On the Distinctness of Some Kloosterman Sums

Yuri Borissov

Institute of Mathematics and Informatics, BAS, Bulgaria

BFA-2019 Florence, Italy
16.06 – 21.06 2019
Outline

- Definitions and Notations
- Introduction and Motivation
- Some Necessary Facts
- Results and Sketch of Proofs
Let $\mathbb{F}_q$ be the finite field of characteristic $p$ and order $q = p^m$.

**Definition 1.**

The absolute \textit{trace} of an element $\gamma$ in $\mathbb{F}_q$ is defined by

$$Tr(\gamma) = \gamma + \gamma^p + \ldots + \gamma^{p^{m-1}}$$

The range of trace function coincides with the prime field $\mathbb{F}_p$, and the number of elements with fixed trace equals $p^{m-1}$. 
Let, as usual, \( \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} \).

**Definition 2.** For each \( u \in \mathbb{F}_q \), the **Kloosterman sum** \( \mathcal{K}_q(u) \) is defined by

\[
\mathcal{K}_q(u) = \sum_{x \in \mathbb{F}_q^*} \omega \text{Tr}(x + \frac{u}{x}),
\]

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

In particular, evidently \( \mathcal{K}_q(0) = -1 \) for any \( q \).
Definitions and Notations (2)

Let, as usual, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

**Definition 2.**
For each $u \in \mathbb{F}_q$, the **Kloosterman sum** $\mathcal{K}_q(u)$ is defined by

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

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

In particular, evidently $\mathcal{K}_q(0) = -1$ for any $q$.

The Kloosterman sum $\mathcal{K}_{q^n}(u), u \in \mathbb{F}_q$ where $\mathbb{F}_{q^n}$ is the finite field of order $q^n, n > 1$, will be referred as a lifted.
Some authors (see, e.g. [Shparl09], [LisMoi11]) do prefer a slightly different definition, i.e. they extend in some sense the sum over the whole $\mathbb{F}_q$ considering $1 + \mathcal{K}_q(u) = \mathcal{K}_q^*(u)$ and study the zeros of latter called Kloosterman zeros;
Some authors (see, e.g. [Shparl09], [LisMoi11]) do prefer a slightly different definition, i.e. they extend in some sense the sum over the whole $\mathbb{F}_q$ considering $1 + K_q(u) = K^*_q(u)$ and study the zeros of latter called Kloosterman zeros;

These studies are partly motivated by the connection of Kloosterman zeros with a certain type of monomial bent functions characterized (in the binary case) by Dillon. (see, e.g. [HelKho06], [KonRinVää10], etc.)
What is basically known in respect of the distinctness of Kloosterman sums? (see, e.g., the survey [Zinoviev19])

- B. Fischer has proved that the sums $K_p(u), u \in \mathbb{F}_p^*$ are distinct [Fischer92];
What is basically known in respect of the distinctness of Kloosterman sums? (see, e.g., the survey [Zinoviev19])

- B. Fischer has proved that the sums $K_p(u), u \in \mathbb{F}_p^*$ are distinct [Fischer92];

- Tend to be distinct for $p$ sufficiently larger than $m$:
  - also, in [Fischer92], it has been proved: $K_q(a) = K_q(b)$ iff $b = a^{p^s}$ for some $s$ when $p > (2.4^m + 1)^2$;
  - indeed, the referee of Fischer’s work has conjectured that holds true for $p \geq 2m$. A weaker version of this conjecture (for $p$ obeying certain additional conditions) was proved in [Wan95].
There are not definitive results concerning the distinctness of the Kloosterman sums when $p$ is small compared with $m$ (see, e.g. [CaoHolXia08]);
There are not definitive results concerning the distinctness of the Kloosterman sums when $p$ is small compared with $m$ (see, e.g. [CaoHolXia08]);

This work makes a partial progress focusing on the cases:

$$m = 2^n \text{ with } n \in \mathbb{N}, \ u \text{ varying over } \mathbb{F}_p \text{ for } p \text{ odd}.$$
We shall refer to next lemma as to main lemma.

**Lemma 3.**

Let the integers $\delta_t$, $0 \leq t \leq p - 1$ satisfy the equality:

$$\sum_{t=0}^{p-1} \delta_t \omega^t = 0 \quad \text{with} \quad \omega = e^{\frac{2\pi i}{p}}.$$

Then $\delta_t = \Delta$, for all $0 \leq t \leq p - 1$. 

