Chiffres dans les corps finis

Cathy Swaenepoel

Institut de Mathématiques de Marseille,
Université d'Aix-Marseille, France.

Recherche soutenue par le projet ANR MUDERA.

LIPN, 8 janvier 2019.

Digits

In $\mathbb{N}$, it is usual to write the integers n in base $g \geq 2$:

$$n = \sum_{j=0}^{r-1} \varepsilon_j g^j$$

where the digits ε_j are such that $0 \leq \varepsilon_j \leq g-1$ and $\varepsilon_{r-1} \geq 1$.

The **connection between the arithmetic properties of n and the properties of its digits** leads to interesting questions.

We can mention results by:
Gelfond, Fouvry-Mauduit, Erdős-Mauduit-Sárközy, Dartyge-Tenenbaum, Mauduit-Rivat, Wolke, Harman, Kátai, Bourgain, Maynard ...

Motivation

In the context of finite fields, Dartyge and Sárközy (2013)

- initiated the study of the **concept of digits**,
- obtained results on the **connection between the "algebraic" properties of an element and the properties of its digits**.

Further results in this spirit:

- Dartyge, Mauduit, Sárközy (2015),
- Gabdullin (2016),
- Dietmann, Elsholtz, Shparlinski (2016).

The **algebraic structure** of finite fields permits us to:

- formulate and study new questions (of analytic NT),
- solve problems whose analog in $\mathbb{N}$ might be out of reach.

Basic properties of $\mathbb{F}_q$

Let p be a prime number and $q = p^r$ with $r \geq 1$.
$\mathbb{F}_q$ denotes the finite field with q elements.

- $\mathbb{F}_q$ is a vector space over $\mathbb{F}_p$ of dimension r,
- $(\mathbb{F}_q^*, \times)$ is a cyclic group of order $q - 1$,
- the set $\mathcal{G}$ of primitive elements (generators of $\mathbb{F}_q^*$) satisfies $|\mathcal{G}| = \varphi(q - 1)$.

Concept of digits in $\mathbb{F}_q$

Let $q = p^r$, p prime, $r \geq 2$.
Given a basis $\mathcal{B} = \{e_1, \ldots, e_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$, every $x \in \mathbb{F}_q$ can be written uniquely

$$x = \sum_{j=1}^{r} \varepsilon_j e_j \tag{1}$$

where $\varepsilon_1, \ldots, \varepsilon_r \in \mathbb{F}_p$ are called (Dartyge, Sárközy) the "**digits**" of x.

If $\mathcal{B} = \{1, g, \ldots, g^{r-1}\}$ where $g \in \mathcal{G}$ then (1) becomes:

$$x = \sum_{j=1}^{r} \varepsilon_j g^{j-1},$$

which reminds us of the representation of an integer x in base g.

Sum of digits function in base $\mathcal{B}$: $s_{\mathcal{B}}(x) = \sum_{j=1}^{r} \varepsilon_j$.

Known results on digits in $\mathbb{F}_q$

Question: Given a subset $\mathcal{F}$ of $\mathbb{F}_q$ and a property of the digits, how many elements of $\mathcal{F}$ satisfy this property?
(This is a way to study the pseudo-random properties of the digits of the elements of $\mathcal{F}$.)

Dartyge and Sárközy (2013): number of

- $x \in \mathbb{F}_q$ such that $s_{\mathcal{B}}(P(x)) = s$,
- $g \in \mathcal{G}$ such that $s_{\mathcal{B}}(P(g)) = s$.

Dartyge, Mauduit, Sárközy (2015): idem with missing digits.

Gabdullin (2016): squares with missing digits.

Dietmann, Elsholtz, Shparlinski (2016): number of squares with restricted digits.

For polynomial values in $\mathbb{N}$ with degree ≥ 3, only partial results are known.

