On primitive elements of finite fields avoiding affine hyperplanes

Arthur Fernandes\textsuperscript{a}, Lucas Reis\textsuperscript{a,}\textsuperscript{*}

\textsuperscript{a}Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte MG (Brazil), 30270-901

Abstract

Let \( n \geq 2 \) be an integer and let \( \mathbb{F}_q \) be the finite field with \( q \) elements, where \( q \) is a prime power. Given \( \mathbb{F}_q \)-affine hyperplanes \( A_1, \ldots, A_n \) of \( \mathbb{F}_q^n \) in general position, we study the existence and distribution of primitive elements of \( \mathbb{F}_q^n \), avoiding each \( A_i \). We obtain both asymptotic and concrete results, relating to past works on digits over finite fields.

Keywords: finite fields; primitive elements; affine spaces; character sums

2010 MSC: 11T24, 12E20

1. Introduction

Let \( \mathbb{F}_q \) be the finite field with \( q \) elements, where \( q \) is a prime power. It is well known that the multiplicative group \( \mathbb{F}_q^* \) is cyclic and any generator of such group is called primitive. For an integer \( n \geq 2 \), the \( n \)-degree extension \( \mathbb{F}_q^n \) of \( \mathbb{F}_q \) can be regarded as an \( \mathbb{F}_q \)-vector space of dimension \( n \). If \( \mathcal{B} = \{b_1, \ldots, b_k\} \) is an \( \mathbb{F}_q \)-basis for \( \mathbb{F}_q^n \), then every element \( y \in \mathbb{F}_q^n \) is written uniquely as

\[ y = a_1 b_1 + \cdots + a_n b_n, \quad a_i \in \mathbb{F}_q. \]

Inspired by works on the digital expansion of integers in a given basis \[8, 9\], Dartyge and Sarkozy \[2\] introduced the notion of digits over finite fields. In the previous setting, the elements \( a_1, \ldots, a_n \) are the digits of \( y \) with respect to the basis \( \mathcal{B} \). In the past few years, many authors have explored the existence and number of special elements of finite fields (squares, perfect powers and primitive elements) with prescribed digits \[2, 3, 10, 11, 12, 13\].

In \[3\], the authors study the existence of special elements (squares and polynomial values with primitive arguments) with missing digits, i.e., elements \( y = \sum_{i=1}^{n} a_i b_i \), where each digit \( a_i \) is restricted to a subset \( D_i \) of \( \mathbb{F}_p \) (\( p \) is a prime). In particular, they proved that a square of this form always exists if

\*Corresponding author

Email addresses: arthurfapa@gmail.com (Arthur Fernandes), lucasreismat@gmail.com (Lucas Reis)
each quantity $\#D_i$ is (roughly) at least $\frac{(\sqrt{5} - 1)p}{2}$ as $p \to +\infty$. This result is further improved in [4], where milder conditions are imposed on the quantities $\#D_i$. The main idea employed in the proof of those results is to provide a nontrivial bound for the sum

$$s(S, \chi) := \left| \sum_{y \in S} \chi(y) \right|,$$

where $\chi$ is a nontrivial multiplicative character of $\mathbb{F}_{q^n}$ and $S$ corresponds to the elements of $\mathbb{F}_{q^n}$ whose digits are restricted to certain subsets of $\mathbb{F}_q$. By nontrivial we mean a bound $s(S, \chi) = O(\#S)$ as $\#S \to +\infty$.

Motivated by the latter, this paper aims to address a concrete result on the existence of primitive elements with missing digits. More specifically, for elements $c_1, \ldots, c_n \in \mathbb{F}_q$ and an $\mathbb{F}_q$-basis $B$ of $\mathbb{F}_{q^n}$, we study the existence of primitive elements $y \in \mathbb{F}_{q^n}$ such that, for each $1 \leq i \leq n$, the corresponding digit $a_i$ satisfies $a_i \neq c_i$. This is equivalent to consider the case where $\#D = 1$.