*Sketch of proof:*
The proof is based on the fact that the minimal polynomial of $\omega$ over $\mathbb{Q}$ is $\phi_p(y) = 1 + y + y^2 + \ldots + y^{p-1}$. 

Yuri Borissov

*On the Distinctness of Some Kloosterman Sums*
We shall refer to next lemma as to main lemma.

**Lemma 3.**

Let the integers $\delta_t$, $0 \leq t \leq p - 1$ satisfy the equality:

$$
\sum_{t=0}^{p-1} \delta_t \omega^t = 0 \quad \text{with} \quad \omega = e^{\frac{2\pi i}{p}}.
$$

Then $\delta_t = \Delta$, for all $0 \leq t \leq p - 1$.

**Sketch of proof:**

The proof is based on the fact that the minimal polynomial of $\omega$ over $\mathbb{Q}$ is $\phi_p(y) = 1 + y + y^2 + \ldots + y^{p-1}$. 

Yuri Borissov

On the Distinctness of Some Kloosterman Sums
Proposition 4.
For each pair $a, b \in \mathbb{F}_q$ it holds $\mathcal{K}_q(a) + \mathcal{K}_q(b) \neq 0$ if $p > 2$.

Proof:
The Kloosterman sum can be rewritten in the form:

$$\mathcal{K}_q(u) = \sum_{t=0}^{p-1} N_t(u) \omega^t$$

(1)

with

$$N_t(u) = |\{x \in \mathbb{F}_q^* : \text{Tr}(x + \frac{u}{x}) = t\}|.$$

Obviously, it holds:

$$\sum_{t=0}^{p-1} N_t(u) = |\mathbb{F}_q^*| = p^m - 1.$$
Suppose there exist \(a, b \in \mathbb{F}_q\) s.t. \(\mathcal{K}_q(a) + \mathcal{K}_q(b) = 0\).

Combining Eq. (1) and the main lemma, one gets:

\[
N_t(a) + N_t(b) = N > 0,
\]

for all \(0 \leq t \leq p - 1\).

Next, summing up the above equalities and using Eq. (2):

\[
pN = \sum_{t=0}^{p-1} [N_t(a) + N_t(b)] = \sum_{t=0}^{p-1} N_t(a) + \sum_{t=0}^{p-1} N_t(b) = 2(p^m - 1).
\]

Thus, \(p\) divides \(2(p^m - 1)\) which is impossible if \(p > 2\).
Remarks

Proposition 4 is valid even for Kloosterman sums from different finite fields of the same odd characteristic.
Remarks

- Proposition 4 is valid even for Kloosterman sums from different finite fields of the same odd characteristic.

- Note that "a = b" case of Proposition 4 implies for every $u \in \mathbb{F}_q$ it holds $\mathcal{K}_q(u) \neq 0$, which is a well-known fact.
The Carlitz lifting formula expresses $K_{q^n}(u)$ by the degree of extension $n$, order $q$ and sum $K_q(u)$, namely:

**Fact 5.**

([Carlitz69, Eq. 1.4]) For arbitrary $u \in \mathbb{F}_q^*$, it holds:

$$K_{q^n}(u) = - \sum_{2t \leq n} (-1)^{n-t} \frac{n}{n-t} \binom{n-t}{t} q^t (K(u))^{n-2t}$$

Alternatively, it can be rephrased in terms of the $n$–th Dickson polynomial $D_n$ (of the first kind).
Making use of the lifting formula for \( n = 2 \), one gets

**Lemma 6.**

\[
\text{If } u \in \mathbb{F}_q^* \text{ then it holds } \mathcal{K}_{q^2}(u) = 2q - \mathcal{K}_q^2(u).
\]
Making use of the lifting formula for $n = 2$, one gets

**Lemma 6.**

\[ \text{If } u \in \mathbb{F}_q^* \text{ then it holds } \mathcal{K}_{q^2}(u) = 2q - \mathcal{K}_q^2(u). \]

Lemma 6 and Proposition 4 imply

**Proposition 7.**

For each pair $a, b \in \mathbb{F}_q^*$, $p > 2$, the equality $\mathcal{K}_{q^2}(a) = \mathcal{K}_{q^2}(b)$ holds iff $\mathcal{K}_q(a) = \mathcal{K}_q(b)$.
The main result of that work is the following theorem:

**Theorem 8.**

For every $n \geq 0$, the $(p - 1)$ Kloosterman sums $K_{p^{2n}}(u), u \in \mathbb{F}_p^*$ are distinct.
The main result of that work is the following theorem:

**Theorem 8.** For every $n \geq 0$, the $(p - 1)$ Kloosterman sums $\mathcal{K}_{p^{2n}}(u), u \in \mathbb{F}_p^*$ are distinct.

