Relaxations of almost perfect nonlinearity

Alexander Pott

A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if $f(x+a)+f(x)=b$ for all a, b has at most 2 solutions. One may also formulate this as follows: there is no 4-set $\{x, y, z, w\} \in \mathbb{F}_2^n$ such that

$$f(x) + f(y) + f(z) + f(w) = 0 \tag{1}$$

which is sometimes called the Rodier condition.

Several relaxations of APN functions have been introduced: a function f is called partially APN [1] if $f(y) + f(z) + f(y+z) \neq 0$ for all $y, z \neq 0$, $y \neq z$. That means that the APN property 1 is satisfied for $x = 0$ only. Another popular relaxation are differentially 4-uniform functions where $f(x+a) + f(x) = b$ has at most 4 solutions.

In my talk, I will discuss the question about the number of 4-sets $\{x, y, z, w\} \in \mathbb{F}_2^n$ such that $f(x)+f(y)+f(z)+f(w) = 0$ for certain functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ where $m \leq n$ [3, 2].

This gives rise to a design theoretic interpretation of the APN property and can be used to show, in a purely combinatorial way, that partially APN permutations exist for all n, thanks to [4].

References

[1] Lilya Budaghyan, Nikolay S. Kaleyski, Nikolay S, Soonhak Kwon, Constanza Riera and Pantelimon Stanica, *Partially APN Boolean functions and classes of functions that are not APN infinitely often*. Cryptography and Communications **12** (2020), 1159–1177.

[2] Shuxing Li, Wilfried Meidl, Alexandr Polujan, Alexander Pott,, Constanza Riera and Pantelimon Stănică, *Vanishing flats: a combinatorial viewpoint on the planarity of functions and their application*. IEEE-IT **66** (2020), 7101–7112.

[3] Wilfried Meidl, Alexandr Polujan and Alexander Pott, *Linear codes and incidence structures of bent functions and their generalizations*, arXiv:2012.06866v1.

[4] Luc Teirlinck, *On Making Two Steiner Systems Disjoint*. Journal of Combinatorial Theory A **23** (1977), 349–350.