Our approach also relies on providing a non trivial bound for a sum like the one in Eq. (1) and, in particular, we asymptotically recover the bound in [3] for $\#D = 1$. However, our approach is quite simpler in this case, where we only use a known bound for multiplicative character sums over affine spaces. The latter allows us to obtain a more precise estimate for specific values of $q$ and $n$, which is quite helpful in the proof of Theorem 1.1. Moreover, we obtain a fairly more general result. For elements $c_1, \ldots, c_n \in \mathbb{F}_q$ and an $\mathbb{F}_q$-basis $B = \{b_1, \ldots, b_n\}$ of $\mathbb{F}_{q^n}$, we observe that each set

$$\mathcal{A}_i = \left\{ \sum_{i=1}^n a_i b_i \mid a_i = c_i \right\},$$

determines an $\mathbb{F}_q$-affine hyperplane of $\mathbb{F}_{q^n}$. Moreover the set $C = \{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ comprises $\mathbb{F}_q$-affine hyperplanes in general position, i.e., for each $1 \leq k \leq n$, the intersection of any $k$ distinct elements of $C$ is an $\mathbb{F}_q$-affine space of dimension $n - k$. In this context, our main result can be stated as follows.

**Theorem 1.1.** Let $n \geq 2$ be a positive integer and let $C = \{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ be a set of $\mathbb{F}_q$-affine hyperplanes of $\mathbb{F}_{q^n}$ in general position. Then the set $S_C^* = \bigcup_{i=1}^n \mathbb{F}_{q^n} \setminus \mathcal{A}_i$ contains a primitive element of $\mathbb{F}_{q^n}$ provided that one of the following holds:

(i) $q \geq 16$;

(ii) $q = 13$ and $n \neq 4$;

(iii) $q = 11$ and $n \neq 4, 6, 12$;

(iv) $q = 7, 8, 9$ and $n$ is large enough.

In particular for $q \geq 16$, $n \geq 2$ and $c \in \mathbb{F}_q$, there exist primitive elements in $\mathbb{F}_{q^n}$ whose corresponding digits (in a given $\mathbb{F}_q$-basis) are all distinct from $c$. 

2
Here goes the structure of the paper. In Section 2 we provide some tools that are used along the way. In Section 3 we estimate the number of primitive elements avoiding $\mathbb{F}_q$-affine hyperplanes, culminating in the proof of Theorem 1.1. In Section 4 we comment on the possible extensions of Theorem 1.1.

2. Preliminaries

In this section we provide background material that is used throughout the paper.

2.1. Characters

A multiplicative character $\chi$ of a finite field $\mathbb{F}$ is a group homomorphism from $\mathbb{F}^*$ to $\mathbb{C}^*$. In other words, $\chi(ab) = \chi(a) \cdot \chi(b)$ for every $a, b \in \mathbb{F}^*$. We usually extend $\chi$ to $0 \in \mathbb{F}$ by setting $\chi(0) = 0$. It is known that the set of multiplicative characters of a finite field $\mathbb{F}$ is a cyclic group of order $#\mathbb{F} - 1$. In particular, for each divisor $d$ of $#\mathbb{F} - 1$, there exist $\varphi(d)$ multiplicative characters of $\mathbb{F}$ of order $d$. The multiplicative character $\chi_0$ with $\chi_0(a) = 1$ for every $a \in \mathbb{F}^*$ is the trivial multiplicative character; this is the unique multiplicative character of $\mathbb{F}$ of order $d = 1$.

The following lemma, due to Vinogradov, provides a character sum formula for the characteristic function of the set of primitive elements in a finite field. Its proof is simple so we omit details.

