The linear spectrum of a quadratic APN function and related open problems

Anastasiya Gorodilova
Sobolev Institute of Mathematics SB RAS, Novosibirsk, Russia
gorodilova@math.nsc.ru

A Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be uniquely represented in *algebraic normal form* (ANF) as a n-variable polynomial with coefficients in $\mathbb{F}_2^n$. The *algebraic degree* of F is degree of its ANF. A function F is *affine* (*linear*) if its algebraic degree is not more than 1 (additionally, $F(\mathbf{0}) = \mathbf{0}$); and *quadratic* if its algebraic degree is equal to 2. F and F' are called *extended affine equivalent* (EA-equivalent) if $F' = A' \circ F \circ A'' + A$, where A', A'' are affine permutations of $\mathbb{F}_2^n$ and A is an affine function on $\mathbb{F}_2^n$.

A function F is called *almost perfect nonlinear* (APN) if for any $a, b \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$, equation $F(x)+F(x+a) = b$ has at most 2 solutions. Equivalently, F is APN if $|B_a(F)| = |\{F(x) + F(x+a) \mid x \in \mathbb{F}_2^n\}| = 2^{n-1}$ for any nonzero vector a. APN functions are of a great interest for using in cryptographic applications as S-boxes due to their optimal differential properties. Despite the fact that this class has been intensively studied for about half a century there are many open problems concerning APN functions.

Further we consider only quadratic APN functions. In this case $B_a(F)$ is an affine hyperplane for all nonzero $a \in \mathbb{F}_2^n$ and $B_a(F + L) = B_a(F)$ or $B_a(F + L) = \mathbb{F}_2^n \setminus B_a(F)$, where F is a quadratic APN function and L is a linear function. Let us denote by $k_L^F = |\{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\} : \ B_a(F) = B_a(F + L)\}|$. By the *linear spectrum* of F we will mean the vector of values $\Lambda^F = (\lambda_0^F, \ldots, \lambda_{2^n-1}^F)$, where λ_k^F is equal to the number of linear functions L such that $k_L^F = k$. It is easy to see that $\sum_{k=0}^{2^n-1} \lambda_k^F = 2^{n^2}$.

Statement 1. *The linear spectrum of a quadratic APN function is a EA-invariant.*

Statement 2. *Let F be a quadratic APN function in n variables, n is even. Then the following statements hold: 1) $\lambda_k^F = 0$ for all even $k = 0, \ldots, 2^n - 1$ and also for all odd $k < (2^n - 1)/3$; 2) $\lambda_{2^n-1}^F \geqslant 2^n$.*

Hypothesis. *Let F be a quadratic APN function in n variables, n is odd. Then the following statements hold: 1) $\lambda_k^F = 0$ for all even $k = 0, \ldots, 2^n - 1$ and also for all odd $k < (2^{n-1} - 1)/3$; 2) $\lambda_{2^n-1}^F = 2^n$.*

This hypothesis is computationally proved for $n = 3, 5$; the second item is also verified for all known quadratic APN functions in 7 variables.

Let us consider two open problems related to the linear spectrum of a quadratic APN function. The first one consists in obtaining an iterative construction of quadratic APN functions mentioned in [1]. For this construction, given a quadratic APN function F in n variables, we need to find a linear function L such that the special admissibility conditions hold for F and L. It can be shown that if $k_L^F > 2^{n-1}$, then these conditions do not hold. The questions arise: what is the minimal k, say k_{min}, such that $\lambda_k^F > 0$ and does there always exist a linear function L with $k_L^F = k_{min}$ such that the admissibility conditions hold?

The second problem consists in finding $\lambda_{2^n-1}^F$ for an arbitrary quadratic APN function F. An answer to this problem will be the first step in solving the wider open problem formulated in [2] by C. Carlet but that was in minds of many specialists. The problem is to describe all APN functions G for a given APN function F such that $B_a(F) = B_a(G)$ for all $a \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$. We prove the following theorem for one known class of quadratic APN functions.

Theorem. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a Gold function $F(x) = x^{2^k+1}$, where $gcd(k, n) = 1$. Then the following statements hold: 1) if $n = 4t$ for some t and $k = n/2 \pm 1$, then $\lambda_{2^n-1}^F = 2^{n+n/2}$; 2) otherwise $\lambda_{2^n-1}^F = 2^n$.*

The research is supported by the Russian Foundation for Basic Research (project no. 15-31-20635).

References

[1] A. Gorodilova, A characterization of almost perfect nonlinear functions in terms of subfunctions. *Diskretnaya Matematika* **27(3)** (2015) 3–16 (in Russian).

[2] C. Carlet, Open Questions on Nonlinearity and on APN Functions. *Arithmetic of Finite Fields, Lecture Notes in Computer Science* **9061** (2015) 83–107.