The Equivalence Problem for Functions $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Alexander Pott

Institute for Algebra and Geometry, Faculty of Mathematics, Otto-von-Guericke-University Magdeburg, D-39016 Magdeburg, Germany

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function. Motivated by many applications, the following numbers are of interest, which measure the differential and the linear properties of F: The numbers

$$\delta_F(a,b) := \sharp\{x \in \mathbb{F}_{p^n} \ : \ F(x+a) - F(x) = b\}$$

measure the differential properties, and the numbers

$$\mathcal{W}_F(a,b) := \sum_{x \in \mathbb{F}_{p^n}, y \in \mathbb{F}_{p^m}} \zeta_p^{trace(ax+bF(x))}$$

describe the nonlinearity properties of F. The goal is that the maximum of all $\delta_F(a,b)$ $(a \neq 0)$ is small, and that the maximum of the $|\mathcal{W}_F(a,b)|$ is small $(b \neq 0)$.

Functions where these maxima are small include the important classes of bent functions (both p odd and $p = 2$), and perfect nonlinear (for p odd), almost perfect nonlinear as well as almost bent functions (for $p = 2$).

Definition 1. *A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is* **bent** *if $\delta_F(a,b) = p^{n-m}$ for all $a \neq 0$. Bent functions with $n = m$ are called* **perfect nonlinear** *or* **planar**. *If $n = m$, $p = 2$ and $\delta_F(a,b) \in \{0,2\}$ for all $a \neq 0$, then F is called* **almost perfect nonlinear**.

There are several concepts of equivalence for functions F. We identify $\mathbb{F}_{p^n}$ with the vector space $\mathbb{F}_p^n$, and we define the **graph** G_F of F:

$$\{(x, F(x)) \ : \ x \in \mathbb{F}_p^n\} \subseteq \mathbb{F}_p^{n+m}.$$

Definition 2. *Two functions $F_1, F_2 : \mathbb{F}_p^n \to \mathbb{F}_p^m$ are called* **affine equivalent** *if there are linear permutations P and Q and an affine mapping L such that $F_1 = P \circ F_2 \circ Q + L$. The functions are called* **graph (or CCZ) equivalent** *if there is a linear permutation $H : \mathbb{F}_p^{n+m} \to \mathbb{F}_p^{n+m}$ such that $H(G_{F_1}) = G_{F_2} + v$ for some $v \in \mathbb{F}_p^{n+m}$, where $G_F + v := \{(x+a, F(x)+b) \ : \ x \in \mathbb{F}_p^n\}$, $v = (a,b)$.*

Any function defines a **design**, which is an incidence structure consisting of points and blocks (whcih are subsets of points): The points are the elements in $\mathbb{F}_p^{n+m}$, the lines are the "translates" $G_F + v$.

Definition 3. *Two functions F_1 and F_2 are called* **isomorphic** *if the corresponding designs are isomorphic.*

In general. isomorphism is an equivalence relation which is coarser than graph equivalence which is coarser than extended affine equivalence. However, in some cases the concepts coincide. I my talk, I will discuss relations between these concepts of equivalence for various classes of functions.

It may be possible to define even more general equivalence relations. There is a well known object ("Knuth cube") studied in connection with perfect nonlinear functions. I will discuss possible extensions of this concept to the almost perfect nonlinear case, which is related to the work of Taniguchi.

Another possible extension is the "switching equivalence" introduced by Edel and Pott.

The introduction of new concepts of equivalence is not just of academic interest in order to combine equivalence classes with respect to graph or extended affine equivalence. We may actually use them to construct new examples.

Part of the talk is based on joint work with my student Yue Zhou.