Lemma 2.1 ([7], Exercise 5.14). Let $\mu$ be the M"{o}bius function, let $\varphi$ be the Euler Totient function and, for each divisor $d$ of $q^n - 1$, let $\Lambda(d)$ be the set of the multiplicative characters of $\mathbb{F}_{q^n}$ of order $d$. The characteristic function $\mathbb{1}_P$ for the set of primitive elements in $\mathbb{F}_{q^n}$ can be expressed by

$$
\mathbb{1}_P(\omega) = \frac{\varphi(q^n - 1)}{q^n - 1} \sum_{d | (q^n - 1)} \mu(d) \frac{\varphi(d)}{\varphi(q^n)} \sum_{\chi \in \Lambda(d)} \chi(\omega).
$$

2.2. Inequalities

Here we provide some bounds that are useful along the way.

Lemma 2.2. For a positive integer $t$, let $W(t)$ denote the number of squarefree divisors of $t$. For $t \geq 3$, the following hold:

1. $W(t) < 4.9 \cdot t^{1/4}$;
2. $W(t) < 4514.7 \cdot t^{1/8}$;
3. $W(t - 1) < t^{0.66}$.

Proof. Items 1 and 2 follow by Lemma 4.1 of [8], while item 3 follows by inequality (4.1) in [1].
The following lemma provides a general bound for multiplicative character sums over affine spaces in finite fields. An interesting proof of this bound is essentially given in Corollary 3.5 of [10], with the help of Weil’s bound. Here we provide a more direct proof, using a result from [5].

**Lemma 2.3.** Let \( A \subseteq \mathbb{F}_{q^n} \) be an \( \mathbb{F}_q \)-affine space of dimension \( t \geq 0 \) and let \( \chi \) be a non-trivial multiplicative character of \( \mathbb{F}_{q^n} \). We have that
\[
s(A, \chi) \leq q^{\min\{t, \frac{n}{2}\}},
\]
where \( s(A, \chi) \) is as in \( \ref{2.3} \).

**Proof.** We have the trivial bound \( s(A, \chi) \leq \#A = q^t \), so it suffices to prove that \( s(A, \chi) \leq q^{n/2} \). Let \( A = u + V \), where \( V \subseteq \mathbb{F}_{q^n} \) is an \( \mathbb{F}_q \)-vector space of dimension \( t \). Corollary 2 of [5] implies that
\[
s(X + Y, \chi) \leq (\#X \cdot \#Y \cdot q^n)^{1/2},
\]
for any sets \( X, Y \subseteq \mathbb{F}_{q^n} \). Taking \( X = A \) and \( Y = V \), we observe that \( s(A + V, \chi) = \#V \cdot s(A, \chi) \) and so
\[
\#V \cdot s(A, \chi) \leq \#V \cdot q^{n/2},
\]
from where the result follows. \( \square \)

3. Primitive elements avoiding affine hyperplanes

The following theorem provides a nice application of Lemma 2.3

**Theorem 3.1.** Let \( C = \{A_1, \ldots, A_n\} \) be a set of \( \mathbb{F}_q \)-affine hyperplanes of \( \mathbb{F}_{q^n} \) in general position and let \( \chi \) be a non-trivial multiplicative character over \( \mathbb{F}_{q^n} \).

If \( S_C^* = \cap_{i=1}^n \mathbb{F}_{q^n} \setminus A_i \) and \( \delta(q, n) = \sum_{i=0}^{n-1} \binom{n}{i} q^{\min\{i, \frac{n}{2}\}} \), then
\[
s(S_C^*, \chi) \leq \delta(q, n) \leq (2^n - 1)q^{n/2}.
\]

