THE SUM OF DIGITS FUNCTION IN FINITE FIELDS

CÉCILE DARTYGE AND ANDRÁS SÁRKÖZY

(Communicated by Matthew A. Papanikolas)

Abstract. We define and study certain sum of digits functions in the context of finite fields. We give the number of polynomial values of $\mathbb{F}_q$ with a fixed sum of digits. We also state a result for the sum of digits of polynomial values with generator arguments.

1. Introduction

Let $g \in \mathbb{N}$ be fixed with $g \geq 2$. If $n \in \mathbb{N}$, then representing $n$ in the number system to base $g$,

$$n = \sum_{j=0}^{r-1} c_j g^j, \quad 0 \leq c_j \leq g - 1, \quad c_r \geq 1,$$

we write

$$S(n) = \sum_{j=0}^{r-1} c_j.$$

Many papers have been written on the connection between this sum of digits function $S(n)$ and the arithmetic properties of $n$ (for example [1], [3], [4], [5], [6], [7], [8], [13]). In particular, Mauduit and Sárközy [12] studied the arithmetic structure of the integers whose sum of digits is fixed, while Mauduit and Rivat [10], [11] obtained some asymptotic formulae for the number of squares and also for the number of primes whose sum of digits is even, resp. odd. In this paper our goal is to study the analogs of some of these problems in finite fields.

Indeed, let $p$ be a prime number, $q = p^r$ with $r \geq 2$, and consider the field $\mathbb{F}_q$. Let $B = \{a_1, \ldots, a_r\}$ be a basis of the linear vector space formed by $\mathbb{F}_q$ over $\mathbb{F}_p$; i.e., let $a_1, a_2, \ldots, a_r$ be linearly independent over $\mathbb{F}_p$. Then every $x \in \mathbb{F}_q$ has a unique representation

$$x = \sum_{j=1}^{r} c_j a_j.$$
with \( c_j \in \mathbb{F}_p \). Write

\[
s_B(x) = \sum_{j=1}^r c_j.
\]

An important special case is when the basis \( B \) consists of the first \( r \) powers of a generator of \( \mathbb{F}_q^* \):

\[
B = \{a_1, a_2, \ldots, a_r\} = \{1, z, z^2, \ldots, z^{r-1}\}.
\]

Then (1.3) becomes

\[
x = \sum_{j=1}^r c_j z^{j-1}.
\]

Equations (1.4) and (1.5) are of the same form as (1.1) and (1.2); thus we may consider (1.3) as the finite field analog of the representation (1.1), and we may call \( c_1, \ldots, c_r \) in (1.3) “digits”, and \( s_B(x) \) can be called the “sum of digits” function. If we consider the generators (or primitive elements) as finite field analogs of primitive roots of \( \mathbb{F}_p \), we then end up with the finite field analogs of some problems mentioned above:

How many squares are there in \( \mathbb{F}_q \) with a fixed sum of digits and, more generally, how many values \( f(x) \) of a polynomial \( f \) have a fixed sum of digits? How many generators of \( \mathbb{F}_q^* \) are there whose sum of digits is a fixed value? In this paper our goal is to study these problems.

Let \( c \in \mathbb{F}_p \). We define \( Q_c \) as the set of the squares of \( \mathbb{F}_q \) such that their sum of digits is equal to \( c \):

\[
Q_c = \{ x \in \mathbb{F}_q : s_B(x) = c \text{ and } \exists y \in \mathbb{F}_q \text{ such that } y^2 = x \}.
\]

We prove the following result:

**Theorem 1.1.** For all \( c \in \mathbb{F}_p \), we have

\[
\left| |Q_c| - \frac{p^{r-1}}{2} \right| \leq \sqrt{q}.
\]

Let \( f \in \mathbb{F}_q[X] \) be of degree \( n \) with \( (n, q) = 1 \). We are now interested in the cardinality of the sets

\[
D(f, c) = \{ x \in \mathbb{F}_q : s_B(f(x)) = c \}.
\]

While Theorem 1.1 can be proved elementarily, we will need Weil’s Theorem [14] to estimate \( |D(f, c)| \):

**Theorem 1.2.** Let \( f \in \mathbb{F}_q[X] \) be of degree \( n \) with \( (n, q) = 1 \). Then for all \( c \in \mathbb{F}_p \), we have

\[
\left| |D(f, c)| - p^{r-1} \right| \leq (n - 1)\sqrt{q}.
\]

The main term of this estimate is larger than the one of Theorem 1.1 because here the values \( f(x) \) are taken with multiplicities. We denote by \( \mathcal{G} \) the set of the generators (or primitive elements) of \( \mathbb{F}_q^* \), and for \( c \in \mathbb{F}_p \) we consider the sets

\[
G(f, c) = \{ g \in \mathcal{G} : s_B(f(g)) = c \}.
\]
Theorem 1.3. Let \( f \in \mathbb{F}_q[X] \) be of degree \( n \) with \((n, q) = 1\). Then for all \( c \in \mathbb{F}_p \) we have
\[
\left| |G(f, c)| - \frac{\varphi(q - 1)}{p} \right| \leq (n - 1)\tau(q - 1)\sqrt{q}
\]
where \( \tau(n) \) denotes the divisor function.