New results

1. Prescribing the sum of digits of some special sequences in $\mathbb{F}_q$:

$$s_{\mathcal{B}}(P(x)) = s \text{ and } s_{\mathcal{B}}(P(g)) = s$$

2. "Distribution" of the sum of digits of products in $\mathbb{F}_q$:

$$s_{\mathcal{B}}(cd) = s, c \in \mathcal{C}, d \in \mathcal{D}$$

3. Prescribing the digits of some special sequences in $\mathbb{F}_q$:

$$\varepsilon_{j_1}(P(x)) = \alpha_{j_1}, \ldots, \varepsilon_{j_k}(P(x)) = \alpha_{j_k}$$
$$\varepsilon_{j_1}(P(g)) = \alpha_{j_1}, \ldots, \varepsilon_{j_k}(P(g)) = \alpha_{j_k}$$

Prescribing the sum of digits of polynomial values

Consider first $\{P(x) : x \in \mathbb{F}_q\}$.

Given a polynomial $P \in \mathbb{F}_q[X]$ and $s \in \mathbb{F}_p$, let

$$\mathcal{D}(P, s) = \{x \in \mathbb{F}_q : s_{\mathcal{B}}(P(x)) = s\}.$$

Question: Estimate $|\mathcal{D}(P, s)|$.

Heuristically, we expect: $|\mathcal{D}(P, s)| \approx \dfrac{q}{p}$.

Prescribing the sum of digits of $P(x)$

Theorem (Dartyge, Sárközy, 2013)

If $P \in \mathbb{F}_q[X]$ is of degree $n \geq 1$ with $(n, q) = 1$ then, for $s \in \mathbb{F}_p$,

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

If $P = X^d$, we can save a factor $1/\sqrt{p}$:

Theorem (S.)

If d divides $q - 1$ then, for any $s \in \mathbb{F}_p^*$,

$$\left| |\mathcal{D}(X^d, s)| - \frac{q}{p} \right| \leq \begin{cases} (d-1)\,\sqrt{q}/p & \text{if } d \mid \delta, \\ (d-1)\sqrt{q}/\sqrt{p} & \text{otherwise,} \end{cases} \tag{2}$$

where $\delta = (q-1)/(p-1) \in \mathbb{N}$.

In the special case where $d = 2$, (2) is an equality.

In degree 2, we obtain the exact formula:

Theorem (S.)

If $p \geq 3$ and if $P(X) = a_2X^2 + a_1X + a_0 \in \mathbb{F}_q[X]$ with $a_2 \neq 0$ then, writing $\nu_P = s_{\mathcal{B}}(a_0 - a_1^2(4a_2)^{-1})$, for any $s \in \mathbb{F}_p$, we have

$$\left| |\mathcal{D}(P,s)| - \frac{q}{p} \right| = \begin{cases} \sqrt{q}/\sqrt{p} & \text{if } s \neq \nu_P \text{ and } r \text{ is odd,} \\ \sqrt{q}/p & \text{if } s \neq \nu_P \text{ and } r \text{ is even,} \\ 0 & \text{if } s = \nu_P \text{ and } r \text{ is odd,} \\ (1-p^{-1})\sqrt{q} & \text{if } s = \nu_P \text{ and } r \text{ is even.} \end{cases}$$

Key argument: multiplicative character sums of the form:

$$\sum_{\substack{x \in \mathbb{F}_q^* \\ s_{\mathcal{B}}(x) = s}} \chi(x)$$

can be expressed as a product of Gaussian sums.

Prescribing the sum of digits of $P(g)$

The set $\mathcal{G}$ of generators is a set of remarkable elements in $\mathbb{F}_q$.
More generally, we can consider $\{P(g) : g \in \mathcal{G}\}$.

Given a polynomial $P \in \mathbb{F}_q[X]$ and $s \in \mathbb{F}_p$, let

$$\mathcal{D}_{\mathcal{G}}(P, s) = \{g \in \mathcal{G} : s_{\mathcal{B}}(P(g)) = s\} = \mathcal{D}(P, s) \cap \mathcal{G}.$$

Question: Estimate $|\mathcal{D}_{\mathcal{G}}(P, s)|$.