**Proof.** For each set \( X \subseteq \mathbb{F}_{q^n} \), let \( 1_X \) be the characteristic function of the set \( X \). Since \( S_C^* = \cap_{i=1}^n \mathbb{F}_{q^n} \setminus A_i \), we obtain that
\[
1_{S_C^*}(\omega) = \prod_{i=1}^n (1 - 1_{A_i}(\omega))
\]
For each nonempty set \( J \subseteq [1, n] := \{1, \ldots, n\} \), we set \( A_J = \cap_{j \in J} A_j \). In
particular, we have the following equalities

\[
\begin{align*}
\mathcal{S}_C^* \cap \mathcal{P} = & \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega) \cdot \mathbb{I}_{\mathcal{S}_C}(\omega) \\
= & \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega) \cdot \prod_{i=1}^{n} (1 - \mathbb{I}_{\mathcal{A}_i}(\omega)) \\
= & \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega) \cdot \left( 1 + \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \mathbb{I}_{\mathcal{A}_J}(\omega) \right) \\
= & \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega) + \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega) \left( \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \mathbb{I}_{\mathcal{A}_J}(\omega) \right).
\end{align*}
\]

Since \( \chi \) is non trivial, \( \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega) = 0 \) by orthogonality. In particular, we have

\[
\begin{align*}
\mathcal{S}_C^* \cap \mathcal{P} = & \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \left( \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega) \mathbb{I}_{\mathcal{A}_J}(\omega) \right) \\
= & \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \left( \sum_{\omega \in \mathcal{A}_J} \chi(\omega) \right).
\end{align*}
\]

From hypothesis, each \( \mathcal{A}_J \) is an \( \mathbb{F}_q \)-affine space of dimension \( n - |J| \). In particular, Lemma \ref{lem:2.3} and the Triangle Inequality imply that

\[
\begin{align*}
\mathcal{S}_C^* \cap \mathcal{P} \leq & \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \left( \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega) \mathbb{I}_{\mathcal{A}_J}(\omega) \right) \\
= & \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \left( \sum_{\omega \in \mathcal{A}_J} \chi(\omega) \right) \\
= & \sum_{J \subseteq [1,n]} (-1)^{|J|} \sum_{\omega \in \mathcal{A}_J} \chi(\omega) \\
= & \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \left( \sum_{\omega \in \mathcal{A}_J} \chi(\omega) \right) \\
= & \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \left( \sum_{\omega \in \mathcal{A}_J} \chi(\omega) \right) \\
= & \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \left( \sum_{\omega \in \mathcal{A}_J} \chi(\omega) \right) \\
= & \sum_{i=1}^{n} \sum_{J \subseteq [1,n]} (-1)^i \left( \sum_{\omega \in \mathcal{A}_J} \chi(\omega) \right).
\end{align*}
\]

We obtain the following result.

**Theorem 3.2.** Let \( C = \{A_1, \ldots, A_n\} \) be a collection of \( \mathbb{F}_q \)-affine hyperplanes in general position in \( \mathbb{F}_q^n \) and let \( \mathcal{P}(\mathcal{S}_C^*) \) be the number of primitive elements in \( \mathcal{S}_C^* \cap \mathcal{P} \). Then

\[
\mathcal{S}_C^* \cap \mathcal{P} = \frac{q^n - 1}{\varphi(q^n - 1)} \mathcal{P}(\mathcal{S}_C^*) > (q - 1)^n - \delta(q,n) \cdot W(q^n - 1),
\]

where \( \delta(q,n) \) is as in Theorem \ref{thm:1.1}.

**Proof.** From Lemma \ref{lem:2.1}, we obtain that

\[
\mathcal{P}(\mathcal{S}_C^*) = \sum_{\omega \in \mathcal{S}_C^*} \mathbb{I}_{\mathcal{P}}(\omega) = \sum_{\omega \in \mathcal{S}_C^*} \frac{\varphi(q^n - 1)}{q^n - 1} \sum_{d|q^n - 1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \Lambda(d)} \chi(\omega).
\]
Therefore,
\[ \frac{q^n - 1}{\varphi(q^n - 1)} P(S_C^*) = \sum_{\omega \in S_C^*} \sum_{d \mid q^n - 1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \Lambda(d)} \sum_{\omega \in S_C^*} \chi(\omega) = \sum_{\omega \in S_C^*} \chi_0(\omega) + \sum_{d \mid q^n - 1} \sum_{\omega \in S_C^*} \chi(\omega). \]