2. The sum of digits of the squares

In this section we prove Theorem 1.1. First we suppose that \( c \in \mathbb{F}_p^* \). We use the quadratic character to detect the elements of \( Q_c \):
\[
|Q_c| = \frac{1}{2} \sum_{(c_1, c_2, \ldots, c_r) \in \mathbb{F}_p^r} \left[ 1 + \gamma \left( \sum_{j=1}^r c_j a_j \right) \right],
\]
where \( \gamma \) is the quadratic character. We replace \( c_r \) by \( c - (c_1 + \cdots + c_{r-1}) \):
\[
|Q_c| = \frac{p^{r-1}}{2} + \frac{1}{2} \sum_{(c_1, \ldots, c_{r-1}) \in \mathbb{F}_p^{r-1}} \gamma \left( ca_r + \sum_{j=1}^{r-1} c_j (a_j - a_r) \right).
\]
To make the \( c_j \) independent, it is convenient to switch to the additive characters via the Gaussian sums. We recall that if \( \chi \) is a multiplicative character of \( \mathbb{F}_q^* \) and \( \psi \) is an additive character of \( \mathbb{F}_q \), then the Gaussian sum of \( \chi \) and \( \psi \) is defined by
\[
(2.1) \quad G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \psi(x)
\]
(see [4]). Then we can switch to additive characters with the following formula for all \( x \in \mathbb{F}_q^* \):
\[
\chi(x) = \frac{1}{q} \sum_{\psi} G(\chi, \overline{\psi}) \psi(x).
\]

Since \( c \neq 0 \), \( ca_r + \sum_{j=1}^{r-1} c_j (a_j - a_r) \in \mathbb{F}_q^* \) for all \( c_1, \ldots, c_{r-1} \in \mathbb{F}_p \). Then we obtain for \( |Q_c| \):
\[
(2.2) \quad |Q_c| = \frac{p^{r-1}}{2} + \frac{1}{2q} \sum_{\psi} G(\gamma, \overline{\psi}) \sum_{(c_1, \ldots, c_{r-1}) \in \mathbb{F}_p^{r-1}} \psi(ca_r) \prod_{j=1}^{r-1} \psi(c_j (a_j - a_r)).
\]
If \( \psi(a_j) \neq \psi(a_r) \), then \( \psi(a_j - a_r) \) is a \( p \)-th root of the unity. There exists \( \lambda_j \in \{1, \ldots, p-1\} \) such that \( \psi(a_j - a_r) = e(\lambda_j/p) \) with the standard notation \( e(t) = \exp(2i\pi t) \). In this case,
\[
\sum_{c_j \in \mathbb{F}_p} \psi(c_j (a_j - a_r)) = \sum_{c_j \in \mathbb{F}_p} e \left( \frac{c_j \lambda_j}{p} \right) = 0.
\]
Thus, in the right hand side of (2.2), the summation over \( (c_1, \ldots, c_{r-1}) \) is not 0 if and only if \( \psi(a_j) = \psi(a_r) \) for all \( 1 \leq j \leq r-1 \). This means that \( \psi \) is a power of \( \psi_1 \) where \( \psi_1 \) is the additive character defined by \( \psi_1(a_j) = e(1/p) \) for all \( 0 \leq j \leq r-1 \). Then we have
\[
|Q_c| = \frac{p^{r-1}}{2} + \frac{1}{2p} \sum_{j=0}^{p-1} G(\gamma, \overline{\psi_1^j}) \psi_1^j(c).
\]
Next we use the classical fact ([9] Theorem 5.1) that $|G(\chi, \psi)| \leq \sqrt{q}$ if $(\chi, \psi) \neq (\chi_0, \psi_0)$, the couple of the trivial multiplicative, respectively additive, character. We obtain

$$\left| Q_c - \frac{p^{r-1}}{2} \right| \leq \sqrt{q}.$$ 

If $c = 0$, then we have to remove the term with $c_1 = c_2 = \cdots = c_{r-1} = 0$ in (2.2). This gives an extra error term $\sqrt{q}/2$, and we obtain

$$\left| Q_0 - \frac{p^{r-1}}{2} \right| \leq \sqrt{q}.$$ 

3. The sum of digits of the polynomial values

Let $f \in \mathbb{F}_q[X]$ be of degree $n$ such that $(n, q) = 1$. We are now interested in the cardinality of the sets $D(f, c)$. The character $\psi_1$ defined in the previous section is connected with the sum of digits function $s_B$ by the formula

$$\psi_1(x) = e \left( \frac{s_B(x)}{p} \right).$$

Thus we have

$$|D(f, c)| = \frac{1}{p} \sum_{h=0}^{p-1} \sum_{x \in \mathbb{F}_q} \psi_1^h(f(x)) e \left( -\frac{hc}{p} \right).$$

