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

Assen Bojilov[1], Lyubomir Borissov[1], Yuri Borissov[2]

**Abstract**

Let $\mathbb{F}_q = \mathbf{GF}(p^m)$ be the finite field of characteristic $p$ and order $q = p^m$. For every $i, j \in \mathbb{F}_p$, let us consider the subsets $\{x : tr(x) = i, tr(x^{-1} = j\}$ of the multiplicative group $\mathbb{F}_q^*$, where $tr$ denotes the ordinary trace function in $\mathbb{F}_q$. More specifically, we are interested in obtaining closed-form formulae for the cardinalities $t_{i,j}$ of these subsets. Regarding articles with related topics, we refer to [1], [2] and more recent [3].

First, notice that it is straightforward that $t_{i,j} = t_{j,i}$ and for any $i \geq 1 : \quad t_{i,j} = t_{1,ij}$, in particular $t_{i,0} = t_{1,0}$. In addition, based on the well-known fact that the number of elements in $\mathbb{F}_q$ with fixed trace equals $q/p$ one easily deduces:

$$t_{0,0} = q/p - 1 - (p-1)t_{0,1}; \;\; t_{0,1} = t_{1,0} = q/p - \sum_{j=1}^{p-1} t_{1,j} \tag{1}$$

In other words, the quantities $t_{0,0}$ and $t_{0,1}$ are expressible in terms of the unknowns $t_{1,j}, j = 1, \ldots, p-1$.

Our aim will be to find a system of $p-1$ linear equations for these unknowns. To this end, we make use of the classical Kloosterman sums over $\mathbb{F}_q^*$ (see, e.g. [4] about their definition), proceeding for each $a \in \mathbb{F}_p^*$ as follows:

$$\mathcal{K}^{(m)}(a) \triangleq \sum_{x \in \mathbb{F}_q^*} \omega^{tr(x+ax^{-1})} = \sum_{i,j=0}^{p-1} t_{i,j}\omega^{i+aj} = t_{0,0} + \sum_{j=1}^{p-1} t_{0,j}\omega^{aj} + \sum_{i=1}^{p-1} t_{i,0}\omega^{i} + \sum_{i,j=1}^{p-1} t_{1,ij}\omega^{i+aj}$$

$$= t_{0,0} - 2t_{0,1} + \sum_{l=1}^{p-1}\Big(\sum_{i=1}^{p-1}\omega^{i+\frac{al}{i}}\Big)t_{1,l} = t_{0,0} - 2t_{0,1} + \sum_{l=1}^{p-1}\mathcal{K}^{(1)}(al)t_{1,l},$$

where $\omega = e^{2\pi i/p}$ is a primitive $p-$th root of unity. Finally, rewriting the above and using (1) we get:

$$\sum_{j=1}^{p-1}[\mathcal{K}^{(1)}(aj) + p + 1]t_{1,j} = \mathcal{K}^{(m)}(a) + q + 1, \quad a = 1, \ldots, p-1. \tag{2}$$

For fixed $a$, the RHS $B(a) = \mathcal{K}^{(m)}(a) + q + 1$ is explicitly expressible in terms of $\mathcal{K}(a) = \mathcal{K}^{(1)}(a)$, the field extension $m$ and order $q$, taking into consideration the main result of [4] (see, Eq. 1.3 or Eq. 1.4 on pp. 179–180).

Let $g$ be a generating element of $\mathbb{F}_p^*$. Properly arranging equations (2) and renaming the unknowns by $x_j \triangleq t_{1,g^{j-1}}$ one gets a system of the form:

$$\sum_{j=1}^{p-1} A_{l+j-1}x_j = B(g^l) \quad l = 0, \ldots, p-2, \tag{3}$$

where the subscript of $A_{l+j-1} \triangleq \mathcal{K}(g^{l+j-1}) + p + 1$ is taken modulo $p-1$. Observe that the matrix of coefficients of system (3) is a left-circulant matrix (as it is called by a definition given in [5]) with size $p-1$. For the necessary properties of the real circulant matrices, we refer again to the introductory section of [5]. A less-known helpful fact is that the determinant of a circulant matrix of even size can be represented as a product of two determinants of the half size, one being of circulant and the other one of skew-symmetric circulant type.

The ref. [6] is focused on the case $p = 2$. In this paper, applying the described approach we study the next two cases $p = 3, 5$.

## References


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

[2] 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).

[3] M. Moisio, K. Ranto, Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed, *Finite Fields and Their Applications* **14**, 798–815, (2008).

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

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

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


[1] The author is with Faculty of Mathematics and Informatics, Sofia University "St. Kl. Ohridski", Sofia, Bulgaria.
[2] The author is with Department of Mathematical Foundations of Informatics, Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences, Sofia, Bulgaria, e-mail: youri@math.bas.bg