Kloosterman Zeros and Vectorial Bent Functions

Petr Lisoněk
Simon Fraser University, Burnaby, BC, Canada
plisonek@sfu.ca

Abstract

The Kloosterman sum is the mapping $\mathcal{K} : \mathbb{F}_{2^m} \to \mathbb{Z}$ defined by $\mathcal{K}(a) = 1 + \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}(x^{-1}+ax)}$. An a such that $\mathcal{K}(a) = 0$ is called a Kloosterman zero. Dillon proved that the function $f : \mathbb{F}_{2^{2m}} \to \mathbb{F}_2$ given by $f(x) = \mathrm{Tr}(ax^{2^m-1})$ is (hyper-)bent if and only if $\mathcal{K}(a) = 0$. We use the connection between Kloosterman sums and elliptic curves due to Lachaud and Wolfmann to develop an algorithm for listing of all Kloosteran zeros in a given field. Previously in the literature Kloosterman zeros were exhaustively listed only for fields of orders up to 2^{14}. With our new method we are able to list all Kloosterman zeros in all binary fields of order up to 2^{63} in a few days of CPU time. We make some observations based on our computational results. In particular we note that most binary fields on which we performed computations contain many triples $\{a, b, c\}$ of Kloosterman zeros such that $a+b = c$. This gives rise to a new class of vectorial bent functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_4$.

In the second part of the talk we prove new non-existence results for vectorial monomial Dillon type bent functions mapping the field of order 2^{2m} to the field of order $2^{m/3}$. When m is odd and $m > 3$ we show that there are no such functions. When m is even we derive a condition for the bent coefficient. The latter result allows us to find examples of bent functions with $m = 6$ in a simple way. These results are proved using new techniques that are based on divisibility of Kloosterman sums by powers of 2 and they use higher order trace functions. We discuss further possible applications of these new techniques.