Polynomial values and generators
with missing digits in finite fields

Cécile Dartyge (Nancy), Christian Mauduit (Marseille) and András Sárközy (Budapest)

Abstract. We consider the linear vector space formed by the elements of the finite field $$\mathbb{F}_q$$ with $$q = p^r$$ over $$\mathbb{F}_p$$. Then the elements $$x$$ of $$\mathbb{F}_q$$ have a unique representation in the form $$x = \sum_{j=1}^{r} c_j a_j$$ with $$c_j \in \mathbb{F}_p$$; the coefficients $$c_j$$ will be called digits. Let $$\mathcal{D}$$ be a subset of $$\mathbb{F}_p$$ with $$2 \leq |\mathcal{D}| < p$$. We consider elements $$x$$ of $$\mathbb{F}_q$$ such that for their every digit $$c_j$$ we have $$c_j \in \mathcal{D}$$; then we say that the elements of $$\mathbb{F}_p \setminus \mathcal{D}$$ are “missing digits”. We will show that if $$\mathcal{D}$$ is a large enough subset of $$\mathbb{F}_p$$, then there are squares with missing digits in $$\mathbb{F}_q$$; if the degree of the polynomial $$f(x) \in \mathbb{F}_q[X]$$ is at least 2 then it assumes values with missing digits; there are generators $$g$$ in $$\mathbb{F}_q$$ such that $$f(g)$$ is of missing digits.

1. Introduction

Let $$b \in \mathbb{N}$$ be fixed with $$b \geq 2$$. If $$n \in \mathbb{N}$$, then consider the representation of $$n$$ in the number system to base $$b$$:

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

and write

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

Many papers have been written on the connection between the arithmetic properties of $$n$$ and certain properties of its digits $$c_0, c_1, \ldots, c_{r-1}$$. In particular the sum of digits function $$S(n)$$ restricted to polynomial or prime numbers has been studied in [12], [13], [15-17], [20-22], [27], [28], [30], [31], [32]. In some other papers [1-9], [14], [18], [19], [24], [25], [29] the arithmetic properties of integers with missing digits have been studied.

In [11] Dartyge and Sárközy initiated the study of 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 $$\mathcal{B} = \{a_1, a_2, \ldots, a_r\}$$ 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 in form

$$x = \sum_{j=1}^{r} c_j a_j.$$ 

2010 Mathematics Subject Classification: Primary 11A63; Secondary 11L99.

Key words and phrases: digits properties, finite fields, character sums, squares, polynomials, generators, primitive roots.

* Research partially supported by the Hungarian National Foundation for Scientific Research, Grant K77231 and K100291 and the Agence Nationale de la Recherche, grant ANR-10-BLAN 0103 MNUM and French-Hungarian “Balaton” exchange program TET-09-1-2010-0056.
with \( c_j \in \mathbb{F}_p \). Write

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

(1.4)

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

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

Then (1.3) becomes

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

(1.5)

(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 \( c_1, c_2, \ldots, c_r \) in (1.3) as “digits”, and \( S_B(x) \) can be called as “sum of digits” function. It was shown in [11] that if we fix an \( s \in \mathbb{F}_p \) and \( f(x) \in \mathbb{F}_q[x] \) satisfying certain assumptions then there are squares \( x^2 \), elements \( y \in \mathbb{F}_q \) and generators \( g \in \mathbb{F}_q \) with \( S_B(x^2) = s \), \( S_B(f(y)) = s \), \( S_B(f(g)) = s \) respectively.

In this paper our goal is to prove similar results for the elements \( x \in \mathbb{F}_q \) with missing digits. More precisely, let us fix a set \( D \subset \{0, 1, 2, \ldots, p - 1\} \) with \( 2 \leq |D| \leq p - 1 \). We define the set \( W_D \) as the set of all elements \( x \in \mathbb{F}_q \) such that all their digits belong to \( D \) in the basis \( B = \{a_1, a_2, \ldots, a_r\} \):

\[
W_D = \{x = \sum_{j=1}^{r} c_j a_j \text{ with } (c_1, \ldots, c_r) \in D^r\}.
\]

