ENUMERATION OF THE ELEMENTS OF GF(3^m) WITH PRESCRIBED TRACE AND CO-TRACE

Lyubomir Borissov, Assen Bojilov

In this note, we address the issue for enumerating the elements of finite fields of characteristic 3 having prescribed trace and co-trace. It turns out that quantities of interest can be linearly expressed in terms of the field order \( q = 3^m \) and the ternary Kloosterman sums \( K(m)(1) \) and \( K(m)(2) \). The asymptotic behavior of all of them resembles \( q/9 \).

1. Introduction and statement of the problem. Let \( \mathbb{F}_q \) be the finite field of characteristic \( p \) of order \( q = p^m \) and let \( \mathbb{F}_q^\ast \) stand for the multiplicative group of non-zero elements in \( \mathbb{F}_q \).

Definition 1.1. The trace of an element \( \gamma \) in \( \mathbb{F}_q \) over \( \mathbb{F}_p \) is equal to
\[
\text{tr}(\gamma) = \gamma + \gamma^p + \cdots + \gamma^{p^{m-1}}.
\]
The co-trace of an element \( \gamma \) in \( \mathbb{F}_q^\ast \) over \( \mathbb{F}_p \) is equal to \( \text{tr}(\gamma^{-1}) \).

It is well-known that the traces belong to the ground field \( \mathbb{F}_p \).

Also, we need the notion of Kloosterman sums \([1]\) defined in general case as follows.

Definition 1.2 (see, e.g. [4]). For each \( a \in \mathbb{F}_q^\ast \)
\[
K(m)(a) = \sum_{x \in \mathbb{F}_q^\ast} \omega^{\text{tr}(x+a)},
\]
where \( \omega = e^{\frac{2\pi i}{p}} \).

If \( m = 1 \), we shall skip it for the sake of simplicity.

Next, we recall the definition of the first kind Dickson polynomials.

Definition 1.3. The \( n^{\text{th}} \) Dickson polynomial \( D_n(x, \alpha) \), \( n \geq 0 \), is defined as follows:
\[
D_0(x, \alpha) = 2;
\]
\[
D_n(x, \alpha) := \sum_{i=0}^{[n/2]} \frac{n}{n-i} \binom{n-i}{i} (-\alpha)^i x^{n-2i},
\]
for \( n > 0 \).

The first few Dickson polynomials are:
\[
D_1(x, \alpha) = x
\]

*2010 Mathematics Subject Classification: 05C35.
Key words: Kloosterman sums, Dickson polynomials.
\[ D_2(x, \alpha) = x^2 - 2\alpha \]
\[ D_3(x, \alpha) = x^3 - 3x\alpha \]
\[ D_4(x, \alpha) = x^4 - 4x^2\alpha + 2\alpha^2 \]

Hereinafter, we list some of the basic properties of the Dickson polynomials:

- **P1**: \[ D_n(2xa, a^2) = 2^a n T_n(x), \] where \( T_n(x) \) stands for the \( n \)-th Chebyshev polynomial of the first kind. (Recall that these polynomials satisfy the recurrence relation \( T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x) \), \( T_0(x) = 1 \) and \( T_1(x) = x \).)
- **P2**: \[ D_n(x, \alpha) = xD_{n-1}(x, \alpha) - \alpha D_{n-2}(x, \alpha). \]
- **P3**: \[ D_n(x + \alpha x - 1, \alpha) = x^n + (\alpha x)^{-n}. \]

In fact, it can be seen (by induction on \( n \)) that property \( P_3 \) is a consequence of the second one \( P_2 \).

There exists a connection between the Dickson polynomials and Kloosterman sums which is stated in the following proposition.

**Proposition 1.4** (see, Proposition 15 in [1]),

\[ K^{(m)}(a) = -D_m(-K(a), p) \]

As an immediate consequence of the above proposition and property \( P_2 \), we obtain the following

**Corollary 1.5.** If \( K(a) \) is an integer for some \( a \in \mathbb{F}_p^* \), then the Kloosterman sum \( K^{(m)}(a) \) is an integer for all \( m \).

Further on, we make use of the following notations:

\[ T_k = |\{x \in \mathbb{F}_q^* : \text{tr}(x) = k\}|, \]
\[ T_{ij} = |\{x \in \mathbb{F}_q^* : \text{tr}(x) = i, \text{tr}(x^{-1}) = j\}|, \]

for \( i, j, k \in \mathbb{F}_p^* \).

