The geometry of intersecting codes and applications to additive combinatorics and factorization theory

Martino Borello, Wolfgang Schmid, Martin Scotti

THE GEOMETRY OF INTERSECTING CODES AND APPLICATIONS TO ADDITIVE COMBINATORICS AND FACTORIZATION THEORY

MARTINO BORELLO*[1,2], WOLFGANG SCHMID[1], AND MARTIN SCOTTI[1]

Abstract. Intersecting codes are linear codes where every two nonzero codewords have non-trivially intersecting support. In this article we expand on the theory of this family of codes, by showing that nondegenerate intersecting codes correspond to sets of points (with multiplicities) in a projective space that are not contained in two hyperplanes. This correspondence allows the use of geometric arguments to demonstrate properties and provide constructions of intersecting codes. We improve on existing bounds on their length and provide explicit constructions of short intersecting codes. Finally, generalizing a link between coding theory and the theory of the Davenport constant (a combinatorial invariant of finite abelian groups), we provide new asymptotic bounds on the weighted 2-wise Davenport constant. These bounds then yield results on factorizations in rings of algebraic integers and related structures.

Keywords: Intersecting codes; Projective systems; Zero-sum problem; Factorization
MSC2020: 51E20, 94B27, 05B25, 11P70, 11R29

Contents

[1] Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA, Université Sorbonne Paris Nord, CNRS, UMR 7539, France.
[2] INRIA Saclay & LIX, CNRS UMR 7161, École Polytechnique, France
E-mail addresses: martino.borello@univ-paris8.fr, martin.scotti@etud.univ-paris8.fr, wolfgang.schmid@univ-paris8.fr.

Introduction

Intersecting codes are linear codes for which every two nonzero codewords have non-trivially intersecting support. Intersecting codes are a classical object of study in coding theory introduced in [38,44] and subsequently investigated in many articles (see for example [19,21,23,51]), but with a primary focus on the binary case. In this case, such codes coincide with minimal codes, which have been intensively studied in the last 20 years. Several practical applications of intersecting and minimal codes are known: they allow communication over AND channels, they may be used in secret sharing schemes, and they are related to other structures such as frameproof codes [13] and $(2,1)$-separating systems [50]. In this article, we primarily focus on the geometric interpretation of intersecting codes, which has remained completely unexplored to date, and to the interactions of these objects with other areas of mathematics, in particular additive combinatorics and algebraic number theory.

It is well-known that a nondegenerate linear code can be associated with a set of points (with multiplicities) in a projective space and some coding-theoretical properties can be interpreted geometrically. This view is what connects MDS codes to problems with arcs in projective spaces (the famous MDS conjecture was initially formulated as a problem in projective geometry in [54]), covering problems to saturating sets, minimal codes to strong blocking sets, etc. Intersecting codes correspond to sets of points that are not contained in any pair of hyperplanes. We will refer to such sets as *non-2-cohyperplanar*. This geometric interpretation of intersecting codes allows us to visualize some fundamental properties, but above all, it allows for the introduction of new constructions.

It is clear from the definition of non-2-cohyperplanar sets that adding a point to these sets leaves them non-2-cohyperplanar. Hence, it is fundamental, for constructing purposes, to investigate small sets with this property, possibly minimal with respect to inclusion. We prove some lower bounds on the cardinality of non-2-cohyperplanar sets and a probabilistic existence results. For some low parameters, we provide constructions of the smallest non-2-cohyperplanar sets. We revisit a property proven in [50] regarding intersecting AG codes, along with the concatenation method, to provide explicit constructions of short intersecting codes over any finite field. Quite surprisingly, these explicit constructions improve the probabilistic bound in many cases (more precisely, they almost always improve it for codes over non-prime fields). Moreover, in the binary case it provides the shortest known explicit construction of intersecting codes, which in this case are minimal. Furthermore, we introduce an explicit construction, based on the very recent paper [7], stemming from the union of projective lines, which employs a sufficient geometrical condition called the avoidance property (introduced in [26]) and some expander graphs.

The last part of the paper is devoted to the interpretation of our results to additive combinatorics and factorization theory. In particular, continuing the research along the path traced by [42,48], we link the theory of intersecting codes to the one of weighted Davenport constants. Actually, the value of this constant is strictly related to the function describing the length of the shortest intersecting code for a given dimension and base field, as we will show in Theorem 5.12. We will then show the impact of the results on this function and of the explicit constructions of the previous sections on the knowledge of the weighted Davenport constants. Finally, we will explore the connection with factorization theory in algebraic number fields (and more generally certain Dedekind domains and Krull monoids). In particular, at the very end of the paper, we will explore the interplay between problems about intersecting codes over non-prime fields and Hilbert's ramification theory of some particular number fields with elementary abelian class group.

Outline: In Section 1, we delve into the definition and fundamental properties of intersecting codes. Section 2 explores the geometry of intersecting codes, particularly showcasing their correspondence with non-2-cohyperplanar sets and highlighting their properties and examples. Section 3 addresses the size of small non-2-cohyperplanar sets, or equivalently, the length of short intersecting codes, providing both lower and upper bounds. Section 4 presents constructions utilizing AG codes

and expander graphs. Finally, the paper concludes with applications of the preceding results to the theory of Davenport constants (Section 5) and to factorization theory (Section 6).

1. Intersecting codes: definitions and fundamental properties

Throughout the paper q will be a prime power, $\mathbb{F}_q$ will be a finite field of order q, and we will endow the vector space $\mathbb{F}_q^n$ with the Hamming metric, defined as follows: the *support* of a vector $x \in \mathbb{F}_q^n$ is

$$\sigma(x) = \{i \mid x_i \neq 0\},$$

and its *Hamming weight* is

$$\mathrm{w}(x) = \#\sigma(x).$$

The *Hamming distance* is then defined as $\mathrm{d}(x, y) = \mathrm{w}(x - y)$, for $x, y \in \mathbb{F}_q^n$.

We start with some classical fundamental definitions.

Definition 1.1. A (linear) *code* $\mathcal{C}$ over a finite field $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. We denote its *dimension* $k = \dim(\mathcal{C})$, and its *minimum distance* $d = \mathrm{d}(\mathcal{C}) = \min_{c,c' \in \mathcal{C}, c \neq c'} \mathrm{d}(c, c')$. We say that a code of dimension k and minimum distance d over $\mathbb{F}_q^n$ is an $[n, k, d]_q$-code (or an $[n, k]_q$ code if the minimum distance is unknown).

A *generator matrix* of an $[n, k, d]_q$-code $\mathcal{C}$ is a matrix $G \in \mathbb{F}_q^{k \times n}$ such that $\mathcal{C} = \mathrm{rowsp}(G)$. A code is said *nondegenerate* if no column of G is the zero vector. A code is said *projective* if there are no two linearly dependent columns in G. It is straightforward to observe that these last two properties do not depend on the chosen generator matrix. A *parity-check matrix* of an $[n, k, d]_q$-code $\mathcal{C}$ is a matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ such that $\mathcal{C} = \{v \in \mathbb{F}_q^n \mid Hv^T = \mathbf{0}\}$.

Two $[n, k, d]_q$-codes $\mathcal{C}$ and $\mathcal{C}'$ are *equivalent* if there is a linear isometry from $\mathbb{F}_q^n$ to itself mapping $\mathcal{C}$ to $\mathcal{C}'$ (actually, it is easy to prove that such an isometry should be a monomial transformation).

The *Singleton bound* is a fundamental concept in coding theory, which provides a relation between the parameters of a code: if $\mathcal{C}$ is an $[n, k, d]_q$ code, then

$$d \leq n - k + 1.$$

If equality holds, the code is called *Maximum Distance Separable* (MDS).

Definition 1.2. A family of codes $\mathcal{F}$ over $\mathbb{F}_q$ is said to be *asymptotically good* if there is an $\varepsilon > 0$ and a sequence of codes $\mathcal{C}_s \in \mathcal{F}$ with parameters $[n_s, k_s, d_s]_q$ such that $n_s \to \infty$, as well as both

$$\liminf_{s \to \infty} \frac{k_s}{n_s} \geq \varepsilon \quad \text{and} \quad \liminf_{s \to \infty} \frac{d_s}{n_s} \geq \varepsilon.$$

The main object of this paper is the following.

Definition 1.3. A code is called *intersecting* if for any two nonzero codewords the intersection of their supports is nonempty.

Intersecting codes were first introduced in [38,44] and generalized in [19] to the case of two distinct codes $\mathcal{C}_1$ and $\mathcal{C}_2$ for which all codewords $c_1 \in \mathcal{C}_1$ and $c_2 \in \mathcal{C}_2$ share a nonzero coordinate. They have been further investigated in [45,51,52,55]. In [21], Cohen and Zémor provide constructions of asymptotically good intersecting codes and they examine the case where the intersection must have a specific size. All of these contributions focus mainly on the binary case. A study for the case when the base field is of prime cardinality is done (implicitly) in [42]. As we will see, a particularly relevant construction of explicit families of asymptotically good intersecting codes is provided in [50].

It is useful to define the concatenation of two codes to construct new intersecting codes from old ones.

Definition 1.4. Let $\mathcal{I}$ be an $[n,k,d]_q$ code and $\mathcal{C}$ be a $[N,K,D]_{q^k}$ code. Let $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n$ be a linear map such that $\mathrm{Im}(\varphi) = \mathcal{I}$. The *concatenation* of $\mathcal{I}$ and $\mathcal{C}$ by φ is noted $\mathcal{I}\square_\varphi\mathcal{C}$ and is defined as

$$\mathcal{I}\square_\varphi\mathcal{C} = \{(\varphi(c_1),\dots,\varphi(c_N)) \mid (c_1,\dots,c_N) \in \mathcal{C}\}.$$

It is easy to prove that the code $\mathcal{I}\square_\varphi\mathcal{C}$ has parameters $[Nn, Kk, \geq Dd]_q$, for any φ. In the following, all considered properties will not depend on φ. Therefore, we will simply denote the concatenation with $\mathcal{I}\square\mathcal{C}$.

The following is a straightforward result, which appears also in [16, Lemma 4.1.] and which is used implicitly in [24].

Lemma 1.5. Let $\mathcal{C}$ be an intersecting $[N,K,D]_{q^k}$ code and $\mathcal{I}$ an intersecting $[n,k,d]_q$ code. Then $\mathcal{I}\square\mathcal{C}$ is an intersecting $[Nn, Kk, \geq Dd]_q$ code.

A family directly related to intersecting codes is that of minimal codes. Let us start from their definition.

Definition 1.6. Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. A nonzero codeword $c \in \mathcal{C}$ is called *minimal* if for every codeword $c' \in \mathcal{C}$ such that $\sigma(c') \subseteq \sigma(c)$, there exists some $\lambda \in \mathbb{F}_q^*$ such that $c' = \lambda c$.
A code is called *minimal* if all its nonzero codewords are minimal.

Minimal codewords in linear codes were initially investigated in the context of decoding algorithms [36] and have been employed by Massey [43] to define the access structure in his code-based secret sharing scheme. The work in [8] introduced what is now known as the *Ashikhmin-Barg condition*, which serves as a sufficient criterion for code minimality and has been widely utilized in code constructions. In [17], minimal codes are investigated in the context of secure two-party computation. Recent research has particularly focused on the parameters of minimal codes, see [3,5,17,20,40] and short constructions [7,10]. As shown in the following straightforward result, minimal codes constitute a subfamily of intersecting codes and they coincide in the binary case.

Lemma 1.7. Every minimal code is intersecting. Every binary intersecting code is minimal.

Proof. The first part is straightforward: if there are two codewords with non-intersecting support, their sum is a nonzero codeword which is not minimal.
Now consider the binary case. If the code is not minimal, then there are two different nonzero codewords c, c' such that $\sigma(c) \subseteq \sigma(c')$. Hence, $\sigma(c+c') \cap \sigma(c') = \emptyset$, so that the code is not intersecting. □

Another family of related codes is that of outer minimal codes, very recently introduced in [4].

Definition 1.8. Let $\mathcal{C}$ be an $[N,K]_{q^k}$ code. A nonzero codeword $c \in \mathcal{C} \subseteq \mathbb{F}_{q^k}^N$ is called (q-)*outer minimal*, if, for all $c' \in \mathcal{C}$,

$$\big(\,\sigma(c') \subseteq \sigma(c) \wedge \forall i \in \sigma(c),\, \exists \lambda_i \in \mathbb{F}_q \text{ s.t. } c'_i = \lambda_i c_i\,\big) \quad\Longrightarrow\quad \exists \lambda \in \mathbb{F}_q \text{ s.t. } c' = \lambda c.$$

A code is called (q-)*outer minimal* if all its nonzero codewords are (q-)outer minimal.

As shown in [4], any outer minimal code concatenated with a minimal code yields a minimal code. This allows to construct short minimal codes and prove some optimal existence results of short minimal codes. Quite unexpectedly, the 2-outer minimal codes are precisely the intersecting codes.

Proposition 1.9. Let $\mathcal{C}$ be an $[N,K]_{2^k}$ code. Then $\mathcal{C}$ is 2-outer minimal if and only if it is intersecting.

Proof. Suppose that $\mathcal{C}$ is intersecting. Let $c, c' \in \mathcal{C}$ nonzero codewords such that $\sigma(c') \subseteq \sigma(c)$ and $c'_i = c_i$, for all $i \in \sigma(c')$. Then $c' = c$, otherwise their sum would be a nonzero codeword with support disjoint from the support of c'.

Suppose that $\mathcal{C}$ is 2-outer minimal. Let $c, c' \in \mathcal{C}$ nonzero codewords such that $\sigma(c) \cap \sigma(c') = \emptyset$. Then $\sigma(c) \subseteq \sigma(c + c')$ and $c_i = c_i + c'_i$ for all $i \in \sigma(c)$ (because $c'_i = 0$ for these indexes). However, $c \neq c + c'$, a contradiction. □

Let us conclude the section with a very basic and well-known sufficient condition for a code to be intersecting. Let us remark that this condition can be seen as an analogue of the previously mentioned Ashikhmin-Barg condition for minimal codes. Indeed, it relies exclusively on the weight distribution of the code.

Lemma 1.10. Let $\mathcal{C}$ be an $[n, k, d]_q$ code. If $2d > n$, then $\mathcal{C}$ is intersecting.

Proof. The statement follows by an elementary pigeonhole argument on the supports of codewords. □

2. The geometry of intersecting codes

A classical approach to study linear codes is to consider their geometrical counterparts: researchers have extensively utilized the connections between linear codes and point sets within projective spaces. Notably, the MDS conjecture originated from Segre's inquiry into arcs within finite geometry [54]. Other remarkable connections exist between covering codes and saturating sets [25], or between minimal codes and strong blocking sets [3,56]. The aim of this section is to highlight the geometric interpretation of intersecting codes, which is, to our knowledge, an up to now unexplored topic.

Let us start from two basic definitions.

Definition 2.1. In $\mathbb{F}_q^k$, define the equivalence relation $\sim$ such that $x \sim y$ if x and y are collinear. The *projective space* $\mathrm{PG}(k-1, q)$ of dimension $k-1$ over $\mathbb{F}_q$ is then defined as

$$\mathrm{PG}(k-1, q) = \left(\mathbb{F}_q^k \setminus \{0\}\right) / \sim.$$

Definition 2.2. A *projective* $[n, k, d]_q$ *system* $\mathcal{P}$ is a finite set of n points (counted with multiplicity) of $\mathrm{PG}(k-1, q)$ that do not all lie on a hyperplane and such that

$$d = n - \max_{\mathcal{H} \text{ hyperplane}} \{|\mathcal{H} \cap \mathcal{P}|\}.$$

Projective $[n, k, d]_q$ systems $\mathcal{P}$ and $\mathcal{P}'$ are *equivalent* if there exists some $\varphi \in \mathrm{PGL}(k, q)$ mapping $\mathcal{P}$ to $\mathcal{P}'$ which preserves the multiplicities of the points.

There is a well-known correspondence between the equivalence classes of nondegenerate $[n, k, d]_q$ linear codes and the equivalence classes of projective $[n, k, d]_q$ systems (see [57, Theorem 1.1.6]) which works as follows: let $\mathcal{C}$ be a nondegenerate $[n, k, d]_q$-code, and let G be a generator matrix of $\mathcal{C}$. Since there is no zero column in G, it is possible to take the equivalence classes of the columns of G in $\mathrm{PG}(k-1, q)$, say $P_1, \ldots, P_n$. It is straightforward to prove that the multiset $\mathcal{P}_G = \{P_1, \ldots, P_n\}$ is a projective $[n, k, d]_q$ system (see Remark 2.3). Note that if the code $\mathcal{C}$ is projective, all points in $\mathcal{P}_G$ have multiplicity 1. Varying the generator matrix results in equivalent projective systems. The same holds by taking an equivalent code.

Remark 2.3. Consider a nondegenerate code $\mathcal{C}$ with parameters $[n, k, d]_q$ and let G be a generator matrix. Let $\mathcal{P}_G = \{P_1, \ldots, P_n\}$ be defined as above. A codeword $c \in \mathcal{C}$ is of the form xG, where $x \in \mathbb{F}_q^k$, and $c_i = 0$ if and only if P_i belongs to the hyperplane corresponding to $\langle x \rangle^\perp$ in $\mathrm{PG}(k-1, q)$. From our preceding remarks it follows that the support of a codeword corresponds to the points (with multiplicities) in the projective space that are *outside* the corresponding hyperplane.

Let us introduce a general definition which will be fundamental in describing the geometry of intersecting codes.

Definition 2.4. Let t be a positive integer. A set of points in a projective space $\mathrm{PG}(k-1,q)$ that is contained in the union of t hyperplanes is called *t-cohyperplanar*. A set which is not t-cohyperplanar is called *non-t-cohyperplanar*.

Example 2.5. The union of any t hyperplanes in $\mathrm{PG}(k-1,q)$ and one point not in any of these hyperplanes also yields a non-t-cohyperplanar set.

Non-2-cohyperplanar sets are the geometric counterpart of intersecting codes, as shown in the following result, which is essentially a remark, but it is named theorem because of its importance for the rest of the paper.

Theorem 2.6. Let $\mathcal{C}$ be a nondegenerate code over $\mathbb{F}_q$ of dimension k with generator matrix G. Consider the projective system $\mathcal{P}_G \subseteq \mathrm{PG}(k-1,q)$ defined as above. Then $\mathcal{P}_G$ is non-t-cohyperplanar if and only if for any set of t codewords the intersection of their support is nonempty. In particular, $\mathcal{C}$ is intersecting if and only if $\mathcal{P}_G$ is non-2-cohyperplanar.

Proof. Let $c_1 = x_1G, \dots, c_t = x_tG$ be t nonzero codewords of $\mathcal{C}$. Let $\mathcal{H}_1, \dots, \mathcal{H}_t$ be the projective hyperplanes corresponding to $\langle x_1\rangle^\perp, \dots, \langle x_t\rangle^\perp$ respectively. Since $\sigma(c_j) = \{i \mid P_i \notin \mathcal{H}_j\}$, the pointset $\mathcal{P}_G$ is not contained in $\bigcup_{j=1}^t \mathcal{H}_j$ if and only if there is an $i \in \bigcap_{j=1}^t \sigma(c_j)$. □

Since this paper is focused on intersecting codes, from now on we will only consider the case $t = 2$. However, in the context of linear frameproof codes [13,34], considering the general case may be of interest.

Let us introduce a related family of geometric structures.

Definition 2.7. A point set $\mathcal{S}$ in $\mathrm{PG}(k-1,q)$ is called a *strong blocking set* if for every hyperplane $\mathcal{H} \subseteq \mathrm{PG}(k-1,q)$ we have that

$$\langle \mathcal{S} \cap \mathcal{H} \rangle = \mathcal{H}.$$

The notion of a *strong blocking set* was first introduced in [25] as a means to construct saturating sets within projective spaces over finite fields. They were later reintroduced in [14] as *cutting blocking sets*, aiming to generate a family of minimal codes.

Theorem 2.8 ([3,56])**.** Let $\mathcal{C}$ be a nondegenerate code over $\mathbb{F}_q$ of dimension k with generator matrix G. Consider the projective system $\mathcal{P}_G \subseteq \mathrm{PG}(k-1,q)$ defined as above. Then $\mathcal{P}_G$ is a strong blocking set if and only if $\mathcal{C}$ is a minimal code.

As shown in the following, strong blocking sets form a subfamily of non-2-cohyperplanar sets.

Corollary 2.9. Strong blocking sets in $\mathrm{PG}(k-1,q)$ are non-2-cohyperplanar. If $q = 2$, the converse is also true.

Proof. This is a direct consequence of Lemma 1.7, Theorem 2.6 and Theorem 2.8. □

The result above entails that all the numerous known examples of strong blocking sets provide examples of non-2-cohyperplanar sets. We will see, however, that apart from the binary case (where the two concepts coincide), these examples are "larger" than necessary (in the sense that they contain many superfluous points).

To illustrate this, let us introduce a general result on non-2-cohyperplanar sets constructed from unions of lines. We first recall the avoidance property, introduced in [26].

Definition 2.10. Let $\mathcal{L}$ be a set of lines of $\mathrm{PG}(k-1,q)$. We say that $\mathcal{L}$ has the *avoidance property* if there is no projective subspace of codimension 2 that meets every line.

In [26], it is proved that a set of lines having the avoidance property is a strong blocking set (and hence a non-2-cohyperplanar set). However, as the next result shows, it is enough to take 3 points on each line to get a non-2-cohyperplanar set.

Proposition 2.11. Let $\mathcal{L}$ be a set of lines with avoidance property and let $\mathcal{S}$ be a set of points such that for every $\ell \in \mathcal{L}$,

$$|\mathcal{S} \cap \ell| \geq 3.$$

Then $\mathcal{S}$ is a non-2-cohyperplanar set.

Proof. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two projective hyperplanes and let $\mathcal{V} = \mathcal{H}_1 \cap \mathcal{H}_2$. The subspace $\mathcal{V}$ is of codimension 2, so there exists $\ell \in \mathcal{L}$ such that $\ell \cap \mathcal{V} = \emptyset$. The line ℓ cannot be contained in $\mathcal{H}_1$, since otherwise ℓ would meet also $\mathcal{H}_2$, contradicting $\ell \cap \mathcal{V} = \emptyset$. Symmetrically, ℓ also cannot be contained in $\mathcal{H}_2$. This means that

$$|\ell \cap \mathcal{H}_1| = |\ell \cap \mathcal{H}_2| = 1.$$

Therefore, since $\mathcal{S}$ contains at least 3 points of ℓ, $\mathcal{S}$ contains at least one point outside of $\mathcal{H}_1 \cup \mathcal{H}_2$, meaning that $\mathcal{S}$ is non-2-cohyperplanar. □

Remark 2.12. Proposition 1.9 and Theorem 2.6 imply that, when q is even, the geometric counterparts of 2-outer minimal codes, that is the 2-outer strong blocking sets, are non-2-cohyperplanar. See [4] for more details about 2-outer strong blocking sets and their geometric properties.

We will now give two examples of non-2-cohyperplanar sets of quite small size (with respect to the projective space in which they are defined).

Example 2.13 (Arcs with at least $2k-1$ points). An *arc* in $\mathrm{PG}(k-1,q)$ is a set of points with the property that any k of them span the whole space. It is well-known that arcs in $\mathrm{PG}(k-1,q)$ correspond to MDS codes of dimension k over $\mathbb{F}_q$. Any arc $\mathcal{A}$ with at least $2k-1$ points is non-2-cohyperplanar: the maximum number of points of $\mathcal{A}$ contained in a hyperplane is $k-1$, by definition. Hence, if $|A| > 2(k-1)$, for any couple of hyperplanes $\mathcal{H}_1, \mathcal{H}_2$ there is always a point of $\mathcal{A}$ not contained in $\mathcal{H}_1 \cup \mathcal{H}_2$.

Example 2.14 (The Sparse Tetrahedron). Consider k points $V_1, \ldots, V_k$ of $\mathrm{PG}(k-1,q)$ spanning the whole space. For any $i, j \in \{1, \ldots, k\}, i < j$, consider a point $P_{i,j}$ on the line $\langle V_i, V_j \rangle$, $P_{i,j} \notin \{V_i, V_j\}$. The set

$$\mathcal{T} = \{V_1, \ldots, V_k\} \cup \{P_{i,j} \mid i, j \in \{1, \ldots, k\}, i < j\}$$

is called *sparse tetrahedron*. Such a set is non-2-cohyperplanar. Indeed, the intersection of $\mathcal{T}$ with any hyperplane $\mathcal{H}$ cannot contain all $V_1, \ldots, V_k$. If $\mathcal{T} \cap \mathcal{H}$ does not contain V_i, it also does not contain any line passing through V_i, and in particular, it does not contain any of the lines $\langle V_i, V_j \rangle$. For each of these lines, there is at least a point distinct from V_i not contained in $\mathcal{H}$ (otherwise the whole line would be contained in $\mathcal{H}$). Therefore, we have identified a set of points not contained in $\mathcal{H}$ spanning the whole space. This means that any other hyperplane $\mathcal{H}'$ will not suffice to cover all the points, guaranteeing that we have a non-2-cohyperplanar set.

We may introduce a notion of minimality.

Definition 2.15. A non-2-cohyperplanar set $\mathcal{S}$ is said to be *minimal* if there exist two hyperplanes $\mathcal{H}_1$ and $\mathcal{H}_2$ and a point $P \in \mathcal{S}$ such that $\mathcal{S} \setminus \{P\} \subset \mathcal{H}_1 \cup \mathcal{H}_2$.

Remark 2.16. It is easy to observe that arcs with $2k-1$ points in $\mathrm{PG}(k-1,q)$ and sparse tetrahedrons are examples of minimal non-2-cohyperplanar sets.

Let us conclude the section with a geometric property of non-2-cohyperplanar sets, with a strong coding theoretical implication.

Theorem 2.17. Let $\mathcal{S}$ be a non-2-cohyperplanar set and $\mathcal{H}$ be a hyperplane in $\mathrm{PG}(k-1,q)$. Then

$$|\mathcal{S} \setminus (\mathcal{S} \cap \mathcal{H})| \geq k.$$

Equivalently, if $\mathcal{C}$ is an $[n,k,d]_q$ intersecting code, then $d \geq k$.

Proof. The set $\mathcal{S} \setminus (\mathcal{S} \cap \mathcal{H})$ cannot be contained in a hyperplane, since otherwise $\mathcal{S}$ would be 2-cohyperplanar. Hence, it must contains at least k points. The statement about intersecting codes is a direct consequence of Theorem 2.6. □

3. On the size of small non-2-cohyperplanar sets

While it is easy to give examples of non-2-cohyperplanar sets with many points, it is not clear how small they can be. Moreover, if we add a point to a set that is already non-2-cohyperplanar, it remains non-2-cohyperplanar. Hence, finding the minimum size of a non-2-cohyperplanar set in $\mathrm{PG}(k-1,q)$ is a natural problem and this is the aim of this section.

Definition 3.1. We define $i(k,q)$ to be the *size of the smallest non-2-cohyperplanar set* in $\mathrm{PG}(k-1,q)$ (equivalently, the *length of the shortest linear intersecting code* over $\mathbb{F}_q$ of dimension k).

3.1. Lower bounds.

We start with an easy lower bound.

Theorem 3.2. Let $\mathcal{S}$ be a non-2-cohyperplanar set in $\mathrm{PG}(k-1,q)$. Then $|\mathcal{S}| \geq 2k-1$. Hence

$$i(k,q) \geq 2k-1.$$

If $|\mathcal{S}| = 2k-1$, then $\mathcal{S}$ is an arc.

Proof. Suppose $|\mathcal{S}| \leq 2k-2$. Since any $k-1$ points are always contained in a hyperplane, there must exist two hyperplanes containing $\mathcal{S}$, which gives a contradiction, proving the inequality. Suppose now that $|\mathcal{S}| = 2k-1$. In coding theoretical language, this means that the corresponding code has length $n = 2k-1$. Now, its minimum distance d satisfies $d \geq k$, by Theorem 2.17, and

$$d \leq 2k-1-k+1 = k,$$

by the Singleton bound. Hence $d = k$ and the code is MDS, so that $\mathcal{S}$ is an arc. □

Remark 3.3. Let us underline that Theorem 3.2 implies that the sets introduced in Example 2.13 are the smallest whenever arcs of cardinality $2k-1$ exist. It is well-known that arcs with $q+1$ points exist. The celebrated MDS conjecture, posed by Segre in [54], states that the maximal size of an arc in $\mathrm{PG}(k-1,q)$ (where $2 \leq k \leq q-1$) is $q+1$, up to two exceptional cases for which it is $q+2$. Moreover, if $k \geq q$, the maximal size of an arc is $k+1$. The conjecture has been demonstrated across various parameter sets q and k (see [33] for a survey). In [9], Ball achieved a significant breakthrough by demonstrating that the MDS conjecture holds when q is a prime. In particular, if q is a prime, he proved that every arc with $q+1$ points in $\mathrm{PG}(k-1,q)$, with $2 \leq k \leq q-1$, is a rational normal curve (the geometric counterpart of Reed-Solomon codes). So, under the MDS conjecture,

$$i(k,q) = 2k-1$$

if and only if $k \leq \frac{q+2}{2}$ (or $k \leq \frac{q+3}{2}$ in the exceptional cases). Note that it is not necessary to invoke the MDS conjecture to say that the bound is not tight for large k, because it is well-known that, if $2 \leq k \leq q-1$, arcs cannot exist for k larger than $2q-2$ (see [35, Corollary 7.4.4]).

The following result is a Plotkin-like bound.

Theorem 3.4. For $1 \leq t \leq k$,

$$i(k,q) \geq k + \frac{q^t-1}{q^t-q^{t-1}}(k-t). \tag{1}$$

Proof. Let us give a proof in coding theoretical language. Let $G = (I_k \mid A)$ be a generator matrix of an intersecting $[n, k, d]_q$ code $\mathcal{C}$, and consider t rows of G. Let $\mathcal{V}$ be the multiset of vectors formed by the last $n-k$ coordinates of the nonzero vectors in the rowspan of these t rows. We aim to compute the sum of the weights of all vectors in $\mathcal{V}$, called the total weight of $\mathcal{V}$ and denoted $\mathrm{w}(\mathcal{V})$. Since the t rows are linearly independent, there are $q^t - 1$ vectors in $\mathcal{V}$ (counted with multiplicities). Since any codeword corresponding to a vector of $\mathcal{V}$ has at most t nonzero elements in the first k coordinates, each element of $\mathcal{V}$ must have weight at least $d - t \geq k - t$ (the last inequality comes from Theorem 2.17). This means that

$$\mathrm{w}(\mathcal{V}) \geq (q^t - 1)(k - t).$$

On the other hand, each vector of $\mathcal{V}$ has length exactly $n - k$, and for each coordinate there are at most $q^t - q^{t-1}$ codewords of $\mathcal{V}$ that are nonzero at this coordinate. This yields that the total weight is at most

$$\mathrm{w}(\mathcal{V}) \leq (n - k)(q^t - q^{t-1}).$$

Combining both inequalities finishes the proof. □

Remark 3.5. Note that (1) reduces to the bound in Theorem 3.2 for $t = 1$. By Remark 3.3, the case $t = 1$ give the best bound for small k. When q is large, the case $t = 1$ also gives the best bound. So Theorem 3.4 improves on Theorem 3.2 only when k is large compared with q.

Remark 3.6. For $q = 2$, non-2-cohyperplanar sets coincide with strong blocking sets. In [5], it is proved that $i(k, 2) \geq 3k - 3$. This means that (1) is never tight for $q = 2$, $k > 2$ and any $t \in \{1, \ldots, k\}$. Note also that some structural results on non-2-cohyperplanar sets of cardinality $3k - 3$ are given in [53].

3.2. **Asymptotic lower bounds.** After demonstrating general bounds, we now present asymptotic bounds, which improve upon previous ones for large k (with fixed q). It is worth noting that similar methods have also been employed for general strong blocking sets in [12,53] and for intersecting codes over prime fields in [19,38,42].

Before stating our bound, we must define q-ary upper-bounding functions.

Definition 3.7. Let $\mathcal{C}$ be a code with parameters $[n, k, d]_q$. We define its *rate* $R = k/n$ and its *relative minimum distance* $\delta = d/n$. Let $f : [0, 1] \to [0, 1]$ be a continuous decreasing function. We say that f is *q-ary upper-bounding* if, for any R and δ verifying $R > f(\delta)$, there is no sequence of codes with parameters $[n_s, R \cdot n_s, \delta \cdot n_s]_q$ such that $n_s \to \infty$.

Example 3.8. The Singleton bound stated in Section 1 implies that the function $f(\delta) = 1 - \delta$ is q-ary upper-bounding for any q.

Notice that, by Theorem 2.17, the parameters of intersecting codes must lie in the region

$$\{(\delta, R) \in \mathbb{R}^2_{\geq 0} \mid R \leq \delta\}.$$

By combining this with a suitable q-ary upper-bounding function, one may deduce an upper bound on the asymptotic rate of intersecting codes over $\mathbb{F}_q$, or, equivalently, a lower bound on their length.

Theorem 3.9.

$$\liminf_{k \to \infty} \frac{i(k, q)}{k} \geq 2 + \frac{1}{q - 1}.$$

Proof. The asymptotic Plotkin bound [35, Theorem 2.10.2] corresponds to the q-ary upper-bounding function

$$f(x) = 1 - \frac{q}{q - 1}\, x.$$

The intersection of the graphs of this function and the function $g(x) = x$ corresponding to the bound $R \leq \delta$ is the point $\left(\frac{q-1}{2q-1}, \frac{q-1}{2q-1}\right)$. This produces the upper bound on the asymptotic rate and hence the lower bound above. □

Remark 3.10. Note that the previous result can be also be obtained by Theorem 3.4, by letting t grow to infinity.

By considering the MRRW bound [35, Theorem 2.10.6], instead of the Plotkin bound, one is able to provide a stronger upper bound on the rate for small values of q.

Let H_q be the q-ary entropy function, that is

$$H_q(x) = -x \log_q \left(\frac{x}{q-1}\right) - (1-x)\log_q(1-x).$$

The MRRW bound states that

$$M_q(x) = H_q\left(\frac{1}{q}\left(q-1-(q-2)x - 2\sqrt{(q-1)x(1-x)}\right)\right)$$

is a q-ary upper-bounding function. Using the same argument as above, we get stronger upper bounds on the maximum rate of intersecting codes whenever $q \leq 17$.

Table 1 summarizes the improved bounds obtained this way (some of them were already known in the references cited above).

TABLE 1. Lower bound on the asymptotic length of intersecting codes

q	$\liminf_{k\to\infty} \frac{i(k,q)}{k}$
2	3.5276
3	2.8272
4	2.5713
5	2.4342
7	2.2862
8	2.2411
9	2.2060
11	2.1547
13	2.1185
16	2.0802
17	2.0703

Theorem 3.11. The MRRW bound yields a better upper bound on the rate of intersecting codes than the Plotkin bound when $q \leq 17$. In other words, if and only if $q \geq 19$, the following holds :

$$M_q\left(\frac{q-1}{2q-1}\right) \geq \frac{q-1}{2q-1}.$$

Proof. First we must compute $A(x) = \frac{1}{q}\left(q-1-(q-2)x - 2\sqrt{(q-1)x(1-x)}\right)$ with $x = \frac{q-1}{2q-1}$. This yields

$$A\left(\frac{q-1}{2q-1}\right) = \frac{(q-1)(\sqrt{q}-1)^2}{q(2q-1)}.$$

We now want to know for what values of q it is true that

$$M_q\left(\frac{q-1}{2q-1}\right) \geq \frac{q-1}{2q-1}.$$

Now, for simplicity, set $B(q) = q(2q-1) - (q-1)(\sqrt{q}-1)^2$, $C(q) = (2q-1)q$ and $D(q) = (q-1)(\sqrt{q}-1)^2$, and define $g(x) = x\log_q(x)$. Note that $B(q)$, $C(q)$ and $D(q)$ are all positive. By

straightforward computations, the above inequality is equivalent to

$$g(B(q)) - (q-1)g\left(\frac{D(q)}{q-1}\right) + g(C(q)) \geq q(q-1).$$

Since g is a convex function, and since $D(q) = C(q) - B(q)$, we can give the following lower bound

$$g(C(q)) - g(B(q)) \geq D(q)g'(B(q)) = D(q)\log_q(eB(q)).$$

Therefore it is sufficient to establish

$$D(q)\log_q(eB(q)) - D(q)\log_q((\sqrt{q}-1)^2) \geq q(q-1)$$

and this simplifies to

$$(\sqrt{q}-1)^2 \log_q\left(\frac{eB(q)}{(\sqrt{q}-1)^2}\right) \geq q.$$

Since $(\sqrt{q}-1)^2 \leq q$, in order for the above inequality to be true it is enough to have

$$\begin{aligned}(\sqrt{q}-1)^2 \log_q\left(\frac{eB(q)}{q}\right) &\geq q\\ (\sqrt{q}-1)^2 \log_q(eq) &\geq q\\ q &\geq 2\sqrt{q}(\ln(q)+1)\\ 1 + \frac{1}{2}\cdot\sqrt{q} &\geq \ln(q)\end{aligned}$$

Writing $f(x) = 1 + \frac{1}{2}\cdot\sqrt{x} - \ln(x)$, it is easy to check that f is increasing as soon as $x \geq 16$.

In particular, straightforward computation shows that $f(144) > 0$, meaning that as soon as $q \geq 144$ we have

$$M_q\left(\frac{q-1}{2q-1}\right) \geq \frac{q-1}{2q-1}.$$

For the remaining values of q, that is for $19 \leq q \leq 144$, the theorem can be checked by direct computation. □

3.3. **Upper bounds.** The sparse tetrahedron construction, presented in the Example 2.14, yields a non-2-cohyperplanar set of size $k(k+1)/2$ in $\mathrm{PG}(k-1,q)$, therefore providing an upper bound on $i(k,q)$, namely

$$i(k,q) \leq \frac{k(k+1)}{2}.$$

Note that this construction correspond to codes with parameters $\left[\frac{k(k+1)}{2}, k, k\right]$ (the minimum distance can be easily obtained by a geometric argument). In particular, this is not a family of asymptotically good codes.

The following result is an upper bound obtained from a probabilistic existence result (equivalent to taking random points in the projective space). Let us highlight the fact that this is already known for prime fields: for $q = 2$ it is due to Komlós (unpublished proof, 1983, cited in [19]), and for the more general case when q is a prime, we know of no earlier proof than [42, Theorem 7.3]. Our proof follows the same arguments and we write it explicitly for the sake of completeness.

Let us recall that the *Gaussian coefficient* $\begin{bmatrix}N\\K\end{bmatrix}_q$ is the number of subspace of dimension K in a vector space of dimension N over $\mathbb{F}_q$, that is

$$\begin{bmatrix}N\\K\end{bmatrix}_q = \prod_{i=0}^{K-1} \frac{q^N - q^i}{q^K - q^i}.$$

Theorem 3.12. If

$$n \geq \frac{2}{\log_q(\frac{q^2}{2q-1})}\ k$$

then an $[n,k,d]_q$ intersecting code, or equivalently, a non-2-cohyperplanar set in $\mathrm{PG}(k-1,q)$ of cardinality n, exists. Hence

$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq \frac{2}{\log_q(\frac{q^2}{2q-1})}.$$

Proof. We follow the classical counting arguments used, for example, in the well-know Gilbert–Varshamov bound (see [35, Theorem 2.10.8]). Again, we will use coding-theoretical language.

Let

$$\mathcal{B}_n = \{\{x,y\} \subseteq \mathbb{F}_q^n \mid \sigma(x) \cap \sigma(y) = \emptyset\}.$$

For each coordinate $i \in \{1,\dots,n\}$ of a pair of vectors $\{x,y\}$ in $\mathcal{B}_n$ we have three possibilities:

$$(x_i \neq 0 \wedge y_i = 0) \vee (x_i = 0 \wedge y_i \neq 0) \vee (x_i = 0 \wedge y_i = 0).$$

Hence $|\mathcal{B}_n| = (2(q-1)+1)^n = (2q-1)^n$.

Let

$$\mathcal{F}_{n,k} = \{\mathcal{C} \subseteq \mathbb{F}_q^n \mid \dim \mathcal{C} = k\},$$

whose cardinality is clearly $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Now, each pairs of vectors in $\mathcal{B}_n$ is contained in exactly $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_q$ elements of $\mathcal{F}_{n,k}$. A code in $\mathcal{F}_{n,k}$ is interesting if and only if it does not contain any element of $\mathcal{B}_n$. Since there are at most

$$(2q-1)^n \cdot \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_q$$

codes in $\mathcal{F}_{n,k}$ which contains an element of $\mathcal{B}_n$, if

$$(2q-1)^n \cdot \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}_q \leq \begin{bmatrix} n \\ k \end{bmatrix}_q$$

then there exist intersecting codes with parameters $[n,k]_q$. By straightforward calculations we get that the above condition is implied by $q^{n\log_q(2q-1)+2(k-n)} \leq 1$, hence the statement. □

Corollary 3.13. Intersecting codes are asymptotically good.

Proof. Theorem 3.12 and Theorem 2.17 yield that a family of

$$\left[\frac{2}{\log_q(\frac{q^2}{2q-1})}\ k, k, \geq k\right]_q$$

intersecting codes exist. This is an asymptotically good family. □

Remark 3.14. Even though Theorem 3.12 provides a very good upper bound (converging to the same value as the lower bound for large q), it has the drawback of not providing guidance on how to *explicitly* construct such small cardinality sets. The following section will be dedicated to such constructions.

TABLE 2. Values of $i(k,q)$ for small q and k

q \ k	2	3	4	5	6	7	8	9
2	3	6	9	13	15	20	24	26
3	3	6	9	10	13	[17, 18]	[19, 21]	[21, 30]
4	3	5	8	10	[12, 13]	[15, 16]	[17, 21]	[21, 25]
5	3	5	8	10	[12, 13]	[15, 17]	[18, 21]	[20, 25]
7	3	5	7	10	[12, 13]	14	[17, 21]	[19, 25]
8	3	5	7	9	[12, 13]	[14, 15]	[16, 21]	[19, 25]
9	3	5	7	9	12	[14, 15]	[16, 21]	[18, 25]

3.4. **Explicit examples for low dimensions and small base fields.** We end this section with a list of explicit computations of the actual value of $i(k,q)$ for small values of k and q. We summarize in Table 2 all the known results, whose proof is given below. Whenever we write $[n_1, n_2]$ we mean that $i(k,q)$ is not known but contained in this interval. The colors indicate the argument used to prove the lower or upper bound, as we will explain at the end of this subsection.

For the first line of Table 2, we refer to [39], where these values are given in the context of minimal codes.

Whenever $2k-1 \leq q+1$, we may take a $[2k-1, k, k]_q$ MDS code, that is $2k-1$ points on an arc. In dimension 2, it is always sufficient to take 3 distinct points.

For $q = 3$, the $[6, 3, 3]_3$ code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

is intersecting and it is clearly the shortest (a $[5, 3, \geq 3]_3$ code does not exist).

For $q = 3$, there is no $[8, 4, 4]_3$ intersecting code by MAGMA calculations, but an intersecting $[9, 4, 4]_3$ exists by concatenation (see Lemma 1.5).

For $q = 4$, the $[8, 4, 4]_4$ code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & \alpha \\ 0 & 0 & 0 & 1 & 0 & \alpha & \alpha^2 & 1 \end{bmatrix}$$

(here α is a primitive element of $\mathbb{F}_4$) is intersecting and it is clearly the shortest (a $[7, 4, \geq 4]_4$ code does not exist).

For $q = 5$, the $[8, 4, 4]_5$ code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 & 4 & 2 & 4 & 0 \\ 0 & 0 & 1 & 0 & 0 & 4 & 2 & 4 \\ 0 & 0 & 0 & 1 & 4 & 1 & 3 & 4 \end{bmatrix}$$

is intersecting and it is clearly the shortest (a $[7, 4, \geq 4]_5$ code does not exist).

For $q \in \{3,4,5,7\}$, the $[10,5,5]_q$ code with generator matrix G_q equal to

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 \end{bmatrix}, \quad G_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \alpha & 0 & 1 & \alpha^2 & \alpha \\ 0 & 1 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 0 & 1 & 0 & \alpha^2 & \alpha & 1 & 0 & \alpha^2 \\ 0 & 0 & 0 & 0 & 1 & \alpha^2 & 1 & 1 & \alpha & 1 \end{bmatrix},$$

$$G_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 2 & 4 & 3 \\ 0 & 0 & 1 & 0 & 0 & 4 & 2 & 1 & 4 & 3 \\ 0 & 0 & 0 & 1 & 0 & 4 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 & 4 & 3 & 0 & 1 & 4 \end{bmatrix}, \quad G_7 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 3 & 6 & 6 & 3 \\ 0 & 0 & 1 & 0 & 0 & 3 & 4 & 2 & 5 & 1 \\ 0 & 0 & 0 & 1 & 0 & 5 & 5 & 0 & 4 & 2 \\ 0 & 0 & 0 & 0 & 1 & 6 & 1 & 6 & 6 & 0 \end{bmatrix},$$

is intersecting and it is clearly the shortest (a $[9,5,\geq 5]_q$ code does not exist).

For $q = 3$, the $[13,6,6]_3$ code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 0 & 0 & 1 & 1 & 2 \end{bmatrix}$$

is intersecting and it is the shortest: actually, there is no $[11,6,\geq 6]_3$ code and every $[12,6,6]_3$ is equivalent to the extended ternary Golay code (see [49]), which is not intersecting.

For $q = 9$, the $[12,6,6]_9$ code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \alpha^7 & 2 & \alpha^6 & \alpha^3 & \alpha^6 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 2 & \alpha & \alpha^7 & \alpha & 1 & \alpha \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & \alpha^7 & 2 & \alpha & \alpha^6 & \alpha^2 \\ 0 & 0 & 0 & 1 & 0 & 0 & \alpha^6 & 0 & \alpha^2 & 1 & 1 & \alpha \\ 0 & 0 & 0 & 0 & 1 & 0 & \alpha^3 & \alpha^2 & 1 & \alpha & \alpha^6 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & \alpha^3 & \alpha^6 & \alpha & \alpha & \alpha & \alpha^3 \end{bmatrix}$$

is intersecting and it is clearly the shortest (a $[11,6,\geq 6]_9$ code does not exist).

For $q = 7$, the $[14,7,7]_7$ code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 4 & 3 & 2 & 2 & 6 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 6 & 3 & 3 & 4 & 3 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 6 & 3 & 3 & 4 & 3 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 6 & 3 & 3 & 4 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 3 & 2 & 2 & 6 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 3 & 2 & 2 & 6 & 3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 4 & 3 & 2 & 2 & 6 & 3 \end{bmatrix}$$

is intersecting and it is clearly the shortest (a $[13,7,\geq 7]_7$ code does not exist).

The lower bounds are all in blue and they follow from Theorem 2.17 and from the database of the codes with the best known parameters in Magma. The upper bounds in orange (that is, exactly for the columns corresponding to $k = 8$ and $k = 9$) may be obtained by concatenating the shortest intersecting codes over proper extensions (see Lemma 1.5). The bounds in green come from extensive research in Magma. This has been done by starting from an $[n,k-1,d]_q$ optimal intersecting code and randomly building an $[n,k,d]_q$ code from it or simply taking the codes with the best known parameters in Magma.

4. Small explicit constructions for large dimensions

In the previous sections we provided bounds on the size of the smallest non-2-cohyperplanar sets in projective spaces of given dimensions, together with a non-constructive existence result. The sets presented in Example 2.13 meet the bound for small dimensions, as we have already observed. The aim of this section is to provide *explicit* constructions of small non-2-cohyperplanar sets, or equivalently of short intersecting codes, for large dimensions.

4.1. **Algebraic geometry intersecting codes.** Algebraic geometry is a useful tool for constructing families of codes with good parameters. These codes, called *algebraic geometry codes*, are a generalization of Reed-Solomon codes: whereas Reed-Solomon codes are obtained from the evaluation of polynomials of bounded degree in several points of $\mathbb{F}_q$, algebraic geometry codes are obtained by evaluating polynomials from the Riemann-Roch space of a divisor over an algebraic curve over $\mathbb{F}_q$. For a more extensive introduction to algebraic geometry codes, we refer the reader to [34, Chapter 15]. The family of algebraic geometry codes provides *explicit* constructions of asymptotically good codes, some of which turn out to be intersecting. In many cases however, in order to obtain explicit constructions with maximum rate we need to concatenate algebraic geometry codes with well-chosen intersecting codes of low dimension. For instance, when q is a prime, there are no constructions of asymptotically good AG codes, meaning we must concatenate intersecting AG codes over some extension of $\mathbb{F}_q$ with suitable intersecting codes over $\mathbb{F}_q$.

First we define the Singleton defect of a code.

Definition 4.1. Let $\mathcal{C}$ be a code with parameters $[n, k, d]_q$. Its *Singleton defect* is the quantity

$$\Delta = 1 - \frac{k+d}{n+1}.$$

Notice that a code is MDS if and only if $\Delta = 0$, while a code with "bad" parameters has a large Singleton defect.

Definition 4.2. The *Ihara constant* of $\mathbb{F}_q$ is

$$A(q) = \limsup_{g(X)\to\infty} \frac{n(X)}{g(X)},$$

where X ranges over all curves over $\mathbb{F}_q$, $n(X) = |X(\mathbb{F}_q)|$ is the number of rational points of X and $g(X)$ is the genus of X.

The best possible Singleton defect attainable by AG codes is $A(q)^{-1}$ ([34, Chapter 15, Corollary 15.3.14]). Note also that, provided the Singleton defect is at least $A(q)^{-1}$, any choice of parameters R and δ that sum to $1-A(q)^{-1}$ is attainable. The Drinfeld-Vladut bound [57, Theorem 2.3.22] states that $A(q) \leq \sqrt{q} - 1$, which gives a lower bound on the best possible Singleton defect reachable by AG codes. Nevertheless, there exist explicit constructions of AG codes with Singleton defect close to this lower bound. Most notably, when q is a square it is possible to reach the Drinfeld-Vladut bound, as first proved in [37].

In [50], the author establishes the following theorem:

Theorem 4.3 (Theorem 2, [50])**.** Suppose that $A(q) \geq 4$. Then there exists an explicit family of asymptotically good intersecting codes with asymptotic rate

$$R = \frac{1}{2} - \frac{1}{2A(q)}.$$

Remark 4.4. The proof of Theorem 4.3 relies on non-trivial algebraic geometric arguments. A simpler way to construct intersecting AG codes would be to consider families of AG codes with

$\delta > 1/2$, which are intersecting, by Lemma 1.10. The best possible rate using this method is

$$R = \frac{1}{2} - \frac{1}{A(q)}.$$

Hence, Theorem 4.3 is an improvement over this simpler method.

Theorem 4.3 often yields the best-known explicit constructions of intersecting codes over $\mathbb{F}_q$. However, when q is small, or a prime, $A(q) \leq 4$. In these cases, it is therefore necessary to use concatenation in order to construct explicit sequences of intersecting AG codes of short length.

Remark 4.5. Before diving into the details, we make one more observation. The highest rate of a non-trivial intersecting code is attained by a code with parameters $[3, 2, 2]_q$ (over any base field), corresponding to three distinct points on the projective line. Moreover, an intersecting AG code constructed with the above theorem must have rate lower than $1/2$. This means that any non-trivial concatenation of an intersecting code with intersecting AG codes must have a rate of at most $1/3$. Consequently, if over some field $\mathbb{F}_q$ there are intersecting AG codes that have rate larger than $1/3$, there is no construction involving concatenation that will yield a better rate.

Theorem 4.6. The following upper bounds, which stem from *explicit* constructions involving (possibly concatenated) AG codes, hold:

- if q is a square and $q \geq 25$, then
$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq 2 + \frac{2}{\sqrt{q}-2};$$
- if $q = p^{2m+1}$ is an uneven power of a prime (but not a prime) and $q \geq 32$, then
$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq \frac{4}{2 - \frac{1}{p^m-1} - \frac{1}{p^{m+1}-1}},$$
- If q is a prime and $q \geq 11$, then
$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq 3 + \frac{3}{q-2}.$$

For the remaining values of q, Table 3 provides the upper bounds obtained by concatenating AG codes with suitable intersecting codes.

TABLE 3. Upper bounds obtained with AG codes, for exceptional values of q

q	Parameters of inner code	Upper bound for $\limsup_{k\to\infty} i(k,q)/k$	Probabilistic bound
2	$[15, 6]_2$	5.8334	4.8189
3	$[10, 5]_3$	4.3561	3.7382
4	$[5, 3]_4$	4.1667	3.3539
5	$[5, 3]_5$	3.9025	3.1507
7	$[7, 4]_7$	3.5745	2.9331
8	$[3, 2]_8$	3.5	2.8666
9	$[3, 2]_9$	3.4286	2.8148
16	$[3, 2]_{16}$	3.2143	2.6266
27	$[3, 2]_{27}$	3.12	2.5146

Proof. In all three cases we call R_q the largest rate reached by AG codes over $\mathbb{F}_q$. Recall that we will then obtain the asymptotic upper bound

$$\limsup_{k\to\infty} \frac{i(k,q)}{k} \leq R_q^{-1}.$$

- As we have already mentioned, when q is a square, there are explicit constructions of AG codes reaching the Drinfeld-Vladut bound, that is, with Singleton defect equal to $(\sqrt{q}-1)^{-1}$. The best possible rate yielded by Theorem 4.3 is
$$R_q = \frac{1}{2} - \frac{1}{2(\sqrt{q}-1)}.$$
For the hypotheses of Theorem 4.3 to be verified, we must have $q \geq 25$. Note that Remark 4.5 tells that we do not need to concatenate, since as soon as $q \geq 25$, we have $R \geq 3/8 \geq 1/3$.
- When $q = p^{2m+1}$ (with $m \geq 1$), a prominent result shown in [11] provides an explicit construction of AG codes satisfying the lower bound
$$A(q) \geq 2\left(\frac{1}{p^m - 1} + \frac{1}{p^{m+1} - 1}\right)^{-1}.$$
In order to satisfy the hypothesis of Theorem 4.3, we need $A(q) \geq 4$. This is the case for every value of q except $q = 8$ and $q = 27$. Again, in this case Remark 4.5 tells that we do not need to concatenate.
- If q is a prime, there are no explicit constructions of asymptotically good intersecting AG codes. Hence we need to concatenate. When $q \geq 11$ it is straightforward to check that concatenating AG codes over $\mathbb{F}_{q^2}$ whose parameters meet the Drinfeld-Vladut bound with a $[3, 2, 2]_q$ code will always produce the shortest explicit construction. This yields
$$R_q \geq \frac{2}{3} \cdot \left(\frac{1}{2} - \frac{1}{2(q-1)}\right) = \frac{1}{3} - \frac{1}{3(q-1)}.$$

The remaining cases are obtained by concatenation, in each case using Theorem 4.3 and the best known lower bounds on $A(q)$ to obtain the best possible rate for the outer code. □

Remark 4.7 (Comparison with the probabilistic bound of Theorem 3.12)**.** The bound from Theorem 4.6 outperforms the probabilistic bound exactly in the following cases:

- if $q \geq 49$ is a square;
- if $q \geq 128$ is an odd power of a prime.

Hence the asymptotic upper bound provided by Theorem 4.6 is best for almost all non-prime q. Moreover, this is a *constructive* bound: the codes that reach it can be explicitly constructed in polynomial time, as noted in [50].

Remark 4.8. Recall that in the binary case intersecting codes coincide with minimal codes (see Lemma 1.7). There exist numerous short constructions of minimal codes, for instance in [7,10,21]. To the best of our knowledge, the shortest explicit construction was given in [21]. The construction recorded in Table 3 provides an improvement and it is, to the best of our knowledge, the shortest *explicit* construction of minimal codes over $\mathbb{F}_2$.

4.2. **A construction using expander graphs.** In this subsection we provide an explicit construction of non-2-cohyperplanar sets using expander graphs, based on the approach used in [7] for strong blocking sets. Even though the resulting construction will be longer than the one in the previous subsection, we believe that it is still interesting because it provides a geometric insight into non-2-cohyperplanar sets, as well as a link with other well-known combinatorial and geometric objects. We will construct small sets of lines with avoidance property and we will take 3 points on each line, obtaining a small non-2-cohyperplanar set, by Proposition 2.11.

Definition 4.9. Let $\mathcal{G} = (V, E)$ be a graph with n vertices, say $V = \{u_1, \ldots, u_n\}$. The *adjacency matrix* $A_{\mathcal{G}}$ of $\mathcal{G}$ is the $n \times n$ matrix with coefficients $a_{i,j} = |\{\text{edges connecting } u_i \text{ and } u_j\}|$.

The matrix is clearly diagonalizable over the real field (it is symmetric). Let us call $\lambda_1(\mathcal{G}) \geq \lambda_2(\mathcal{G}) \geq \ldots \geq \lambda_n(\mathcal{G})$ its eigenvalues. Recall that if $\mathcal{G}$ is t-regular, then $\lambda_1(\mathcal{G}) = t$. We also define

$$\lambda(\mathcal{G}) = \max\{|\lambda_2(\mathcal{G})|, \ldots, |\lambda_n(\mathcal{G})|\}.$$

Definition 4.10. An (n, t, λ)-*graph* $\mathcal{G}$ is a t-regular graph with n vertices such that $\lambda(\mathcal{G}) \leq \lambda$. A t-regular graph $\mathcal{G}$ with $\lambda(\mathcal{G}) \leq 2\sqrt{t-1}$ is called *Ramanujan graph*.

Theorem 4.11 (Alon-Bopanna)**.** For an (n, t, λ)-graph,

$$\lambda \geq 2\sqrt{t-1} - o(1)$$

as $n \to \infty$.

In [6], the author proves the following.

Theorem 4.12 (Theorem 1.3, [6])**.** For every degree t, every ε and all sufficiently large $n \geq n_0(t, \varepsilon)$, where nt is even, there is an explicit construction of an (n, t, λ)-graph with

$$\lambda \leq 2\sqrt{t-1} + \varepsilon.$$

The following is an invariant of graphs, which will be fundamental to get our construction.

Definition 4.13. Let $\mathcal{G} = (V, E)$ be a simple connected graph. For any subgraph $\mathcal{H}$, let $\kappa(\mathcal{H})$ denote the largest size of a connected component in $\mathcal{H}$. The *integrity* of $\mathcal{G}$ is the integer

$$\iota(\mathcal{G}) = \min\{|S| + \kappa(\mathcal{G} - S) \mid S \subseteq V\}.$$

Proposition 4.14 (Corollary 3.4, [7])**.** For an (n, t, λ)-graph $\mathcal{G}$,

$$\iota(\mathcal{G}) \geq n \cdot \frac{t-\lambda}{t+\lambda}.$$

The next result, proved in [7], is the link between the theory of expander graphs and lines with the avoidance property, and then with strong blocking sets and non-2-cohyperplanar sets.

Proposition 4.15 (Lemma 4.4, [7])**.** Let $\mathcal{M} = \{P_1, \ldots, P_n\} \subseteq \mathrm{PG}(k-1, q)$ be a projective $[n, k, d]_q$ system and $\mathcal{G} = (\mathcal{M}, E)$ a graph. If

$$\iota(\mathcal{G}) \geq n - d + 1,$$

then the set of lines

$$\mathcal{L}(\mathcal{M}, \mathcal{G}) = \{\langle P_i, P_j\rangle \mid P_iP_j \in E\}$$

satisfies the avoidance property.
Hence, if $\mathcal{G}$ is an (n, t, λ)-graph and

$$\frac{t-\lambda}{t+\lambda} \geq 1 - \delta + \frac{1}{n},$$

then $\mathcal{L}(\mathcal{M}, \mathcal{G})$ satisfies the avoidance property.

Combining Theorem 4.11, Theorem 4.12, Proposition 4.15 and Proposition 2.11, we obtain the following result.

Theorem 4.16. Assume that there is an explicit construction of projective $[n, Rn, \delta n]_q$ systems and an integer t such that

$$\frac{t - 2\sqrt{t-1}}{t + 2\sqrt{t-1}} > 1 - \delta.$$

Then there exist *explicit* families of non-2-cohyperplanar sets with size tending to

$$\left(1 + \frac{t}{2}\right) n,$$

as $n \to \infty$.

Proof. Let $\varepsilon > 0$ and choose $n \geq n_0(t, \varepsilon)$ such that nt is even. We call $\mathcal{M}$ the projective $[n, Rn, \delta n]_q$ system. By Theorem 4.12, there is an explicit construction of a (n, t, λ)-graph with $\lambda = 2\sqrt{t-1}+\varepsilon$. Let us call this graph $\mathcal{G}_{n,t} = (V_{n,t}, E_{n,t})$. Notice that by our assumptions it is possible to choose ε small enough and n large enough so that

$$\frac{t-\lambda}{t+\lambda} \geq 1 - \delta + \frac{1}{n}.$$

Therefore, $\mathcal{L}(\mathcal{M}, \mathcal{G}_{n,t})$ satisfies the avoidance property.

By Proposition 2.11, if we choose 3 points on every line of $\mathcal{L}(\mathcal{M}, \mathcal{G}_{n,t})$, we get a non-2-cohyperplanar set. In order to get the smallest such set, we choose every vertex and one point (different from the vertices) on every edge of $\mathcal{G}_{n,t}$. This yields $n + nt/2$ points. □

Let us give one example of an application of Theorem 4.16. For simplicity's sake, we will consider only the case when q is a square, since this yields the best possible AG codes as well as the simplest formula for the Singleton defect (which is nice for computations). Consider a family of AG $[n, Rn, \delta n]_q$ codes such that

$$R + \delta = 1 - \frac{1}{\sqrt{q}-1}.$$

Note that the size of the non-2-cohyperplanar set that we may obtain is

$$\left(1 + \frac{t}{2}\right) n = \frac{1 + t/2}{R} \cdot k,$$

where k is the dimension of the AG code. According to Theorem 4.16, we need t verifying

$$\frac{t - 2\sqrt{t-1}}{t + 2\sqrt{t-1}} > 1 - \delta = R + \frac{1}{\sqrt{q}-1}.$$

Setting

$$R(q,t) = \frac{t - 2\sqrt{t-1}}{t + 2\sqrt{t-1}} - \frac{1}{\sqrt{q}-1}$$

and

$$\alpha(q,t) = \frac{1 + t/2}{R(q,t)},$$

we want to minimize the value of $\alpha(q,t)$. Notice that since t is the degree of a vertex, t has to be an integer, which rather limits the possibilities for optimization for a given q.

When $q \to \infty$, the second term in the expression of $R(q,t)$ vanishes. This yields an expression of $\alpha(q,t)$ which does not depend on q, for which it is easy to check that the minimum value is reached for $t = 10$. Hence we get explicit constructions of non-2-cohyperplanar sets with

$$R(q,10) = \frac{1}{4} - \frac{1}{\sqrt{q}-1}$$

and

$$\alpha(q,10) = \frac{6}{R(q,10)} \to 24,$$

as $q \to \infty$.

By computing the value of $\alpha(q,t)$ for integer values of t, it is possible to verify that, for $q \geq 89^2$, $t = 10$ gives the minimum value for $\alpha(q,t)$. For smaller values of q, the best values of t and of $\alpha(q,t)$ are reported in Table 4. For $q = 4$ the Singleton defect is 1 so $R > 0$ is impossible, meaning that our construction does not work.

TABLE 4. Smallest values of $\alpha(q,t)$ for small square q

q	t	$\alpha(q,t)$
3^2	86	299.5378
4^2	39	110.0490
5^2	27	71.8927
7^2	20	48.6300
8^2	18	43.7121
9^2	17	40.4255
11^2	15	36.2747
13^2	14	33.7937
16^2	13	31.5103
$17^2 \leq q \leq 19^2$	13	~ 30
$23^2 \leq q \leq 27^2$	12	~ 28
29^2	12	27.7441
$31^2 \leq q \leq 32^2$	11	~ 27
$37^2 \leq q \leq 49^2$	11	~ 26
$53^2 \leq q \leq 83^2$	11	~ 25

5. On the 2-wise weighted Davenport constants

In this section we investigate links between intersecting codes and zero-sum problems over finite abelian groups, in particlar with generalizations of the Davenport constant. Zero-sum problems over finite abelian groups have been studied since the 1960s, and the Davenport constant and its generalizations remain a main subject in this area (see [27] for a general survey on the topic). The coding theoretical approach to problems about zero-sum subsequences in finite abelian groups is not new (see for example [22,41]) and an investigation of the Davenport constant with these methods has been already done in [42,48]. However, our framework is more general: we consider intersecting codes over any finite field and their relation with weighted Davenport constants.

5.1. The general setting.

Let G be a finite abelian group.

Definition 5.1. Let $a_1, \ldots, a_n \in G$ be a finite sequence of elements of G. For such a sequence, we define a *zero-sum subsequence* as a sequence $a_{i_1}, \ldots, a_{i_r}$, with $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$, verifying $\sum_{k=1}^{r} a_{i_k} = 0$.

If a sequence is long enough, then necessarily it admits a zero-sum subsequence. Therefore, it makes sense to ask from which threshold this occurs for all sequences.

Definition 5.2. The *Davenport constant* of G, noted $\mathrm{D}(G)$, is the smallest integer ℓ such that every sequence of ℓ elements of G has a zero-sum subsequence.
The quantity $\mathrm{d}(G)$ is the largest integer ℓ such that there is a sequence of length ℓ with no zero-sum subsequences.

Remark 5.3. The quantity $\mathrm{d}(G)$ is sometimes also referred to as the small Davenport constant in the literature. This will also be the case in the present article. One has

$$\mathrm{D}(G) = \mathrm{d}(G) + 1.$$

Remark 5.4. Another definition of the Davenport constant (which is equivalent in this setting) goes as follows: consider only zero-sum sequences of G, that is sequences $a_1, \ldots, a_n \in G$ such that $\sum_{i=1}^{n} a_i = 0_G$. Then $\mathrm{D}(G)$ is the length of the longest such sequence that does not split into 2 disjoint non-trivial zero-sum subsequences. Indeed, considering a zero-sum sequence of length $n > \mathrm{D}(G)$, it is possible to take the first $\mathrm{D}(G)$ terms, among which there will be a zero-sum subsequence by

definition. Its complement must be a zero-sum subsequence as well. Therefore the whole zero-sum sequence splits into 2 disjoint zero-sum subsequences. Conversely, there are sequences of length $\mathrm{d}(G)$ with no zero-sum subsequence, meaning that by adding one last element in order to form a zero-sum sequence of length exactly $\mathrm{D}(G) = \mathrm{d}(G)+1$ we get a sequence which clearly does not have 2 disjoint zero-sum subsequences.

Example 5.5. Let C_n be the (additive) cyclic group with n elements and let 1 denote a generating element. The sequence $a_1 = 1, \ldots, a_{n-1} = 1$ is a sequence of length $n-1$ with no zero-sum subsequence. Therefore $\mathrm{d}(C_n) \geq n-1$, which implies $\mathrm{D}(C_n) \geq n$. It is well-known that $\mathrm{D}(G) \leq |G|$. Hence, $\mathrm{D}(C_n) = n$.

The Davenport constant has been studied intensively, and in fact it has been generalized in a number of ways, two of which we present and use here.

Let us define first the multiwise Davenport constants, a generalization introduced by Halter-Koch in [32].

Definition 5.6. Let $a_1, \ldots, a_n \in G$ be a finite sequence of elements of G and j be a positive integer. We say that j zero-sum subsequences are *disjoint* if their indices belong to j disjoint subsets of $\{1, \ldots, n\}$.

The *j-wise Davenport constant* $\mathrm{D}_j(G)$ is the smallest integer ℓ such that every sequence of ℓ elements of G has j disjoint zero-sum subsequences.

The usual Davenport constant is $\mathrm{D}_1(G) = \mathrm{D}(G)$. Clearly, one has

$$\mathrm{D}(G) \leq \mathrm{D}_j(G) \leq j\mathrm{D}(G). \tag{2}$$

The second generalization arises when considering weighted zero-sum subsequences. There are various natural ways to introduce weights in these types of problems. The one that we recall below received considerable attention in the last two decades since the work of Adhikari et al. [1,2].

Definition 5.7. Let $a_1, \ldots, a_n \in G$ be a finite sequence of elements of G and let

$$\emptyset \neq W \subseteq \{0, 1, \ldots, \exp(G) - 1\}.$$

A *W-weighted zero-sum subsequence* is a sequence $a_{i_1}, \ldots, a_{i_r}$, with $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$, verifying

$$\sum_{i=1}^{r} \varepsilon(i) a_{j_i} = 0$$

for some $\varepsilon : \mathbb{N} \to W$. In case $W = \{1, \ldots, \exp(G) - 1\}$ the sequence is called a *fully-weighted zero-sum subsequence*.

The *W-weighted Davenport constant* $\mathrm{D}^W(G)$ is the smallest integer ℓ such that every sequence of ℓ elements of G has a W-weighted zero-sum subsequence.

The *fully-weighted Davenport constant* $\mathrm{D}^f(G)$ is the smallest integer ℓ such that every sequence of ℓ elements of G has a fully-weighted zero-sum subsequence.

Instead of considering subsets of $\{0, 1, \ldots, \exp(G) - 1\}$ one could also consider subsets of the integers, yet this is essentially equivalent.

It is also possible to examine multiwise weighted Davenport constants.

Definition 5.8. The *j-wise W-weighted Davenport constant* $\mathrm{D}_j^W(G)$ is the smallest integer ℓ such that every sequence of length ℓ of G has j disjoint W-weighted zero-sum subsequences. The *j-wise fully-weighted Davenport constant* $\mathrm{D}_j^f(G)$ is $\mathrm{D}_j^W(G)$ with $W = \{1, \ldots, \exp(G) - 1\}$.

When $j = 2$, there is a relation between this last constant and intersecting codes over prime fields, as remarked in [42,48]. We will explain this link in a more general scenario (see Theorem 5.12), including intersecting codes over any finite field.

5.2. **Our generalization.** We are now ready to properly define our generalization of the fully-weighted Davenport constant. Let us first recall the definition of $\mathcal{W}$-weighted Davenport constant where the set of weights $\mathcal{W}$ is defined as a non-empty subset of endomorphisms of G. This was first introduced in [58]. The interested reader may also refer to [31].

Definition 5.9. Let G be a finite abelian group and let $\mathcal{W}$ be a non-empty set of group endomorphisms of G, which we call a *set of weights* for G. Let $a_1, \ldots, a_n \in G$ be a finite sequence of elements of G and $\mathcal{W}$ a set of weights for G. A *$\mathcal{W}$-weighted zero-sum subsequence* is a sequence $a_{i_1}, \ldots, a_{i_r}$, with $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$, verifying

$$\sum_{i=1}^{r} \varepsilon_i(a_{j_i}) = 0$$

for some $\varepsilon_i \in \mathcal{W}$.

Let j be a positive integer. The *j-wise $\mathcal{W}$-weighted Davenport constant* $\mathrm{D}_j^{\mathcal{W}}(G)$ is the smallest integer ℓ such that any sequence of length ℓ of G has j disjoint $\mathcal{W}$-weighted zero-sum subsequences. Similarly, the *j-wise $\mathcal{W}$-weighted small Davenport constant* $\mathrm{d}_j^{\mathcal{W}}(G)$ is the largest integer ℓ such that there exists a sequence of length ℓ of G that does not have j disjoint $\mathcal{W}$-weighted zero-sum subsequences.

When G is an elementary p-group, that is, when

$$G = E_{p^{hr}} = \underbrace{C_p \oplus \ldots \oplus C_p}_{hr \text{ times}},$$

the elementary abelian group of order p^{hr} (here p is a prime and h and r are positive integers), it is possible to consider a group isomorphism $E_{p^{hr}} \cong \mathbb{F}_q^r$, where $q = p^h$. Clearly, this concerns only the additive part. Below we use the multiplicative structure on $\mathbb{F}_q^r$ to introduce a set of weights that can be seen as a generalization of fully-weighted for elementary abelian groups.

Definition 5.10. For $G = E_{p^{hr}}$ an elementary abelian group of order p^{hr}, consider a group isomorphism $\varphi : E_{p^{hr}} \to \mathbb{F}_q^r$. Define

$$\mathcal{Q}_h = \{m_x : y \mapsto \varphi^{-1}(x\varphi(y)) \in \mathrm{End}(E_{p^{hr}}) \mid x \in \mathbb{F}_q\}$$

the set of weights induced by the scalar multiplication of $\mathbb{F}_q = \mathbb{F}_{p^h}$.

While the sets of weights $\mathcal{Q}_h$ depend in principle on our choice of isomorphism φ, it is easy to see that the value of the associated Davenport constants does not depend on this choice. This is why we do not include φ in the notation of $\mathcal{Q}_h$.

Below, we study the j-wise $\mathcal{Q}_h$-weighted Davenport constant $\mathrm{D}_j^{\mathcal{Q}_h}(E_{p^{hr}})$. In order to simplify the notation, we will denote it by $\mathrm{D}_j^h(E_{p^{hr}})$.

Remark 5.11. For an elementary abelian group $E_{p^{hr}}$ of cardinality p^{hr}, let us underline that $\mathrm{D}_j^h(E_{p^{hr}}) = \mathrm{D}_j^f(E_{p^{hr}})$ if $h = 1$ and that $\mathrm{D}_j^h(E_{p^{hr}}) = \mathrm{D}_j(E_{p^{hr}})$ if $p = 2$ and $h = 1$. Furthermore, when $j = 1$, note that $D_j^h(E_{p^{hr}}) = r + 1$ for elementary reasons of linear algebra over $\mathbb{F}_q$.

The following theorem establishes the main link between these objects and the theory of intersecting codes.

Theorem 5.12. Let $E_{p^{hr}}$ be an elementary abelian group of order p^{hr}, where p is a prime and h, r are positive integers. Then $\mathrm{D}_2^h(E_{p^{hr}})$ is the smallest integer n such that all $[n, n-r]_{p^h}$ codes are not intersecting. Therefore

$$\mathrm{D}_2^h(E_{p^{hr}}) = \min\{m \geq r+1 \mid m < i(m-r, p^h)\}.$$

Proof. Let $m = \mathrm{D}_2^h(E_{p^{hr}}) - 1$. By definition, there exists a sequence $a_1, \dots, a_m \in E_{p^{hr}}$ that does not admit two disjoint weighted zero-sum subsequences. Note that m must be greater than r by the above remark 5.11. Via the isomorphism $E_{p^{hr}} \cong \mathbb{F}_{p^h}^r$, every a_i can be seen as a (column) vector. Let H be the matrix defined as

$$H = \left[\begin{array}{c|c|c} & & \\ a_1 & \cdots & a_m \\ & & \end{array}\right].$$

The matrix H is full-rank, because otherwise there would be a sequence of length $\mathrm{D}_2^h(E_{p^{hr}})$ that does not admit two disjoint weighted zero-sum subsequences, contradicting the definition: simply consider $b \notin \langle a_1, \dots, a_m \rangle$ and the prolonged sequence $a_1, \dots, a_m, b$.

Let $\mathcal{C}$ be the $[m, m-r]_{p^h}$ code defined by the parity-check matrix H. A codeword of $\mathcal{C}$ corresponds to a $\mathcal{W}$-weighted zero-sum subsequence of $a_1, \dots, a_m$. By the above assumption, $\mathcal{C}$ is then an intersecting code. Therefore

$$m \geq i(m-r, p^h).$$

Hence

$$\mathrm{D}_2^h(E_{p^{hr}}) = \max\{m > r \mid m \geq i(m-r, p^h)\} + 1.$$

which is equivalent to the statement of the theorem. □

Example 5.13. Consider the elementary abelian group E_{16} of order 16. Let $h = 1$ and $r = 4$. The set $\{m \geq 5 \mid m < i(m-4, 2)\} = \{8, 9, \dots\}$ (see Table 2), so that $\mathrm{D}_2(E_{16}) = 8$. On the other hand, if $h = 2$ and $r = 2$, the set $\{m \geq 3 \mid m < i(m-2, 4)\} = \{6, 7, \dots\}$ (see again Table 2), so that $\mathrm{D}_2^2(E_{16}) = 6$.

Example 5.14. Consider the elementary abelian group E_{1024} of order 1024. The set $\{m \geq 11 \mid m < i(m-10, 2)\} = \{17, 18, \dots\}$ (see Table 2), so that $\mathrm{D}_2(E_{1024}) = 17$. On the other hand, if $h = 2$ and $r = 5$, the set $\{m \geq 6 \mid m < i(m-5, 4)\} = \{11, 12, \dots\}$ (see again Table 2), so that $\mathrm{D}_2^2(E_{1024}) = 11$.

Remark 5.15. Below we record the values of $(r, \mathrm{D}_2(E_{2^r}))$ deduced from Table 2: $(1, 4)$, $(2, 5)$, $(3, 7)$, $(4, 8)$, $(5, 10)$, $(6, 11)$, $(7, 12)$, $(8, 14)$, $(9, 16)$, $(10, 17)$, $(11, 18)$, $(12, 19)$, $(13, 21)$, $(14, 22)$, $(15, 23)$, $(16, 25)$, $(17, 27)$. Any further improvement on the knowledge of $i(k, 2)$ would allow to extend this list.

5.3. **Asymptotic bounds.** Let us fix a prime p and a positive integer h. Let us denote $q = p^h$. We investigate the asymptotic behavior of $\mathrm{D}_2^h(E_{p^{hr}})$ when r grows.

Lemma 5.16. Let $\alpha \leq \liminf_{k\to\infty} i(k, p^h)/k$, and $\beta \geq \limsup_{k\to\infty} i(k, p^h)/k$. Then

$$\limsup_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \leq \frac{\alpha}{\alpha - 1}$$

and

$$\liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \geq \frac{\beta}{\beta - 1}.$$

Proof. Let $\varepsilon > 0$ and let r be large enough so that, for all $m \geq r + 1$, one has both

$$i(m-r, p^h) \leq (\beta + \varepsilon) \cdot (m - r) \text{ and } i(m-r, p^h) \geq (\alpha - \varepsilon) \cdot (m - r).$$

Recall that, by Theorem 5.12,

$$\mathrm{D}_2^h(E_{p^{hr}}) = \min\{m \geq r + 1 \mid m < i(m-r, q)\}.$$

Hence $\mathrm{D}_2^h(E_{p^{hr}}) < i(\mathrm{D}_2^h(E_{p^{hr}}) - r, q) \leq (\beta + \varepsilon) \cdot (\mathrm{D}_2^h(E_{p^{hr}}) - r)$, from which we obtain

$$\mathrm{D}_2^h(E_{p^{hr}}) \geq r \cdot \frac{\beta + \varepsilon}{\beta - 1 + \varepsilon}.$$

The other bound follows similarly by considering that

$$\mathrm{D}_2^h(E_{p^{hr}}) - 1 \geq i(\mathrm{D}_2^h(E_{p^{hr}}) - 1 - r, q) \geq (\alpha - \varepsilon) \cdot (\mathrm{D}_2^h(E_{p^{hr}}) - 1 - r),$$

from which we obtain

$$\mathrm{D}_2^h(E_{p^{hr}}) \leq 1 + r \cdot \frac{\alpha - \varepsilon}{\alpha - 1 - \varepsilon}.$$

□

Using the above lemma we can transform our asymptotic upper and lower bounds from the previous sections into respectively lower and upper bounds for the asymptotic value of $\mathrm{D}_2^h(E_{p^{hr}})$, as well as give the length of constructions of long sequences with no zero-sum subsequence.

Theorem 5.17. For all primes p and positive integers h, one has

$$\limsup_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \leq 2 - \frac{1}{p^h}.$$

Moreover, for $p^h \leq 17$, this bound is improved in Table 5.

TABLE 5. Upper bound on the asymptotic 2-wise weighted Davenport constant

p	h	$\limsup_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r}$
2	1	1.3956
2	2	1.6364
2	3	1.8057
2	4	1.9257
3	1	1.5472
3	2	1.8291
5	1	1.6972
7	1	1.7774
11	1	1.8660
13	1	1.8940
17	1	1.9343

Proof. Simply apply Lemma 5.16 using $\alpha = 2 + \frac{1}{p^h - 1}$ from Theorem 3.9. As observed, α may be improved by looking at the Table 1 and applying Lemma 5.16. □

Theorem 5.18. For every prime p and every positive integer h, the following holds:

- if $h = 1$ or $p^h \in \{4, 8, 9, 16, 25, 27, 32, 125\}$,

$$\liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \geq \frac{2}{\log_{p^h}(2p^h - 1)};$$

- if $h = 2m$ is even and $p^h \notin \{4, 9, 16, 25\}$, then

$$\liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \geq 2 - \frac{2}{p^m};$$

- if $h = 2m + 1$ is odd and $p^h \notin \{8, 27, 32, 125\}$, then

$$\liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \geq 2 - \frac{2}{2\frac{(p^m-1)(p^{m+1}-1)}{(p^{m+1}+p^m-2)} + 1}.$$

Proof. Simply apply Lemma 5.16 using β from Theorem 3.12 and Theorem 4.6. □

Remark 5.19. Whenever $h = 1$, we obtain the same asymptotic upper and lower bounds as in [42].

Remark 5.20. Notice that Theorem 5.17 and Theorem 5.18 can be considered to be an improvement on (2) for $j = 2$. Indeed, notice that (2) also holds for weighted versions of the Davenport constant. Moreover, since $D_1^h(E_{p^{hr}}) = r + 1$, as stated in Remark 5.11, an asymptotic weighted version of (2) is

$$1 \leq \liminf_{r\to\infty} \frac{\mathrm{D}_2^h(E_{p^{hr}})}{r} \leq 2.$$

Similar improvements for other values of j have been presented in [42].

Note that since Theorem 4.6 provides explicit constructions of short intersecting codes, combined with Lemma 5.16 it can be used to construct long sequences of elements of $E_{p^{hr}}$ with no 2 disjoint weighted zero-sum subsequences. This is stated precisely in the following remark.

Remark 5.21. Let p be a prime and let h and r be positive integers. There exist *explicit* sequences of elements of $E_{p^{hr}}$ with no 2 disjoint weighted zero-sum subsequences of length ℓr with

- $\ell = 2 - \frac{2}{p^m}$, if $p \geq 5$, $h = 2m$ and $p^h \geq 25$;
- $\ell = 2 - \frac{2}{2\frac{(p^m-1)(p^{m+1}-1)}{(p^{m+1}+p^m-2)}+1}$, if $h = 2m+1$ and $p^h \geq 32$;
- $\ell = \frac{3p-3}{2p-1}$, if $p \geq 11$ and $h = 1$.

The remaining cases are summarized in Table 6.

Table 6. Values of ℓ in the exceptional cases

p	h	ℓ	Probabilistic bound
2	1	1.206	1.261
3	1	1.297	1.365
2	2	1.315	1.424
5	1	1.344	1.464
7	1	1.388	1.517
2	3	1.4	1.535
3	2	1.411	1.551
2	4	1.451	1.614
3	3	1.471	1.660

6. Applications to factorization theory

In the following section we will illustrate the impact of the previous results on factorization in the ring of integers of number fields. It is well-known that problems of factorization in ring of integers of number fields and more generally in Dedekind domains and Krull monoids are related to problems of zero-sum sequences in their class group (see [28]). We will use some notions of algebraic number theory and we highlight their connection with the previous part of the paper. For the sake of brevity, we will not recall all the definitions, but we refer the interested reader to [46] for more details.

6.1. **The classic scenario.** Let K be a number field, and let $\mathcal{O}_K$ be its integer ring. It is well-known that $\mathcal{O}_K$ is a Dedekind domain. We can define its ideal class group

$$\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Frac}(\mathcal{O}_K)/\mathrm{Prin}(\mathcal{O}_K)$$

where $\mathrm{Frac}(\mathcal{O}_K)$ is the set of fractional ideals of $\mathcal{O}_K$ and $\mathrm{Prin}(\mathcal{O}_K)$ its set of principal ideals.

For number fields it is well-known that the class group is finite and each class contains a prime ideal. In fact, all of the following assertions remain true for Dedekind domains (or even more generally for Krull monoids) with finite class group where each class contains a prime ideal.

Indeed, the original motivation for studying the Davenport constant stems from its connection to factorizations; see for example [47], which already mentions the link recalled below between the Davenport constant of $\mathrm{Cl}(\mathcal{O}_K)$ and factorizations in $\mathcal{O}_K$.

Lemma 6.1. The Davenport constant $\mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$ is the largest number of prime ideals (with multiplicities) occurring in the factorization of the ideal generated by an irreducible element $x \in \mathcal{O}_K$. Equivalently, the small Davenport constant $\mathrm{d}(\mathrm{Cl}(\mathcal{O}_K))$ is the largest number of prime ideals such that their product is not divisible by a non-trivial principal ideal.

Since we will expand on this lemma, we consider it useful to provide the reader with a proof.

Proof. Let $(x) = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$ be the unique factorization of (x) as a product of prime ideals. The image of this factorization in $\mathrm{Cl}(\mathcal{O}_K)$ (considered with additive notation) is an identity of the form

$$0_{\mathrm{Cl}(\mathcal{O}_K)} = [\mathfrak{p}_1] + \cdots + [\mathfrak{p}_n]$$

because (x) is a principal ideal. Note that the above identity means that $[\mathfrak{p}_1], \ldots, [\mathfrak{p}_n]$ is a zero-sum sequence in $\mathrm{Cl}(\mathcal{O}_K)$. If this zero-sum subsequence can be decomposed into 2 disjoint zero-sum subsequences, then (x) is the product of 2 (non-trivial) principal ideals, meaning that x cannot be irreducible. Therefore the zero-sum sequence must have length smaller than $\mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$.

Conversely, consider a zero-sum sequence in $\mathrm{Cl}(\mathcal{O}_K)$ of length $n = \mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$ with no 2 disjoint zero-sum subsequences (such a sequence must exist from the definition of the Davenport constant). Such a sequence is of the form

$$0_{\mathrm{Cl}(\mathcal{O}_K)} = [\mathfrak{a}_1] + \cdots + [\mathfrak{a}_n].$$

Every class in $\mathrm{Cl}(\mathcal{O}_K)$ is represented by a prime ideal in $\mathcal{O}_K$. Every $[\mathfrak{a}_n]$ can therefore be represented by a prime ideal, say $\mathfrak{p}_i$. Let $x \in \mathcal{O}_K$ be a generator of the principal ideal $\prod_{i=1}^n \mathfrak{p}_i$. Since there are no 2 disjoint zero-sum subsequences, x must be irreducible, and its unique factorization into prime ideals has length $\mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$.

Therefore $\mathrm{D}(\mathrm{Cl}(\mathcal{O}_K))$ is the largest number of prime ideals contained in the factorization of an irreducible element, as claimed. □

For every ideal $\mathcal{I}$ in $\mathcal{O}_K$, the ideal $\mathcal{I}^{\exp(\mathrm{Cl}(\mathcal{O}_K))}$ is principal. In particular $(\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n)^{\exp(\mathrm{Cl}(\mathcal{O}_K))}$ is always principal.

In view of the preceding lemma, a natural question is: considering an ideal $\mathcal{I}$ in $\mathcal{O}_K$, which powers of $\mathcal{I}$ are divisible by a non-trivial principal ideal? Consider for example the case

$$\mathcal{I} = \prod_{i=1}^n \mathfrak{p}_i$$

where the $\mathfrak{p}_i$ are prime ideals. If $\mathcal{I}^k$ is divisible by a non-trivial principal ideal, then there must be a product

$$\prod_{i=1}^n \mathfrak{p}_i^{\alpha_i}$$

(with $0 \leq \alpha_i \leq k$) which is a non-trivial principal ideal. This can of course be interpreted as a $\{1, \ldots, k\}$-weighted zero-sum subsequence in the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$. The fully-weighted Davenport constant is a particular case of this general question, namely for $k = \exp(\mathrm{Cl}(\mathcal{O}_K)) - 1$.

Lemma 6.2. The following interpretation of the different Davenport constants holds:

- for every $k \in \mathbb{N}$, the weighted small Davenport constant $\mathrm{d}^{\{1,\dots,k\}}(\mathrm{Cl}(\mathcal{O}_K))$ is the largest number $\ell \in \mathbb{N}$ such that there exist ℓ prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_\ell$ such that the product
$$(\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_\ell)^k$$
is not divisible by a non-trivial principal ideal;
- the fully-weighted small Davenport constant $\mathrm{d}^f(\mathrm{Cl}(\mathcal{O}_K))$ is the largest number $\ell \in \mathbb{N}$ such that there exist ℓ prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_\ell$ such that the product
$$(\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_\ell)^{\exp(\mathrm{Cl}(\mathcal{O}_K))-1}$$
is not divisible by a non-trivial principal ideal;
- the 2-wise small Davenport constant $\mathrm{d}_2(\mathrm{Cl}(\mathcal{O}_K))$ is the largest number $\ell \in \mathbb{N}$ such that there exist ℓ prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_\ell$ such that the product
$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_\ell$$
is not divisible by a product of two non-trivial principal ideals (or equivalently, this product is divisible only by principal ideals generated by an irreducible element);
- the 2-wise fully-weighted small Davenport constant $\mathrm{d}_2^f(\mathrm{Cl}(\mathcal{O}_K))$ is the largest number $\ell \in \mathbb{N}$ such that there exist ℓ prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_\ell$ such that the product
$$(\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_\ell)^{\exp(\mathrm{Cl}(\mathcal{O}_K))-1}$$
is not divisible by a product of two non-trivial principal ideals (or equivalently, this product is divisible only by principal ideals generated by an irreducible element).

Proof. The proof is a straightforward adaptation of the arguments of the proof of Lemma 6.1, taking into account the different definitions of the Davenport constants. □

We merely mention the 2-wise case explicitly as the preceding section focused on this case.

6.2. **The elementary abelian case: multiplicative action.** We are now going to focus only on the case when $\mathrm{Cl}(\mathcal{O}_K)$ is an elementary abelian group $E_{p^{hr}}$. As in the previous section, writing $q = p^h$, we can consider a multiplicative action of $\mathbb{F}_q$ on $E_{p^{hr}}$. Note that there is no unique way of defining such a multiplicative action (because there is no canonical isomorphism $\mathbb{F}_q^r \cong E_{p^{hr}}$). However, our results do not depend on the choice of this isomorphism.

In this case, we have the following.

Theorem 6.3. Let p be a prime and h, r be positive integers. Let K be an algebraic number field such that $\mathrm{Cl}(\mathcal{O}_K) = E_{p^{hr}}$.

The 2-wise weighted small Davenport constant $\mathrm{d}_2^h(\mathrm{Cl}(\mathcal{O}_K))$ is the largest number $\ell \in \mathbb{N}$ such that there exist ℓ prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_\ell$ such that any product
$$\prod_{i=1}^{\ell} \mathfrak{q}_i,$$
where $\mathfrak{q}_i$ is an ideal in the class of $\varphi_i([\mathfrak{p}_i])$, with $\varphi_i \in \mathcal{Q}_h$, is not divisible by a product of two non-trivial principal ideals.

Proof. Again, the proof is an adaptation of the Lemma 6.1's proof to the definition of 2-wise weighted Davenport constant. □

Remark 6.4. It is quite remarkable that the above property does not depend on the chosen multiplicative action. It would be nice to have a general number-theoretical interpretation of such an invariant. At the end of this section, we will illustrate a link to the Galois action, which holds in some particular cases.

Note that it is not known if every abelian group is the class group of the ring of integers of a number field. However, it is well-established that all (finite) abelian groups are the ideal class group of some Dedekind ring, as proved in [18]. For illustrative purposes of the results above, we use the explicit construction presented in [30, Theorem 2], as well as explicit calculation in MAGMA, to provide the following examples.

Example 6.5. Let

$$\alpha = 5 \cdot 13 \cdot 29 \cdot 41 \cdot 61$$

and $K = \mathbb{Q}(\sqrt{\alpha})$. We have that $\mathrm{Cl}(\mathcal{O}_K) \cong E_{16}$. By Example 5.13 we know that $\mathrm{d}_2(E_{16}) = \mathrm{D}_2(E_{16}) - 1 = 7$, and $\mathrm{d}_2^2(E_{16}) = \mathrm{D}_2^2(E_{16}) - 1 = 5$. Hence there exist 7 prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_7$ such that their product is not divisible by a product of two non-trivial principal ideals and 5 prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_5$ such that any product

$$\prod_{i=1}^{5} \mathfrak{q}_i,$$

where $\mathfrak{q}_i$ is an ideal in the class of $\varphi_i([\mathfrak{p}_i])$, with $\varphi_i \in \mathcal{Q}_2$, is not divisible by a product of two non-trivial principal ideals.

Example 6.6. Let

$$\alpha = 316861 \cdot 451897 \cdot 455333 \cdot 476977 \cdot 490549 \cdot 523793 \cdot 560641 \cdot 724481 \cdot 736993 \cdot 828829 \cdot 916621$$

and $K = \mathbb{Q}(\sqrt{\alpha})$. We have that $\mathrm{Cl}(\mathcal{O}_K) \cong E_{1024}$. By Example 5.14 we know that $\mathrm{d}_2(E_{1024}) = \mathrm{D}_2(E_{1024}) - 1 = 16$ and $\mathrm{d}_2^2(E_{1024}) = D_2^2(E_{1024}) - 1 = 10$.

Hence there exist 16 prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_{16}$ such that their product is not divisible by a product of two non-trivial principal ideals and 10 prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_{10}$ such that any product

$$\prod_{i=1}^{10} \mathfrak{q}_i,$$

where $\mathfrak{q}_i$ is an ideal in the class of $\varphi_i([\mathfrak{p}_i])$, with $\varphi_i \in \mathcal{Q}_2$, is not divisible by a product of two non-trivial principal ideals.

6.3. **The elementary abelian case: Galois group action.** By recent work [15, Theorem 7.1] it is known that the monoids of norms of rings of algebraic integers of Galois number fields admit a transfer homomorphism to monoids of weighted zero-sum sequences where the weights correspond to the elements of the Galois group. For a generalization, see [29]. Therefore studying weighted zero-sum problems over class groups with weights corresponding to the action of the Galois group has an immediate motivation from the point of view of factorization theory.

It is well-known that the Galois group defines an action on the ideal class group (see Hilbert's Ramification Theory [46, Chapter 1,§9]). It is then interesting to determine when this action is the same as that of $\mathcal{Q}_h$ defined above. This will give a natural interpretation of our definition of $\mathcal{Q}_h$ and our notion of generalized weights. Recall that the action of $\mathcal{Q}_h$ is the same as the multiplicative action of $\mathbb{F}_q$ on $E_{p^{hr}}$. The multiplicative group of $\mathbb{F}_q$ is the cyclic group C_{q-1}, and the orbits of the scalar action of $\mathbb{F}_q$ on $\mathbb{F}_q^r$ all have size $q-1$, that is the action is free on $\mathbb{F}_q^r \setminus \{0\}$. The following theorem shows that this is actually also a sufficient condition.

Theorem 6.7. Let p be a prime, and let h and r be positive integers, and let $q = p^h$. Let K be a number field, with Galois group $\mathrm{Gal}(K/\mathbb{Q}) = C_{q-1}$ and ideal class group $\mathrm{Cl}(\mathcal{O}_K) = E_{p^{hr}}$. If the action of $\mathrm{Gal}(K/\mathbb{Q})$ is free on $\mathrm{Cl}(\mathcal{O}_K) \setminus \{0\}$, then there exists an isomorphism $\varphi : E_{p^{hr}} \to \mathbb{F}_q^r$ such that the action of $\mathrm{Gal}(K/\mathbb{Q})$ on the class group is the same as that of $\mathcal{Q}_h$.

Proof. First note that the action of the Galois group on the ideal class group preserves the group addition of $\mathrm{Cl}(\mathcal{O}_K)$.