Then we have \(|W_D| = |D|^r\), and the elements of \( \{0, 1, \ldots, p - 1\} \setminus D \) are called missing digits. Let \( Q \) denote the set of the quadratic residues of \( \mathbb{F}_q \) and for \( f(x) \in \mathbb{F}_q[x] \), \( W_D(f) \) the set of the polynomial values of \( f(x) \) with missing digits:

\[
W_D(f) = \{ x \in \mathbb{F}_q : f(x) \in W_D \}.
\]

In order to formulate some of our results we will also use the notation

\[
C(p, t) = \begin{cases} 
\frac{\log p}{t} + \frac{1}{t} \left( \frac{4}{3} - \frac{\log 3}{2} \right) + \frac{1}{p} & \text{if } 2 \leq t < p - 2, \\
\frac{2}{p} + \frac{2}{\pi(p-1)} (1 - \log(2 \sin \frac{\pi}{2p})) & \text{if } t = p - 2.
\end{cases}
\]

(1.6)

We will show that if \( D \) is a large subset of \( \mathbb{F}_p \), then there are many squares in \( Q \) with missing digits; if the degree of the polynomial \( f(x) \in \mathbb{F}_q[x] \) is at least 2 then it assumes values with missing digits; there are generators \( g \) in \( \mathbb{F}_q \) such that \( f(g) \) is of missing digits. We remark that the analog problems in \( \mathbb{N} \) (on squares, polynomial values and primes with missing digits) are open and seem to be very difficult.
2. Squares with missing digits

First we prove that if $|\mathcal{D}|$ is close to $p$, then half of the elements of $W_\mathcal{D}$ are quadratic residues.

**Theorem 2.1.** Let $\mathcal{D} \subset \mathbb{F}_p$ with $2 \leq |\mathcal{D}| \leq p - 1$. Then we have

$$
|W_\mathcal{D} \cap Q| - \frac{|W_\mathcal{D}|}{2} \leq \frac{1}{2 \sqrt{q}} (|\mathcal{D}| + p \sqrt{p - |\mathcal{D}|})^r.
$$

**Remark.** Theorem 2.1 gives a non-trivial upper bound if

$$
|\mathcal{D}| + p \sqrt{p - |\mathcal{D}|} < |\mathcal{D}| \sqrt{p},
$$

that is

$$
|\mathcal{D}| > \frac{-p^2 + \sqrt{p^4 + 4p^3(\sqrt{p} - 1)^2}}{2(\sqrt{p} - 1)^2}
$$

$$
\sim \frac{(\sqrt{5} - 1)p}{2} \quad (p \to +\infty).
$$

**Proof.**

The first step of the proof of Theorem 2.1 is to prove the following lemma. We will use the standard notation $e(t) = \exp(2it\pi)$.

**Lemma 2.2.** We have

$$
|W_\mathcal{D} \cap Q| - \frac{|W_\mathcal{D}|}{2} \leq \frac{1}{2 \sqrt{q}} \left( \sum_{h=0}^{p-1} \left| \sum_{c \in \mathcal{D}} c \left( \frac{ch}{p} \right) \right| \right)^r.
$$

Let $\gamma$ denote the quadratic character of $\mathbb{F}_q$. Then we have

$$
|W_\mathcal{D} \cap Q| = \frac{1}{2} \sum_{x \in W_\mathcal{D}} (1 + \gamma(x)) = \frac{|W_\mathcal{D}|}{2} + \frac{1}{2} \sum_{x \in W_\mathcal{D}} \gamma(x).
$$

Next following [11], we switch to additive characters by using Gaussian sums in order to separate the digits $c_1, \ldots, c_r$. 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

$$
G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x)
$$

(see [26]). Then we use the following formula for all $x \in \mathbb{F}_q^*$:

$$
\chi(x) = \frac{1}{q} \sum_{\psi} G(\chi, \overline{\psi})\psi(x).
$$

Inserting this in (2-3) we obtain:

$$
|W_\mathcal{D} \cap Q| = \frac{|W_\mathcal{D}|}{2} + \frac{1}{2q} \sum_{\psi} G(\gamma, \overline{\psi})S(\psi)
$$
with
\[ S(\psi) = \sum_{c_1, \ldots, c_r \in D} \psi \left( \sum_{i=1}^{r} c_i a_i \right) = \prod_{i=1}^{r} \left( \sum_{c \in D} \psi(ca_i) \right). \]

If \( \psi \) and \( \chi \) are not both trivial, then \(|G(\chi, \psi)| \leq \sqrt{q}\).