In the binary case, i.e. of characteristic 2, closed-form formulae for \( T_{ij} \) (in terms of the field extension \( m \)) are presented in [2].

In this article, we study the ternary case, and give expressions for \( T_{ij} \) in terms of the order of the field and corresponding Kloosterman sums \( K^{(m)}(1) \) and \( K^{(m)}(2) \). Then using the connection described in Proposition 1.4 and the basic properties of the Dickson polynomials listed above, one can compute these numbers for every \( m \). A recent work devoted to the study of ternary Kloosterman sums is Bassalygo and Zinoviev’s paper [5].

2. **Some necessary properties of \( T_k \) and \( T_{ij} \).** Taking into account the meaning of already introduced notations, we recall the following well-known proposition (see, e.g., [3, Ch. 4.8]).

**Proposition 2.1.** For any finite field \( \mathbb{F}_q \) of characteristic \( p \), it holds: \( T_k = p^{n-1} \) whenever \( k > 0 \) while \( T_0 = p^{n-1} - 1 \).

Furthermore, we prove the following proposition.

**Proposition 2.2.** For each finite field \( \mathbb{F}_q \) of characteristic \( p \) and arbitrary \( i, j \) and \( k \) from \( \mathbb{F}_p \), it holds:

\[ (i) \ T_{ij} = T_{ji}; \]
\[ (ii) \ T_k = \sum_{j \in \mathbb{F}_p} T_{kj}. \]
Moreover, in case $p = 3$, we have: $T_{01} = T_{02}$ and $T_{11} = T_{22}$.

**Proof.** Indeed, the obvious equality $(x^{-1})^{-1} = x$ for any $x \neq 0$ immediately implies the first claim. The second one follows by the evident fact that the set of elements with a given trace can be partitioned by disjoint subsets of elements having a fixed co-trace.

To prove the last claim, we note that the mapping $x \to 2x$ is a bijection (in fact, involution) on $F^2_2$ and the obvious relations: $tr(2x) = 2tr(x)$ and $tr((2x)^{-1}) = tr(2x^{-1}) = 2tr(x^{-1})$. □

**3. A theorem for $T_{ij}$ in ternary case.** Proposition 2.2 implies that in case of characteristic 3 it is enough to find out $T_{00}, T_{01}, T_{11}$ and $T_{22}$. Bellow, we obtain for these unknowns four linear equations taking into consideration Proposition 2.1 and the definition of Kloosterman sums. Namely, the first two of these equations have as right-hand sides $T_0 = 3^{m-1} - 1$ and $T_1 = 3^{m-1}$, respectively, while the remaining two have as right-hand sides $K^m(l)$ for $l = 1, 2$.

The results obtained are summarized in the next (main) theorem of this paper:

**Theorem 3.1.** If the field order equals $q = 3^m$ then:

$$T_{00} = \frac{q}{9} + \frac{2K^{(m)}(2) + 2K^{(m)}(1) - 5}{9},$$

$$T_{01} = T_{02} = T_{10} = T_{20} = \frac{q}{9} - \frac{K^{(m)}(2) + K^{(m)}(1) + 2}{9},$$

$$T_{11} = T_{22} = \frac{q}{9} + \frac{2K^{(m)}(2) - K^{(m)}(1) + 1}{9}$$

and

$$T_{12} = T_{21} = \frac{q}{9} + \frac{-K^{(m)}(2) + 2K^{(m)}(1) + 1}{9}.$$

**Proof.** Taking into account Propositions 2.1 and 2.2, we consecutively get:

$$T_0 = T_{00} + T_{01} + T_{02} = T_{00} + 2T_{01} = 3^{m-1} - 1.$$

Similarly:

$$T_1 = T_{10} + T_{11} + T_{12} = T_{01} + T_{11} + T_{12} = 3^{m-1},$$

and in this way we obtain two linear equations for the unknowns $T_{00}, T_{01}, T_{11}$ and $T_{22}$.

