Relative Difference Sets from Almost Perfect Nonlinear Functions

Zeying Wang

Department of Mathematical and Statistics
American University

Irsee, Sept. 2025

Relative Difference Sets

Let G be a finite group of order mn containing a normal subgroup N. A subset R of G is called a *relative (m, n, k, λ)-difference set* if the following holds:

- $|G| = mn$, $|N| = n$.
- $|R| = k$.
- The list of differences $r - r'$ with $r, r' \in R$ and $r \neq r'$ covers every element in $G \setminus N$ exactly λ times and no element in $N \setminus \{0\}$ is covered.

Examples of Relative Difference Sets:

If $n = 1$, this is the usual definition of a difference set (each nonidentity element has the same number of representations $r - r'$).

$\{1, 2, 4\}$ is a (7, 1, 3, 1)-difference set in $\mathbb{Z}_7$.

$\{(0,0),\ (1,1),\ (1,2),\ (1,3)\} \in \mathbb{Z}_2 \times \mathbb{Z}_4$ is a (4, 2, 4, 2)-difference set relative to $\mathbb{Z}_2 \times \{0\}$.

The relative difference set is called *splitting* if $G = K \times N$, that is, if N has a complement in G. If $k = m$ the relative difference set is called *semiregular*.

Almost perfect nonlinear (APN) functions

Let p be a prime and $q = p^n$, and f be a map from $\mathbb{F}_q$ to $\mathbb{F}_q$. For any a, $b \in \mathbb{F}_q$, let

$$\delta_f(a, b) := |\{x \in \mathbb{F}_q \ : \ f(x + a) - f(x) = b\}|.$$

If $\delta_f(a, b) \leq d$ for all $a \neq 0$ and $b \in \mathbb{F}_q$, then f is called a differentially d-uniform (abbreviated d-uniform).

A 1-uniform map $f : \mathbb{F}_q \to \mathbb{F}_q$ is called planar, that is, f is planar if $f(x + a) - f(x)$ is a permutation for any $a \in \mathbb{F}_q^*$. Planar maps exists if and only if q is odd.

A map f is called *almost perfect nonlinear (APN)* if f is 2-uniform. that is, if for every $a \neq 0$ and every $b \in \mathbb{F}$, the equation

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

admits at most 2 solutions.

When q is even, the equation $f(x+a) + f(x) = b$ has always an even number of solutions, since if x is a solution, then $x+a$ is also a solution.

In particular, there are no 1-uniform maps for q even, and the APN maps have the smallest possible uniformity on binary fields.

APN functions on a finite field of characteristic 2 were introduced by K. Nyberg in 1993 and have been widely studied.

APN maps and more generally maps in characteristic 2 with low uniformity are an important research object in cryptography, mainly because they provide good resistance to differential attacks, when used as an S(Substitution)-box of a block cipher.

Examples of APN functions:

Some monomial APN functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$:

- Gold function: x^d, where $d = 2^i + 1$, and $\gcd(i, n) = 1$, $1 \leq i \leq \frac{n-1}{2}$.
- Kasami function: x^d, where $d = 2^{2i} - 2^i + 1$, and $\gcd(i, n) = 1$, $1 \leq i \leq \frac{n-1}{2}$.
- Welch function: x^d, where $d = 2^k + 3$, and $n = 2k + 1$.

Some APN functions which are not monomials:

- the function $x^3 + Tr(x^9)$ is APN on $\mathbb{F}_{2^n}$ for any n.
- If $n = 2m$, m is even and $\gcd(n, i) = 1$, then $x^{2^i+1} + (x + x^{2^m})^{2^i+1}$ is APN on $\mathbb{F}_{2^n}$.

A family of APN functions

In 2009, *L. Budaghyan, C. Carlet, G. Leander* proved that

Theorem

Let n be a positive integer and $a \in \mathbb{F}_{2^n}^*$. Then the function $x^3 + a^{-1}Tr(a^3x^9)$ is APN over $\mathbb{F}_{2^n}$. Here $Tr(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$.