Since the elements of $C$ are in general position, a simple inclusion-exclusion argument implies that $S_C^*$ has cardinality $(q - 1)^n$. In particular,
\[ \sum_{\omega \in S_C^*} \chi_0(\omega) = \sum_{\omega \in S_C^*} 1 \geq (q - 1)^n - 1. \]

Therefore, from Theorem 3.1 and the Triangle Inequality we obtain that
\[ \frac{q^n - 1}{\varphi(q^n - 1)} P(S_C^*) \geq (q - 1)^n - 1 - \sum_{d \mid q^n - 1} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \Lambda(d)} \sum_{\omega \in S_C^*} \chi(\omega) \]
\[ \geq (q - 1)^n - 1 - \sum_{d \mid q^n - 1} \sum_{\omega \in S_C^*} \sum_{\chi \in \Lambda(d)} \delta(q, n) \]
\[ = (q - 1)^n - \delta(q, n) - \sum_{d \mid q^n - 1} \sum_{\omega \in S_C^*} \sum_{\chi \in \Lambda(d)} \delta(q, n) \]
\[ > (q - 1)^n - \delta(q, n) \cdot W(q^n - 1). \]

\[ \square \]

3.1. Concrete results: proof of Theorem 1.1

In this section we provide the proof of Theorem 1.1. Here and throughout, $C = \{A_1, \ldots, A_n\}$ is a collection of $F_q$-affine hyperplanes of $F_q^n$ in general position and $S_C^* = \cup_{i=1}^n F_q^n \setminus A_i$. Theorem 3.2 entails that $S_C^*$ contains a primitive element whenever the following inequality holds
\[ W(q^n - 1) \leq \left( \frac{q - 1}{2 \sqrt{q}} \right)^n. \tag{2} \]

Since $W(t) \geq 2$ for every $t \geq 2$, we have the trivial restriction $q - 1 > 2\sqrt{q}$, i.e., $q \geq 7$. Moreover, if $q \geq 7$ is fixed, item 3 of Lemma 2.2 entails that Eq. (2) holds if $n$ is large enough. The latter proves item (iv) of Theorem 1.1.
From now on, we assume that $q \geq 7$. If we set $F_1(t) = 4.9 \cdot t^{1/4}$, $F_2(t) = 4514.7 \cdot t^{1/8}$ and $F_3(t) = t^{0.96 \log \log t}$, Lemma 2.2 entails that $W(q^n - 1) \leq \min_{1 \leq i \leq 3} F_i(q^n)$. So it suffices to have the following inequality

$$\min_{1 \leq i \leq 3} F_i(q^n)^{1/n} \leq \frac{q - 1}{2\sqrt{q}} \quad (3)$$

We observe that the functions $F_i(q^n)^{1/n}$ are decreasing on $n$ in the range $q \geq 7$ and $n \geq 2$. By a direct computation we obtain Table 1 that displays some ranges where Eq. (3) holds.

| $q$   | $n$   | $F_i$ |
|-------|-------|-------|
| $\geq 389$ | $\geq 2$ | $F_1$ |
| $\geq 76$   | $\geq 4$ | $F_3$ |
| $\geq 16$    | $\geq 25$ | $F_3$ |
| $\geq 13$    | $\geq 45$ | $F_2$ |
| $\geq 11$    | $\geq 76$ | $F_2$ |

Table 1: Pairs $(q, n)$ satisfying Eq. (3) and the function $F_i$ employed.

