# DISTINCTNESS OF THE "LIFTED" KLOOSTERMAN SUMS OVER THE PRIME FIELD $\mathbb{F}_p$

LYUBOMIR BORISSOV

ABSTRACT. In this talk I consider the Kloosterman sums over the finite field $\mathbb{F}_q$ of characteristic $p$, defined by

$$\mathcal{K}_q(u) = \sum_{x\in\mathbb{F}_q^*} \omega^{\,Tr(x+ux^{-1})},$$

where $\omega = e^{\frac{2\pi i}{p}}$ is a primitive $p-$th root of unity, and $Tr(a)$ is the absolute trace of $a \in \mathbb{F}_q$ over $\mathbb{F}_p$.

The focus of special attention are the so-called "lifted" Kloosterman sums over $\mathbb{F}_q$ (see, [1]), i.e., $\mathcal{K}_{q^n}(u), u \in \mathbb{F}_q$, where $\mathbb{F}_{q^n}$ is the finite field of order $q^n, n > 1$.

It is well-known that the Kloosterman sums play an important role in algebraic coding theory and cryptography (see, e.g., the surveys [2]-[3]).

Firstly I clashed with them in the problem of enumerating the elements of a finite field having prescribed trace and co-trace:

https://arxiv.org/pdf/1711.08306.pdf

The issue of their distinctness is considered and partly solved for the first time by Benjamin Fisher in 1992 [4]. In particular, this author has proved that fact for the simplest sums, i.e., over the prime fields.

Recently, in a personal communication with us, Daqing Wan has announced that as a co-product of his research [5] (based on deep algebraic number theory such as Stickelberger's theorem) it follows the distinctness of "lifted" Kloosterman sums over any prime field $\mathbb{F}_p$ whenever the extension degree is not a multiple of $p$. This statement generalizes our result for the fields whose extension degree is a power of 2:

https://link.springer.com/article/10.1007/s12095-020-00443-1

Here I am giving a proof for the distinctness of the "lifted" Kloosterman sums over $\mathbb{F}_3$ for any degree of extension thus improving Wan's result in case $p = 3$.

I believe that (jointly with Y. Borissov), we have found a proof that all "lifted" Kloosterman sums over each prime field of characteristic $\geq 3$ and any extension degree, are distinct. In the final slides I present some arguments concerning this fact which is to be elaborated in a future work.

## REFERENCES

[1] L. Carlitz, "Kloosterman sums and finite field extensions", Acta Arithmetika vol. XVI.2 (1969), pp. 179-193.
[2] N. E. Hurt, "Exponential sums and coding theory: a review", Acta Appl. Math., vol. 46.1 (1997), pp. 49-91.
[3] V. A. Zinoviev, "On classical Kloosterman sums", Cryptogr. and Commun., 11.3 (2019), pp. 461-496.
[4] B. Fischer, "Distinctness of Kloosterman sums", Contemporary Mathematics, vol. 133 (1992), pp. 81-102.
[5] D. Wan, "Minimal polynomials and distinctness of Kloosterman sums", Finite Fields Appl., 1 (1995), pp. 189-203.

INSTITUTE OF MATHEMATICS AND INFORMATICS, BULGARIAN ACADEMY OF SCIENCES, SOFIA, BULGARIA