Heuristically, we expect: $|\mathcal{D}_{\mathcal{G}}(P, s)| \approx \dfrac{\varphi(q-1)}{p}$.

Prescribing the sum of digits of $P(g)$

Theorem (S.)

If $P \in \mathbb{F}_q[X]$ is of degree n with $(n,q)=1$ and if $s \in \mathbb{F}_p$, then

$$\left| |\mathcal{D}_{\mathcal{G}}(P,s)| - \frac{\varphi(q-1)}{p} \right| < \frac{\varphi(q-1)}{q-1} \left((n2^{\omega(q-1)} - 1)\sqrt{q} + 1 \right)$$

where $\omega(q-1)$ is the number of distinct prime factors of $q-1$.

This improves a result of Dartyge and Sárközy by a factor $\frac{\varphi(q-1)}{q-1}$.

Key argument: In the upper bound for additive character sums of the form

$$\sum_{g \in \mathcal{G}} \psi(P(g))$$

used by Dartyge and Sárközy, we save a factor $\frac{\varphi(q-1)}{q-1}$.

1. Prescribing the sum of digits of some special sequences in $\mathbb{F}_q$:

$$s_{\mathcal{B}}(P(x)) = s \text{ and } s_{\mathcal{B}}(P(g)) = s$$

2. "Distribution" of the sum of digits of products in $\mathbb{F}_q$:

$$s_{\mathcal{B}}(cd) = s, c \in \mathcal{C}, d \in \mathcal{D}$$

3. Prescribing the digits of some special sequences in $\mathbb{F}_q$:

$$\varepsilon_{j_1}(P(x)) = \alpha_{j_1}, \ldots, \varepsilon_{j_k}(P(x)) = \alpha_{j_k}$$
$$\varepsilon_{j_1}(P(g)) = \alpha_{j_1}, \ldots, \varepsilon_{j_k}(P(g)) = \alpha_{j_k}$$

Products in $\mathbb{F}_q$

Given $\mathcal{C} \subset \mathbb{F}_q^*$ and $\mathcal{D} \subset \mathbb{F}_q^*$ large enough, the products cd with $c \in \mathcal{C}$ and $d \in \mathcal{D}$ are expected to be "well distributed".

The challenge is to find a lower bound for $|\mathcal{C}|$ and $|\mathcal{D}|$ to ensure this behaviour for a given randomness criterion.

Sárközy and co-authors have studied many problems in this spirit.

Given $\mathcal{C} \subset \mathbb{F}_q^*$, $\mathcal{D} \subset \mathbb{F}_q^*$ and $\mathcal{A} \subset \mathbb{F}_p$, let

$$\mathcal{E} = \{(c,d) \in \mathcal{C} \times \mathcal{D} : s_{\mathcal{B}}(cd) \in \mathcal{A}\}.$$

Question (Sárközy):
Find a sharp lower bound on $|\mathcal{C}|$ and $|\mathcal{D}|$ to ensure that $\mathcal{E} \neq \emptyset$.

Interesting subsets $\mathcal{A}$ of $\mathbb{F}_p$ include:

- $\{s\}$ for $s \in \mathbb{F}_p$,
- subgroups of $\mathbb{F}_p^*$ (for instance squares),
- set of all generators of $\mathbb{F}_p^*$.

Products cd whose sum of digits is fixed

If $\mathcal{A} = \{s\}$ with $s \in \mathbb{F}_p^*$, what is the **expected value for** $|\mathcal{E}|$?