In 2023, Kolsch, Kriepke, and Kyureghyan in [3] proved that

Theorem

Let n be odd and $a \in \mathbb{F}_{2^n}$ non-zero. Then the APN map $x \to x^3 + a^{-1}Tr(a^3x^9)$ is 2-to-1.

Main Result:

Theorem (Z. Wang, 2025)

Let $n = 2k + 1$ be odd and $a \in \mathbb{F}_{2^n}$ non-zero. Then the image of the APN map $x \to x^3 + a^{-1}Tr(a^3x^9)$ is a $(2^{2k}, 2, 2^{2k}, 2^{2k-1})$-relative difference set in $(\mathbb{F}_{2^n}, +)$ relative to the subgroup $N = \{a^{-1}, 0\}$.

Rough Sketch of the Proof:

Let $D = \{x^3 + a^{-1}\,Tr(a^3x^9), x \in \mathbb{F}_{2^n}\}$.
Step 1:. Show that a^{-1} cannot be represented by any differences $x_1 - y_1$, where x_1, $y_1 \in D$.
Step 2: Count the number of pairs (x, y) which satisfy the equation

$$x^3 + a^{-1}\,Tr(a^3x^9) - (y^3 + a^{-1}\,Tr(a^3y^9)) = b$$

We can show there are $2^n = 2^{2k+1}$ solutions to the above equation. This relies on the fact that x^3 is a permutation in $\mathbb{F}_{2^n}$ when n is odd. According to the result in [3], the APN map is 2-to-1, thus there are $2^n/4 = 2^{2k+1-2} = 2^{2k-1}$ difference representations of b with $b = x_1 - y_1$, $x_1 \neq y_1$, and x_1, $y_1 \in D$ whenever $b \neq a^{-1}$.

Current and Future Work

Besides the above mentioned APN functions, there are more APN functions which are also 2-to-1 functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$.

Question: For any given 2-to-1 APN function in $\mathbb{F}_q$, where $q = 2^{2k+1}$, is it true that the image set D is always a $(2^{2k}, 2, 2^{2k}, 2^{2k-1})$-relative difference set?

Comment: In the case I have proved, the proof is dependent on the format of the function, not just on the fact that the function is a 2-to-1 APN function.

In 2004, A. Pott [1] proved the following theorem

Theorem

Let K and N be arbitrary finite groups and $f: K \to N$, the set

$$R := \{(g, f(g)) : g \in K\} \subset K \times N$$

is a semiregular splitting $(|K|, |N|, |K|, |K|/|N|)$-difference set in $K \times N$ relative to $\{1\} \times N$ if and only if f is perfect nonlinear.

In my result, the image D of the APN map $x \to x^3 + a^{-1}Tr(a^3x^9)$ is a $(2^{2k}, 2, 2^{2k}, 2^{2k-1})$-relative difference set in $(\mathbb{F}_{2^n}, +)$ relative to the subgroup $N = \{a^{-1}, 0\}$, which is a semiregular splitting difference set satisfying the condition in the above result. Thus there is a perfect nonlinear function f corresponding to it.

Question: Can we give a detailed description of the corresponding perfect nonlinear function f?

References:

- **Nonlinear functions in abelian groups and relative difference sets**, Alexander Pott, Discrete Applied Mathematics, 138 (2004), 177-193.
- **On a construction of quadratic APN functions**, Lilya Budaghyan, Claude Carlet, and Gregor Leander, 2009 IEEE Information Theory Workshop.
- **Image Sets of Perfectly nonlinear maps**, Lukas Kolsch, Bjorn Kriepke, Gohar M. Kyureghyan, Designs, Codes and Cryptography (2023), 91: 1-27.
- **Relative difference sets from almost perfect nonlinear functions**, Zeying Wang, manuscript.

THANKS!