Generalized weights of codes over rings and invariants of monomial ideals

Elisa Gorla[1] and Alberto Ravagnani*[2]

[1]*Institut de Mathématiques, Université de Neuchâtel, Switzerland*
elisa.gorla@unine.ch
[2]*Department of Mathematics and Computer Science, Eindhoven University of Technology, the Netherlands*
a.ravagnani@tue.nl

Submitted: Feb 4, 2022; Accepted: May 17, 2023; Published: Sep, 15 2023

Abstract. We develop an algebraic theory of supports for R-linear codes of fixed length, where R is a finite commutative unitary ring. A support naturally induces a notion of generalized weights and allows one to associate a monomial ideal to a code. Our main result states that, under suitable assumptions, the generalized weights of a code can be obtained from the graded Betti numbers of its associated monomial ideal. In the case of $\mathbb{F}_q$-linear codes endowed with the Hamming metric, the ideal coincides with the Stanley–Reisner ideal of the matroid associated to the code via its parity-check matrix. In this special setting, we recover the known result that the generalized weights of an $\mathbb{F}_q$-linear code can be obtained from the graded Betti numbers of the ideal of the matroid associated to the code. We also study subcodes and codewords of minimal support in a code, proving that a large class of R-linear codes is generated by its codewords of minimal support.

Keywords. Linear codes, codes over rings, supports, generalized weights, monomial ideal of a code, graded Betti numbers, matroid

Mathematics Subject Classifications. 94B05, 13D02, 13F10

1. Introduction

In the past seventy years, much effort has been devoted to the study of algebraic and combinatorial objects associated to linear error-correcting codes. Of particular interest is the matroid associated to a linear code via its parity-check matrix, whose circuits are the minimal *Hamming supports* of the codewords. Many central results in classical coding theory, including the celebrated *MacWilliams identities*, their generalizations, and the duality between puncturing and shortening can be elegantly obtained via this correspondence; see e.g. [Bar97, Bri07, Bri10, JP13] and the references therein.

*A.R. is supported by the Dutch Research Council through grants VI.Vidi.203.045, OCENW.KLEIN.539, and by the Royal Academy of Arts and Sciences of the Netherlands.

The matroid associated to a linear code via its parity check matrix retains a wealth of information about the structure of the code, including its length, dimension, minimum distance, weight distribution, and generalized weights. Moreover, the *weight enumerator* is determined by the Tutte polynomial of the matroid, see [Gre76]. In addition, in [JV13] it is shown that the code's *generalized weights* are determined by the *graded Betti numbers* of the *Stanley–Reisner ideal* of the matroid. The approach of [JV13] heavily relies on matroid theory and on the properties of the Hamming support.

In this paper, we depart from the classical theory of linear codes over a finite field and consider instead R-linear codes $C \subseteq R^n$, where R is a finite commutative unitary ring. We start by proposing a general definition of support as a function $\sigma : R^n \to \mathbb{N}^u$ that enjoys a few natural properties. This naturally extends the notion of *Hamming support* traditionally studied in coding theory [MS77, page 177]. We give several examples of supports and operations to construct new supports from old. We define the support of a code $C \subseteq R^n$ as the join of the supports of its elements.

We then define the generalized weights of a code via the supports of its subcodes. Moreover, we identify a class of supports under which the algebra of the module R^n is compatible with the combinatorics of the poset $\mathbb{N}^u$ with the product order. We call these supports *modular* and establish some of their structural properties. As one might expect, the Hamming support is an example of a modular support.

Most of the paper is devoted the study of codes $C \subseteq R^n$ endowed with modular supports. We characterize their minimal codewords and prove that, if R is a principal ideal ring, then their generalized weights are attained by subcodes that are minimally generated by codewords of minimal support in C. We also provide evidence in various examples that our results do not extend to support functions that are not modular.

The centerpiece of this paper is a result connecting the theory of modular supports with invariants of monomial ideals. We associate a monomial ideal to a code $C \subseteq R^n$ via the supports of its codewords. Under this correspondence, inclusion of supports translates into divisibility among monomials. In Theorem 5.4 we prove that, under suitable assumptions, the generalized weights of an R-linear code endowed with a modular support are determined by the graded Betti numbers of the associated monomial ideal. This generalizes a result of [JV13], with a stand-alone proof that does not rely on matroid theory.

