Geometrical and combinatorial aspects of APN functions

Yves Edel
Department of Pure Mathematics and Computer Algebra
Ghent University
Krijgslaan 281, S22, B-9000 Ghent, Belgium

Motivated by applications in cryptography, a lot of research has been done to construct vectorial boolean functions functions which are "as nonlinear as possible" (see e.g. [1, 2]). One class of such functions are *almost perfect nonlinear (APN)* functions.

Definition 1. *A function* $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *is called* APN *if and only if for all* $a \in \mathbb{F}_2^n \setminus \{0\}$ *and* $b \in \mathbb{F}_2^n$ *the equation* $f(x+a) + f(x) = b$ *has at most two solutions.*

APN functions have links to other mathematical objects. An APN function is equivalent to a binary error correcting $[2^n, 2^n - 2n - 1, 6]_2$ code, which is contained in the dual of the first order Reed-Muller code. Quadratic APN functions are equivalent to a certain subclass of dual hyperovals in the projective geometry [3]. Also there are several ways to construct semibiplanes from APN functions.

In this talk we will present these links in more detail.

References

[1] C. Carlet, Vectorial Boolean functions for cryptography, chapter of the monography "Boolean Methods and Models", Y. Crama and P. Hammer eds., Cambridge University Press, to appear.

[2] Y. Edel and A. Pott, "A new almost perfect nonlinear function which is not quadratic," *Advances in Mathematics of Communications*, vol. 3, no. 1, pp. 59–81, 2009.

[3] Y. Edel, "On quadratic APN functions and dimensional dual hyperovals," *Designs, Codes and Cryptography*, submitted.