $\mathbb{F}_q$ with q even:

$$F(x+a) + F(x) = x^2a + a^2x + a^3$$

is 2 to 1-mapping for all $a \neq 0$.

Problem

Find functions F on $\mathbb{F}_{2^n}$ such that $F(x+a) + F(x)$ are 2 to 1-mappings for all $a \neq 0$.

Note: Only additive properties are needed in the definition, but many constructions use multiplicative properties in $\mathbb{F}_{2^n}$ which realizes $\mathbb{F}_2^n$.

And now the important definition

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is almost perfect nonlinear (APN) if

$$x \mapsto F(x + a) + F(x)$$

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

Motivation: Codes

$$\begin{pmatrix} 1 \\ x \\ F(x) \end{pmatrix}_{x \in \mathbb{F}_2^n} \qquad \in \mathbb{F}_2^{(2n+1, 2^n)}$$

row space generates a code. The dual code has minimum weight 6:

$$F(a) + F(x+a) + F(y+a) + F(x+y+a) \neq 0$$

for all distinct a, x, y. This is optimal.

Motivation: Cryptography

An APN function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is highly nonlinear.

Such functions are used as S-boxes (substitution boxes) in many popular symmetric schemes:

- Data Encryption Standard
- Advanced encryption standard

See also the talk by Simona Samardjiska on friday.

Some infinite families

Example

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

Example (Budaghyan, Carlet, Leander 2009)

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

Example

x^{-1} is APN on $\mathbb{F}_{2^n}$ if n is odd.

quadratic vs. non-quadratic

F is called quadratic if

$$F(x+a)+F(x)$$

is affine. In Finite Fields version:

$$F(x)=\sum_{i<j}\alpha_{i,j}x^{2^i+2^j}+\sum_j\beta_j x^{2^j}+\gamma.$$

Linear and constant terms are not important for $F(x+a)+F(x)$.

Until 2006, only few families of non-quadratic APN monomials were known, and only the classical quadratic monomials x^{2^k+1}.

2006

This changed dramatically in 2006 (Edel, P., Kyureghyan; Bierbrauer; Dillon McQuistan, Wolfe), where several new **quadratic** APN's were constructed:

Example

- $x \mapsto x^3 + x^{10} + \alpha x^{24}$ on $\mathbb{F}_{2^6}$
- more on $\mathbb{F}_{2^6}$
- $x \mapsto x^3 + \beta x^{2^5+2^2}$ on $\mathbb{F}_{2^{10}}$
- $x \mapsto x^3 + \gamma x^{2^9+2^4}$ on $\mathbb{F}_{2^{12}}$

α, β, γ must be choosen properly.

My favorite problems

Many more quadratic families and sporadic examples have been found since 2006, but only one example of a non-quadratic with $n = 6$ (Edel, P. 2009).

Problem

Show that

- *Number of APN functions grows quickly.*
- *Non-quadratic examples?*
- *APN permutation if n is even.*

The BIG APN problem

Problem

Are there APN permutations if n is even?

- Would be useful for cryptographic applications.
- Easy to construct if n is odd.
- No quadratic APN permutations can exist if n is even.
- There is only one example if n is even known. This is equivalent to $x \mapsto x^3 + x^{10} + \alpha x^{24}$ on $\mathbb{F}_{2^6}$ (Browning, Dillon, McQuistan, Wolfe 2010), hence equivalent to quadratic.

Designs

STEINER triple systems:

- v points
- blocks of size 3
- Any two different points are contained in exactly one block.

Example (Classical)

Points and linear 2-dimensional subspaces (without 0) in $\mathbb{F}_2^n \setminus \{0\}$.

Designs

STEINER triple systems:

- v points
- blocks of size 3
- Any two different points are contained in exactly one block.

Example (Classical)

Points and linear 2-dimensional subspaces (without 0) in $\mathbb{F}_2^n \setminus \{0\}$.

STEINER quadruple systems:

- v points
- blocks of size 4
- Any three different points are contained in exactly one block.

Example (Classical)

Points and affine 2-dimensional subspaces in $\mathbb{F}_2^n$.

Rodier Condition

- $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN function if and only if

  $$F(x) + F(y) + F(z) + F(u) \neq 0$$

  for all subsets $\{x, y, z, u\}$ of order 4 with $x + y + z + u = 0$.
- Note that the subsets $\{x, y, z, u\}$ of order 4 with $x + y + z + u = 0$ form a Steiner quadruple system: Given any three different points x, y, z in $\mathbb{F}_2^n$, there is a unique 4-th point u such that $x + y + z + u = 0$.

APN permutations and Steiner quadrupel systems

Important Observation:

There is an APN permutation F iff there is a collection $\mathcal{D}$ of sets of size 4 on $\mathbb{F}_2^n$ forming a classical Steiner quadruple system such that none of the sets is an affine subspace of dimension 2.

$$\mathcal{D} = \Big\{ \{F(x), F(y), F(z), F(u)\} \, : \, x + y + z + u = 0 \Big\}.$$

- Are there APN permutations for other Steiner quadruple systems?
- Is there perhaps a design/loop theoretic approach to attack this problem for the classical Steiner quadruple system?

Partially APN functions

Budaghyan, Kaleyski, Kwon, Riera, Stănică (2019) studied functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that

$$F(x) + F(y) + F(x + y) \neq 0$$

for all $x, y \in \mathbb{F}_2^n$, $x \neq y$. That is the Rodier condition for $u = 0$. They called these partially APN.

- There are many more partially APN than APN.
- For quadratic functions: Partially APN if and only if APN.
- They found many partially APN permutations, but no infinite family.

Main Theorem

Theorem

For any $n \geq 3$ there are partially APN permutations on $\mathbb{F}_2^n$.

Proof:

- The blocks $\{x, y, x + y \ : \ x \neq y\}$ form a Steiner triple system on $\mathbb{F}_2^n \setminus \{0\}$ (any two different points are contained in exactly one triple).
- TEIRLINCK (1977) proved that any two Steiner triple systems $\mathcal{S}$ and $\mathcal{T}$ defined on a point set V have a disjoint realization (i.e. there is an isomorphic copy $\mathcal{T}'$ of $\mathcal{T}$ on V such that no triple occurs both in $\mathcal{S}$ and $\mathcal{T}'$).
- If we begin with $\mathcal{T} = \mathcal{S}$ above, this gives the desired permutation.

Comments

- TEIRLINCK's result has a short (1 page) and elementary but non-trivial proof.
- TEIRLINCK's result is needed only for one triple system, the classical one defined on $\mathbb{F}_2^n \setminus \{0\}$.
- We tried to extend this to quadruple systems, but could not succeed.
- TEIRLINCK's result is not constructive.

Summary

- Almost perfect nonlinear functions.
- BIG problem: APN permutations with $n \geq 6$.
- Translation into a much more general problem for Steiner quadruple systems (disjoint?).
- Non-constructive proof for the existence of permutation partially APN for all n.
- TEIRLINCK for the classical APN permutation is equivalent to the BIG APN problem.

Bent functions and Steiner triple systems

A bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ maximizes the number of quadruples in the classical Steiner quadruple system with $f(x) + f(y) + f(z) + f(u) = 1$.

- Other quadruple systems?
- For Steiner triple systems, this question is trivial ($f = 1$), but perhaps non-trivial for balanced functions.
- Difference between classical and non-classical Steiner systems?