UNIVERSITÄT SALZBURG

Fachbereich Mathematik
Hellbrunnerstraße 34
5020 Salzburg

Gastvortrag

Montag, 29. Mai 2017
13 Uhr c.t.
Seminarraum II

Dr. Wilfried Meidl
RICAM Linz

Bent, generalized bent, and shifted bent functions

Abstract:

A bent function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ or more general from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$ is a function for which the Walsh transform

$$\mathcal{W}_f(a,b) = \sum_{x\in\mathbb{F}_2^n} \varsigma_p^{b\cdot f(x)+u\cdot x}, \quad \varsigma_p = e^{2\pi i/p},$$

has absolute value $p^{n/2}$ for all nonzero $b \in \mathbb{F}_p^m$ and $a \in \mathbb{F}_p^n$. Alternatively, f is bent if and only if $f(x+a)-f(x)$ is balanced for every nonzero $a \in \mathbb{F}_p^n$. In the first part, properties of bent functions and their relations to combinatorics, finite geometry, cryptography are recalled.
The second part is about two generalizations. The first are bent functions f from $\mathbb{F}_2^n$ to the cyclic group $\mathbb{Z}_{2^k}$, which are functions for which

$$\mathcal{H}_f(\alpha,u) = \sum_{x\in\mathbb{F}_2^n} \varsigma_{2^k}^{\alpha\cdot f(x)} (-1)^{u\cdot x}, \quad \varsigma_{2^k} = e^{2\pi i/2^k},$$

has absolute value $2^{n/2}$ for all nonzero $\alpha \in \mathbb{Z}_{2^k}$ and $u \in \mathbb{F}_{2^n}$, and functions with the weaker condition that $\left|\mathcal{H}_f(\alpha,u)\right| = 2^{n/2}$ for $\alpha = 1$ and all $u \in \mathbb{F}_2^n$. The latter are called generalized bent (gbent), and have been introduced motivated by applications in CDMA systems (for $k = 2$). In joint work with Hodzic and Pasalic we completely characterized gbent functions as affine spaces of bent or semibent functions with certain additional properties. This is a crucial step towards a possible classification of gbent functions.
A generalization of a different type, given in the framework of finite fields, is obtained if one requires that $f(a+x)+f(x)+\mathrm{Tr}(cax)$ is balanced for a function $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$. For $c=0$ such a function is bent, for $c=1$ it is called a univariate negabent function. In joint work with N. Anbar we described these functions with character sums over certain groups, and described their connections with relative difference sets, the recently introduced modified planar functions which induce projective (semifield) planes.

Einladender: Peter Hellekalek