Observe first that:

- $|\{z \in \mathbb{F}_q : s_{\mathcal{B}}(z) = s\}| = p^{r-1} = q/p$,
- the proportion of $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ such that $s_{\mathcal{B}}(xy) = s$ is

$$\frac{1}{(q-1)^2} \cdot \underbrace{(q-1)}_{x} \cdot \underbrace{q/p}_{y \text{ s.t. } s_{\mathcal{B}}(xy)=s} = \frac{q}{(q-1)p}.$$

If the pairs (c, d) were reasonably well distributed, we would expect:

$$|\mathcal{E}| \approx |\mathcal{C}||\mathcal{D}| \frac{q}{(q-1)p}.$$

Products cd whose sum of digits is fixed

Theorem (S.)

If $\mathcal{A} = \{s\}$ with $s \in \mathbb{F}_p^*$ and $\mathcal{C} \subset \mathbb{F}_q^*$, $\mathcal{D} \subset \mathbb{F}_q^*$ then

$$\left| |\mathcal{E}| - \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)} \frac{q}{p} \right| \leq \frac{\sqrt{q}}{\sqrt{p}} \sqrt{|\mathcal{C}||\mathcal{D}|}.$$

Corollary (S.)

If $s \in \mathbb{F}_p^*$ and $|\mathcal{C}||\mathcal{D}| \geq pq$ then there exists $(c, d) \in \mathcal{C} \times \mathcal{D}$ such that $s_{\mathcal{B}}(cd) = s$.

Remark: This result is *optimal up to a constant factor*: there are explicit sets $\mathcal{C}$ and $\mathcal{D}$ such that $pq/16 < |\mathcal{C}||\mathcal{D}| < pq$ and $\mathcal{E} = \emptyset$.

Corollary (S.)

If $\displaystyle\lim_{q \to +\infty} \frac{|\mathcal{C}||\mathcal{D}|}{p^2 q} = +\infty$, the sums $s_{\mathcal{B}}(cd)$ are well distributed in $\mathbb{F}_p$.

Let $\mathcal{A}$ be a nontrivial subgroup of $\mathbb{F}_p^*$ and $m = |\mathcal{A}|$.

Theorem (S.)

If $\mathcal{C}$ and $\mathcal{D}$ satisfy the two conditions:

(1) $|\mathcal{C}||\mathcal{D}| \geq 4pq/m^2$

(2) $\Delta_{\mathcal{A}}(\mathcal{C}) \leq \frac{1}{m}$ *and* $\Delta_{\mathcal{A}}(\mathcal{D}) \leq \frac{1}{m}$

then, there exists $(c, d) \in \mathcal{C} \times \mathcal{D}$ such that $s_{\mathcal{B}}(cd) \in \mathcal{A}$.

The technical condition (2) is true with a probability close to 1 (see below).

Remark: This result is *optimal up to a constant factor*: there are explicit sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (2) such that $pq/(16m^2) < |\mathcal{C}||\mathcal{D}| < pq/m^2$ and $\mathcal{E} = \emptyset$.

If $p \geq 3$ and $\mathcal{A}$ is the set of squares in $\mathbb{F}_p^*$ (thus $m = |\mathcal{A}| = \frac{p-1}{2}$), this implies:

Corollary (S.)

If $\mathcal{C}$ and $\mathcal{D}$ satisfy the two conditions:

(1) $|\mathcal{C}||\mathcal{D}| \geq \dfrac{16p}{(p-1)^2}\, q$

(2) $\Delta_{\mathcal{A}}(\mathcal{C}) \leq \frac{1}{m}$ *and* $\Delta_{\mathcal{A}}(\mathcal{D}) \leq \frac{1}{m}$

then, there exists $(c,d) \in \mathcal{C} \times \mathcal{D}$ such that $s_{\mathcal{B}}(cd)$ is a square in $\mathbb{F}_p^*$.

If $|\mathcal{C}| = |\mathcal{D}|$, it suffices to suppose $|\mathcal{C}| \geq \dfrac{4\sqrt{p}}{p-1}\sqrt{q}$ to ensure that (1) is satisfied. Notice that this lower bound is usually below $\sqrt{q}$.