The main term is provided by $h = 0$:

$$|D(f, c)| = \frac{q}{p} + \frac{1}{p} \sum_{h=1}^{p-1} E(h),$$

with

$$E(h) = \sum_{x \in \mathbb{F}_q} \psi_1^h(f(x)) e \left( -\frac{hc}{p} \right).$$

We will use the following theorem of Weil ([14]; see also [9], Theorem 5.38, p. 223) to obtain an upper bound for the terms $E(h)$.

**Theorem 3.1** (Weil). Let $g \in \mathbb{F}_q[X]$ be of degree $n \geq 1$ with $(n, q) = 1$ and $\psi$ a nontrivial additive character of $\mathbb{F}_q$. Then

$$\left| \sum_{x \in \mathbb{F}_q} \psi(g(x)) \right| \leq (n-1) \sqrt{q}.$$ 

By this theorem, we deduce that $|E(h)| \leq (n-1) \sqrt{q}$ for all $1 \leq h \leq p-1$. Thus we obtain

$$\left| |D(f, c)| - \frac{q}{p} \right| \leq (n-1) \sqrt{q}.$$ 

4. The sum of digits of polynomial values with primitive element arguments

As in the previous section, we consider a polynomial $f \in \mathbb{F}_q[X]$ of degree $n$ with $(n, q) = 1$, but we now study the sets $G(f, c)$. By the same argument as in the previous section we have

$$|G(f, c)| = \frac{1}{p} \sum_{h=0}^{p-1} \sum_{g \in \mathcal{G}} \psi_1^h(f(g)) e \left( -\frac{hc}{p} \right).$$
By using Weil’s Theorem 3.1 we will deduce the following bound for additive character sums with primitive element arguments.

**Lemma 4.1.** Let \( f \in \mathbb{F}_q[X] \) be of degree \( n \) with \( (n, q) = 1 \). Let \( \psi \) be a nontrivial additive character of \( \mathbb{F}_q \). Then

\[
\left| \sum_{g \in \mathcal{G}} \psi(f(g)) \right| \leq (n - 1)\tau(q - 1)\sqrt{q} + \frac{\varphi(q - 1)}{q - 1}.
\]

**Proof.** The proof follows the argument of Lemma 2.3 of [2], which gives a similar upper bound for the sum with multiplicative characters over \( \mathbb{F}_p \). Let \( g_0 \) be a primitive root of \( \mathbb{F}_q^\ast \). Then we have

\[
\sum_{g \in \mathcal{G}} \psi(f(g)) = \sum_{1 \leq k < q \atop (k, q - 1) = 1} \psi(f(g_0^k)).
\]

Then as in [2], we use the M"obius function to handle the coprimality condition, and next we remark that \( g_0^{kd} \) is periodic in \( k \) with period \( (q - 1)/d \):

\[
\sum_{g \in \mathcal{G}} \psi(f(g)) = \sum_{d | q - 1} \mu(d) \sum_{k = 1}^{(q - 1)/d} \psi(f(g_0^{kd})) = \sum_{d | q - 1} \mu(d) \sum_{x \in \mathbb{F}_q^\ast} \psi(f(x^d)).
\]

When \( d | q - 1 \), the degree of \( f(X^d) \) is coprime with \( q \), and we can apply Theorem 3.1. This ends the proof of Lemma 4.1. the \( \varphi(q - 1)/(q - 1) \) term is the contribution of \( x = 0 \) excluded in (4.2).

It remains to insert Lemma 4.1 into (4.1), which gives

\[
\left| |G(f, c)| - \frac{\varphi(q - 1)}{p} \right| \leq (n - 1)\tau(q - 1)\sqrt{q} + 1.
\]

This ends the proof of Theorem 1.3.

**References**


**Institut Élie Cartan, Université de Lorraine, BP 239, 54506 Vandœuvre Cedex, France**

*E-mail address: Cecile.Dartyge@univ-lorraine.fr*

**Department of Algebra and Number Theory, Eötvös Loránd University, 1117 Budapest, Pázmány Péter sétány 1/C, Hungary**

*E-mail address: sarkozy@cs.elte.hu*