**Sketch of proof:**

By induction on $n$ with basis the property of distinctness of the sums $\mathcal{K}_p(u), u \in \mathbb{F}_p^*$ ([Fischer92, p.83]) and induction step based on Proposition 7.
Finally, we deduce

**Corollary 9.**

*For every* \( n \geq 0 \), *the sums* \( K_{p^{2n}}(u) \) *when* \( u \) *varies over the prime subfield* \( \mathbb{F}_p \), *\( p > 2 \) are distinct.*

**Sketch of proof:**

Adjoining Theorem 8 with the known result that a Kloosterman zero cannot belong to a proper subfield of \( \mathbb{F}_q \) whenever \( q \neq 16 \).

(see, e.g. [Moisio09])
In this talk, we show:

- there is not a pair of Kloosterman sums over the fields of same odd characteristic which are opposite to each other;
In this talk, we show:

- there is not a pair of Kloosterman sums over the fields of same odd characteristic which are opposite to each other;

- the distinctness of the Kloosterman sums $K_{p^{2n}}(u)$ obtained when $u$ varies over the prime subfield $\mathbb{F}_p$, $p > 2$. 


THANKS FOR YOUR ATTENTION!
Herein, we present an alternative proof of Fischer’s result.

**Proposition 10.**

The Kloosterman sums $K_p(u), u \in \mathbb{F}_p^*$ are distinct.

**Proof:**

Now, it can be easily shown that $N_t(u) = \chi(t^2 - 4u) + 1$ with $\chi(.)$ being the Legendre symbol (see, Eq. (1)). Thus,

\[ K_p(u) = \sum_{t=0}^{p-1} \chi(t^2 - 4u)\omega^t \quad [\text{H.Salie32}] \]
Suppose there exist \( a \neq b \in \mathbb{F}_p^* \) s.t. \( K_p(a) - K_p(b) = 0 \).

By Lemma 3, one gets:

\[
\chi(t^2 - 4a) - \chi(t^2 - 4b) = \Delta,
\]

for all \( 0 \leq t \leq p - 1 \). Obviously \( |\Delta| \leq 2 \) and there are 3 cases to be considered.

- \( \Delta = 0 \), i.e. \( \chi(t^2 - 4a) = \chi(t^2 - 4b) \neq 0 \) for all \( t \).

So,

\[
\frac{\chi(t^2 - 4a)}{\chi(t^2 - 4b)} = \chi\left(\frac{t^2 - 4a}{t^2 - 4b}\right) = 1,
\]

which is a contradiction to injectivity of the function

\[
g(t) = \frac{t^2 - 4a}{t^2 - 4b} = 1 + \frac{4b - 4a}{t^2 - 4b}
\]

in the interval \( I = [0, \frac{p-1}{2}] \);
\(|\Delta| = 1\). In this case it is easily seen that for each \(t\) either \(\chi(t^2 - 4a) = 0\) or \(\chi(t^2 - 4b) = 0\), which is impossible if \(p > 3\) since the quadratic \(t^2 - 4u, u \in \mathbb{F}_p^*\) has at most one zero in the considered interval \(I\);
$|\Delta| = 1$. In this case it is easily seen that for each $t$ either $\chi(t^2 - 4a) = 0$ or $\chi(t^2 - 4b) = 0$, which is impossible if $p > 3$ since the quadratic $t^2 - 4u, u \in \mathbb{F}_p^*$ has at most one zero in the considered interval $I$;

$|\Delta| = 2$, i.e. $\chi(t^2 - 4a) = -\chi(t^2 - 4b) \neq 0$ for all $t$. Then proceed as in the case $\Delta = 0$. \hfill \Box