On the Distinctness of Some Kloosterman Sums

Yuri Borissov[1]

Dedicated to Prof. Claude Carlet's 70^{th} Birthday

Abstract

Let $\mathbb{F}_q$ be the finite field with odd characteristic p of order $q = p^m, m \geq 1$; $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, Tr be the absolute trace function over $\mathbb{F}_q$ and $a \in \mathbb{F}_q$. The Kloosterman sum $K_q(a)$ is defined as follows

Definition: (see, e.g. [1])

$$K_q(a) = \sum_{x \in \mathbb{F}_q^*} \omega^{\ Tr(x + \frac{a}{x})}, \tag{1}$$

where $\omega = e^{\frac{2\pi i}{p}}$ is a complex primitive $p-$th root of unity.

Let us notice that some authors do prefer a slightly different definition, i.e. they add a 1 to $K_q(a)$ to extend in some sense that sum over the whole $\mathbb{F}_q$ and study its zeros (see, e.g. [2], [3]). Throughout this work the classical definition (1) will be utilized. The lifted Kloosterman sum $K_{q^l}(a)$ over an extension $\mathbb{F}_{q^l}, l > 1$ is defined in obvious way.

In general, the Kloosterman sums $K_q(a), a \in \mathbb{F}_q^*$ tend to be distinct with sufficiently large p (of course, up to the action of the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ generated by the Frobenius automorphism), i.e. $K_q(a) = K_q(b)$ if and only if $b = a^{p^s}$ for some s. For instance, in [4] it has been proved that this holds true for the finite fields obeying $p > (2.4^m + 1)^2$. Indeed, the referee of [4] has conjectured that $p^m - 1$ Kloosterman sums of interest are distinct up to the action of corresponding group if $p \geq 2m$ (a weaker version of this conjecture was proved in [5]). However, as far as we know, there aren't definite results about the distinctness of these sums when p is small compared with m and a varies over a subfield. In the light of foregoing, the present work seems to be of some interest.

First, based on the fact that the minimal polynomial of ω over $\mathbb{Q}$ is $1 + y + y^2 + \ldots + y^{p-1}$, we prove the following:

PROPOSITION 1: For each pair $a, b \in \mathbb{F}_q$ it holds $K_q(a) \neq -K_q(b)$.

We also make use of the Carlitz lifting formula [1, Eq. 1.4] for degree of extension 2, stated by the next lemma.

LEMMA 2: If $a \in \mathbb{F}_q^*$ then it holds $K_{q^2}(a) = 2q - K_q^2(a)$.

Lemma 2 and Proposition 1 immediately imply the following corollary.

COROLLARY 3: For each pair $a, b \in \mathbb{F}_q^*$, the relation $K_{q^2}(a) = K_{q^2}(b)$ holds if and only if $K_q(a) = K_q(b)$.

The main result of that work is formulated by the next theorem.

Theorem: For every $n \geq 0$, the $(p-1)$ Kloosterman sums $K_{p^{2^n}}(a), a \in \mathbb{F}_p^*$ are distinct.

The proof is carried out by induction on n with basis the property of distinctness of the sums $K_p(a), a \in \mathbb{F}_p^*$ (see, [4, p. 83]) while the induction step makes use of Corollary 3.

Finally, based on the known facts that $K_q(0) = -1$ for any q and the non-existence of zeros of the extended Kloosterman sum when $p > 3$ [6], we deduce the following corollary.

COROLLARY 4: For every $n \geq 0$, the p Kloosterman sums $K_{p^{2^n}}(a)$ obtained when a varies over the prime subfield $\mathbb{F}_p, p > 3$, are distinct.

Acknowledgments. The author is grateful to Victor Zinoviev for suggesting this research problem.

REFERENCES

[1] L. Carlitz, "Kloosterman sums and finite field extensions", *Acta Arithmetica*, vol.XVI.2: 179-193, 1969.

[2] L.A. Bassalygo and V.A. Zinoviev, "On Kloosterman sums over finite fields of characteristic 3", *Discrete Applied Mathematics*, vol. 216: 518-523, 2017.

[3] P. Lisonek and M. Moisio, "On zeros of Kloosterman sums", *Designs, Codes and Cryptography*, vol. 59 #3: 223-230, 2011.

[4] B. Fischer, "Distinctness of Kloosterman sums", in *Contemporary Mathematics: p-adic Methods in Number Theory and Algebraic Geometry*, American Mathematical Society, 81-102, 1992.

[5] D. Wan, "Minimal polynomials and distinctness of Kloosterman sums", *Finite Fields Appl.* vol. 1: 189-203, 1995.

[6] K.P. Kononen, M. Rinta-aho, K. Väänänen, "On integer values of Kloosterman sums", *IEEE Transactions on Inform. Theory*, vol. 57(3): 4011-4013, 2010.

[1] The author is from the Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria.