



**HAL**  
open science

## A nullstellensatz for sequences over $F_p$

Eric Balandraud, Benjamin Girard

► **To cite this version:**

| Eric Balandraud, Benjamin Girard. A nullstellensatz for sequences over  $F_p$ . 2012. hal-00684502v1

**HAL Id: hal-00684502**

**<https://hal.sorbonne-universite.fr/hal-00684502v1>**

Preprint submitted on 2 Apr 2012 (v1), last revised 29 Jun 2014 (v2)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# A NULLSTELLENSATZ FOR SEQUENCES OVER $\mathbb{F}_p$

ÉRIC BALANDRAUD AND BENJAMIN GIRARD

ABSTRACT. Let  $p$  be a prime and let  $A = (a_1, \dots, a_\ell)$  be a sequence of nonzero elements in  $\mathbb{F}_p$ . In this paper, we study the set of all 0-1 solutions to the equation

$$a_1x_1 + \dots + a_\ell x_\ell = 0.$$

We prove that whenever  $\ell \geq p$ , this set actually characterizes  $A$  up to a nonzero multiplicative constant, which is no longer true for  $\ell < p$ . The critical case  $\ell = p$  is of particular interest. In this context, we prove that whenever  $\ell = p$  and  $A$  is nonconstant, the above equation has at least  $p - 1$  minimal 0-1 solutions, thus refining a theorem of Olson. The subcritical case  $\ell = p - 1$  is studied in detail also. Our approach is algebraic in nature and relies on the Combinatorial Nullstellensatz as well as on a Vosper type theorem.

## 1. INTRODUCTION

The study of the existence and variety of 0-1 solutions to linear equations over a finite Abelian group is a central topic in zero-sum combinatorics. Promoted by applications in algebraic number theory, many results have been proved in this area since the seminal paper of Erdős, Ginzburg and Ziv [6]. The interested reader is referred to [7, 8] for an exposition and many references on this subject.

Let  $p$  be a prime and let  $A = (a_1, \dots, a_\ell)$  be a sequence of nonzero elements in  $\mathbb{F}_p$ . In this paper, we study the set  $\mathcal{S}_A$  of all 0-1 solutions to the equation

$$(1) \quad a_1x_1 + \dots + a_\ell x_\ell = 0.$$

Equivalently, one has

$$\mathcal{S}_A = A^\perp \cap \{0, 1\}^\ell$$

where  $A^\perp = \{x \in \mathbb{F}_p^\ell : A \cdot x = 0\}$  and  $A \cdot x$  denotes the usual inner product of  $A$  and  $x$  over  $\mathbb{F}_p^\ell$ . This very definition readily makes of  $\mathcal{S}_A$  an ambivalent object that can be expressed as the intersection of an algebraic structure, namely a hyperplane of  $\mathbb{F}_p^\ell$ , and the  $\ell$ -cube  $\{0, 1\}^\ell$ , which has a more combinatorial flavor.

Seen as a set of vectors,  $\mathcal{S}_A$  will be studied through the subspace  $\langle \mathcal{S}_A \rangle$  of  $A^\perp$ . For this reason, we will set

$$\dim(A) = \dim(\langle \mathcal{S}_A \rangle).$$

In particular, since  $\dim(A^\perp) = \ell - 1$ , it can easily be noticed that  $\dim(A) \leq \ell - 1$  always holds. Alternatively, every element of  $\mathcal{S}_A$  can be seen as a subset of  $[1, \ell]$ . Therefore, it is not surprising that  $\mathcal{S}_A$  also has set theoretic properties. For instance,  $\mathcal{S}_A$  is easily seen to be closed under disjoint union. It is also closed under complement if and only if the sum  $\sigma(A)$  of all elements in  $A$  is equal to zero. In what follows, we will be particularly interested in the number of *minimal* elements in  $\mathcal{S}_A \setminus \{0\}$  ordered by inclusion.

In this paper, we address three problems which appear to be closely related. First, we determine the value of  $\dim(A)$  for any sequence  $A$  of  $\ell \geq p - 1$  nonzero

---

IMJ, Équipe Combinatoire et Optimisation, Université Pierre et Marie Curie (Paris 6), 4 place Jussieu, 75005 Paris, France, email: [balandraud@math.jussieu.fr](mailto:balandraud@math.jussieu.fr) | [bgirard@math.jussieu.fr](mailto:bgirard@math.jussieu.fr).

elements in  $\mathbb{F}_p$ . Then, we apply our results to solve the reconstruction problem of knowing whether  $\mathcal{S}_A$  characterizes  $A$  up to a nonzero multiplicative constant. Finally, we study the number of minimal elements in  $\mathcal{S}_A$ .

The main idea behind our results is the following. For every  $\ell \geq p - 1$ , the equality  $\dim(A) = \ell - 1$  holds true except for a very limited number of exceptional sequences which can be fully determined. Our first theorem deals with large values of  $\ell$ , namely  $\ell > p$ .

**Theorem 1.1.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_\ell)$  be a sequence of  $\ell > p$  nonzero elements in  $\mathbb{F}_p$ . Then*

$$\dim(A) = \ell - 1.$$

Consequently, whenever  $A$  is a sequence of  $\ell > p$  nonzero elements in  $\mathbb{F}_p$ , the hyperplane  $A^\perp$  has a basis consisting solely of elements in  $\mathcal{S}_A$ , and is thus fully characterized by its intersection with the  $\ell$ -cube. This solves the reconstruction problem for large values of  $\ell$ .

**Corollary 1.2.** *Let  $p$  be a prime. Let also  $A, B$  be two sequences of  $\ell > p$  nonzero elements in  $\mathbb{F}_p$ . Then  $\mathcal{S}_A = \mathcal{S}_B$  if and only if  $A$  and  $B$  are colinear.*

Theorem 1.1 also implies a lower bound on the number of minimal elements in  $\mathcal{S}_A$ . Indeed, one can notice that any basis of  $A^\perp$  consisting of elements in  $\mathcal{S}_A$  can be turned into a basis of  $A^\perp$  consisting exclusively of minimal elements in  $\mathcal{S}_A$  (see Proposition 3.3). This yields the following result.

**Corollary 1.3.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_\ell)$  be a sequence of  $\ell > p$  nonzero elements in  $\mathbb{F}_p$ . Then  $\mathcal{S}_A$  contains at least  $\ell - 1$  minimal elements.*

In the case  $\ell = p$ , there are exceptional sequences  $A$  such that  $\dim(A) < \ell - 1$ . However, such exceptions are very rare, since they have to be highly structured. The following analogue of Theorem 1.1 is our first result in this direction.

**Theorem 1.4.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_p)$  be a sequence of  $p$  nonzero elements in  $\mathbb{F}_p$ . Then one of the following statements holds.*

(i)  $\dim(A) = 1$  and there exists  $r \in \mathbb{F}_p^*$  such that

$$(a_1, \dots, a_p) = (r, \dots, r).$$

(ii)  $\dim(A) = p - 2$  and there exist  $t \in [1, p - 3]$ ,  $\sigma \in \mathfrak{S}_p$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p)}) = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-2-t}, -(t+1)r, -(t+1)r).$$

(iii)  $\dim(A) = p - 1$ .

Therefore, in all cases where  $\dim(A) = p - 1$ , the same argument as above readily implies that  $A^\perp$  has a basis consisting of elements in  $\mathcal{S}_A$ . In addition, the two exceptional cases (i) and (ii) correspond to highly structured sequences, for which we can easily check by hand that  $\mathcal{S}_A$  characterizes  $A^\perp$  indeed. This answers the reconstruction problem affirmatively in the case  $\ell = p$ .

**Corollary 1.5.** *Let  $p$  be a prime. Let also  $A, B$  be two sequences of  $p$  nonzero elements in  $\mathbb{F}_p$ . Then  $\mathcal{S}_A = \mathcal{S}_B$  if and only if  $A$  and  $B$  are colinear.*

In his last paper [9], Olson proved a conjecture of Erdős stating that if  $A$  is a nonconstant sequence of  $p$  nonzero elements in  $\mathbb{F}_p$ , then  $\mathcal{S}_A$  contains at least  $p - 1$  nonzero elements. In this respect, Theorem 1.4 actually yields a strong version of the original conjecture of Erdős. More precisely, this conjecture still holds when we restrict ourselves to counting minimal elements in  $\mathcal{S}_A$  only. This gives the following refinement of Olson's theorem.

**Corollary 1.6.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_p)$  be a nonconstant sequence of  $p$  nonzero elements in  $\mathbb{F}_p$ . Then  $\mathcal{S}_A$  contains at least  $p - 1$  minimal elements.*

In the case  $\ell = p - 1$ , the situation becomes a little more involved but similar results can still be proved. On the one hand, all sequences  $A$  with  $\sigma(A) \neq 0$  can easily be handled (see Lemma 5.1). On the other hand, the following theorem fully describes the case of sequences  $A$  with  $\sigma(A) = 0$ , which will be called *zero-sum* sequences.

**Theorem 1.7.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_{p-1})$  be a zero-sum sequence of  $p - 1$  nonzero elements in  $\mathbb{F}_p$ . Then one of the following statements holds.*

(i)  $\dim(A) = 1$  and there exist  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (r, \dots, r, 2r).$$

(ii)  $\dim(A) = p - 4$  and there exist  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (\underbrace{r, \dots, r}_{p-5}, -r, 2r, 2r).$$

(iii)  $\dim(A) = p - 3$  and there exist  $t \in [0, p - 6]$ ,  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-4-t}, 2r, -(t+3)r, -(t+3)r).$$

(iv)  $\dim(A) = p - 3$  and there exist  $t \in [1, p - 4]$ ,  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-3-t}, -(t+1)r, -(t+2)r).$$

(v)  $p = 7$ ,  $\dim(A) = p - 3 = 4$  and there exists  $\sigma \in \mathfrak{S}_6$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(6)}) = (-1, 1, -2, 2, -3, 3).$$

(vi)  $\dim(A) = p - 2$ .

It turns out that  $\ell = p$  actually is the critical case for our reconstruction problem, since there are sequences  $A$  of  $p - 1$  nonzero elements in  $\mathbb{F}_p$  for which  $\mathcal{S}_A$  does not fully characterize  $A^\perp$ . However, we can prove there are essentially two families of such exceptions.

**Corollary 1.8.** *Let  $p$  be a prime. Let also  $A, B$  be two sequences of  $p - 1$  nonzero elements in  $\mathbb{F}_p$ . Then  $\mathcal{S}_A = \mathcal{S}_B$  if and only if  $A$  and  $B$  are either colinear or have one of the following forms.*

(i) There exist  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$ ,  $\lambda \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (r, \dots, r, r, 2r)$$

and

$$(b_{\sigma(1)}, \dots, b_{\sigma(p-1)}) = (\lambda r, \dots, \lambda r, 2\lambda r, \lambda r).$$

(ii) There exist  $t \in [1, p - 4]$ ,  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$ ,  $\lambda \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-3-t}, -(t+1)r, -(t+2)r)$$

and

$$(b_{\sigma(1)}, \dots, b_{\sigma(p-1)}) = (\underbrace{\lambda r, \dots, \lambda r}_t, \underbrace{-\lambda r, \dots, -\lambda r}_{p-3-t}, -(t+2)\lambda r, -(t+1)\lambda r).$$

(iii)  $p = 7$  and there exist  $\sigma \in \mathfrak{S}_6$ ,  $\lambda \in \mathbb{F}_7^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(6)}) = (-1, 1, -2, 2, -3, 3)$$

and

$$(b_{\sigma(1)}, \dots, b_{\sigma(6)}) = (-\lambda, \lambda, 3\lambda, -3\lambda, 2\lambda, -2\lambda).$$

As for the number of minimal elements in  $\mathcal{S}_A$  when  $\ell = p - 1$ , the following result easily follows from Theorem 1.7.

**Corollary 1.9.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_{p-1})$  be a sequence of  $p - 1$  nonzero elements in  $\mathbb{F}_p$ . Then  $\mathcal{S}_A$  contains at least  $p - 3$  minimal elements unless  $A$  has one of the following forms.*

(i) *There exists  $r \in \mathbb{F}_p^*$  such that*

$$(a_1, \dots, a_{p-1}) = (r, \dots, r).$$

(ii) *There exist  $\sigma \in \mathfrak{S}_{p-1}$  and  $r \in \mathbb{F}_p^*$  such that*

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (r, \dots, r, 2r).$$

The outline of the paper is as follows. In Section 2, we recall some useful tools. In Section 3, we introduce the notion of a ratio set, which makes it possible to deduce our Theorem 1.1 from the Combinatorial Nullstellensatz. In Section 4, we prove Theorem 1.4 and its corollaries. Our method is similar in nature to the one used in Section 3, except that a Vosper type theorem comes into play. In Section 5, this approach is further refined to solve our three problems in the case  $\ell = p - 1$ . Finally, in Section 6, we extend our results to the affine setting.

## 2. SOME TOOLS

In this section, we present a series of results we will use throughout the paper. As already mentioned, our method relies on the Combinatorial Nullstellensatz [1], a useful algebraic tool having a wide range of applications in Combinatorics.

**Theorem 2.1** (Alon [1]). *Let  $\mathbb{F}$  be an arbitrary field, and let  $P$  be a polynomial in  $\mathbb{F}[X_1, \dots, X_d]$ . Suppose that the degree of  $P$  is  $\sum_{i=1}^d t_i$  and the coefficient of  $\prod_{i=1}^d X_i^{t_i}$  is nonzero. Then, for any subsets  $S_1, \dots, S_d$  of  $\mathbb{F}$  with  $|S_i| > t_i$ , there exists  $(s_1, \dots, s_d) \in S_1 \times \dots \times S_d$  such that*

$$P(s_1, \dots, s_d) \neq 0.$$

In Additive Combinatorics, this theorem provides a unified way to estimate the cardinality of all kinds of sumsets in  $\mathbb{F}_p$ . These objects often are restrictions of the *Minkowski sum*

$$A + B = \{a + b : a \in A, b \in B\}$$

of two nonempty subsets  $A$  and  $B$  of  $\mathbb{F}_p$ . A collection of such estimates can be found in [10, Chapter 9]. For instance, a first corollary of Theorem 2.1 is the well-known Cauchy-Davenport Theorem.

**Theorem 2.2** (Cauchy-Davenport [3, 4, 5]). *Let  $p$  be a prime and let  $A, B$  be two nonempty subsets of  $\mathbb{F}_p$ . Then*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Let us mention that equality in Cauchy-Davenport Theorem only holds for highly structured sets, which are characterized by Vosper's Theorem [11, 12]. To be more precise, the essential part of Vosper's Theorem states that whenever  $|A|, |B| \geq 2$ , the relation

$$|A + B| = |A| + |B| - 1 < p - 1$$

holds if and only if  $A$  and  $B$  are arithmetic progressions with the same difference.

Another central object of interest in Additive Combinatorics is the set of subsums

$$\Sigma(A) = \sum_{i=1}^{\ell} \{0, a_i\}$$

of a sequence  $A = (a_1, \dots, a_\ell)$  over  $\mathbb{F}_p$ . Thanks to the properties of some binomial determinants, a sharp lower bound for the cardinality of the set of subsums could recently be deduced from the Combinatorial Nullstellensatz [2, Theorem 8]. To state this result, we require the following definition. For any element  $a \in \mathbb{F}_p^*$ , the total number of appearances of  $a$  and  $-a$  in the sequence  $A$  will be called the *multiplicity* of the pair  $\{a, -a\}$  in  $A$ .

**Theorem 2.3.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_\ell)$  be a sequence of  $\ell \geq 1$  nonzero elements in  $\mathbb{F}_p$ . Let also  $\ell_1 \geq \ell_2 \geq \dots \geq \ell_k$  denote the multiplicities of the pairs  $\{a, -a\}$  in  $A$ . Then*

$$|\Sigma(A)| \geq \min \left\{ p, 1 + \sum_{i=1}^k i\ell_i \right\}.$$

In this paper, we will also need structural information on sequences whose set of subsums is relatively small. For this purpose, the following two Vosper type results can easily be obtained from Theorem 2.3.

**Lemma 2.4.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_\ell)$  be a sequence of  $\ell \geq 1$  nonzero elements in  $\mathbb{F}_p$  such that*

$$|\Sigma(A)| = \ell + 1 < p.$$

*Then there exists  $r \in \mathbb{F}_p^*$  such that  $a_i \in \{\pm r\}$  for all  $i \in [1, \ell]$ .*

*Proof.* Denoting by  $\ell_1 \geq \ell_2 \geq \dots \geq \ell_k$  the multiplicities of the pairs  $\{a, -a\}$  in  $A$ , we readily obtain  $\sum_{i=1}^k \ell_i = \ell$ . Since  $\ell + 1 < p$ , Theorem 2.3 yields

$$1 + \sum_{i=1}^k i\ell_i \leq \ell + 1,$$

so that  $\sum_{i=1}^k (i-1)\ell_i = 0$ . Then  $\ell_1 = \ell$ , which is the desired result.  $\square$

Going one step further, we can also prove the following lemma.

**Lemma 2.5.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_\ell)$  be a sequence of  $\ell \geq 2$  nonzero elements in  $\mathbb{F}_p$  such that*

$$|\Sigma(A)| = \ell + 2 < p.$$

*Then one of the following two statements holds.*

- (i) *There exist  $r \in \mathbb{F}_p^*$  and  $i_0 \in [1, \ell]$  such that  $a_{i_0} \in \{\pm 2r\}$  and  $a_i \in \{\pm r\}$  for all  $i \neq i_0$ .*
- (ii) *One has  $\ell = 2$ .*

*Proof.* Denoting by  $\ell_1 \geq \ell_2 \geq \dots \geq \ell_k$  the multiplicities of the pairs  $\{a, -a\}$  in  $A$ , we readily obtain  $\sum_{i=1}^k \ell_i = \ell$ . Since  $\ell + 2 < p$ , Theorem 2.3 gives

$$1 + \sum_{i=1}^k i\ell_i \leq \ell + 2,$$

so that  $\sum_{i=1}^k (i-1)\ell_i \leq 1$ . Then either  $\ell_1 = \ell$  or  $(\ell_1, \ell_2) = (\ell-1, 1)$ . If  $\ell_1 = \ell$ , then there exists  $r \in \mathbb{F}_p^*$  such that  $a_i \in \{\pm r\}$  for all  $i \in [1, \ell]$ , which implies  $|\Sigma(A)| = \ell + 1$ , a contradiction. Now, suppose that  $(\ell_1, \ell_2) = (\ell-1, 1)$  and  $\ell > 2$ . Then there exist  $r \in \mathbb{F}_p^*$  and  $i_0 \in [1, \ell]$  such that  $a_i \in \{\pm r\}$  for all  $i \neq i_0$ . It follows that  $\Sigma(A \setminus (a_{i_0}))$

and  $a_{i_0} + \Sigma(A \setminus (a_{i_0}))$  both are arithmetic progressions of length  $\ell > 2$  with same difference  $r$ . Thus, for the equality  $|\Sigma(A)| = |\{0, a_{i_0}\} + \Sigma(A \setminus (a_{i_0}))| = \ell + 2$  to hold, we must have  $a_{i_0} \in \{\pm 2r\}$ .  $\square$

### 3. RATIO SETS AND LONG SEQUENCES

Let  $p$  be a prime and let  $A$  be a sequence of  $\ell \geq 1$  nonzero elements in  $\mathbb{F}_p$ . In this section, we describe first our general approach to proving  $\dim(A) = \ell - 1$ . Then, we prove Theorem 1.1 and its corollaries.

**3.1. Ratio sets.** Let  $p$  be a prime. Let also  $A = (a_1, \dots, a_\ell)$  and  $B = (b_1, \dots, b_\ell)$  be two sequences of  $\ell \geq 1$  elements in  $\mathbb{F}_p$  such that the elements of  $A$  are nonzero. For every  $\lambda \in \mathbb{F}_p$ , we consider the set

$$I_\lambda = \{i \in [1, \ell] : b_i/a_i = \lambda\}.$$

Any element  $\lambda \in \mathbb{F}_p$  such that  $I_\lambda \neq \emptyset$  will be called a *ratio* associated to  $(A, B)$ . Now, let  $\lambda_1, \dots, \lambda_d$  be the pairwise distinct ratios associated to  $(A, B)$ . For every  $i \in [1, d]$ , we define the subsequence

$$S_i = (a_j : j \in I_{\lambda_i}).$$

In particular, one has

$$\sum_{i=1}^d |S_i| = \ell.$$

Finally, for every  $i \in [1, d]$ , we introduce the *ratio set*

$$\Sigma_i = \Sigma(S_i).$$

It follows from Cauchy-Davenport Theorem that

$$(2) \quad |\Sigma_i| \geq \min\{p, |S_i| + 1\}.$$

In this paper, our main argument to prove that  $\dim(A) = \ell - 1$  is as follows. First, note that such an equality holds if and only if for every sequence  $B$  of  $\ell$  elements in  $\mathbb{F}_p$  such that  $\mathcal{S}_A \subset \mathcal{S}_B$ ,  $A$  and  $B$  are colinear, that is,  $d = 1$ . In order to prove that  $d = 1$ , properties of the ratio sets  $\Sigma_i$  will be deduced from the Combinatorial Nullstellensatz. Before stating our first result in this direction, we observe that the ratio sets  $\Sigma_i$  associated to  $(A, B)$  readily have the following interesting feature.

**Lemma 3.1.** *Let  $p$  be a prime. Let  $A, B$  be two sequences of  $\ell \geq 1$  elements in  $\mathbb{F}_p$  such that the elements of  $A$  are nonzero and  $\mathcal{S}_A \subset \mathcal{S}_B$ . Let also  $\lambda_1, \dots, \lambda_d$  be the ratios associated to  $(A, B)$ . Then  $\Sigma_i \cap (-\Sigma_j) = \{0\}$  for any two distinct elements  $i, j \in [1, d]$ .*

*Proof.* By definition, we readily have  $0 \in \Sigma_i$  for all  $i \in [1, d]$ . Now, assume there is an element  $s \in \Sigma_i \cap (-\Sigma_j)$  such that  $s \neq 0$ . By definition of  $\Sigma_i$  and  $\Sigma_j$ , there exist  $J_i \subset I_{\lambda_i}$  and  $J_j \subset I_{\lambda_j}$  such that  $\sum_{k \in J_i} a_k = s = -\sum_{k \in J_j} a_k$ . Since  $\mathcal{S}_A \subset \mathcal{S}_B$ , then

$$\sum_{k \in J_i} a_k + \sum_{k \in J_j} a_k = 0$$

yields

$$\sum_{k \in J_i} b_k + \sum_{k \in J_j} b_k = 0$$

which is equivalent to

$$\sum_{k \in J_i} \lambda_i a_k + \sum_{k \in J_j} \lambda_j a_k = 0$$

so that

$$(\lambda_i - \lambda_j)s = 0,$$

which is a contradiction.  $\square$

On the one hand, an immediate corollary of Lemma 3.1 is that whenever  $d \geq 2$ , one has  $|\Sigma_i| < p$  and  $|\Sigma_i| \geq |S_i| + 1$  for all  $i \in [1, d]$ , so that

$$(3) \quad \sum_{i=1}^d (|\Sigma_i| - 1) \geq \ell.$$

On the other hand, the ratio sets also have the following general property, which will be useful throughout the paper.

**Theorem 3.2.** *Let  $p$  be a prime. Let  $A, B$  be two sequences of  $\ell \geq 1$  elements in  $\mathbb{F}_p$  such that the elements of  $A$  are nonzero and  $\mathcal{S}_A \subset \mathcal{S}_B$ . Let also  $\lambda_1, \dots, \lambda_d$  be the ratios associated to  $(A, B)$ . If  $d \geq 2$ , then*

$$\sum_{i=1}^d (|\Sigma_i| - 1) \leq p.$$

In addition,  $\sum_{i=1}^d (|\Sigma_i| - 1) = p$  implies  $\sum_{i=1}^d \lambda_i (|\Sigma_i| - 1) = 0$  in  $\mathbb{F}_p$ .

*Proof.* Let  $\lambda_1, \dots, \lambda_d$  be the ratios associated to  $(A, B)$  and assume  $d \geq 2$ . We shall consider the polynomial

$$P(X_1, \dots, X_d) = \left( \sum_{i=1}^d \lambda_i X_i \right) \left( \left( \sum_{i=1}^d X_i \right)^{p-1} - 1 \right),$$

which has degree  $p$ . Since  $\mathcal{S}_A \subset \mathcal{S}_B$ ,  $P$  is easily seen to vanish on  $\prod_{i=1}^d \Sigma_i$ . In addition, the monomials of degree  $p$  in  $P$  are the same as those of

$$\begin{aligned} \left( \sum_{i=1}^d \lambda_i X_i \right) \left( \sum_{i=1}^d X_i \right)^{p-1} &= \left( \sum_{i=1}^d \lambda_i X_i \right) \left( \sum_{\substack{(t_1, \dots, t_d) \\ \sum_{i=1}^d t_i = p-1}} \frac{(p-1)!}{\prod_{i=1}^d t_i!} \prod_{i=1}^d X_i^{t_i} \right) \\ &= \sum_{i=1}^d \lambda_i X_i^p + \sum_{\substack{(t_1, \dots, t_d) \\ \sum_{i=1}^d t_i = p \\ \max\{t_i\} < p}} \frac{(p-1)!}{\prod_{i=1}^d t_i!} \left( \sum_{i=1}^d \lambda_i t_i \right) \prod_{i=1}^d X_i^{t_i}. \end{aligned}$$

Assume  $\sum_{i=1}^d (|\Sigma_i| - 1) > p$ . Then there exists  $(t_i)_{i \in [1, d]}$  such that  $\sum_{i=1}^d t_i = p$ , where  $0 \leq t_i \leq |\Sigma_i| - 1$  for all  $i \in [1, d]$ , and two distinct elements  $i_0, j_0 \in [1, d]$  such that  $t_{i_0} > 0$  and  $t_{j_0} < |\Sigma_{j_0}| - 1$ . We define  $(t'_i)_{i \in [1, d]}$  by  $t'_{i_0} = t_{i_0} - 1$ ,  $t'_{j_0} = t_{j_0} + 1$  and  $t'_i = t_i$  otherwise.

Now, suppose that the coefficients of  $\prod_{i=1}^d X_i^{t_i}$  and  $\prod_{i=1}^d X_i^{t'_i}$  in  $P$  both vanish. Then, both sums  $\sum_{i=1}^d \lambda_i t_i$  and  $\sum_{i=1}^d \lambda_i t'_i$  are zero, so that

$$\sum_{i=1}^d \lambda_i t_i - \sum_{i=1}^d \lambda_i t'_i = \lambda_{i_0} - \lambda_{j_0} = 0,$$

which is a contradiction. Thus, one of these coefficients is nonzero, and by Theorem 2.1,  $P$  cannot vanish on  $\prod_{i=1}^d \Sigma_i$ , a contradiction too. It follows that

$$\sum_{i=1}^d (|\Sigma_i| - 1) \leq p.$$



In addition, if one has  $\sum_{i=1}^d (|\Sigma_i| - 1) = p$ , then since  $P$  vanishes on  $\prod_{i=1}^d \Sigma_i$ , Theorem 2.1 implies that the coefficient of  $\prod_{i=1}^d X_i^{|\Sigma_i|-1}$  in  $P$  is zero, that is to say  $\sum_{i=1}^d \lambda_i (|\Sigma_i| - 1) = 0$  in  $\mathbb{F}_p$ .  $\square$

**3.2. The case of long sequences.** Thanks to Theorem 3.2, it is now easy to deduce our first theorem and its corollaries.

*Proof of Theorem 1.1.* Let  $A$  be a sequence of  $\ell > p$  nonzero elements in  $\mathbb{F}_p$ . For any given sequence  $B$  of  $\ell > p$  elements in  $\mathbb{F}_p$  such that  $\mathcal{S}_A \subset \mathcal{S}_B$ , let  $\lambda_1, \dots, \lambda_d$  be the ratios associated to  $(A, B)$  and assume  $d \geq 2$ . On the one hand, the inequality (3) implies that  $\sum_{i=1}^d (|\Sigma_i| - 1) \geq \ell > p$ . On the other hand, it follows from Theorem 3.2 that  $\sum_{i=1}^d (|\Sigma_i| - 1) \leq p$ , which is a contradiction. Therefore  $d = 1$ , and the desired result is proved.  $\square$

Corollary 1.2 now is a straightforward consequence of Theorem 1.1. In addition, one can easily notice that Corollary 1.3 follows directly from Theorem 1.1 and the following general proposition.

**Proposition 3.3.** *Let  $p$  be a prime and let  $A$  be a sequence of  $\ell \geq 1$  nonzero elements in  $\mathbb{F}_p$  such that  $\dim(A) = \ell - 1$ . Then there exists a basis of  $A^\perp$  consisting of minimal elements of  $\mathcal{S}_A$ .*

*Proof.* Let  $(e_1, \dots, e_{\ell-1})$  be a basis of  $A^\perp$  consisting of elements in  $\mathcal{S}_A$ . Let  $F$  be the set of all minimal elements in  $\mathcal{S}_A$  that are contained in at least one  $e_i$ . Now, since each  $e_i$  is a disjoint union of minimal elements in  $\mathcal{S}_A$ , we obtain  $\langle \mathcal{S}_A \rangle \subset \langle F \rangle \subset A^\perp$ . Since  $\dim(A) = \ell - 1$ , it follows that  $\langle F \rangle = A^\perp$  and  $F$  contains a basis of  $A^\perp$ .  $\square$

#### 4. SEQUENCES OF LENGTH $p$

Let  $p$  be a prime and let  $\ell \leq p$ . In this section, we introduce a special class of sequences  $A$  of  $\ell$  nonzero elements in  $\mathbb{F}_p$  for which  $\dim(A) < \ell - 1$  readily holds. In the case  $\ell = p$ , we determine all sequences in this class. We then refine the approach of Section 3 to prove that  $\dim(A) = p - 1$  for all remaining sequences.

**4.1. Exceptional and regular sequences.** Let  $A$  be a sequence of  $\ell \leq p$  nonzero elements in  $\mathbb{F}_p$ . Then,  $A$  will be called *exceptional* whenever there exist two distinct elements  $i, j \in [1, \ell]$  such that for all  $x \in \mathcal{S}_A$ , one has

$$|\{i, j\} \cap x| \in \{0, 2\}.$$

Any sequence which is not exceptional will be called *regular*. In others terms,  $A$  is a regular sequence if and only if for any two distinct elements  $i, j \in [1, \ell]$ , there is  $x \in \mathcal{S}_A$  such that  $i \in x$  and  $j \notin x$ .

On the one hand, regular sequences have the following useful property.

**Lemma 4.1.** *Let  $p$  be a prime. Let  $A$  be a regular sequence of  $\ell$  elements in  $\mathbb{F}_p^*$ , and  $B$  be a sequence of  $\ell$  elements in  $\mathbb{F}_p$  such that  $\mathcal{S}_A \subset \mathcal{S}_B$ . Then*

$$\forall i, j \in [1, \ell], (a_i = a_j) \implies (b_i = b_j).$$

*Proof.* Let  $i, j$  be two distinct elements of  $[1, \ell]$  such that  $a_i = a_j$ . Since  $A$  is regular, there exists  $x \in \mathcal{S}_A$  such that  $i \in x$  and  $j \notin x$ . Therefore,  $x' = (x \setminus \{i\}) \cup \{j\} \in \mathcal{S}_A$ . By assumption, it follows that  $x, x' \in \mathcal{S}_B$  and  $B \cdot x - B \cdot x' = b_i - b_j = 0$ , which is the desired result.  $\square$

On the other hand, one can notice that  $\dim(A) < \ell - 1$  readily holds whenever  $A$  is exceptional. However, it turns out that for large values of  $\ell$ , exceptional sequences are highly structured and can easily be determined. For instance, the following lemma fully characterizes all exceptional sequences in the case  $\ell = p$ .

**Proposition 4.2.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_p)$  be an exceptional sequence. Then one of the following statements holds.*

(i)  $\dim(A) = 1$  and there exists  $r \in \mathbb{F}_p^*$  such that

$$(a_1, \dots, a_p) = (r, \dots, r).$$

(ii)  $\dim(A) = p - 2$  and there exist  $t \in [1, p - 3]$ ,  $\sigma \in \mathfrak{S}_p$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p)}) = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-2-t}, -(t+1)r, -(t+1)r).$$

*Proof.* Since  $A$  is exceptional, there exist two distinct elements  $i, j \in [1, p]$  such that for all  $x \in \mathcal{S}_A$ , one has  $|\{i, j\} \cap x| \in \{0, 2\}$ . Now, let  $A'$  be the sequence obtained from  $A$  by deleting  $a_i$  and  $a_j$ . Then, Cauchy-Davenport Theorem gives

$$|\Sigma(A')| \geq \min\{p, (p-2) + 1\} = p - 1.$$

By assumption, one has  $-a_i \notin \Sigma(A')$  and  $-a_j \notin \Sigma(A')$ , so that  $|\Sigma(A')| = p - 1$  and  $a_i = a_j$ . Thus, by Lemma 2.4, there exists  $r \in \mathbb{F}_p^*$  such that  $a_k \in \{\pm r\}$  for all  $k \notin \{i, j\}$ . If  $a_k = r$  for all  $k \notin \{i, j\}$ , then one has  $-a_i = (p-1)r$ , which gives  $a_i = a_j = r$ . Therefore,  $A$  is of the form given in (i), and it can easily be checked that  $\dim(A) = p - 1$ . Note that the same conclusion holds if  $a_k = -r$  for all  $k \notin \{i, j\}$ . Otherwise, there is  $t \in [1, p - 3]$  such that  $A'$  consists of  $t$  copies of  $r$  and  $p - 2 - t$  copies of  $-r$ . In this case, we obtain  $a_i = a_j = -(t+1)r$ , so that, by relabelling if necessary,  $A$  is of the form given in (ii). The following table then gives a basis of  $\langle \mathcal{S}_A \rangle$ .

	$\overbrace{\hspace{2cm}}^t$			$\overbrace{\hspace{2cm}}^{p-2-t}$			
	$r$	$\dots$	$r$	$-r$	$\dots$	$-r$	$-(t+1)r$
$p-2-t$ {	1	$\dots$	$r$	1	$\dots$	(0)	$-(t+1)r$
	$\vdots$	(0)	$\dots$	$\ddots$	$\dots$	(0)	$-(t+1)r$
	1	$\dots$	$\ddots$	$\dots$	(0)	$\vdots$	(0)
	(0)	$\dots$	1	$\dots$	(0)	1	$-(t+1)r$
$t$ {	1	$\dots$	1	1	$\dots$	1	1

□

**4.2. A second property of ratio sets.** Before proving Theorem 1.4, we need the following general result on ratio sets, which will not only be useful in the case  $\ell = p$ , but in subsequent sections also.

**Proposition 4.3.** *Let  $p$  be a prime. Let  $A, B$  be two sequences of  $\ell \geq 1$  elements in  $\mathbb{F}_p$  such that the elements of  $A$  are nonzero and  $\mathcal{S}_A \subset \mathcal{S}_B$ . Let also  $\lambda_1, \dots, \lambda_d$  be the ratios associated to  $(A, B)$  and assume  $d \geq 2$ . Given any two distinct elements  $i_0, j_0 \in [1, d]$  and  $r_{i_0} \in \mathcal{S}_{i_0}$ , define*

$$\Sigma'_{i_0} = \Sigma(\mathcal{S}_{i_0} \setminus (r_{i_0})), \quad \Sigma'_{j_0} = \Sigma(\mathcal{S}_{j_0} \cup (r_{i_0})) = \Sigma_{j_0} + \{0, r_{i_0}\}$$

and  $\Sigma'_i = \Sigma_i$  otherwise. Then the polynomial

$$Q_{i_0, j_0}(X_1, \dots, X_d) = \left( \sum_{i=1}^d \lambda_i X_i \right) \left( \sum_{i=1}^d \lambda_i X_i - \chi \right) \left( \left( \sum_{i=1}^d X_i \right)^{p-1} - 1 \right),$$

where  $\chi = (\lambda_{j_0} - \lambda_{i_0})r_{i_0}$ , vanishes on  $\prod_{i=1}^d \Sigma'_i$ .

In addition, the coefficient of a monomial  $\prod_{i=1}^d X_i^{t_i}$  in  $Q_{i_0, j_0}$  with  $\sum_{i=1}^d t_i = p+1$  and  $\max\{t_i\} < p$  is

$$\frac{(p-1)!}{\prod_{i=1}^d t_i!} \left( \left( \sum_{i=1}^d \lambda_i t_i \right)^2 - \left( \sum_{i=1}^d \lambda_i^2 t_i \right) \right).$$

*Proof.* Since  $\mathcal{S}_A \subset \mathcal{S}_B$ , the polynomial

$$P(X_1, \dots, X_d) = \left( \sum_{i=1}^d \lambda_i X_i \right) \left( \left( \sum_{i=1}^d X_i \right)^{p-1} - 1 \right)$$

vanishes on  $\prod_{i=1}^d \Sigma_i$  and divides  $Q_{i_0, j_0}$ . Therefore,  $Q_{i_0, j_0}$  vanishes on  $\prod_{i=1}^d \Sigma_i$ .

Now, for any  $(x'_i)_{i \in [1, d]} \in \left( \prod_{i=1}^d \Sigma'_i \right) \setminus \left( \prod_{i=1}^d \Sigma_i \right)$ , let us consider  $(x_i)_{i \in [1, d]}$  defined by  $x_{i_0} = x'_{i_0} + r_{i_0}$ ,  $x_{j_0} = x'_{j_0} - r_{i_0}$  and  $x_i = x'_i$  otherwise, which is an element of  $\prod_{i=1}^d \Sigma_i$ . Note that  $\sum_{i=1}^d x'_i = \sum_{i=1}^d x_i$ . In addition, since  $\mathcal{S}_A \subset \mathcal{S}_B$ , the equality  $\sum_{i=1}^d x'_i = 0$  implies  $\sum_{i=1}^d \lambda_i x_i = 0$ , so that

$$\begin{aligned} \sum_{i=1}^d \lambda_i x'_i &= \lambda_{i_0} (x_{i_0} - r_{i_0}) + \lambda_{j_0} (x_{j_0} + r_{i_0}) + \sum_{\substack{i=1 \\ i \neq i_0, i \neq j_0}}^d \lambda_i x_i \\ &= (\lambda_{j_0} - \lambda_{i_0}) r_{i_0} + \sum_{i=1}^d \lambda_i x_i \\ &= (\lambda_{j_0} - \lambda_{i_0}) r_{i_0}, \end{aligned}$$

which proves that  $Q_{i_0, j_0}$  vanishes on  $\prod_{i=1}^d \Sigma'_i$ . Finally,  $Q_{i_0, j_0}$  clearly has degree  $p+1$  and the monomials of degree  $p+1$  in  $Q_{i_0, j_0}$  are the same as those of

$$\begin{aligned} & \left( \sum_{i=1}^d \lambda_i X_i \right)^2 \left( \sum_{i=1}^d X_i \right)^{p-1} \\ &= \left( \sum_{i=1}^d \lambda_i^2 X_i^2 + 2 \sum_{1 \leq i < j \leq d} \lambda_i \lambda_j X_i X_j \right) \left( \sum_{\substack{(t_1, \dots, t_d) \\ \sum_{i=1}^d t_i = p-1}} \frac{(p-1)!}{\prod_{i=1}^d t_i!} \prod_{i=1}^d X_i^{t_i} \right) \\ &= \sum_{i=1}^d \lambda_i^2 X_i^{p+1} + \sum_{i=1}^d \sum_{\substack{j=1 \\ j \neq i}}^d (-\lambda_i^2 + 2\lambda_i \lambda_j) X_i^p X_j \\ & \quad + \sum_{\substack{(t_1, \dots, t_d) \\ \sum_{i=1}^d t_i = p+1 \\ \max\{t_i\} < p}} \frac{(p-1)!}{\prod_{i=1}^d t_i!} \left( \sum_{i=1}^d \lambda_i^2 t_i (t_i - 1) + 2 \sum_{1 \leq i < j \leq d} \lambda_i \lambda_j t_i t_j \right) \prod_{i=1}^d X_i^{t_i} \\ &= \sum_{i=1}^d \lambda_i^2 X_i^{p+1} + \sum_{i=1}^d \sum_{\substack{j=1 \\ j \neq i}}^d \lambda_i (2\lambda_j - \lambda_i) X_i^p X_j \\ & \quad + \sum_{\substack{(t_1, \dots, t_d) \\ \sum_{i=1}^d t_i = p+1 \\ \max\{t_i\} < p}} \frac{(p-1)!}{\prod_{i=1}^d t_i!} \left( \left( \sum_{i=1}^d \lambda_i t_i \right)^2 - \left( \sum_{i=1}^d \lambda_i^2 t_i \right) \right) \prod_{i=1}^d X_i^{t_i}. \end{aligned}$$

□

**4.3. Proof of Theorem 1.4.** We can now prove the main result of this section and its corollaries.

*Proof of Theorem 1.4.* Let  $A$  be a sequence of  $p$  nonzero elements in  $\mathbb{F}_p$  not being of the forms given in (i) or (ii). Thanks to Proposition 4.2, we can assume that  $A$  is regular. For any given sequence  $B$  of  $p$  elements in  $\mathbb{F}_p$  such that  $\mathcal{S}_A \subset \mathcal{S}_B$ , let  $\lambda_1, \dots, \lambda_d$  be the ratios associated to  $(A, B)$  and assume  $d \geq 2$ . On the one hand, (3) implies that  $\sum_{i=1}^d (|\Sigma_i| - 1) \geq p$ . On the other hand, it follows from Theorem 3.2 that  $\sum_{i=1}^d (|\Sigma_i| - 1) \leq p$ , which yields

$$\sum_{i=1}^d (|\Sigma_i| - 1) = p \quad \text{and} \quad \sum_{i=1}^d \lambda_i (|\Sigma_i| - 1) = 0 \text{ in } \mathbb{F}_p.$$

Suppose that  $d = 2$ . Since  $|\Sigma_1| + |\Sigma_2| \geq p + 2$ , we obtain  $|\Sigma_1 \cap (-\Sigma_2)| \geq 2$ , which would contradict Lemma 3.1. From now on, we thus assume  $d \geq 3$ . Since  $A$  is regular, Lemmas 3.1 and 4.1 give  $|\Sigma_i| < p - 1$  for all  $i \in [1, d]$ . It follows that  $|\Sigma_i| = |S_i| + 1$  for all  $i \in [1, d]$ , and Lemma 2.4 implies that there exists  $r_i \in \mathbb{F}_p^*$  such that all elements of  $S_i$  are equal to  $r_i$  or  $-r_i$ .

For any two distinct elements  $i_0, j_0 \in [1, d]$  and any  $r_{i_0} \in S_{i_0}$ , let us consider the sets  $\Sigma'_i$  defined by

$$\Sigma'_{i_0} = \Sigma(S_{i_0} \setminus (r_{i_0})), \quad \Sigma'_{j_0} = \Sigma(S_{j_0} \cup (r_{i_0})) = \Sigma_{j_0} + \{0, r_{i_0}\}$$

and  $\Sigma'_i = \Sigma_i$  otherwise. Let also  $Q_{i_0, j_0}$  be as in Proposition 4.3.

Since  $\Sigma_{i_0}$  is an arithmetic progression with difference  $r_{i_0}$ , one has  $|\Sigma'_{i_0}| = |\Sigma_{i_0}| - 1$ . In addition, since  $A$  is regular, Lemmas 3.1 and 4.1 imply that  $r_{i_0} \neq \pm r_{j_0}$ . It follows from Lemma 2.4 that  $|\Sigma'_{j_0}| \geq |\Sigma_{j_0}| + 2$ .

We now define  $(t_i)_{i \in [1, d]}$  by  $t_{i_0} = |\Sigma_{i_0}| - 2$ ,  $t_{j_0} = |\Sigma_{j_0}| + 1$  and  $t_i = |\Sigma_i| - 1$  otherwise. In particular,  $t_i \leq |\Sigma'_i| - 1 < p$  for all  $i \in [1, d]$  and  $\sum_{i=1}^d t_i = p + 1$ . Since  $\sum_{i=1}^d \lambda_i (|\Sigma_i| - 1) = 0$  in  $\mathbb{F}_p$ , Proposition 4.3 implies that, up to a nonzero multiplicative constant, the coefficient of  $\prod_{i=1}^d X_i^{t_i}$  in  $Q_{i_0, j_0}$  is

$$\begin{aligned} \left( \sum_{i=1}^d \lambda_i t_i \right)^2 - \left( \sum_{i=1}^d \lambda_i^2 t_i \right) &= (2\lambda_{j_0} - \lambda_{i_0})^2 - \left( 2\lambda_{j_0}^2 - \lambda_{i_0}^2 + \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1) \right) \\ &= (2\lambda_{j_0}^2 - 4\lambda_{i_0}\lambda_{j_0} + 2\lambda_{i_0}^2) - \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1) \\ &= 2(\lambda_{j_0} - \lambda_{i_0})^2 - \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1). \end{aligned}$$

Note that  $\sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1)$  is independent of  $i_0$  and  $j_0$ . In addition, the coefficient of  $\prod_{i=1}^d X_i^{t_i}$  in  $Q_{i_0, j_0}$  is zero if and only if

$$(\lambda_{j_0} - \lambda_{i_0})^2 = \frac{1}{2} \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1).$$

Since  $d \geq 3$ , there is at least one pair  $(i_0, j_0)$  such that this equality does not hold. It follows from Theorem 2.1 that for this actual pair,  $Q_{i_0, j_0}$  cannot vanish on  $\prod_{i=1}^d \Sigma'_i$ , which contradicts Proposition 4.3. □

*Proof of Corollary 1.5.* Let  $A, B$  be two sequences of  $p$  nonzero elements in  $\mathbb{F}_p$ . One direction of the implication is trivial. Thus, we shall prove that  $A$  and  $B$  are colinear whenever  $\mathcal{S}_A = \mathcal{S}_B$ . By Theorem 1.4, there are three cases to consider. If  $\dim(A) = p - 1$ , then  $\mathcal{S}_A \subset \mathcal{S}_B$  already implies the required result. If  $A$  is constant, it is also easily seen that  $\mathcal{S}_A = \mathcal{S}_B$  holds if and only if  $B$  is constant. Otherwise,  $A$  and  $B$  both are of the form given in Theorem 1.4 (ii). In particular, there exist  $t \in [1, p - 3]$  and  $r \in \mathbb{F}_p^*$  such that, by relabelling if necessary, one has

$$A = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-2-t}, -(t+1)r, -(t+1)r).$$

Since  $\mathcal{S}_A \subset \mathcal{S}_B$ , we deduce that

$$B = (\underbrace{\lambda r, \dots, \lambda r}_t, \underbrace{-\lambda r, \dots, -\lambda r}_{p-2-t}, -(t+1)\lambda r + d, -(t+1)\lambda r - d),$$

for some  $\lambda \in \mathbb{F}_p^*$  and  $d \in \mathbb{F}_p$ . Thus,  $B$  is of the form given in Theorem 1.4 (ii) if and only if  $d = 0$ , which completes the proof.  $\square$

*Proof of Corollary 1.6.* Let  $A$  be a nonconstant sequence of  $p$  nonzero elements in  $\mathbb{F}_p$ . By Theorem 1.4, there are two cases to consider. If  $\dim(A) = p - 1$ , the required result directly follows from Proposition 3.3. Otherwise, there exist  $t \in [1, p - 3]$  and  $r \in \mathbb{F}_p^*$  such that  $A$  consists of  $t$  copies of  $r$ ,  $p - 2 - t$  copies of  $-r$  and two copies of  $-(t + 1)r$ . Denoting the minimum and maximum of  $t$  and  $p - 2 - t$  by  $m$  and  $M$  respectively, it is easily seen that the number of minimal elements in  $\mathcal{S}_A$  is

$$mM + \binom{M}{m}.$$

Now, if  $t \in [2, p - 4]$ , then  $p \geq 7$  and  $\mathcal{S}_A$  contains at least  $2(p - 4) \geq p - 1$  minimal elements. If  $t \in \{1, p - 3\}$ , then  $p \geq 5$  and  $\mathcal{S}_A$  contains exactly  $2(p - 3) \geq p - 1$  minimal elements, which completes the proof.  $\square$

## 5. SEQUENCES OF LENGTH $p - 1$

Let  $p$  be prime and let  $A$  be a sequence of  $p - 1$  nonzero elements in  $\mathbb{F}_p$ . In this section, we start by showing that the dimension and structure of  $A$  can easily be deduced from Theorem 1.4 whenever  $\sigma(A) \neq 0$ . Then, we concentrate on the case where  $\sigma(A) = 0$  and prove Theorem 1.7 as follows. On the one hand, we determine all exceptional zero-sum sequences. On the other hand, we further refine our general approach to handle the case of regular zero-sum sequences.

**5.1. The case of nonzero-sum sequences.** Given a sequence  $A = (a_1, \dots, a_\ell)$  of  $\ell \geq 1$  nonzero elements in  $\mathbb{F}_p$  such that  $\sigma(A) \neq 0$ , we consider the sequence  $A' = (a_1, \dots, a_\ell, -\sigma(A))$ . The aim of the following lemma is to show that the value of  $\dim(A)$  can easily be derived from  $\dim(A')$ .

**Lemma 5.1.** *Let  $p$  be a prime and let  $A$  be a sequence of  $\ell \geq 1$  nonzero elements in  $\mathbb{F}_p$  such that  $\sigma(A) \neq 0$ . Then  $A'$  is a zero-sum sequence and*

$$\dim(A') = \dim(A) + 1.$$

*Proof.* Let us set  $X = \{(x_1, \dots, x_{\ell+1}) \in \mathcal{S}_{A'} : x_{\ell+1} = 0\}$ . We clearly have  $\sigma(A') = 0$ , which implies that  $\mathcal{S}_{A'}$  is closed under complement. Therefore,

$$\langle \mathcal{S}_{A'} \rangle = \langle X \cup \{(1, \dots, 1)\} \rangle.$$

In addition, it follows from the very definition of  $X$  that  $(1, \dots, 1) \in \mathcal{S}_{A'} \setminus \langle X \rangle$  and  $\dim(X) = \dim(A)$ . Thus,

$$\dim(A') = \dim(\langle \mathcal{S}_{A'} \rangle) = \dim(X) + 1 = \dim(A) + 1,$$

which completes the proof.  $\square$

In particular, Lemma 5.1 implies that for every sequence  $A$  of  $p - 1$  nonzero elements in  $\mathbb{F}_p$  such that  $\sigma(A) \neq 0$ , then either  $\dim(A) = p - 2$ , or  $\dim(A) = 0$  and  $A$  is constant, or  $\dim(A) = p - 3$  and  $A$  can be obtained by deleting any element in a sequence of type (ii) in Theorem 1.4.

The reconstruction problems on  $A$  and  $A'$  are also closely related to each other.

**Lemma 5.2.** *Let  $p$  be a prime and let  $A, B$  be two sequences of  $\ell \geq 1$  nonzero elements in  $\mathbb{F}_p$  such that  $\sigma(A) \neq 0$ . Then  $\mathcal{S}_{A'} = \mathcal{S}_{B'}$  if and only if  $\mathcal{S}_A = \mathcal{S}_B$ .*

*Proof.* Since  $\sigma(A') = 0$ , the desired result is a straightforward consequence of the fact that  $\mathcal{S}_{A'}$  is closed under complement.  $\square$

For instance, let  $A, B$  be two sequences of  $p - 1$  nonzero elements in  $\mathbb{F}_p$  such that  $\sigma(A) \neq 0$  and  $\mathcal{S}_A = \mathcal{S}_B$ . Specifying  $\ell = p - 1$  in Lemma 5.2, we obtain that  $\mathcal{S}_{A'} = \mathcal{S}_{B'}$ . Then, it easily follows from Corollary 1.5 that  $A'$  and  $B'$  are colinear, and so are  $A$  and  $B$ . From now on, we thus consider zero-sum sequences only.

**5.2. The case of exceptional zero-sum sequences.** We now state and prove the following lemma, which fully characterizes all exceptional zero-sum sequences in the case  $\ell = p - 1$ .

**Proposition 5.3.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_{p-1})$  be an exceptional zero-sum sequence. Then one of the following statements holds.*

(i)  $\dim(A) = 1$  and there exist  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (r, \dots, r, 2r).$$

(ii)  $\dim(A) = p - 4$  and there exist  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (\underbrace{r, \dots, r}_{p-5}, -r, 2r, 2r).$$

(iii)  $\dim(A) = p - 3$  and there exist  $t \in [0, p - 6]$ ,  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-4-t}, 2r, -(t+3)r, -(t+3)r).$$

(iv)  $\dim(A) = p - 3$  and there exist  $t \in [1, p - 4]$ ,  $\sigma \in \mathfrak{S}_{p-1}$ ,  $r \in \mathbb{F}_p^*$  such that

$$(a_{\sigma(1)}, \dots, a_{\sigma(p-1)}) = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-3-t}, -(t+1)r, -(t+2)r).$$

*Proof.* Since  $A$  is exceptional, there exist two distinct elements  $i, j \in [1, p - 1]$  such that for all  $x \in \mathcal{S}_A$ , one has  $|\{i, j\} \cap x| \in \{0, 2\}$ . Now, let  $A'$  be the sequence obtained from  $A$  by deleting  $a_i$  and  $a_j$ . Then, Cauchy-Davenport Theorem gives

$$|\Sigma(A')| \geq \min\{p, (p - 3) + 1\} = p - 2.$$

By assumption, one has  $-a_i \notin \Sigma(A')$  and  $-a_j \notin \Sigma(A')$ . We now consider two cases.

- $|\Sigma(A')| = p - 2$ . Then, by Lemma 2.4, there exist  $t \in [0, p - 3]$  and  $r \in \mathbb{F}_p^*$  such that  $A'$  consists of  $t$  copies of  $r$  and  $p - 3 - t$  copies of  $-r$ . Therefore, we obtain that  $\{a_i, a_j\} = \{-(t+1)r, -(t+2)r\}$ . If  $a_i = a_j$ , then  $a_i + a_j \in \{-2(t+1)r, -2(t+2)r\}$ . Since  $\sigma(A') = (2t+3)r$ , we would have  $\sigma(A) \neq 0$ , which is a contradiction. Thus, one has  $a_i \neq a_j$  and, by relabelling if necessary, it follows that either  $t \in \{0, p - 3\}$  and  $A$  is of the form given in (i), or  $t \in [1, p - 4]$  and  $A$  is of the form given in (iv).

- $|\Sigma(A')| = p - 1$ . Then,  $a_i = a_j$  and by Lemma 2.5, there exist  $t \in [0, p - 4]$  and  $r \in \mathbb{F}_p^*$  such that  $A'$  consists of  $t$  copies of  $r$ ,  $p - 4 - t$  copies of  $-r$  and one copy of  $2r$ . If  $t = p - 4$ , then  $\Sigma(A') = \mathbb{F}_p \setminus \{-r\}$  and  $a_i = a_j = r$ , so that  $A$  is of the

form given in (i). If  $t = p - 5$ , then  $\Sigma(A') = \mathbb{F}_p \setminus \{-2r\}$ ,  $a_i = a_j = 2r$  and  $A$  is of the form given in (ii). Otherwise, one has  $t \in [0, p - 6]$ ,  $\Sigma(A') = \mathbb{F}_p \setminus \{(t + 3)r\}$ ,  $a_i = a_j = -(t + 3)r$ , and  $A$  is of the form given in (iii).

The following tables give a basis of  $\langle \mathcal{S}_A \rangle$  for cases (ii) to (iv).

(ii)  $\dim(A) = p - 4$ .

$$p-5 \left\{ \begin{array}{c|ccc|ccc} & \overbrace{r \ \dots \ r}^{p-5} & & -r & 2r & 2r & 2r \\ \hline 1 & & (0) & 1 & & & \\ \vdots & \ddots & & \vdots & & (0) & \\ (0) & & 1 & 1 & & & \\ \hline 1 & \dots & 1 & 1 & 1 & 1 & 1 \end{array} \right.$$

(iii)  $\dim(A) = p - 3$  and  $t \in [1, p - 6]$ .

$$p-4-t \left\{ \begin{array}{c|ccc|ccc|cc} & \overbrace{r \ \dots \ r}^t & & \overbrace{-r \ \dots \ -r}^{p-4-t} & & 2r & & -(t+3)r & -(t+3)r \\ \hline 1 & & & 1 & & (0) & & & \\ \vdots & (0) & & & \ddots & & & & \\ 1 & & & & & 1 & (0) & (0) & (0) \\ \vdots & & & & & \vdots & & & \\ (0) & \ddots & & (0) & & 1 & & & \\ \hline & (0) & & 1 & (0) & 1 & 1 & 0 & 0 \\ \hline 1 & \dots & 1 & 1 & \dots & 1 & 1 & 1 & 1 \end{array} \right.$$

$$t \left\{ \begin{array}{c} (0) \\ \vdots \\ (0) \end{array} \right.$$

And whenever  $t = 0$ ,

$$p-5 \left\{ \begin{array}{c|ccc|cc} & \overbrace{-r \ -r \ \dots \ -r}^{p-4} & & 2r & -3r & -3r \\ \hline 1 & 1 & & (0) & & \\ \vdots & & \ddots & & (0) & (0) \\ 1 & (0) & & 1 & & \\ \hline 0 & 1 & (0) & 1 & 0 & 0 \\ \hline 1 & 1 & \dots & 1 & 1 & 1 \end{array} \right.$$

(iv)  $\dim(A) = p - 3$  and  $t \in [1, p - 4]$ .

$$p-3-t \left\{ \begin{array}{c|ccc|ccc} & \overbrace{r \ \dots \ r}^t & & \overbrace{-r \ \dots \ -r}^{p-3-t} & & -(t+1)r & -(t+2)r \\ \hline 1 & & & 1 & & (0) & \\ \vdots & (0) & & & \ddots & & \\ 1 & & & & & 1 & (0) & (0) \\ \vdots & & & & & \vdots & & \\ (0) & \ddots & & (0) & & 1 & & \\ \hline 1 & \dots & 1 & 1 & \dots & 1 & 1 & 1 \end{array} \right.$$

$$t \left\{ \begin{array}{c} (0) \\ \vdots \\ (0) \end{array} \right.$$

□

**5.3. Preliminary results.** In the proof of Theorem 1.7, we will need the following two lemmas to deal with the cases where the number of distinct ratios is small. The first one gives some nonvanishing properties of a particular quadratic polynomial.

**Lemma 5.4.** *Let  $p \geq 5$  be a prime. Given  $u, v \in \mathbb{F}_p$ , let  $f$  be the quadratic polynomial*

$$f(x, y) = 2x^2 - 6xy + 6y^2 + 2u(3y - x) + v.$$

*Then, for any three pairwise distinct elements  $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_p$ , there exists  $\sigma \in \mathfrak{S}_3$  such that one of the following holds.*

- (i)  $f(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}) f(\alpha_{\sigma(1)}, \alpha_{\sigma(3)}) \neq 0$ ,
- (ii)  $f(\alpha_{\sigma(2)}, \alpha_{\sigma(1)}) f(\alpha_{\sigma(3)}, \alpha_{\sigma(1)}) \neq 0$ ,
- (iii)  $f(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}) f(\alpha_{\sigma(2)}, \alpha_{\sigma(1)}) \neq 0$ ,
- (iv)  $f(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}) f(\alpha_{\sigma(2)}, \alpha_{\sigma(3)}) f(\alpha_{\sigma(3)}, \alpha_{\sigma(1)}) \neq 0$ .

*Proof.* It is an easy exercise to show that, up to a nonzero multiplicative constant, the only quadratic polynomial vanishing on the six points  $(\alpha_1, \alpha_2)$ ,  $(\alpha_2, \alpha_1)$ ,  $(\alpha_1, \alpha_3)$ ,  $(\alpha_3, \alpha_1)$ ,  $(\alpha_2, \alpha_3)$  and  $(\alpha_3, \alpha_2)$  is

$$x^2 + y^2 + xy - (x + y)(\alpha_1 + \alpha_2 + \alpha_3) + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3).$$

Thus, there exist two distinct elements  $i, j \in \{1, 2, 3\}$  such that  $f(\alpha_i, \alpha_j) \neq 0$ . Now, let  $k$  be the remaining element of  $\{1, 2, 3\}$  and assume that for all  $\sigma \in \mathfrak{S}_3$ , none of the properties (i) to (iv) holds. Then one has  $f(\alpha_j, \alpha_i) = 0$ ,  $f(\alpha_i, \alpha_k) = 0$  and  $f(\alpha_k, \alpha_j) = 0$ . In addition, since  $f(\alpha_i, \alpha_j) f(\alpha_j, \alpha_k) f(\alpha_k, \alpha_i) = 0$ , we have that either  $f(\alpha_j, \alpha_k) = 0$  or  $f(\alpha_k, \alpha_i) = 0$ . Therefore, there exists  $\sigma \in \mathfrak{S}_3$  such that

$$f(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}) = f(\alpha_{\sigma(2)}, \alpha_{\sigma(1)}) = f(\alpha_{\sigma(1)}, \alpha_{\sigma(3)}) = f(\alpha_{\sigma(3)}, \alpha_{\sigma(2)}) = 0.$$

Without loss of generality, we may assume that  $\sigma$  is the identity, so that

$$\begin{aligned} f(\alpha_1, \alpha_2) - f(\alpha_2, \alpha_1) &= 0 \iff -4(\alpha_1 - \alpha_2)(\alpha_1 + \alpha_2 + 2u) = 0 \\ f(\alpha_1, \alpha_2) - f(\alpha_1, \alpha_3) &= 0 \iff 6(\alpha_2 - \alpha_3)(-\alpha_1 + \alpha_2 + \alpha_3 + u) = 0 \\ f(\alpha_1, \alpha_2) - f(\alpha_3, \alpha_2) &= 0 \iff 2(\alpha_1 - \alpha_3)(\alpha_1 - 3\alpha_2 + \alpha_3 - u) = 0. \end{aligned}$$

Since  $\alpha_1, \alpha_2, \alpha_3$  are pairwise distinct, they are solution of the linear system

$$\begin{cases} \alpha_1 + \alpha_2 &= -2u \\ -\alpha_1 + \alpha_2 + \alpha_3 &= -u \\ \alpha_1 - 3\alpha_2 + \alpha_3 &= u. \end{cases}$$

Since  $p \geq 5$ , the determinant of this system is  $6 \neq 0$  in  $\mathbb{F}_p$ . Therefore, this system has a unique solution, which is easily seen to be  $\alpha_1 = \alpha_2 = \alpha_3 = -u$ . This contradicts the fact that  $\alpha_1, \alpha_2, \alpha_3$  are pairwise distinct, and the proof is complete.  $\square$

Our second lemma gives the structure of a pair of arithmetic progressions covering almost all  $\mathbb{F}_p$ , but intersecting in only one element.

**Lemma 5.5.** *Let  $p$  be a prime. Let also  $P_1$  and  $P_2$  be two arithmetic progressions in  $\mathbb{F}_p$  with distinct differences, such that  $\min\{|P_1|, |P_2|\} \geq 3$  and  $P_1 \cap P_2 = \{0\}$ .*

• *If  $|P_1| + |P_2| = p$ , then there exists  $r \in \mathbb{F}_p^*$  such that  $P_1$  and  $P_2$  have one of the following forms.*

- (1)  $\{0, 2, 4\}.r$  and  $\{5, 6, \dots, p-1, 0, 1\}.r$ ,
- (2)  $\{-\frac{p-1}{2}, 0, \frac{p-1}{2}\}.r$  and  $\{-\frac{p-5}{2}, -\frac{p-7}{2}, \dots, \frac{p-5}{2}, \frac{p-3}{2}\}.r$ .

• *If  $|P_1| + |P_2| = p-1$ , then there exists  $r \in \mathbb{F}_p^*$  such that  $P_1$  and  $P_2$  have one of the following forms.*

- (3)  $\{0, 2, 4\}.r$  and  $\{5, 6, \dots, p-1, 0\}.r$ ,
- (4)  $\{0, 2, 4\}.r$  and  $\{6, 7, \dots, p-1, 0, 1\}.r$ ,
- (5)  $\{0, 2, 4, 6\}.r$  and  $\{7, 8, \dots, p-1, 0, 1\}.r$ ,
- (6)  $\{0, 3, 6\}.r$  and  $\{7, 8, \dots, 0, 1, 2\}.r$ ,
- (7)  $\{-\frac{p-1}{2}, 0, \frac{p-1}{2}\}.r$  and  $\{-\frac{p-5}{2}, -\frac{p-7}{2}, \dots, \frac{p-7}{2}, \frac{p-5}{2}\}.r$ ,



- (8)  $\{-\frac{p-1}{2}, 0, \frac{p-1}{2}\}.r$  and  $\{-\frac{p-7}{2}, -\frac{p-9}{2}, \dots, \frac{p-5}{2}, \frac{p-3}{2}\}.r$ ,  
(9)  $\{-\frac{p-3}{2}, 0, \frac{p-3}{2}\}.r$  and  $\{-\frac{p-5}{2}, -\frac{p-7}{2}, \dots, \frac{p-7}{2}, \frac{p-5}{2}\}.r$ ,  
(10)  $p = 11$  and  
(a)  $\{-6, -3, 0, 3, 6\}.r$  and  $\{-2, -1, 0, 1, 2\}.r$ ,  
(b)  $\{-4, 0, 4, 8\}.r$  and  $\{-2, -1, 0, 1, 2, 3\}.r$ ,  
(c)  $\{-8, -4, 0, 4, 8\}.r$  and  $\{-2, -1, 0, 1, 2\}.r$ ,  
(11)  $p = 13$  and  $\{-8, -4, 0, 4, 8\}.r$  and  $\{-3, -2, -1, 0, 1, 2, 3\}.r$ .

*Proof.* Without loss of generality, we can suppose that  $|P_1| \geq |P_2|$ . Since  $|P_1| + |P_2| \geq p - 1$ , one has  $|P_1| \geq (p - 1)/2$ . Up to a nonzero multiplicative constant, we can also assume that  $P_1$  has difference 1. Now, we set

$$P_2 = \{-\beta d, \dots, -d, 0, d, \dots, \alpha d\},$$

where  $\alpha$  and  $\beta$  are two nonnegative integers. Note that replacing  $(d, \alpha, \beta)$  by  $(-d, \beta, \alpha)$  yields the same arithmetic progression, so we may assume that  $d \in [2, (p - 1)/2]$ . In addition,  $P_1$  and  $P_2$  satisfy the hypothesis of the lemma if and only if  $-P_1$  and  $-P_2$  do so, which allows us to suppose that  $d \in P_2$ , that is  $\alpha \geq 1$ . Since  $P_1 \cap P_2 = \{0\}$ , we obtain that

$$P_1 = \{p - (|P_1| - (t + 1)), \dots, p - 1, 0, 1, \dots, t\},$$

where  $0 \leq t < d$ .

We consider first the case where  $\beta = 0$ . Then,  $P_2 = \{0, d, \dots, \alpha d\}$  and  $\alpha \geq 2$ . Also, there exists a unique pair of integers  $(q, u)$  such that

$$p - (|P_1| - (t + 1)) = qd + u \quad \text{and} \quad 1 \leq u \leq d.$$

Since  $P_1 \cap P_2 = \{0\}$ , we have  $qd + u \geq \alpha d + 1$ . Now, counting separately the missing elements of  $P_1 \cup P_2$  in the three intervals  $[0, d]$ ,  $[d + 1, \alpha d - 1]$  and  $[\alpha d, p - 1]$ , we obtain that

$$|\mathbb{F}_p \setminus (P_1 \cup P_2)| = ((d - 1) - t) + (\alpha - 1)(d - 1) + ((qd + u) - (\alpha d + 1)).$$

Since  $\alpha, d \geq 2$ , one has  $(\alpha - 1)(d - 1) \geq 1$ . We now distinguish two cases.

- In the case  $|P_1| + |P_2| = p$ , one has  $|P_1 \cup P_2| = p - 1$ , so that  $\alpha = d = q = 2$  and  $u = t = 1$ . This is the structure of case (1) in the statement of the lemma.
- In the case  $|P_1| + |P_2| = p - 1$ , one has  $|P_1 \cup P_2| = p - 2$ , so that  $(qd + u) - (\alpha d + 1) \leq 1$ , which implies  $\alpha = q$ .
  - If  $q = 2$  and  $d = 2$ , one has either  $u = 1$  and  $t = 0$ , this is case (3), or  $u = 2$  and  $t = 1$ , this is case (4).
  - If  $q = 3$  and  $d = 2$ , one has  $u = 1$  and  $t = 1$ , this is case (5).
  - If  $q = 2$  and  $d = 3$ , one has  $u = 1$  and  $t = 2$ , this is case (6).

We now turn to the case where  $\beta \geq 1$ . Since  $P_1 \subset [-d + 1, d - 1]$ , one has

$$\frac{p - 1}{2} \leq |P_1| \leq 2d - 1.$$

- If  $|P_2| = 3$ , then either  $|P_1| = p - 3$  and  $d = (p - 1)/2$ , which is case (2), or  $|P_1| = p - 4$  and  $d \in \{(p - 3)/2, (p - 1)/2\}$ , which yields cases (7), (8), (9).
- If  $|P_2| \geq 4$ , then  $\alpha \geq 2$  or  $\beta \geq 2$ . Therefore, one of the two intervals  $[d + 1, 2d - 1]$  and  $[-2d + 1, -d - 1]$  has to be disjoint from  $P_1$ . Such an interval can contain at most one element of  $P_2$ , and thus contains at least  $d - 2$  elements being neither in  $P_1$  nor in  $P_2$ . Since  $|P_1| + |P_2| \geq p - 1$  and  $|P_1 \cap P_2| = 1$ , one has  $|P_1 \cup P_2| \geq p - 2$  and then  $d - 2 \leq 2$ .
  - If  $d = 2$ , then  $4 \leq |P_2| \leq |P_1| \leq 3$ , a contradiction.
  - If  $d = 3$ , then  $p \leq 11$  and  $4 \leq |P_2| \leq |P_1| \leq 5$ . Since  $|P_1| + |P_2| \geq 8$ , it follows that  $p = 11$  and  $|P_1| = |P_2| = 5$ , which gives (10.a).

- If  $d = 4$ , then  $p \leq 15$  and  $4 \leq |P_2| \leq |P_1| \leq 7$ . Since  $|P_1| + |P_2| \geq 8$ , it follows that either  $p = 11$  and (10.b) or (10.c) holds, or  $p = 13$  and (11) holds.

□

**5.4. Proof of Theorem 1.7.** We can now prove the last of our main theorems.

*Proof of Theorem 1.7.* Let  $A = (a_1, \dots, a_{p-1})$  be a zero-sum sequence of  $p - 1$  nonzero elements in  $\mathbb{F}_p$  not being of the forms given in (i) to (iv). Thanks to Proposition 5.3, we can assume that  $A$  is regular. For any given sequence  $B$  of  $p - 1$  elements in  $\mathbb{F}_p$  such that  $\mathcal{S}_A \subset \mathcal{S}_B$ , let  $\lambda_1, \dots, \lambda_d$  be the ratios associated to  $(A, B)$  and assume  $d \geq 2$ . On the one hand, the inequality (3) implies that  $\sum_{i=1}^d (|\Sigma_i| - 1) \geq p - 1$ . On the other hand, it follows from Theorem 3.2 that  $\sum_{i=1}^d (|\Sigma_i| - 1) \leq p$ , which yields

$$\sum_{i=1}^d (|\Sigma_i| - 1) \in \{p - 1, p\}.$$

**Case 1:**  $d = 2$ .

By Lemma 3.1, one has  $0 \notin (\Sigma_1 \setminus \{0\}) + \Sigma_2$  and Cauchy-Davenport Theorem implies that

$$|(\Sigma_1 \setminus \{0\}) + \Sigma_2| \geq (|\Sigma_1| - 1) + (|\Sigma_2| - 1) \geq |S_1| + |S_2| = p - 1.$$

Therefore, one has  $|\Sigma_i| = |S_i| + 1$  for each  $i \in \{1, 2\}$ . Since  $|\Sigma_i| < p$  by Lemma 3.1, it follows from Lemma 2.4 that there exists  $r_i \in \mathbb{F}_p^*$  such that all elements of  $S_i$  are equal to  $r_i$  or  $-r_i$ . In addition, since  $A$  is a zero-sum sequence, Lemma 3.1 yields  $\sigma(S_1) = \sigma(S_2) = 0$ , so that  $r_i$  occurs as many times as  $-r_i$  in  $S_i$ .

Now, for each  $i \in \{1, 2\}$ , consider the subsequence  $S'_i$  of  $S_i$  which contains only the occurrences of  $r_i$ , and set  $\Sigma'_i = \Sigma(S'_i)$ . We clearly have that

$$|S'_1| + |S'_2| = \frac{p-1}{2} \quad \text{and} \quad |\Sigma'_1| + |\Sigma'_2| = \frac{p+3}{2}.$$

Suppose that there exist  $(x_1, y_1) \in (\Sigma'_1)^2$  and  $(x_2, y_2) \in (\Sigma'_2)^2$  such that  $x_1 + x_2 = y_1 + y_2$ . Then, one has  $x_1 - y_1 = y_2 - x_2$ , where  $x_1 - y_1 \in \Sigma_1$  and  $x_2 - y_2 \in \Sigma_2$ . Thus, Lemma 3.1 implies that  $x_1 = y_1$  and  $x_2 = y_2$ . This proves that all elements of  $\Sigma'_1 + \Sigma'_2$  have a unique representation as a sum  $x_1 + x_2$ , where  $(x_1, x_2) \in \Sigma'_1 \times \Sigma'_2$ , so that

$$|\Sigma'_1 + \Sigma'_2| = |\Sigma'_1| |\Sigma'_2| = |\Sigma'_1| \left( \frac{p+3}{2} - |\Sigma'_1| \right).$$

If  $2 < |\Sigma'_1| < \frac{p-1}{2}$ , one has  $|\Sigma'_1 + \Sigma'_2| > 2 \left( \frac{p-1}{2} \right) = p - 1$ . In addition, since  $p$  is prime, one cannot have  $|\Sigma'_1 + \Sigma'_2| = |\Sigma'_1| |\Sigma'_2| = p$  either. Therefore, one of the two sets, say  $\Sigma'_1$ , has cardinality 2. Then  $|S'_1| = 1$  and  $S_1 = (r_1, -r_1)$ . Now, since  $A$  is regular, there is a subsequence  $T_2$  of  $S_2$  such that  $\sigma(S'_1) + \sigma(T_2) = 0$ . It follows from Lemma 3.1 that  $\sigma(S'_1) = r_1 = 0$ , which is a contradiction.

**Case 2:**  $d \geq 3$  and  $\sum_{i=1}^d (|\Sigma_i| - 1) = p$ .

On the one hand, since  $d \geq 3$  and  $A$  is regular, Lemmas 3.1 and 4.1 imply that  $|\Sigma_i| < p - 1$  for all  $i \in [1, d]$ . On the other hand, there is  $k \in [1, d]$  such that  $|\Sigma_i| = |S_i| + 1$  for all  $i \neq k$ . Using Lemma 2.4, we obtain that for every  $i \neq k$ , there exists  $r_i \in \mathbb{F}_p^*$  such that all elements of  $S_i$  are equal to  $r_i$  or  $-r_i$ .

Now, for any two distinct elements  $i_0, j_0 \in [1, d]$  with  $i_0 \neq k$ , and any  $r_{i_0} \in S_{i_0}$ , let us consider the sets  $\Sigma'_i$  defined by

$$\Sigma'_{i_0} = \Sigma(S_{i_0} \setminus (r_{i_0})), \quad \Sigma'_{j_0} = \Sigma(S_{j_0} \cup (r_{i_0})) = \Sigma_{j_0} + \{0, r_{i_0}\}$$

and  $\Sigma'_i = \Sigma_i$  otherwise. Let also  $Q_{i_0, j_0}$  be as in Proposition 4.3.

Then, one has  $|\Sigma'_{i_0}| = |\Sigma_{i_0}| - 1$ . In addition, since  $A$  is regular, Lemmas 3.1 and 4.1 imply that  $\pm r_{i_0} \notin S_{j_0}$ . It follows from Theorem 2.3 that  $|\Sigma'_{j_0}| \geq |\Sigma_{j_0}| + 2$ .

We now define  $(t_i)_{i \in [1, d]}$  by  $t_{i_0} = |\Sigma_{i_0}| - 2$ ,  $t_{j_0} = |\Sigma_{j_0}| + 1$  and  $t_i = |\Sigma_i| - 1$  otherwise. In particular,  $t_i \leq |\Sigma'_i| - 1 < p$  for all  $i \in [1, d]$  and  $\sum_{i=1}^d t_i = p + 1$ . By Theorem 3.2, we have that  $\sum_{i=1}^d \lambda_i (|\Sigma_i| - 1) = 0$  in  $\mathbb{F}_p$ . Thus, Proposition 4.3 implies that, up to a nonzero multiplicative constant, the coefficient of  $\prod_{i=1}^d X_i^{t_i}$  in  $Q_{i_0, j_0}$  is

$$\begin{aligned} \left( \sum_{i=1}^d \lambda_i t_i \right)^2 - \left( \sum_{i=1}^d \lambda_i^2 t_i \right) &= (2\lambda_{j_0} - \lambda_{i_0})^2 - \left( 2\lambda_{j_0}^2 - \lambda_{i_0}^2 + \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1) \right) \\ &= (2\lambda_{j_0}^2 - 4\lambda_{i_0} \lambda_{j_0} + 2\lambda_{i_0}^2) - \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1) \\ &= 2(\lambda_{j_0} - \lambda_{i_0})^2 - \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1). \end{aligned}$$

Note that  $\sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1)$  is independent of  $i_0$  and  $j_0$ . In addition, the coefficient of  $\prod_{i=1}^d X_i^{t_i}$  in  $Q_{i_0, j_0}$  is zero if and only if

$$(\lambda_{j_0} - \lambda_{i_0})^2 = \frac{1}{2} \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1).$$

Since  $d \geq 3$ , there is at least one pair  $(i_0, j_0)$  such that this equality does not hold. Since  $i_0$  and  $j_0$  play symmetric roles,  $i_0$  can be chosen such that  $i_0 \neq k$  indeed. It follows from Theorem 2.1 that for this actual pair,  $Q_{i_0, j_0}$  cannot vanish on  $\prod_{i=1}^d \Sigma'_i$ , which contradicts Proposition 4.3.

**Case 3:**  $d \geq 3$  and  $\sum_{i=1}^d (|\Sigma_i| - 1) = p - 1$ .

Since  $A$  is regular, Lemmas 3.1 and 4.1 give  $|\Sigma_i| < p - 1$  for all  $i \in [1, d]$ . It follows that  $|\Sigma_i| = |S_i| + 1$  for all  $i \in [1, d]$ , and Lemma 2.4 implies that there exists  $r_i \in \mathbb{F}_p^*$  such that all elements of  $S_i$  are equal to  $r_i$  or  $-r_i$ . Note, in particular, that one has  $\pm r_i \neq r_j$  for any two distinct elements  $i, j \in [1, d]$ .

In addition, if one of the ratio sets, say  $\Sigma_1$ , has cardinality  $p - 2$ , then  $d = 3$  and  $|S_2| = |S_3| = 1$ . Since  $A$  is regular, there would be a subsequence  $T_1$  of  $S_1$  such that  $\sigma(T_1) + \sigma(S_2) = 0$ . By Lemma 3.1, we would have  $\sigma(S_2) = 0$ , a contradiction. This proves that  $|\Sigma_i| < p - 2$  for all  $i \in [1, d]$ .

Now, for any two distinct elements  $i_0, j_0 \in [1, d]$  and any  $r_{i_0} \in S_{i_0}$  such that  $|S_{j_0}| > 1$  and  $\pm \frac{1}{2} r_{i_0} \notin S_{j_0}$ , let us consider the sets  $\Sigma'_i$  defined by

$$\Sigma'_{i_0} = \Sigma(S_{i_0} \setminus (r_{i_0})), \quad \Sigma'_{j_0} = \Sigma(S_{j_0} \cup (r_{i_0})) = \Sigma_{j_0} + \{0, r_{i_0}\}$$

and  $\Sigma'_i = \Sigma_i$  otherwise. Let also  $Q_{i_0, j_0}$  be as in Proposition 4.3.

Then, one has  $|\Sigma'_{i_0}| = |\Sigma_{i_0}| - 1$ . In addition, since  $|S_{j_0}| > 1$  and neither  $\pm r_{i_0}$  nor  $\pm \frac{1}{2} r_{i_0}$  are elements of  $S_{j_0}$ , it follows from Lemma 2.5 that  $|\Sigma'_{j_0}| \geq |\Sigma_{j_0}| + 3$ .

We now define  $(t_i)_{i \in [1, d]}$  by  $t_{i_0} = |\Sigma_{i_0}| - 2$ ,  $t_{j_0} = |\Sigma_{j_0}| + 2$  and  $t_i = |\Sigma_i| - 1$  otherwise. In particular,  $t_i \leq |\Sigma'_i| - 1 < p$  for all  $i \in [1, d]$  and  $\sum_{i=1}^d t_i = p + 1$ . Proposition 4.3 implies that, up to a nonzero multiplicative constant, the coefficient of  $\prod_{i=1}^d X_i^{t_i}$  in  $Q_{i_0, j_0}$  is

$$\begin{aligned}
& \left( \sum_{i=1}^d \lambda_i t_i \right)^2 - \left( \sum_{i=1}^d \lambda_i^2 t_i \right) \\
&= \left( \sum_{i=1}^d \lambda_i (|\Sigma_i| - 1) + 3\lambda_{j_0} - \lambda_{i_0} \right)^2 - \left( \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1) + 3\lambda_{j_0}^2 - \lambda_{i_0}^2 \right) \\
&= (2\lambda_{i_0}^2 - 6\lambda_{i_0}\lambda_{j_0} + 6\lambda_{i_0}^2) + 2 \left( \sum_{i=1}^d \lambda_i (|\Sigma_i| - 1) \right) (3\lambda_{j_0} - \lambda_{i_0}) \\
&\quad + \left( \sum_{i=1}^d \lambda_i (|\Sigma_i| - 1) \right)^2 - \left( \sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1) \right).
\end{aligned}$$

Since  $\sum_{i=1}^d \lambda_i (|\Sigma_i| - 1)$  and  $\sum_{i=1}^d \lambda_i^2 (|\Sigma_i| - 1)$  are independent of  $i_0$  and  $j_0$ , this last expression is a quadratic polynomial  $f$  in  $\lambda_{i_0}$  and  $\lambda_{j_0}$ . In addition, the coefficient of  $\prod_{i=1}^d X_i^{t_i}$  in  $Q_{i_0, j_0}$  is zero if and only if  $f(\lambda_{i_0}, \lambda_{j_0}) = 0$ .

**Case 3.1:** If  $d \geq 5$ , then choose any  $j_0 \in [1, d]$  such that  $|S_{j_0}| > 1$ . On the one hand, there are at most two ratios  $\lambda_i$  such that  $f(\lambda_i, \lambda_{j_0}) = 0$ . On the other hand, there is at most one set  $S_i$  such that  $\pm \frac{1}{2}r_i \in S_{j_0}$ . Since  $d \geq 5$ , the pigeonhole principle implies that there is at least one pair  $(i_0, j_0)$  such that  $f(\lambda_{i_0}, \lambda_{j_0}) \neq 0$  and  $\pm \frac{1}{2}r_{i_0} \notin S_{j_0}$ . It follows from Theorem 2.1 that for this actual pair,  $Q_{i_0, j_0}$  cannot vanish on  $\prod_{i=1}^d \Sigma'_i$ , which contradicts Proposition 4.3.

**Case 3.2:** If  $d \in \{3, 4\}$  and there are at least three sets  $S_i$ , such that  $|S_i| > 1$ , then without loss of generality, we may assume that  $|S_i| > 1$  for each  $i \in \{1, 2, 3\}$ . In particular,  $p \geq 7$ . Now, by Lemma 5.4, one of the following holds.

- If  $f(\lambda_1, \lambda_2) f(\lambda_1, \lambda_3) \neq 0$ , then there is  $j_0 \in \{2, 3\}$  such that  $\pm \frac{1}{2}r_1 \notin S_{j_0}$ . Therefore, setting  $i_0 = 1$ , we have  $f(\lambda_{i_0}, \lambda_{j_0}) \neq 0$  and  $\pm \frac{1}{2}r_{i_0} \notin S_{j_0}$  indeed.
- If  $f(\lambda_2, \lambda_1) f(\lambda_3, \lambda_1) \neq 0$ , then there is  $i_0 \in \{2, 3\}$  such that  $\pm \frac{1}{2}r_{i_0} \notin S_1$ . Therefore, setting  $j_0 = 1$ , we have  $f(\lambda_{i_0}, \lambda_{j_0}) \neq 0$  and  $\pm \frac{1}{2}r_{i_0} \notin S_{j_0}$  indeed.
- If  $f(\lambda_1, \lambda_2) f(\lambda_2, \lambda_1) \neq 0$ , then  $p \geq 7$  implies that one cannot have both  $r_1 = \pm 2r_2$  and  $r_2 = \pm 2r_1$ . Thus, there are two distinct elements  $i_0, j_0 \in \{1, 2\}$  such that  $f(\lambda_{i_0}, \lambda_{j_0}) \neq 0$  and  $\pm \frac{1}{2}r_{i_0} \notin S_{j_0}$  indeed.
- If  $f(\lambda_1, \lambda_2) f(\lambda_2, \lambda_3) f(\lambda_3, \lambda_1) \neq 0$ , then  $p \geq 7$  implies that the three equalities  $r_1 = \pm 2r_2$  and  $r_2 = \pm 2r_3$  and  $r_3 = \pm 2r_1$  can occur only when  $r_i = \pm 8r_i$ , so that  $p = 7$ . Otherwise, there are two distinct elements  $i_0, j_0 \in \{1, 2, 3\}$  such that  $f(\lambda_{i_0}, \lambda_{j_0}) \neq 0$  and  $\pm \frac{1}{2}r_{i_0} \notin S_{j_0}$  indeed.

It follows that whenever  $p \neq 7$ , there is at least one pair  $(i_0, j_0)$  such that  $f(\lambda_{i_0}, \lambda_{j_0}) \neq 0$  and  $\pm \frac{1}{2}r_{i_0} \notin S_{j_0}$ . Theorem 2.1 then implies that for this actual pair,  $Q_{i_0, j_0}$  cannot vanish on  $\prod_{i=1}^d \Sigma'_i$ , which contradicts Proposition 4.3.

The only remaining case to consider is  $p = 7$ ,  $d = 3$  and  $|S_i| = 2$  for each  $i \in \{1, 2, 3\}$ . Therefore, by relabelling if necessary, there are only two possible cases.

- $\Sigma_1 = \{0, 1, 2\}$ ,  $\Sigma_2 = \{0, 2, 4\}$ ,  $\Sigma_3 = \{0, 4, 1\}$ , which gives  $S_1 = (1, 1)$ ,  $S_2 = (2, 2)$  and  $S_3 = (-3, -3)$ . It can easily be checked that such a sequence  $A$  satisfies  $\dim(A) = p - 2$ , so that  $d = 1$ , a contradiction.
- $\Sigma_1 = \{-1, 0, 1\}$ ,  $\Sigma_2 = \{-2, 0, 2\}$ ,  $\Sigma_3 = \{-3, 0, 3\}$ , which gives  $S_1 = (-1, 1)$ ,  $S_2 = (-2, 2)$  and  $S_3 = (-3, 3)$ . Therefore, by relabelling if necessary, one has  $A = (-1, 1, -2, 2, -3, 3)$ . The following table then gives a basis of  $\langle S_A \rangle$ .

-1	1	-2	2	-3	3
1	1	0	0	0	0
0	0	1	1	0	0
0	0	0	0	1	1
1	0	1	0	0	1

**Case 3.3:** If  $d \in \{3, 4\}$  and there are exactly two sets  $S_i$  such that  $|S_i| > 1$ , then without loss of generality, we can suppose that these two sets are  $S_1$  and  $S_2$ , where  $|S_1| \leq |S_2|$ . Therefore  $\Sigma_1$  and  $\Sigma_2$  are two arithmetic progressions such that  $|\Sigma_1| + |\Sigma_2| = p + 3 - d$ . In addition, it follows from Lemma 3.1 that  $\Sigma_1$  and  $-\Sigma_2$  satisfy the hypothesis of Lemma 5.5. We thus consider the following cases.

If  $d = 3$ , then  $p \geq 7$  and since  $\sigma(S_1) + \sigma(S_2) + \sigma(S_3) = 0$ , Lemma 3.1 implies that  $\sigma(S_1)$  and  $\sigma(S_2)$  are nonzero. Therefore, Lemma 5.5 implies there exists  $r \in \mathbb{F}_p^*$  such that  $\Sigma_1 = \{0, 2, 4\}.r$  and  $\Sigma_2 = \{-1, 0, 1, \dots, p-5\}.r$ . On the one hand, this gives  $\sigma(S_1) + \sigma(S_2) = -2r$ . On the other hand, the single element of  $S_3$  has to be in  $\{3, 4\}.r$ , so that  $\sigma(A) \neq 0$ , a contradiction.

If  $d = 4$ , then  $p \geq 11$  and since  $\sigma(S_1) + \sigma(S_2) + \sigma(S_3) + \sigma(S_4) = 0$ , Lemma 3.1 implies that either  $\sigma(S_1)$  or  $\sigma(S_2)$  is nonzero. Therefore, Lemma 5.5 implies there exists  $r \in \mathbb{F}_p^*$  such that one of the following cases holds.