For all \( \psi \) and \( a_i, \psi(a_i) \in \{ e\left( \frac{k}{p} \right), 0 \leq k < p - 1 \} \). There is a correspondence between the additive characters \( \psi \) and \( F_p^r \). This correspondence is given by \( (\psi(a_1), \ldots, \psi(a_r)) = \left( e\left( \frac{k_1}{p} \right), \ldots, e\left( \frac{k_r}{p} \right) \right) \). Thus we have
\[
\left| |W_D \cap Q| - \frac{|W_D|}{2} \right| \leq \frac{1}{2\sqrt{q}} \sum_{0 \leq h_1, \ldots, h_r < p} \prod_{i=1}^{r} \left| \sum_{c \in D} e\left( \frac{h_i c}{p} \right) \right|.
\]

This ends the proof of Lemma 2.2.

The second part of the proof of Theorem 2.1 is to obtain an upper bound for
\[ \sum_{c \in D} e\left( \frac{hc}{p} \right). \]

When \( D \) is large we can use the following very simple fact for \( h \neq 0 \):
\[ \sum_{c \in D} e\left( \frac{-hc}{p} \right) = - \sum_{c \in \overline{D}} e\left( \frac{-hc}{p} \right), \]
with the notation \( \overline{D} = F_p \setminus D \). This remark gives something non-trivial if \( |\overline{D}| < |D| \).

The main tool for the upper bound is the following result of Vinogradov (Lemma 14a in [33], Chapter VI page 128):

**Lemma 2.3 (Vinogradov’s Lemma).** If \( \alpha(x) \) and \( \beta(x) \) are complex valued functions on \( \{0, \ldots, m - 1\} \) and \( a \notin m\mathbb{Z} \) then we have
\[ \left| \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} \alpha(x) \beta(y) e\left( \frac{axy}{m} \right) \right| \leq (XYm)^{1/2}. \]

with
\[ X = \sum_{x=0}^{m-1} |\alpha(x)|^2 \text{ and } Y = \sum_{y=0}^{m-1} |\beta(y)|^2. \]

Recently Gyarmati and the third author [23] obtained a generalization of this lemma in finite fields.

For \( 0 < x < p \) we define
\[ \alpha(x) = \frac{\sum_{d \in \overline{D}} e\left( - \frac{xd}{p} \right)}{\sum_{d \in \overline{D}} e\left( - \frac{xd}{p} \right)} \text{ if } \sum_{d \in \overline{D}} e\left( - \frac{xd}{p} \right) \neq 0, \]
and \( \alpha(x) = 1 \) otherwise. With this notation we have:
\[ \sum_{x=1}^{p-1} \left| \sum_{c \in \overline{D}} e\left( \frac{xc}{p} \right) \right| = \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \alpha(x) \beta(y) e\left( \frac{xy}{p} \right). \]

We can now apply Lemma 2.3:
\[
(2.6) \quad \sum_{h=0}^{p-1} \left| \sum_{c \in \overline{D}} e\left( \frac{ch}{p} \right) \right| \leq |D| + \sqrt{p(p-1)(p-|D|)} \leq |D| + p\sqrt{p-|D|}.
\]

Then we insert this bound in Lemma 2.2 and obtain the estimate (2.1) asserted in Theorem 2.1.
3. Squares with missing digits when $D$ consists of consecutive integers

Now we will prove that if $D$ is a set of consecutive integers with at least $\gg \sqrt{p} \log p$ elements then a similar conclusion holds as in Theorem 2.1:

**Theorem 3.1.** We suppose that $D = \{0, \ldots, t-1\}$ with $2 \leq t \leq p-1$. Then we have:

$$\left| |W_D \cap Q| - \frac{|W_D|}{2}\right| \leq \frac{1}{2} (C(p, t)t\sqrt{p})^r.$$  

**Remark.** Theorem 3.1 is non-trivial if $C(p, t)\sqrt{p} < 1$. 

**Proof.** When $D$ is a set of consecutive integers, we can apply some results of the two first authors.

**Lemma 3.2([9] Lemma 3.1).** (i) If $D = \{0, \ldots, t-1\}$ then

$$\frac{1}{pt} \sum_{h=0}^{p-1} \left| \sum_{c \in D} e\left(\frac{hc}{p}\right) \right| \leq \frac{\log p}{t} + \frac{1}{t} \left(\frac{4}{3} - \frac{\log 3}{2}\right) + \frac{1}{p}.$$  

(ii) If $D = \{0, \ldots, p-2\}$ (and $p \geq 3$) then

$$\frac{1}{pt} \sum_{h=0}^{p-1} \left| \sum_{c \in D} e\left(\frac{hc}{p}\right) \right| \leq \frac{2}{p} + \frac{2}{\pi(p-1)}(1 - \log(2\sin \frac{\pi}{2p})).$$

Then Theorem 3.1 can be proved by combining this lemma with Lemma 2.2.

