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

Definitions and Notations (1)

Let $\mathbb{F}_q$ be the finite field of characteristic p and order $q = p^m$.

Definition 1.

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

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

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}.

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.

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.

Introduction and Motivation (1)

- 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;

Introduction and Motivation (1)

- 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;
- 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.)

Introduction and Motivation (2)

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 $\mathcal{K}_p(u), u \in \mathbb{F}_p^*$ are distinct [**Fischer92**];

Introduction and Motivation (2)

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 $\mathcal{K}_p(u), u \in \mathbb{F}_p^*$ are distinct [**Fischer92**];
- Tend to be distinct for p sufficiently larger than m:
  - also, in [**Fischer92**], it has been proved: $\mathcal{K}_q(a) = \mathcal{K}_q(b)$ 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**].

Introduction and Motivation (3)

- There are not definitive results concerning the distinctness of the Kloosterman sums when p is small compared with m (see, e.g. [**CaoHolXia08**]);

Introduction and Motivation (3)

- 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:

  $m = 2^n$ with $n \in \mathbb{N}$, u varying over $\mathbb{F}_p$ for p odd.

Some Necessary Facts (1)

- We shall refer to next lemma as to **main** lemma.

Lemma 3.

Let the integers δ_t, $0 \le t \le p-1$ satisfy the equality:

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

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

Some Necessary Facts (1)

- We shall refer to next lemma as to **main** lemma.

Lemma 3.

Let the integers δ_t, $0 \le t \le p-1$ satisfy the equality:

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

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

- **Sketch of proof:**

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

Results and Sketch of Proofs (1)

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:

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

with

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

Obviously, it holds:

$$\sum_{t=0}^{p-1} N_t(u) = |\mathbb{F}_q^*| = p^m - 1. \tag{2}$$

Results and Sketch of Proofs: cont'd (2)

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 $p > 2$. $\square$

Results and Sketch of Proofs (3)

Remarks

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

Results and Sketch of Proofs (3)

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.

Some Necessary Facts (2)

The Carlitz lifting formula expresses $\mathcal{K}_{q^n}(u)$ by the degree of extension n, order q and sum $\mathcal{K}_q(u)$, namely:

Fact 5.

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

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

Alternatively, it can be rephrased in terms of the $n-$th Dickson polynomial D_n (of the first kind).

Results and Sketch of Proofs (4)

- Making use of the lifting formula for $n = 2$, one gets

Lemma 6.

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

Results and Sketch of Proofs (4)

- Making use of the lifting formula for $n = 2$, one gets

Lemma 6.

If $u \in \mathbb{F}_q^*$ 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 $\mathcal{K}_q(a) = \mathcal{K}_q(b)$.

Results and Sketch of Proofs (5)

- The **main** result of that work is the following theorem:

Theorem 8.

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

Results and Sketch of Proofs (5)

- The **main** result of that work is the following theorem:

Theorem 8.

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

Results and Sketch of Proofs (6)

Finally, we deduce

Corollary 9.

For every $n \geq 0$, the sums $\mathcal{K}_{p^{2^n}}(u)$ 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**]) $\square$

Summary

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;

Summary

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 $\mathbb{F}_p$, $p > 2$.

Selected References (1)

[**Zinoviev19**] V. A. Zinoviev, "On classical Kloosterman sums", *Cryptography and Communications"*, vol. 11(3): 461-496, 2019.

[**LisMoi11**] P. Lisonek and M. Moisio, "On zeros of Kloosterman sums", *Designs, Codes and Cryptography*, vol. 59(3): 223-230, 2011.

[**KonRinVää10**] K.P. Kononen, M. Rinta-aho, K. Väänänen, "On integer values of Kloosterman sums", *IEEE IT*, vol. 56(8): 4011-4013, 2010.

[**Shparl09**] I. Shparlinski, "On the values of Kloosterman sums", *IEEE IT*, vol. 55(6): 2599-2601, 2009.

[**Moisio09**] M. Moisio, "On certain values of Kloosterman sums", *IEEE IT*, vol. 55(8): 3563-3564, 2009.

Selected References (2)

[**CaoHolXia08**] X. Cao, H. D. L. Hollmann, Q. Xiang, "New Kloosterman sum identities and equalities over finite fields", *Finite Fields Appl.* vol. 14: 823-833, 2008.

[**HelKho06**] T. Helleseth and A. Kholosha, "Monomial and quadratic bent functions over the finite fields of odd characteristic", *IEEE IT*, vol. 52(5): 2018-2032, 2006.

[**Wan95**] D. Wan, "Minimal polynomials and distinctness of Kloosterman sums", *Finite Fields Appl.* vol. 1: 189-203, 1995.

[**Fischer92**] Benji Fischer, "Distinctness of Kloosterman sums", *Contemporary Mathematics*, vol. 133: 81-102, 1992.

[**Carlitz69**] L. Carlitz, Kloosterman sums and finite field extensions, *Acta Arithmetica*, XVI.2, 179-193, 1969.

THANKS FOR YOUR ATTENTION!

Appendix (1)

Herein, we present an alternative proof of Fischer's result.

Proposition 10.

The Kloosterman sums $\mathcal{K}_p(u), u \in \mathbb{F}_p^*$ 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,

$$\mathcal{K}_p(u) = \sum_{t=0}^{p-1} \chi(t^2 - 4u)\omega^t \quad \textbf{[H.Salie32]}$$

Suppose there exist $a \neq b \in \mathbb{F}_p^*$ s.t. $\mathcal{K}_p(a) - \mathcal{K}_p(b) = 0$.
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,
  $$\frac{\chi(t^2 - 4a)}{\chi(t^2 - 4b)} = \chi(\frac{t^2 - 4a}{t^2 - 4b}) = 1,$$
  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 $I = [0, \frac{p-1}{2}]$;

Appendix: cont'd (3)

- $|\Delta| = 1$. 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;

Appendix: cont'd (3)

- $|\Delta| = 1$. 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 $\Delta = 0$. $\square$