For the finite set $\mathcal{X}$ of pairs in the range $q \geq 11$ and $n \geq 2$ that are not included in Table 1, we proceed to direct computations:

(a) Theorem 3.2 also entails that $S_C^*$ contains a primitive element whenever the following inequality holds

$$(q - 1)^n > \delta(q, n)W(q^n - 1).$$

(b) It is known that there exist $\varphi(q^n - 1)$ primitive elements in $\mathbb{F}_{q^n}^\times$. Since the set $S_C^*$ contains $(q - 1)^n$ elements, such a set contains a primitive element whenever the following inequality holds

$$(q - 1)^n + \varphi(q^n - 1) > q^n.$$  

Using a SageMATH program, we directly verify that, with the exception of the pairs

$$(q, n) = (13, 4); (11, 4); (11, 6); (11, 12),$$

the elements of $\mathcal{X}$ satisfy the inequality in one of the items (a) or (b) above. This completes the proof of Theorem 1.1.

4. Conclusions

Motivated by works on special elements of finite fields with restrictions on their digits, this paper discussed the existence of primitive elements of finite fields avoiding affine hyperplanes in general position. We obtained a complete result for extensions $\mathbb{F}_{q^n}$ with $q \geq 16$ and $n \geq 2$. Moreover, the cases $q = 11, 13$
yield only 4 possible exceptions and we also obtained an asymptotic result for
$q = 7, 8, 9$.

By using a sieving method that is traditional in this kind of problem (see [1]),
one can also check that the pair $(q, n) = (11, 12)$ is not a genuine exception in
Theorem 1.1. It would be interesting to achieve concrete results for $q = 7, 8, 9$
or even discuss asymptotic results for $q = 3, 4, 5$ (the case $q = 2$ is a trivial
exception for every $n \geq 2$). In order to accomplish the latter, we believe that
sharper bounds on multiplicative characters sums related to this problem must
be obtained.

Acknowledgments

We would like to thank Fabio Brochero for providing helpful suggestions in an
earlier version of this work.

References

[1] S. D. Cohen., T. Oliveira e Silva and T. Trudgian. On consecutive primitive
elements in a finite field. *Bull. Lond. Math. Soc.* 47(3): 418–426, 2015.

[2] C. Dartyge, A. Sárközy. The sum of digits function in finite fields. *Proc.
Amer. Math. Soc.* 141: 4119–4124, 2013.

[3] C. Dartyge, C. Mauduit, A. Sárközy. Polynomial values and generators
with missing digits in finite fields. *Funct. Approx. Comment. Math.* 52:
65–74, 2015.

[4] R. Dietman, C. Elsholtz, I. Shparlinski. Prescribing the binary digits of
squarefree numbers and quadratic residues *Trans. Amer. Math. Soc.* 369:
8369–8388, 2017.

[5] K. Gyarmati, A. Sárközy, Equations in finite fields with restricted solution
sets. I (Character sums). *Acta Math. Hung.* 118: 129–148, 2008.

[6] G. Kapetanakis and L. Reis. Variations of the Primitive Normal Basis
Theorem. *Des. Codes Cryptogr.* 87(7): 1459–1480, 2019.

[7] R. Lidl and H. Niederreiter. *Finite Fields.* (Encyclopedia of Mathematics
and its Applications). Cambridge: Cambridge University Press, 1996.

[8] C. Mauduit, J. Rivat. La somme des chiffres des carrés. *Acta Math.* 203
(1): 107–148, 2009.

[9] C. Mauduit and J. Rivat. Sur un problème de Gelfond: la somme des
chiffres des nombres premiers. *Ann. of Math.* 171 (3): 1591–1646, 2010.

[10] L. Reis. Arithmetic constraints of polynomial maps
through discrete logarithms. *J. Number Theory* (2020),
https://doi.org/10.1016/j.jnt.2020.10.015
[11] L. Reis. Some applications of character sums over affine subspaces. (submitted), (2021).

[12] C. Swaenepoel. Prescribing digits in finite fields. *J. Number Theory* 189: 97–114, 2018.

[13] C. Swaenepoel. On the sum of digits of special sequences in finite fields. *Monatsh. Math.* 187: 705–728, 2018.