4. Polynomial values with missing digits

We obtain a similar result for $|W_D(f)|$ as the estimates in Sections 2 and 3 (but now we will also need Weil’s theorem to achieve this). We begin by stating the result for large $|D|$.

**Theorem 4.1.** Let $D \subset \mathbb{F}_p$ with $2 \leq |D| \leq p-1$ and $f(x) \in \mathbb{Z}[x]$ with degree $n \geq 2$. Then we have

$$\left| |W_D(f)| - |W_D| \right| \leq \frac{n-1}{\sqrt{q}} \left( |D| + p\sqrt{p - |D|} \right)^r.$$  

When $D$ is a set of consecutive integers we will prove:

**Theorem 4.2.** We suppose that $D = \{0, \ldots, t-1\}$ with $2 \leq t \leq p-1$. Then we have:

$$\left| |W_D(f)| - |W_D| \right| \leq (n-1)(C(p, t)t\sqrt{p})^r.$$  

**Proofs of Theorem 4.1 and Theorem 4.2.** First, we obtain in the following lemma, a similar result as Lemma 2.1 for the sets $W_D(f)$.

**Lemma 4.3.** We suppose that the degree of $f$ is $\geq 2$. Then we have:

$$\left| |W_D(f)| - |D|^r \right| \leq \frac{(n-1)}{\sqrt{q}} \sum_{0 \leq h_1, \ldots, h_r < p \atop (h_1, \ldots, h_r) \neq (0, \ldots, 0)} \prod_{i=1}^r \left| \sum_{c \in D} e\left(\frac{-hc}{p}\right) \right|.$$
For $1 \leq j \leq r$ we consider the additive character $\psi_j$ defined by:

$$\psi_j(a_i) = \begin{cases} 
\exp\left(\frac{i}{p}\right) & \text{if } i = j \\
1 & \text{otherwise} 
\end{cases} \quad (1 \leq i \leq r).$$

Thus for $x = \sum_{i=1}^r x_i a_i \in \mathbb{F}_q$ we have

$$\psi_j(x) = \psi_j(x_1 a_1) \cdots \psi_j(x_r a_r) = \psi_j^{x_1}(a_1) \cdots \psi_j^{x_r}(a_r) = e\left(\frac{x_j}{p}\right).$$

We can use this to detect digit conditions since for $x = x_1 a_1 + \cdots + x_r a_r$ we have

$$\frac{1}{p} \sum_{h=1}^p \psi_j^h(x)e\left(-\frac{hc}{p}\right) = \begin{cases} 
1 & \text{if } x_j = c \\
0 & \text{otherwise.}
\end{cases}$$

If we sum this formula over all $c \in \mathbb{D}$, then we detect the $x$ such that $x_j \in \mathbb{D}$. It remains then to take the product over all the digits to have an indicator of the elements of $W_D$:

$$\prod_{j=1}^r \left(\frac{1}{p} \sum_{h=0}^{p-1} \psi_j^h(x)e\left(-\frac{hc}{p}\right)\right) = \begin{cases} 
1 & \text{if } x \in W_D \\
0 & \text{otherwise.}
\end{cases}$$

We deduce that

$$|W_D(f)| = \sum_{x \in \mathbb{F}_q} \prod_{j=1}^r \frac{1}{p} \sum_{c \in \mathbb{D}} \psi_j^h(x)e\left(-\frac{hc}{p}\right).$$

We develop this product and change the order of summation. The contribution of $h_1 = \ldots = h_r = 0$ provides the main term:

$$|W_D(f)| = |D|^r + \frac{1}{p} \sum_{0 \leq h_1, \ldots, h_r < p} \sum_{x \in \mathbb{F}_q} \left(\prod_{i=1}^r \psi_i^{h_i}(f(x))\right) \prod_{i=1}^r \left(\sum_{c \in \mathbb{D}} e\left(-\frac{hc}{p}\right)\right).$$