- $\Sigma_1 = \{0, 2, 4\}.r$  and  $\Sigma_2 = \{0, 1, \dots, p-5\}.r$ . Then,  $\sigma(S_1) + \sigma(S_2) = -r$  and the elements of  $S_3$  and  $S_4$  have to be in  $\{3, 4\}.r$ . Therefore, one has  $\sigma(A) \neq 0$ , which is a contradiction.
- $\Sigma_1 = \{0, 2, 4\}.r$  and  $\Sigma_2 = \{-1, 0, 1, \dots, p-6\}.r$ . Then,  $\sigma(S_1) + \sigma(S_2) = -3r$  and the elements of  $S_3$  and  $S_4$  have to be in  $\{3, 4, 5\}.r$ . Therefore, one has  $\sigma(A) \neq 0$ , which is a contradiction.
- $\Sigma_1 = \{0, 2, 4, 6\}.r$  and  $\Sigma_2 = \{-1, 0, 1, \dots, p-7\}.r$ . Then,  $\sigma(S_1) + \sigma(S_2) = -2r$  and the elements of  $S_3$  and  $S_4$  have to be in  $\{3, 4\}.r$  when  $p = 11$ , and in  $\{3, 4, 5, 6\}.r$  whenever  $p \geq 13$ . In all cases, one has  $\sigma(A) \neq 0$ , which is a contradiction.
- $\Sigma_1 = \{0, 3, 6\}.r$  and  $\Sigma_2 = \{-2, -1, 0, \dots, p-7\}.r$ . Then,  $\sigma(S_1) + \sigma(S_2) = -3r$  and the elements of  $S_3$  and  $S_4$  have to be in  $\{4, 6\}.r$  when  $p = 11$ , and in  $\{4, 5, 6\}.r$  whenever  $p \geq 13$ . In all cases, one has  $\sigma(A) \neq 0$ , which is a contradiction.
- $\Sigma_1 = \{-\frac{p-1}{2}, 0, \frac{p-1}{2}\}.r$  and  $\Sigma_2 = \{-\frac{p-3}{2}, \dots, -1, 0, 1, \dots, \frac{p-7}{2}\}.r$ . Then,  $\sigma(S_1) + \sigma(S_2) = -2r$  and the elements of  $S_3$  and  $S_4$  have to be in  $\{\frac{p+3}{2}, \frac{p+5}{2}\}.r$ . Therefore, one has  $\sigma(A) \neq 0$ , which is a contradiction.
- $p = 11$ ,  $\Sigma_1 = \{-4, 0, 4, 8\}.r$  and  $\Sigma_2 = \{-2, -1, 0, 1, 2, 3\}.r$ . Then, the elements of  $S_3$  and  $S_4$  have to be in  $\{-5, 5\}.r$ , which would contradict Lemma 3.1.

**Case 3.4:** If  $d \in \{3, 4\}$  and there is only one set  $S_i$  such that  $|S_i| > 1$ , then without loss of generality, we can suppose that this set is  $S_1$ . If  $d = 3$ , and since  $A$  is regular, there is a subsequence  $T_1$  of  $S_1$  such that  $\sigma(T_1) + \sigma(S_2) = 0$ . It follows from Lemma 3.1 that  $\sigma(S_2) = 0$ , which is a contradiction. Thus,  $d = 4$  and Lemma 3.1 implies that, by relabelling if necessary, there exist  $t \in [0, p-4]$  and  $r \in \mathbb{F}_p^*$  such that

$$\Sigma_1 = \{-(p-4-t), \dots, -1, 0, 1, \dots, t\}.r,$$

$$\Sigma_2 = \{0, -(t+1)\}.r, \Sigma_3 = \{0, -(t+2)\}.r, \Sigma_4 = \{0, -(t+3)\}.r.$$

Since  $t \in [0, p-4]$ , one has  $\sigma(A) = -(t+2)r \neq 0$ , which contradicts the fact that  $A$  is a zero-sum sequence.  $\square$

*Proof of Corollary 1.8.* Let  $A, B$  be two sequences of  $p-1$  nonzero elements in  $\mathbb{F}_p$ . It is easily checked that  $\mathcal{S}_A = \mathcal{S}_B$  whenever  $A$  and  $B$  are colinear, or have one of the forms given in (i), (ii) and (iii). Reciprocally, suppose that  $A, B$  are such that  $\mathcal{S}_A = \mathcal{S}_B$ . If  $\sigma(A) \neq 0$  then Lemma 5.2 and Corollary 1.5 imply that  $A$  and  $B$  are colinear. If  $\sigma(A) = 0$  then, using Theorem 1.7, there are six cases to consider.

- If  $\dim(A) = p-2$  then  $\mathcal{S}_A \subset \mathcal{S}_B$  already implies that  $A$  and  $B$  are colinear.
- If  $\dim(A) = 1$ , then  $\dim(B) = 1$  and it is easily seen that there exist  $\lambda, r \in \mathbb{F}_p^*$  such that  $A$  (resp.  $B$ ) consists of  $p-2$  copies of  $r$  (resp.  $\lambda r$ ) and one copy of  $2r$  (resp.  $2\lambda r$ ). Therefore,  $A$  and  $B$  either are colinear or have the form given in (i).
- If  $p = 7$  and, by relabelling if necessary, one has

$$A = (-1, 1, -2, 2, -3, 3),$$

then it can be checked by hand that  $\mathcal{S}_A = \mathcal{S}_B$  if and only there is  $\lambda \in \mathbb{F}_p^*$  such that

$$B = (-\lambda, \lambda, -2\lambda, 2\lambda, -3\lambda, 3\lambda) \quad \text{or} \quad B = (-\lambda, \lambda, 3\lambda, -3\lambda, 2\lambda, -2\lambda).$$

Therefore,  $A$  and  $B$  either are colinear or have the form given in (iii).

- If  $\dim(A) = p-3$  and there exist  $t \in [1, p-4], r \in \mathbb{F}_p^*$  such that, by relabelling if necessary, one has

$$A = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-3-t}, -(t+1)r, -(t+2)r),$$

then  $\mathcal{S}_A \subset \mathcal{S}_B$  implies that

$$B = (\underbrace{\lambda r, \dots, \lambda r}_t, \underbrace{-\lambda r, \dots, -\lambda r}_{p-3-t}, -(t+1)\lambda r + d, -(t+2)\lambda r - d)$$

for some  $\lambda \in \mathbb{F}_p^*$  and  $d \in \mathbb{F}_p$ . By Theorem 1.7, the equality  $\dim(B) = p-3$  holds only when  $d = 0$ , that is  $A$  and  $B$  are colinear, or  $d = -\lambda r$ , which gives case (ii).

- If  $\dim(A) = p-3$  and there exist  $t \in [0, p-6], r \in \mathbb{F}_p^*$  such that, by relabelling if necessary, one has

$$A = (\underbrace{r, \dots, r}_t, \underbrace{-r, \dots, -r}_{p-4-t}, 2r, -(t+3)r, -(t+3)r),$$

then  $\mathcal{S}_A \subset \mathcal{S}_B$  implies that

$$B = (\underbrace{\lambda r, \dots, \lambda r}_t, \underbrace{-\lambda r, \dots, -\lambda r}_{p-4-t}, 2\lambda r, -(t+3)\lambda r + d, -(t+3)\lambda r - d)$$

for some  $\lambda \in \mathbb{F}_p^*$  and  $d \in \mathbb{F}_p$ . By Theorem 1.7, the equality  $\dim(B) = p-3$  holds only when  $d = 0$ , that is  $A$  and  $B$  are colinear.

- If  $\dim(A) = p-4$ , then there exist  $r \in \mathbb{F}_p^*$  such that, by relabelling if necessary, one has

$$A = (\underbrace{r, \dots, r}_{p-5}, -r, 2r, 2r, 2r).$$

Now, either one has  $p = 5$ , which brings us back to the case  $\dim(A) = 1$ , or  $p \geq 7$  and  $\mathcal{S}_A \subset \mathcal{S}_B$  implies that

$$B = (\underbrace{\lambda r, \dots, \lambda r}_{p-5}, -\lambda r, 2\lambda r + a, 2\lambda r + b, 2\lambda r - (a+b))$$

for some  $\lambda \in \mathbb{F}_p^*$  and  $a, b \in \mathbb{F}_p$ . Then, by Theorem 1.7, the equality  $\dim(B) = p-4$  holds only when  $a = b = 0$ , so that  $A$  and  $B$  are colinear.  $\square$

*Proof of Corollary 1.9.* Let  $A$  be a sequence of  $p - 1$  nonzero elements in  $\mathbb{F}_p$  not being of the forms given in (i) and (ii). If  $\sigma(A) \neq 0$ , then Lemma 5.1 and Theorem 1.4 readily imply that  $\dim(A) \geq p - 3$ . Then, the desired result follows directly from Proposition 3.3. If  $\sigma(A) = 0$  then, using Theorem 1.7, there are only two cases to consider. If  $\dim(A) \geq p - 3$ , then Proposition 3.3 implies that the number of minimal elements in  $\mathcal{S}_A$  is at least  $p - 3$ . If  $\dim(A) = p - 4$ , then there exist  $r \in \mathbb{F}_p^*$  such that  $A$  consists of  $p - 5$  copies of  $r$ , one copy of  $-r$  and three copies of  $2r$ . Now, either one has  $p = 5$  and  $A$  has the form given in (ii), or  $p \geq 7$  and the number of minimal elements in  $\mathcal{S}_A$  is  $2(p - 5) \geq p - 3$ .  $\square$

## 6. A CONCLUDING REMARK

Let  $p$  be a prime and let  $A = (a_1, \dots, a_\ell)$  be a sequence of  $\ell \geq 1$  nonzero elements in  $\mathbb{F}_p$ . In this paper, we proved that for every  $\ell \geq p - 1$ , the equality  $\dim(A) = \ell - 1$  holds except for a very limited number of exceptional sequences which can be fully determined. However, our results can easily be extended to the affine setting.

Given any element  $\alpha \in \mathbb{F}_p$ , let  $\mathcal{S}_A^\alpha$  be the set of all 0-1 solutions to the equation

$$a_1x_1 + \dots + a_\ell x_\ell = \alpha,$$

and let

$$\dim(A, \alpha) = \dim(\text{aff}(\mathcal{S}_A^\alpha))$$

be the dimension of the affine hull of  $\mathcal{S}_A^\alpha$ .

For any  $I \subset [1, \ell]$ , we consider the sequence  $A_I = (a'_1, \dots, a'_\ell)$  defined by  $a'_i = -a_i$  if  $i \in I$  and  $a'_i = a_i$  otherwise. Whenever  $\ell \geq p - 1$ , the following lemma shows that there is an affine transformation mapping  $\mathcal{S}_A^\alpha$  onto  $\mathcal{S}_{A_I}$ , for a particular  $I \subset [1, \ell]$ . Therefore, our results provide a full description of the dimension and structure of the sets  $\mathcal{S}_A^\alpha$ , for all  $\alpha \in \mathbb{F}_p$ .

**Lemma 6.1.** *Let  $p$  be a prime and let  $A = (a_1, \dots, a_\ell)$  be a sequence of  $\ell \geq p - 1$  nonzero elements in  $\mathbb{F}_p$ . Then, for every  $\alpha \in \mathbb{F}_p$ , there exists  $I \subset [1, \ell]$  such that*

$$\dim(A, \alpha) = \dim(A_I).$$

*Proof.* By Cauchy-Davenport Theorem, one has  $|\Sigma(A)| \geq \min\{p, \ell + 1\} = p$ . Thus, there exists  $I \subset [1, \ell]$  such that  $\sum_{i \in I} a_i = \alpha$ . Now, let  $A_I = (a'_1, \dots, a'_\ell)$ . Then, for every  $J \subset [1, \ell]$ , one has

$$\sum_{i \in J} a_i = \alpha$$

if and only if

$$\sum_{i \in J} a_i - \sum_{i \in I} a_i = 0$$

which is equivalent to

$$\sum_{i \in J \setminus I} a_i - \sum_{i \in I \setminus J} a_i = 0$$

that is to say

$$\sum_{i \in I \Delta J} a'_i = 0.$$

Therefore,  $\mathcal{S}_{A_I}$  is the image of  $\mathcal{S}_A^\alpha$  by the affine transformation  $(x_1, \dots, x_\ell) \mapsto (y_1, \dots, y_\ell)$ , where  $y_i = 1 - x_i$  if  $i \in I$  and  $y_i = x_i$  otherwise.  $\square$

## REFERENCES

- [1] N. ALON *Combinatorial Nullstellensatz*, *Combin. Probab. Comput.* **8** (1999), 7-29.
- [2] E. BALANDRAUD *An addition theorem and maximal zero-sum free sets in  $\mathbb{Z}/p\mathbb{Z}$* , *Israel J. Math.* **188** (2012), 405-429.
- [3] A.-L. CAUCHY *Recherches sur les nombres*, *J. Ecole Polytech.* **9** (1813), 99-116.
- [4] H. DAVENPORT *On the addition of residue classes*, *J. Lond. Math. Soc.* **10** (1935), 30-32.
- [5] H. DAVENPORT *A historical note*, *J. Lond. Math. Soc.* **22** (1947), 100-101.
- [6] P. ERDŐS, A. GINZBURG AND A. ZIV *Theorem in the additive number theory*, *Bull. Research Council Israel* **10** (1961), 41-43.
- [7] A. GEROLDINGER *Additive group theory and non-unique factorizations*, In A. Geroldinger and I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory*, *Advanced Courses in Mathematics*, CRM Barcelona, Birkhäuser (2009), 1-86.
- [8] A. GEROLDINGER AND F. HALTER-KOCH *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, *Pure and Applied Mathematics* **278**, Chapman & Hall/CRC (2006).
- [9] J. E. OLSON *A problem of Erdős on abelian groups*, *Combinatorica* **7**(3) (1987), 285-289.
- [10] T. TAO AND V. H. VU *Additive Combinatorics*, *Cambridge Studies in Advanced Mathematics* **105** (2006), Cambridge Press University.
- [11] G. VOSPER *The critical pairs of subsets of a group of prime order*, *J. Lond. Math. Soc.* **31** (1956), 200-205.
- [12] G. VOSPER *Addendum to "The critical pairs of subsets of a group of prime order"*, *J. Lond. Math. Soc.* **31** (1956), 280-282.