Let σ be a generator of the Galois group. Observe that $E_{p^{hr}} \cong \mathbb{F}_p^{hr}$ as an $\mathbb{F}_p$-vector space. It is clear that σ corresponds to an endomorphism of $\mathbb{F}_p^{hr}$, which we also write σ. Since $x^q - x = 0$ annihilates σ and σ has order $q-1$, the ring of endomorphisms $\mathbb{F}_p[\sigma]$ is isomorphic to $\mathbb{F}_q$.

Since the orbit of every non-zero element v has order $q-1$, the map

$$f(\sigma) = f_0 + f_1\sigma + \ldots + f_{h-1}\sigma^{h-1} \mapsto f(\sigma)(v) = f_0 v + f_1\sigma(v) + \ldots + f_{h-1}\sigma^{h-1}(v)$$

is a bijection between $\mathbb{F}_p[\sigma]$ and $\{0\} \cup \omega(v)$, which is also an isomorphism of $\mathbb{F}_p$-vector spaces. Via this map, we may endow $\{0\} \cup \omega(v)$ with a multiplicative structure that makes it isomorphic to $\mathbb{F}_q$.

Now, let v_1 be a non-zero element in $\mathrm{Cl}(\mathcal{O}_K)$. Consider a non zero element $v_2 \in \mathrm{Cl}(\mathcal{O}_K) \setminus \omega(v_1)$. As we said, both sets $\{0\} \cup \omega(v_1)$ and $\{0\} \cup \omega(v_2)$ are isomorphic to $\mathbb{F}_q$. The orbits are disjoint. Hence $W = \langle \omega(v_1), \omega(v_2) \rangle \cong \mathbb{F}_q^2$. Moreover, W is stable under the action of the Galois group. Now, we can continue by taking a nonzero element outside W and so on, until getting r elements, say $v_1, \ldots, v_r$. In this way, we have $\langle \omega(v_1), \ldots, \omega(v_r) \rangle \cong \mathbb{F}_q^r$. □

Remark 6.8. If $p = 2$ and $q - 1 = 2^h - 1$ is a Mersenne prime, then the action of $\mathrm{Gal}(K/\mathbb{Q})$ is free on $\mathrm{Cl}(\mathcal{O}_K) \setminus \{0\}$. Actually, it is well-known that any prime $\ell \in \mathbb{Z}$ yields the following decomposition:

$$(\ell) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$$

and er divides $q-1$. Hence, either $e = 1$ and $r = q-1$, so that ℓ splits completely, or $e = q-1$ and $r = 1$, so that ℓ is totally ramified, or $e = r = 1$, so that ℓ is inert. Note in particular that when $(\ell) = (\mathfrak{p})^{q-1}$ (that is when ℓ is totally ramified), the ideal $\mathfrak{p}$ is principal.

To the best of our knowledge, it is unknown in general for which values of p, h, r a number field satisfying all the hypotheses of Theorem 6.7 exists. However, the following is an example, in the easiest case discussed in Remark 6.8.

Example 6.9. Let $p(x) = x^3 - x^2 - 2562x + 48969$ and let $K = \mathbb{Q}[\alpha]$ be the cubic number field obtained extending $\mathbb{Q}$ with a root of $p(x)$. We have that

$$\mathrm{Gal}(K/\mathbb{Q}) = C_3 \text{ and } \mathrm{Cl}(\mathcal{O}_K) = E_{16}.$$

Moreover, $q - 1 = 3$ is a Mersenne prime. In this case, as in the Example 6.5, there exist 7 prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_7$ such that their product is not divisible by a product of two non-trivial principal ideals and 5 prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_5$ such that any product

$$\prod_{i=1}^{5} \mathfrak{q}_i,$$

where $\mathfrak{q}_i$ is an ideal in the class of $\sigma([\mathfrak{p}_i])$, with $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, is not divisible by a product of two non-trivial principal ideals.

We conclude the paper with the following remark, which opens new perspectives for future research.

Remark 6.10. There are number fields satisfying the hypotheses of Theorem 6.7 which are not of prime degree, as in Remark 6.8. For example, let $K = \mathbb{Q}[\alpha]$ where

$$\alpha^6 - \alpha^5 + 22\alpha^4 + 11\alpha^3 + 1038\alpha^2 - 1993\alpha + 16649 = 0.$$

In this case,

$$\mathrm{Gal}(K/\mathbb{Q}) = C_6 \text{ and } \mathrm{Cl}(\mathcal{O}_K) = E_{49}.$$

The action of $\mathrm{Gal}(K/\mathbb{Q})$ is free on $\mathrm{Cl}(\mathcal{O}_K) \setminus \{0\}$ and the 8 orbits of order 6 are those of the following 8 classes: $[\mathfrak{p}_\ell]$ where $\ell \in \{47, 59, 107, 127, 131, 151, 173, 193\}$ and $\mathfrak{p}_\ell$ is a factor of (ℓ).

It would certainly be interesting to further investigate fields that satisfy the hypotheses of Theorem 6.7, as well as to develop the coding-theoretical implications of a non-free action. This is certainly beyond the scope of the present paper, and it may be an interesting topic for future researches.

Acknowledgements. The three authors are partially supported by the ANR-21-CE39-0009 - BARRACUDA (French *Agence Nationale de la Recherche*). They would like to thank Daniele Bartoli, Julien Lavauzelle and Alessandro Neri for the fruitful discussions on the topic and their insightful advice. The first and the third author would also like to warmly thank Inria GRACE team for hospitality and excellent working conditions, while this paper has mainly been written.

References

[1] S. D. Adhikari, Y. Chen, J. B. Friedlander, S. V. Konyagin, and F. Pappalardi. Contributions to zero-sum problems. *Discrete Mathematics*, 306(1):1–10, 2006.
[2] S. D. Adhikari and P. Rath. Davenport constant with weights and some related questions. *Integers*, 6, 2006.
[3] G. N. Alfarano, M. Borello, and A. Neri. A geometric characterization of minimal codes and their asymptotic performance. *Advances in Mathematics of Communications*, 16(1):115–133, 2022.
[4] G. N. Alfarano, M. Borello, and A. Neri. Outer strong blocking sets. *The Electronic Journal of Combinatorics*, 31(2), 2024.
[5] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Three combinatorial perspectives on minimal codes. *SIAM Journal on Discrete Mathematics*, 36(1):461–489, 2022.
[6] N. Alon. Explicit expanders of every degree and size. *Combinatorica*, 41:447 – 463, 2020.
[7] N. Alon, A. Bishnoi, S. Das, and A. Neri. Strong blocking sets and minimal codes from expander graphs. *to appear in Transactions of the American Mathematical Society*, 2024.
[8] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, 1998.
[9] S. Ball. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *Journal of the European Mathematical Society (EMS Publishing)*, 14(3), 2012.
[10] D. Bartoli and M. Borello. Small strong blocking sets by concatenation. *SIAM Journal on Discrete Mathematics*, 37(1):65–82, 2023.
[11] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth. Towers of function fields over non-prime finite fields. *Moscow Mathematical Journal*, 15, 02 2012.
[12] A. Bishnoi, J. D'haeseleer, D. Gijswijt, and A. Potukuchi. Blocking sets, minimal codes, and trifferent codes. *to appear in the Journal of the London Mathematical Society*, 2024.
[13] S. R. Blackburn. Frameproof codes. *SIAM Journal on Discrete Mathematics*, 16(3):499–510, 2003.
[14] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. *Journal of Algebraic Combinatorics*, 53(2):327–341, 2021.
[15] S. Boukheche, K. Merito, O. Ordaz, and W. A. Schmid. Monoids of sequences over finite abelian groups defined via zero-sums with respect to a given set of weights and applications to factorizations of norms of algebraic integers. *Communications in Algebra*, 50(10):4195–4217, 2022.
[16] G. Brassard, C. Crépeau, and M. Santha. Oblivious transfers and intersecting codes. *IEEE Transactions on Information Theory*, 42(6):1769–1780, 1996.
[17] H. Chabanne, G. Cohen, and A. Patey. Towards secure two-party computation from the wire-tap channel. In *International Conference on Information Security and Cryptology*, pages 34–46. Springer, 2013.
[18] L. Claborn. Every abelian group is a class group. *Pacific Journal of Mathematics*, 18:219–222, 1966.
[19] G. D. Cohen and A. Lempel. Linear intersecting codes. *Discrete Mathematics*, 56:35–43, 1984.
[20] G. D. Cohen, S. Mesnager, and A. Patey. On minimal and quasi-minimal linear codes. In *IMA International Conference on Cryptography and Coding*, pages 85–98. Springer, 2013.
[21] G. D. Cohen and G. Zemor. Intersecting codes and independent families. *IEEE Transactions on Information Theory*, 40(6):1872–1881, 1994.
[22] G. D. Cohen and G. Zemor. Subset sums and coding theory. *Astérisque*, 258:327–339, 1999.
[23] G. D. Cohnen, S. Encheva, S. Litsyn, and H. G. Schaathun. Intersecting codes and separating codes. *Discrete Applied Mathematics*, 128(1):75–83, 2003.
[24] C. Crépeau and M. Sántha. Efficient reduction among oblivious transfer protocols based on new self-intersecting codes. In *Sequences II: Methods in Communication, Security, and Computer Science*, pages 360–368. Springer, 1993.

[25] A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco. Linear nonbinary covering codes and saturating sets in projective spaces. *Advances in Mathematics of Communications*, 5(1):119, 2011.
[26] S. Fancsali and P. Sziklai. Lines in higgledy-piggledy arrangement. *Electronic Journal of Combinatorics*, 21, 2014.
[27] W. Gao and A. Geroldinger. Zero-sum problems in finite abelian groups: A survey. *Expositiones Mathematicae*, 24(4):337–369, 2006.
[28] A. Geroldinger and F. Halter-Koch. Non-unique factorizations : Algebraic, combinatorial and analytic theory. 2006.
[29] A. Geroldinger, F. Halter-Koch, and Q. Zhong. On monoids of weighted zero-sum sequences and applications to norm monoids in galois number fields and binary quadratic forms. *Acta Mathematica Hungarica*, 168(1):144–185, 2022.
[30] F. Gerth. Number fields with prescribed ℓ-class groups. *Proceedings of the American Mathematical Society*, 49(2):284–288, 1975.
[31] D. J. Grynkiewicz. *Structural additive theory*, volume 30. Springer, 2013.
[32] F. Halter-Koch. A generalization of Davenport's constant and its arithmetical applications. *Colloquium Mathematicum*, 63:203–210, 1992.
[33] J. W. Hirschfeld and J. A. Thas. Open problems in finite projective spaces. *Finite Fields and Their Applications*, 32:44–81, 2015.
[34] W. C. Huffman, J. Kim, and P. Sole. *Concise Encyclopedia of Coding Theory*. CRC Press, 2021.
[35] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, 2010.
[36] T. Y. Hwang. Decoding linear block codes for minimizing word error rate. *IEEE Transactions on Information Theory*, 25(6):733–737, 1979.
[37] Y. Ihara. Some remarks on the number of rational points of algebratic curves over finite fields. *Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Mathematics*, 28:721–724, 1982.
[38] G. Katona and J. Srivastava. Minimal 2-coverings of a finite affine space based on GF(2). *Journal of statistical planning and inference*, 8(3):375–388, 1983.
[39] S. Kurz. Divisible minimal codes. *arXiv preprint arXiv:2312.00885*, 2023.
[40] W. Lu, X. Wu, and X. Cao. The parameters of minimal linear codes. *Finite Fields their Appl.*, 71:101799, 2021.
[41] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library, 1977.
[42] L. E. Marchan, O. Ordaz, I. Santos, and W. A. Schmid. Multi-wise and constrained fully weighted davenport constants and interactions with coding theory. *Journal of Combinatorial Theory, Series A*, 135:237–267, 2015.
[43] J. L. Massey. Minimal codewords and secret sharing. *In Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279, 1993.
[44] D. Miklós. Linear binary codes with intersection properties. *Discrete Applied Mathematics*, 9(2):187–196, 1984.
[45] C. J. Moreno and O. Moreno. Exponential sums and Goppa codes. ii. *IEEE Transactions on Information Theory*, 38(4):1222–1229, 1992.
[46] J. Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.
[47] J. E. Olson. A combinatorial problem on finite abelian groups, i. *Journal of Number Theory*, 1(1):8–10, 1969.
[48] A. Plagne and W. A. Schmid. An application of coding theory to estimating Davenport constants. *Designs, Codes and Cryptography*, 61:105–118, 2010.
[49] V. Pless. On the uniqueness of the Golay codes. *Journal of Combinatorial theory*, 5(3):215–228, 1968.
[50] H. Randriambololona. (2, 1)-separating systems beyond the probabilistic bound. *Israel Journal of Mathematics*, 195:171–186, 2013.
[51] C. T. Retter. Intersecting Goppa codes. *IEEE Transactions on Information Theory*, 35(4):822–828, 1989.
[52] C. T. Retter. The average binary weight-enumerator for a class of generalized reed-solomon codes. *IEEE Transactions on Information Theory*, 37(2):346–349, 1991.
[53] M. Scotti. On the lower bound for the length of minimal codes. *Discrete Mathematics*, 347(1):113676, 2024.
[54] B. Segre. Curve razionali normali ek-archi negli spazi finiti. *Annali di Matematica Pura ed Applicata*, 39:357–379, 1955.
[55] N. J. Sloane. Covering arrays and intersecting codes. *Journal of Combinatorial Designs*, 1(1):51–63, 1993.
[56] C. Tang, Y. Qiu, Q. Liao, and Z. Zhou. Full characterization of minimal linear codes as cutting blocking sets. *IEEE Transactions on Information Theory*, 67(6):3690–3700, 2021.
[57] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1991.
[58] X. Zeng and P. Yuan. Weighted Davenport's constant and the weighted EGZ theorem. *Discrete mathematics*, 311(17):1940–1947, 2011.