We conclude the paper with a series of observations on the Hamming support. We review known results in the light of our contribution, such as the fact that every $\mathbb{F}_q$-linear code is generated by its codewords of minimal support. We also show that the same is true for those of maximal support, provided that q is sufficiently large (and false in general for binary codes).

Outline. In Section 2, we define R-linear codes and review some algebra results about finite commutative rings and finite local rings. In Section 3, we define (modular) supports and generalized weights, establishing their main properties. Codewords and subcodes of minimal supports are studied in Section 4. In Section 5, we associate a monomial ideal to a code. Moreover, we prove that the generalized weights of the code are determined by the graded Betti numbers of the corresponding ideal. We study the Hamming support in Section 6.

2. Codes and minimal systems of generators

In this section we introduce codes over finite commutative rings and describe some properties of their systems of generators.

Notation 2.1. *Throughout the paper n and m denote positive integers and $(R, +, \cdot)$ is a finite commutative ring. All rings in this paper are unitary with $1 \neq 0$. We denote by $\mathbb{N} = \{0, 1, 2, \ldots\}$ the set of natural numbers. For $a \in \mathbb{N}$ we let $[a] := \{1, \ldots, a\}$.*

A classical theorem in commutative algebra states that every finite commutative ring R is isomorphic to a finite product of finite local rings. We forget the isomorphism and write

$$R = R_1 \times \cdots \times R_\ell, \tag{2.1}$$

where $R_1, \ldots, R_\ell$ are finite local rings. For $i \in [\ell]$, let $\mathfrak{M}_i$ be the maximal ideal of R_i and let $J = J(R)$ be the **Jacobson radical** of R. Recall that the Jacobson radical of a commutative ring R is the intersection of all maximal ideals of R, equivalently

$$J = \{r \in R \,:\, 1 + rs \text{ is invertible for every } s \in R\}.$$

It is easy to check that in our situation

$$J = \mathfrak{M}_1 \times \cdots \times \mathfrak{M}_\ell \subseteq R_1 \times \cdots \times R_\ell = R.$$

If R is a finite principal ideal ring, then each R_i is a finite chain ring. For $i \in [\ell]$, let $\mathfrak{M}_i = (\alpha_i)$. Then $J = (\alpha)$, where $\alpha = (\alpha_1, \ldots, \alpha_\ell)$. In particular, if R is a product of finite fields, then $\mathfrak{M}_i = 0$ for $i \in [\ell]$ and $J = 0$. If $R = \mathbb{F}_q$, then $\ell = 1$ and $J = 0$ is the only maximal ideal of R.

We denote by $(R, \mathfrak{M})$ a local ring R with maximal ideal $\mathfrak{M}$. If $(R, \mathfrak{M})$ is a finite local ring, then $R/\mathfrak{M}$ is a finite field.

In this paper we consider codes of fixed length over the alphabet R. All of our codes are assumed to be linear over R.

Definition 2.2. An **R-linear code**, or simply a **code**, is an R-submodule $C \subseteq R^n$. The elements of C are called **codewords**. A **subcode** of C is an R-submodule $D \subseteq C$.

Denote by e_i the element of R which corresponds to $(0, \ldots, 0, 1, 0, \ldots, 0) \in R_1 \times \cdots \times R_\ell$, where the one appears in the ith component. From the decomposition in (2.1) one has

$$R^n = R_1^n \times \cdots \times R_\ell^n.$$

In the sequel, for $i \in [\ell]$ we denote by $\pi_i : R^n \to R_i^n$ the standard projection on the ith coordinate.

