An approach to computing the number of finite field elements with prescribed trace and co-trace

Yuri Borissov

Institute of Mathematics and Informatics, BAS, Bulgaria

joint work with A. Bojilov and L. Borissov

Faculty of Mathematics and Informatics, Sofia University

MMC-2017 Svolvær, Norway 2017

Content

- Definitions and Notations

Content

- Definitions and Notations
- A Statement of the Problem

Content

- Definitions and Notations
- A Statement of the Problem
- Some Necessary Facts

Content

- Definitions and Notations
- A Statement of the Problem
- Some Necessary Facts
- The Works Prompting Our Study

Content

- Definitions and Notations
- A Statement of the Problem
- Some Necessary Facts
- The Works Prompting Our Study
- An Outline of the Approach:
  - – reducing the number of unknowns;
  - – working out a system of linear equations;
  - – the uniqueness of solution.

Content

- Definitions and Notations
- A Statement of the Problem
- Some Necessary Facts
- The Works Prompting Our Study
- An Outline of the Approach:
  - – reducing the number of unknowns;
  - – working out a system of linear equations;
  - – the uniqueness of solution.
- Examples

Definitions and Notations

Let $\mathbb{F}_q$ be the finite field of characteristic p and order $q = p^m$.
Let $\mathbb{F}_q^*$ stands for the multiplicative group in $\mathbb{F}_q$.

Definition 1.

The **trace** of an element γ in $\mathbb{F}_q$ over $\mathbb{F}_p$ is equal to

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

The **co-trace** of an element γ in $\mathbb{F}_q^*$ is equal to $tr(\gamma^{-1})$.

It is well-known that the trace lies in the prime field $\mathbb{F}_p$.

Definition 2.

(**Kloosterman** sum) For each $u \in \mathbb{F}_q^*$

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

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

For arbitrary $i, j \in \mathbb{F}_p$, we introduce the following notation:

$$\mathrm{T_{ij}} = |\{x \in \mathbb{F}_q^* : tr(x) = i, tr(x^{-1}) = j)\}|,$$

i.e. $\mathrm{T_{ij}}$ **stands for the number of non-zero elements of** $\mathbb{F}_q$ **with trace** i **and co-trace** j.

A Statement of the Problem

- In this work, we search for an approach to finding out closed-form formulae for T_{ij} in terms of m and p in the case of arbitrary characteristic p;

A Statement of the Problem

- In this work, we search for an approach to finding out closed-form formulae for T_{ij} in terms of m and p in the case of arbitrary characteristic p;
- The crucial fact, we make use of, is that according to the main result of 1969's work of L. Carlitz if $u \in \mathbb{F}_p^*$ the Kloosterman sum $\mathcal{K}^{(m)}(u)$ is explicitly expressible in terms of m, q and the sum $\mathcal{K}(u) \triangleq \mathcal{K}^{(1)}(u)$.

Fact 3.

(**[Carlitz69, Eq. 1.3]**) *For arbitrary* $u \in \mathbb{F}_p^*$, *it holds:*

$$\mathcal{K}^{(m)}(u) = (-1)^{m-1} 2^{1-m} \sum_{2r \leq m} \binom{m}{2r} (\mathcal{K}(u))^{m-2r} \{(\mathcal{K}(u))^2 - 4q\}^r$$

The Works Prompting Our Study ($char = 2$)

- S. Dodunekov (1986) proved the quasiperfectness of some classes of double-error correcting codes using essentially the fact: $\mathrm{T}_{01} > 0$, if $m > 2$;

The Works Prompting Our Study (*char* $= 2$)

- S. Dodunekov (1986) proved the quasiperfectness of some classes of double-error correcting codes using essentially the fact: $\mathrm{T}_{01} > 0$, if $m > 2$;

- H. Niederreiter (1990) found implicitly a formula for T_{11} in his efforts to establish an expression for the number of the binary irreducible polynomials of given degree with second and next to the last coefficient equal to 1.

Proposition 4.

For arbitrary i, j *from* $\mathbb{F}_p$*, it holds:*

$$(\mathbf{a}) \quad T_{ij} = T_{ji},$$

and for $i \in \mathbb{F}_p^*$*:*

$$(\mathbf{b}) \quad \mathrm{T_{ij} = T_{1,ij}}.$$

In particular, $T_{0i} = T_{i0} = T_{10} = T_{01}$.