Study of the condition (2)

For any nonempty subset $\mathcal{C} \subset \mathbb{F}_q^*$, let

$$T_{\mathcal{A}}(\mathcal{C}) = \frac{1}{m} \sum_{t \in \mathcal{A} \setminus \{1\}} \frac{|\mathcal{C} \cap t\mathcal{C}|}{|\mathcal{C}|}$$

and

$$\Delta_{\mathcal{A}}(\mathcal{C}) = T_{\mathcal{A}}(\mathcal{C}) - \left(\frac{m-1}{m}\right) \frac{|\mathcal{C}| - 1}{q-2}.$$

Recall condition (2)**:** $\Delta_{\mathcal{A}}(\mathcal{C}) \leq \frac{1}{m}$ and $\Delta_{\mathcal{A}}(\mathcal{D}) \leq \frac{1}{m}$.

Condition (2) **is true "on average":**

Lemma (S.)

For any $1 \leq d \leq q-1$,
the mean value of $\Delta_{\mathcal{A}}(\mathcal{C})$ over all $\mathcal{C} \subset \mathbb{F}_q^*$ with $|\mathcal{C}| = d$ is 0.

Recall condition (2)**:** $\Delta_{\mathcal{A}}(\mathcal{C}) \leq \frac{1}{m}$ and $\Delta_{\mathcal{A}}(\mathcal{D}) \leq \frac{1}{m}$.

Lemma (S.)

For any $1 \leq d \leq q-1$, *the variance of* $\Delta_{\mathcal{A}}(\mathcal{C})$ *over all* $\mathcal{C} \subset \mathbb{F}_q^*$ *with* $|\mathcal{C}| = d$ *satisfies*

$$\frac{1}{\binom{q-1}{d}} \sum_{|\mathcal{C}|=d} \left(\Delta_{\mathcal{A}}(\mathcal{C})\right)^2 = O\left(\frac{1}{mq}\right).$$

The probability that condition (2) **is true is close to 1:**
$\mathbb{P}\left(\Delta_{\mathcal{A}}(\mathcal{C}) \leq \frac{1}{m}\right) = 1 - O\left(\frac{m}{q}\right)$ with $\frac{m}{q} \to 0$ as $q \to +\infty$.

Examples of subsets $\mathcal{C}$ **such that** $\Delta_{\mathcal{A}}(\mathcal{C}) \leq \frac{1}{m}$**:**
all subsets of affine hyperplanes of the form $\{x \in \mathbb{F}_q : f(x) = s\}$ where f is an $\mathbb{F}_p$-linear form and $s \in \mathbb{F}_p^*$.

Quantity $|\mathcal{C} \cap t\mathcal{C}|$

The study of the quantity $|\mathcal{C} \cap t\mathcal{C}|$ is of independent interest.

Green and Konyagin (2009): if $\mathcal{C}$ is a subset of a group G of prime order with $|\mathcal{C}| = \gamma|G|$ then there exists $x \in G$ such that

$$\Big| |\mathcal{C} \cap x\mathcal{C}| - \gamma^2 |G| \Big| = O(|G|(\log\log|G|/\log|G|)^{1/3}).$$

Notice that a similar statement with $G = \mathbb{F}_q^*$ does not hold: if $\mathcal{C}$ is the set of squares then $|\mathcal{C}| = \gamma|G|$ with $\gamma = 1/2$ and $\mathcal{C} \cap x\mathcal{C} = \emptyset$ or $\mathcal{C}$.

Question: for $G = \mathbb{F}_q^*$ and $\mathcal{C}$ such that $|\mathcal{C}| = \gamma|G|$, give natural conditions on $\mathcal{C}$ so that $|\mathcal{C} \cap x\mathcal{C}|$ is "close" to $\gamma^2|G|$ for at least one $x \in G$.