We can check easily that if $(h_1, \ldots, h_r) \neq (0, \ldots, 0)$ then $\prod_{i=1}^r \psi_i^{h_i} \neq \psi_0$. Thus we can apply the following theorem ([34], see also [26] Theorem 5.38 p. 223):

**Theorem 4.4 (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

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

It remains to apply this theorem to finish the proof of Lemma 4.3. (4.1) is obtained by combining Lemma 4.3 with (2.6). It is also sufficient to combine Lemma 4.3 with Lemma 3.2 to end the proof of Theorem 4.2.
5. Polynomial values with generator argument and missing digits

Another variant of these problems is to study polynomial values with generator argument. According to the notations of [11] we will denote the set of the generators (or primitive elements) of $\mathbb{F}_q$ by $\mathcal{G}$. For $f(x) \in \mathbb{F}_q[x]$ we now consider

$$W_\mathcal{D}(f, \mathcal{G}) = \{ g \in \mathcal{G} : f(g) \in W_\mathcal{D} \}.$$

Combining the method of the proof of the previous theorem with the estimates of character sums over generators and with polynomial arguments obtained in [11] we can prove:

**Theorem 5.1.** Let $\mathcal{D} \subset \mathbb{F}_p$ with $2 \leq |\mathcal{D}| \leq p-1$ and $f(x) \in \mathbb{Z}[x]$ with degree $n \geq 2$. Then we have

$$|W_\mathcal{D}(f)| - |\mathcal{D}|^r \frac{\varphi(q-1)}{q} \lesssim \left( \frac{1}{q} + \frac{(n-1)\tau(q-1)}{\sqrt{q}} \right) (|\mathcal{D}| + p\sqrt{p - |\mathcal{D}|}^r)^r.$$

When $\mathcal{D}$ is a set of consecutive integers, the corresponding result is

**Theorem 5.2.** We suppose that $\mathcal{D} = \{0, \ldots, t-1\}$ with $2 \leq t \leq p-1$. Then we have:

$$|W_\mathcal{D}(f)| - |\mathcal{D}|^r \frac{\varphi(q-1)}{q} \lesssim (1 + (n-1)\tau(q-1))(C(p, t)t\sqrt{p})^r.$$

The proof of Lemma 4.3 can be adapted to detect the polynomial values with generator arguments and missing digits:

$$|W_\mathcal{D}(f, \mathcal{G})| = \sum_{g \in \mathcal{G}} \prod_{j=1}^r \frac{1}{p} \sum_{c \in \mathcal{D}} \sum_{h=1}^p \psi_j^h(f(g)c) e \left(-\frac{hc}{p}\right).$$

We argue in the same way as before. The only difference is that instead of applying Theorem 4.4 we use the following lemma proved in [11].

**Lemma 5.3.** (11) Lemma 4.1. Under the notations and hypothesis of Theorem 4.4 we have:

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

The analogue of Lemma 4.3 is then

$$(5.1) \quad \left| W_\mathcal{D}(f, \mathcal{G}) | - |\mathcal{D}|^r \frac{\varphi(q-1)}{q} \right| \lesssim \left( \frac{1}{q} + \frac{(n-1)\tau(q-1)}{\sqrt{q}} \right) \left( \sum_{h=1}^p \sum_{d \in \mathcal{D}} \left| e \left(-\frac{hc}{p}\right) \right| \right)^r.$$

Finally Theorem 5.1 is obtained by (5.1) and (2.6), Theorem 5.2 is proved by using (5.1) and Lemma 3.2.

**References**

Cécile Dartyge
Institut Elie Cartan
UMR 7502
Université de Lorraine,
BP 239
54506 Vandœuvre Cedex, France
Cecile.Dartyge@univ-lorraine.fr

Christian Mauduit
Université Aix-Marseille
Institut de Mathématiques de Luminy
CNRS, UMR 6095
13288 Marseille cedex 9, France
mauduit@iml.univ-mrs.fr

András Sárközy
Department of Algebra
and Number Theory
Eötvös Loránd University
1117 Budapest,
Pázmány Péter sétány 1/C
Hungary
sarkozy@cs.elte.hu