Sketch of proof:

The obvious $(x^{-1})^{-1} = x$ for any $x \neq 0$ implies (**a**);

Claim (**b**) follows by the fact that the mapping $x \to x/i$ permutes the elements of $\mathbb{F}_q$, and the next easily verifiable relations:

$$tr(x/i) = tr(x)/i; \;\; tr((x/i)^{-1}) = tr(i\, x^{-1}) = i\; tr(x^{-1}).$$

(Recall that $i \in \mathbb{F}_p^*$.)

$\square$

Moreover, based on the fact that the number of elements in $\mathbb{F}_q$ with fixed trace equals q/p, one easily deduces:

$$T_{00} = q/p - 1 - (p-1)T_{01}; \;\; T_{01} = T_{10} = q/p - \sum_{j=1}^{p-1} T_{1j}, \qquad (1)$$

i.e, the quantities T_{00} and T_{01} can be expressed in terms of the **unknowns** $T_{1j}, j = 1, \ldots, p-1$.

- Our goal will be to find a system of **linear** equations for T_{1j}.

For each $u \in \mathbb{F}_p^*$, we proceed as follows:

$$\mathcal{K}^{(m)}(u) \triangleq \sum_{x \in \mathbb{F}_q^*} \omega^{tr(x+ux^{-1})} = \sum_{i,j=0}^{p-1} T_{ij}\omega^{i+uj} =$$

$$T_{00} + \sum_{j=1}^{p-1} T_{0j}\omega^{uj} + \sum_{i=1}^{p-1} T_{i0}\omega^{i} + \sum_{i,j=1}^{p-1} T_{1,ij}\omega^{i+uj} =$$

$$T_{00} - 2T_{01} + \sum_{s=1}^{p-1} T_{1s}\left(\sum_{i=1}^{p-1} \omega^{i+\frac{us}{i}}\right) = T_{00} - 2T_{01} + \sum_{s=1}^{p-1} T_{1s}\mathcal{K}(us).$$

(Recall that $\omega = e^{\frac{2\pi i}{p}}$.)

Working out a System of Linear Equations 2

Rewriting the above and using (1) we get:

$$\sum_{s=1}^{p-1}[\mathcal{K}(us)+p+1]T_{1s}=\mathcal{K}^{(m)}(u)+q+1,\ u\in\mathbb{F}_p^* \qquad (2)$$

Note that the RHS can be expressed in terms of $\mathcal{K}(u)$, m and q taking into consideration Carlitz' result (Fact 3).

As a by-product, if for some p all $\mathcal{K}(u)$, $u\in\mathbb{F}_p^*$ are integers then so are $\mathcal{K}^{(m)}(u)$ for any m. In fact, this is a weaker version of the general property valid for each particular $u\in\mathbb{F}_p^*$ proved e.g. in [MoiRan07].

The Uniqueness of Solution 1

Let g be a generating element of $\mathbb{F}_p^*$. Renaming the unknowns by $x_l \stackrel{\triangle}{=} T_{1\ g^l}$ and properly arranging equations (2) one gets a system of the form:

$$\sum_{l=0}^{p-2} k'_{s+l} x_l = \mathcal{K}^{(m)}(g^s) + q + 1, \quad s = 0, \ldots, p-2, \qquad (3)$$

where the subscript of $k'_{s+l} \stackrel{\triangle}{=} \mathcal{K}(g^{s+l}) + p + 1$ is taken modulo $p - 1$, of course.

- Observe that matrix $\mathbf{K}' \stackrel{\triangle}{=} \mathbf{K}'(g)$ of coefficients of system (3) is a real **left-circulant matrix** with first row:

$$[k'_0, k'_1, \ldots, k'_{p-2}],$$

where $k'_l = \mathcal{K}(g^l) + p + 1, \ l = 0, \ldots, p-2.$

Definition 5.

(see, e.g. [Carmona et al.15])
An $n \times n$ matrix $\mathbf{A}$ is called a **left-circulant matrix** if the $i-$th row of $\mathbf{A}$ is obtained from the first row of $\mathbf{A}$ by a left cyclic shift of $i-1$ steps, i.e. the general form of the left-circulant matrix is

$$\mathbf{A} = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & a_0 \\ a_2 & a_3 & a_4 & \dots & a_0 & a_1 \\ . & . & . & . & . & . \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-3} & a_{n-2} \end{bmatrix}.$$

The left-circulant matrices are symmetric and the inverse of an invertible matrix of this type is again left-circulant.