1. Prescribing the sum of digits of some special sequences in $\mathbb{F}_q$:

$$s_{\mathcal{B}}(P(x)) = s \text{ and } s_{\mathcal{B}}(P(g)) = s$$

2. "Distribution" of the sum of digits of products in $\mathbb{F}_q$:

$$s_{\mathcal{B}}(cd) = s, c \in \mathcal{C}, d \in \mathcal{D}$$

3. Prescribing the digits of some special sequences in $\mathbb{F}_q$:

$$\varepsilon_{j_1}(P(x)) = \alpha_{j_1}, \ldots, \varepsilon_{j_k}(P(x)) = \alpha_{j_k}$$
$$\varepsilon_{j_1}(P(g)) = \alpha_{j_1}, \ldots, \varepsilon_{j_k}(P(g)) = \alpha_{j_k}$$

Prescribing the digits of polynomial values

Let $P \in \mathbb{F}_q[X]$ and consider $\{P(x) : x \in \mathbb{F}_q\}$.

If $1 \leq k \leq r$, what is the number of $x \in \mathbb{F}_q$ such that $P(x)$ has k prescribed digits?

Prescribing the digits of polynomial values

Let $P \in \mathbb{F}_q[X]$ and consider $\{P(x) : x \in \mathbb{F}_q\}$.

If $1 \leq k \leq r$, what is the number of $x \in \mathbb{F}_q$ such that $P(x)$ has k prescribed digits?

Given $J \subset \{1, \ldots, r\}$ with $|J| = k$ and $\alpha = (\alpha_j)_{j \in J} \in (\mathbb{F}_p)^k$, let

$$\mathcal{F}_q(P, k, J, \alpha) = \{x \in \mathbb{F}_q : \varepsilon_j(P(x)) = \alpha_j \text{ for all } j \in J\}$$

be the set of all elements $x \in \mathbb{F}_q$ such that for any $j \in J$, the j-th digit of $P(x)$ in base $\mathcal{B}$ is α_j.

Question: Estimate $|\mathcal{F}_q(P, k, J, \alpha)|$.

Prescribing the digits of polynomial values

Theorem (S.)

If $P \in \mathbb{F}_q[X]$ is of degree $n \geq 1$ with $(n, q) = 1$ then, for any $1 \leq k \leq r$, for any $J \subset \{1, \ldots, r\}$ with $|J| = k$ and any $\alpha \in (\mathbb{F}_p)^k$, we have

$$\left| |\mathcal{F}_q(P, k, J, \alpha)| - \frac{q}{p^k} \right| \leq \frac{p^k - 1}{p^k}(n-1)\sqrt{q};$$

in particular, if

$$(n-1)(p^k - 1) < \sqrt{q} = p^{r/2}$$

then $\mathcal{F}_q(P, k, J, \alpha) \neq \emptyset$.

Consequence: if $p \geq 3$ and if $k \leq r/2$ then $\mathcal{F}_q(X^2, k, J, \alpha) \neq \emptyset$.

Prescribing the digits of polynomial values

Corollary (S.)

For any $n \geq 1$, *for any* $\varepsilon > 0$, *uniformly over* $k \leq (1/2 - \varepsilon)r$, $P \in \mathbb{F}_{p^r}[X]$ *of degree* n, J *with* $|J| = k$ *and* $\alpha \in (\mathbb{F}_p)^k$*:*

$$|\mathcal{F}_{p^r}(P, k, J, \alpha)| = p^{r-k}(1 + o(1)), \quad (p^r \to +\infty, p \nmid n, r \geq 2).$$

Let $\mathcal{Q}_{p^r}$ be the set of squares in $\mathbb{F}_{p^r}$.
The number of squares with a given proportion < 0.5 of prescribed digits is asymptotically as expected:

Corollary (S.)

For any $\varepsilon > 0$, *uniformly over* $k \leq (1/2 - \varepsilon)r$, J *with* $|J| = k$ *and* $\alpha \in (\mathbb{F}_p)^k$, $\alpha \neq 0$,

$$|\{y \in \mathcal{Q}_{p^r} : \varepsilon_j(y) = \alpha_j \text{ for all } j \in J\}| = \frac{p^{r-k}}{2}(1 + o(1))$$

as $p^r \to +\infty, p \geq 3, r \geq 2$.