Let $\omega$ be the primitive third root of unity (so, $\omega^2 + \omega + 1 = 0$). Then by Definition 1.2 and the corresponding parts of Propositions 2.1 and 2.2, we easily get:

$$(T_{00} + T_{12} + T_{21}) + (T_{01} + T_{10} + T_{22})\omega + (T_{02} + T_{11} + T_{20})\omega^2 =$$

$$T_{00} + 2(\omega + \omega^2)T_{01} + (\omega + \omega^2)T_{11} + 2T_{12} =$$

$$T_{00} - 2T_{01} - T_{11} + 2T_{12} = K^m(1).$$

And, proceeding similarly we obtain the fourth linear equation:

$$T_{00} + T_{11} + T_{22} + (T_{02} + T_{10} + T_{21})\omega + (T_{01} + T_{12} + T_{20})\omega^2 =$$

$$T_{00} + (\omega + \omega^2)T_{01} + 2T_{11} + (\omega + \omega^2)T_{10} + (\omega + \omega^2)T_{12} =$$

$$T_{00} - 2T_{01} + 2T_{11} - T_{12} = K^m(2).$$
So, we get the needed system of linear equations with following matrix of coefficients:

\[
T = \begin{pmatrix}
1 & 2 & 0 & 0 \\
0 & 1 & 1 & 1 \\
1 & -2 & -1 & 2 \\
1 & -2 & 2 & -1
\end{pmatrix}
\]

and right-hand sides \(3^{m-1} - 1, 3^{m-1}, K^{(m)}(1)\) and \(K^{(m)}(2)\), respectively.

Finally, it can be easily shown that \(\text{rank}(T) = 4\) and the solution (given in the claim of this theorem) could be obtained by Gaussian elimination, for instance. □

As a consequence of Theorem 3.1, we obtain the following

**Corollary 3.2.** The asymptotic behavior of all \(T_{ij}\) in the finite field of characteristic 3 and order \(q\) resembles \(q/9\).

**Proof.** Indeed, taking into consideration the famous Weil bound on Kloosterman sums [7], we have: \(|K^{(m)}(a)| \leq 2q^{1/2}\) for all \(q\) and all \(a\) (in particular, for \(a = 1, 2\)). This easily implies that for sufficiently large field extension \(m\) the right-hand sides of formulae for \(T_{ij}\) given in Theorem 3.1 are close to \(q/9\). □

4. **Conclusion.** In this work, we address the issue for enumerating the elements of finite fields of characteristic 3 with given trace and co-trace. Similarly as it is carried out in [6] for the binary case, the obtained results could be applied to find out the exact numbers of the ternary irreducible polynomials of given degree with prescribed second and next to the last coefficient. For future work we intend to address the considered problem in cases of characteristic greater than 3.

**Appendix A. Some numerical results.**

<table>
<thead>
<tr>
<th>(m)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>(K^{(m)}(1))</td>
<td>-1</td>
<td>5</td>
<td>8</td>
<td>-7</td>
<td>-31</td>
<td>-10</td>
</tr>
<tr>
<td>(K^{(m)}(2))</td>
<td>2</td>
<td>2</td>
<td>-10</td>
<td>14</td>
<td>2</td>
<td>-46</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(m)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>(T_{00})</td>
<td>0</td>
<td>2</td>
<td>10</td>
<td>20</td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>(T_{10})</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>30</td>
<td>87</td>
<td></td>
</tr>
<tr>
<td>(T_{11})</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>13</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>(T_{12})</td>
<td>0</td>
<td>2</td>
<td>6</td>
<td>20</td>
<td>84</td>
<td></td>
</tr>
</tbody>
</table>

**REFERENCES**


Lyubomir Borissov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev St, bl. 8
1113 Sofia, Bulgaria
e-mail: lubobs90@math.bas.bg

Assen Bojilov
Faculty of of Mathematics and Informatics
Sofia University “ St Kliment Ohridski”
5, James Bourchier Blvd
1164 Sofia, Bulgaria
e-mail: bojilov@fmi.uni-sofia.bg

**БРОЙ НА ЕЛЕМЕНТИТЕ ОТ GF(3^m) С ДАДЕНИ СЛЕДА И КО-СЛЕДА**

Любомир Борисов, Асен Божилов

В този доклад разглеждаме проблема за преброяването на елементите в крайно поле с характеристика 3, които имат зададени следа и ко-следа. Оказва се, че интересуващите ни числа могат да се изразят линейно чрез броя \( q = 3^m \) на елементите на полето и сумите на Kloosterman \( K^{(m)}(1) \) и \( K^{(m)}(2) \). Също така, получените числа са асимптотично равни на \( \frac{q}{9} \).