Fact 6.

Let $\mathbf{A}$ *be a left-circulant matrix with first row* $[a_0, a_1, \ldots, a_{n-1}]$*. Then:*

$$\det \mathbf{A} = (-1)^{\frac{(n-1)(n-2)}{2}} \prod_{l=0}^{n-1} f(\theta_l),$$

where $f(x) = \sum_{r=0}^{n-1} a_r x^r$ *and* $\theta_l,\ l = 0, 1, \ldots, n-1$ *are the* n^{th} *roots of unity.*

Fact 7.

(see, e.g. [Lehmer67, Eq. 1.9])

$$\sum_{u=1}^{p-1} \mathcal{K}(u) = 1.$$

Lemma 8.

$$\det \mathbf{K}' = p^2 \det \mathbf{K},$$

where $\mathbf{K}$ *is the left-circulant matrix having as first row:*

$$[\mathcal{K}(1), \mathcal{K}(g), \mathcal{K}(g^2), \ldots, \mathcal{K}(g^{p-2})].$$

Sketch of proof:

There are two essentially distinct cases to consider in Fact 6:

- $\theta = 1$

$$\sum_{l=0}^{p-2} k_l' \theta^l = \sum_{l=0}^{p-2} \{\mathcal{K}(g^l) + p + 1\} = \sum_{l=0}^{p-2} \mathcal{K}(g^l) + p^2 - 1 =$$

$$p^2 * 1 = p^2 \sum_{l=0}^{p-2} \mathcal{K}(g^l)\theta^l$$

- otherwise

$$\sum_{l=0}^{p-2} k_l' \theta^l = \sum_{l=0}^{p-2} \{\mathcal{K}(g^l)\theta^l + (p+1)\theta^l\} = \sum_{l=0}^{p-2} \mathcal{K}(g^l)\theta^l,$$

since θ is a nontrivial $(p-1)^{\text{st}}$ root of unity.

□

Lemma 9.

Let $\mathbf{A}_n$ *be an* $n \times n$ *matrix having entries equal to* x *over its main diagonal and equal to* y *outside of the main diagonal. Then it holds:*

$$\Delta_n \stackrel{\triangle}{=} \det \mathbf{A}_n = (x-y)^{n-1}\{x+(n-1)y\}.$$

Sketch of proof: By induction on n. □

- We shall refer to Lemma 9 as to xy-lemma.

Fact 10.

(see, e.g. [Lehmer67, Eqs. 3.7 and 3.6])

$$\sum_{u=1}^{p-1} \mathcal{K}^2(u) = p^2 - p - 1,$$

and for any $c \neq 1$ *in* $\mathbb{F}_p^*$*:*

$$\sum_{u=1}^{p-1} \mathcal{K}(u)\mathcal{K}(cu) = -p - 1$$

Proposition 11.

$$|\det \mathbf{K}| = p^{p-2}$$

Sketch of proof:

Using Fact 10, one shows that the matrix $\mathbf{A} = \mathbf{K}^2$ satisfies the assumptions of xy-lemma with $x = p^2 - p - 1$ and $y = -p - 1$. Thus, $\det^2 \mathbf{K} = p^{2(p-2)}$. □

- Finally, we deduce the following:

Corollary 12.

The matrix $\mathbf{K}'$ *of coefficients of system (3) is invertible.*

Proof.

Indeed, Lemma 8 and Proposition 11 immediately imply:

$$|\det \mathbf{K}'| = p^p$$

□

- Finally, we deduce the following:

Corollary 12.

The matrix $\mathbf{K}'$ of coefficients of system (3) is invertible.

Proof.

Indeed, Lemma 8 and Proposition 11 immediately imply:

$$|\det \mathbf{K}'| = p^p$$

□

- **Remark:** It is well-known that linear systems having circulant coefficient matrix can be solved using **discrete Fourier transform** and this approach is much faster than the standard Gaussian elimination, especially if a **FFT** is applied (see, e.g. Davies70).