Prescribing the digits of x^2

When $P = X^2$, we can prove a more precise result.

Theorem (S.)

If $p \geq 3$ then, for any $1 \leq k \leq r$, for any $J \subset \{1, \ldots, r\}$ with $|J| = k$ and any $\alpha \in (\mathbb{F}_p)^k$, $\alpha \neq 0$, we have

$$\left| |\mathcal{F}_q(X^2, k, J, \alpha)| - \frac{q}{p^k} \right| \leq \begin{cases} \dfrac{\sqrt{q}}{\sqrt{p}} & \text{if } r \text{ is odd,} \\ \left(\dfrac{2}{p} - \dfrac{1}{p^k}\right)\sqrt{q} & \text{if } r \text{ is even.} \end{cases} \tag{3}$$

We save a factor

- $1/\sqrt{p}$ if r is odd,
- $2/p$ is r is even.

If $k = 1$ then (3) is an equality.
If $k = 2$ or $k = 3$, there are some values of p and r for which (3) is also an equality.

Prescribing the digits of $P(g)$

Let $P \in \mathbb{F}_q[X]$ and consider $\{P(g) : g \in \mathcal{G}\}$.

If $1 \leq k \leq r$, what is the number of $g \in \mathcal{G}$ such that $P(g)$ has k prescribed digits?

Question: Estimate $|\mathcal{G} \cap \mathcal{F}_q(P, k, J, \alpha)|$.

Prescribing the digits of $P(g)$

Let $P \in \mathbb{F}_q[X]$ and consider $\{P(g) : g \in \mathcal{G}\}$.

If $1 \leq k \leq r$, what is the number of $g \in \mathcal{G}$ such that $P(g)$ has k prescribed digits?

Question: Estimate $|\mathcal{G} \cap \mathcal{F}_q(P, k, J, \alpha)|$.

Theorem (S.)

For any $n \geq 1$, for any $\varepsilon > 0$, uniformly over $k \leq (1/2 - \varepsilon)r$, $P \in \mathbb{F}_{p^r}[X]$ of degree n, J with $|J| = k$ and $\alpha \in (\mathbb{F}_p)^k$:

$$|\mathcal{G} \cap \mathcal{F}_{p^r}(P, k, J, \alpha)| = \frac{\varphi(p^r - 1)}{p^k}(1 + o(1))$$

as $p^r \to +\infty, p \nmid n, r \geq 2$.

In particular, the number of generators with a given proportion < 0.5 of prescribed digits is asymptotically as expected.

Main arguments

- Weil's Theorem,
- orthogonality relations for additive and multiplicative characters of $\mathbb{F}_q$,
- Gaussian sums,
- upper bounds for additive and multiplicative character sums such as

$$\sum_{\substack{x \in \mathbb{F}_q^* \\ s_{\mathcal{B}}(x) = s}} \chi(x), \qquad \sum_{g \in \mathcal{G}} \psi(P(g)).$$

Remarks

If $f : \mathbb{F}_q \to \mathbb{F}_p$ is a linear transformation and $f \neq 0$ then

- there exists a basis $\mathcal{B}$ such that $f = s_{\mathcal{B}}$,
- the previous results can be reformulated with f instead of $s_{\mathcal{B}}$.

The **trace** $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ defined by $\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{r-1}}$ is a linear transformation of basic importance in finite fields.

For instance, we proved that if $p \geq 3$ and if $\mathcal{C}$ and $\mathcal{D}$ satisfy the two conditions:

(1) $|\mathcal{C}||\mathcal{D}| \geq \dfrac{16p}{(p-1)^2}\, q$

(2) technical condition (true with probability close to 1)

then, there exists $(c, d) \in \mathcal{C} \times \mathcal{D}$ such that $\mathrm{Tr}(cd)$ is a square in $\mathbb{F}_p^*$.