Combining Eq. (2) and Carlitz' result (see, e.g. Bor16), we get:

$$T_{11} = \frac{1}{2^{m+1}} \sum_{r=0}^{\lfloor m/2 \rfloor} (-1)^{m+r+1} \binom{m}{2r} 7^r + \frac{2^m + 1}{4}.$$

This formula is obtained as a by-product in Nied90 without making use of Fact 3.

Example: $char = 2$

Table: Values of T_{ij} for $2 \leq m \leq 10$

m	2	3	4	5	6	7	8	9	10
T_{00}	1	0	3	10	13	28	71	126	241
T_{01}	0	3	4	5	18	35	56	129	270
T_{11}	2	1	4	11	14	29	72	127	242

Example: $char = 3$

$$\mathcal{K}(1) = -1; \quad \mathcal{K}(2) = 2$$

$$\det \mathbf{K} = -3; \quad \det \mathbf{K}' = -27$$

Solving system (2), we get:

$$T_{11} = \frac{2\mathcal{K}^{(m)}(2) - \mathcal{K}^{(m)}(1)}{9} + \frac{3^m + 1}{9}$$

$$T_{12} = \frac{2\mathcal{K}^{(m)}(1) - \mathcal{K}^{(m)}(2)}{9} + \frac{3^m + 1}{9},$$

and finally Carlitz' result can be applied.

Table: Values of $K^{(m)}(u)$ for $1 \leq m \leq 6, u = 1, 2$.

m	1	2	3	4	5	6
$K^{(m)}(1)$	-1	5	8	-7	-31	-10
$K^{(m)}(2)$	2	2	-10	14	2	-46

Table: Values of T_{ij} for $1 \leq m \leq 6$.

m	1	2	3	4	5	6
T_{00}	0	2	2	10	20	68
T_{01}	0	0	3	8	30	87
T_{11}	1	1	0	13	31	72
T_{12}	0	2	6	6	20	84

Example: *char* = 5

$$\mathcal{K}(1) = \frac{3-\sqrt{5}}{2}; \quad \mathcal{K}(4) = \frac{3+\sqrt{5}}{2}$$

$$\mathcal{K}(2) = -1-\sqrt{5}; \quad \mathcal{K}(3) = -1+\sqrt{5}$$

$$\det \mathbf{K} = -125; \quad \det \mathbf{K}' = -3125$$

...

Summary

- In this talk, we address the problem for enumerating the number of finite field elements with prescribed trace and co-trace in case of arbitrary characteristic;

Summary

- In this talk, we address the problem for enumerating the number of finite field elements with prescribed trace and co-trace in case of arbitrary characteristic;
- The problem can be reduced to solving a system of linear equations with matrix of coefficients a slight modification of circulant matrix formed by the **Kloosterman sums.** Also, we prove that system has a unique solution based on deep properties of those sums;

Summary

- In this talk, we address the problem for enumerating the number of finite field elements with prescribed trace and co-trace in case of arbitrary characteristic;
- The problem can be reduced to solving a system of linear equations with matrix of coefficients a slight modification of circulant matrix formed by the **Kloosterman sums.** Also, we prove that system has a unique solution based on deep properties of those sums;
- The approach is illustrated in the cases of characteristic $p = 2, 3$.

[Lehmer67] D. H. and Emma Lehmer, The cyclotomy of Kloosterman sums, *Acta Arithmetica*, **XII.4**, 385–407 (1967).

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

[Davies70] P. J. Davis, Circulant Matrices, *Wiley*, New York, (1970).

[Dodu86] S. Dodunekov, Some quasiperfect double error correcting codes, *Problems of Control and Information Theory*, **15.5**, 367–375 (1986).

[Nied90] H. Niederreiter, An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over binary field, *AAECC* **1**, 119–124, (1990).

[MoiRan07] M. Moisio, K. Ranto, Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros, *Finite Fields and Their Applications* **13**, 922–935, (2007).

[Carmona et al.15] A. Carmona, et al. The inverses of some circulant matrices, *Applied Mathematics and Computation* **270**, 785–793 (2015).

[Bor16] Y. Borissov, Enumeration of the elements of $GF(2^n)$ with prescribed trace and co-trace, $7-$*th European Congress of Mathematics, TU-Berlin*, July 18-22, 2016 (poster).

The End

THANK YOU FOR YOUR ATTENTION !