Let $C \subseteq R^n$ be a code. For any $v = (v_1, \ldots, v_\ell) \in C$, with $v_i = \pi_i(v) \in R_i^n$, one has

$$(0, \ldots, 0, v_i, 0, \ldots, 0) = e_i v \in C.$$

Hence, up to isomorphism, C can be uniquely written as

$$C = C_1 \times \cdots \times C_\ell \subseteq R^n, \tag{2.2}$$

where $C_i = \pi_i(C) \subseteq R_i^n$ for all $i \in [\ell]$. We often consider codes $C \subseteq 0 :_{R^n} J$. Recall that

$$0 :_{R^n} J = \{v \in R^n \, : \, rv = 0 \text{ for all } r \in J\}.$$

Then

$$0 :_{R^n} J = \left(0 :_{R_1^n} \mathfrak{M}_1\right) \times \cdots \times \left(0 :_{R_\ell^n} \mathfrak{M}_\ell\right).$$

Since $0 :_{R^n} J$ is an R-module annihilated by J, it is an R/J-module. Hence, if $(R, \mathfrak{M})$ is a local ring, then $0 :_{R^n} \mathfrak{M}$ is a vector space over $R/\mathfrak{M}$.

For $C \subseteq R^n$ a code, we also consider the **socle**

$$0 :_C J = \{v \in C \, : \, rv = 0 \text{ for all } r \in J\} = C \cap (0 :_{R^n} J).$$

The socle of C is a the largest subcode of C which is annihilated by J. In particular, if $(R, \mathfrak{M})$ is a local ring, then $0 :_C \mathfrak{M}$ is an $R/\mathfrak{M}$-vector space.

A **minimal system of generators** of a code $C \subseteq R^n$ is a subset of C whose elements generate C and which is minimal with respect to inclusion. Notice that any system of generators of a code C contains a minimal system of generators of C.

Definition 2.3. We denote by $\mu(C)$ the least cardinality of a system of generators of a code C, with $\mu(0) = 0$ by convention. For a code $C = C_1 \times \cdots \times C_\ell \subseteq R^n$ as in (2.2), let

$$M(C) := \mu(C_1) + \cdots + \mu(C_\ell).$$

Example 2.4. Let $R = R_1 \times \cdots \times R_\ell$, with R_i a finite local ring for $i \in [\ell]$. Then

$$M(R^n) = \mu(R_1^n) + \cdots + \mu(R_\ell^n) = n\ell.$$

Clearly $\mu(C) \leqslant M(C)$ for every code $C \subseteq R^n$. If R is a finite local ring, all minimal systems of generators of a code $C \subseteq R^n$ have the same cardinality $\mu(C) = M(C)$. This is a consequence of the next lemma, which summarizes some well-known properties of systems of generators of modules over local rings; see e.g. [Mat89, Theorem 2.3].

Theorem 2.5. *Let $(R, \mathfrak{M})$ be a local ring and let $C = \langle v_1, \ldots, v_t \rangle$ be an R-module. The elements $v_1, \ldots, v_t$ are a minimal system of generators of C if and only if the equivalence classes $\overline{v_1}, \ldots, \overline{v_t}$ are an $R/\mathfrak{M}$-basis of the vector space $C/\mathfrak{M}C$. In particular, every minimal system of generators of C has cardinality $\mu(C) = \dim_{R/\mathfrak{M}}(C/\mathfrak{M}C)$.*

Over an arbitrary R, however, not all minimal system of generators of a code $C \subseteq R^n$ have the same cardinality.

Example 2.6. Let $R = \mathbb{Z}_6$ and $D = \langle (2,3) \rangle \subseteq C = \mathbb{Z}_6^2$. Then $\mu(D) = 1$. Moreover, $(2,0) = 4(2,3) \in D$ and $(0,3) = 3(2,3) \in D$. Hence $D = \langle (2,0), (0,3) \rangle$ and $\{(2,0), (0,3)\}$ is a minimal system of generators of D of cardinality $2 = M(D)$.

Notation 2.7. *Let $C \subseteq R^n$ be a code and let*

$$\mathcal{S}_j(C) := \{D \subseteq C \text{ subcode} \, : \, D \text{ has a minimal system of generators of cardinality } j\}.$$

In particular, $\mathcal{S}_j(R^n)$ is the set of codes $C \subseteq R^n$ which have a minimal system of generators of cardinality j.

One can show that $M(C)$ is the largest cardinality of a minimal system of generators of $C \subseteq R^n$.

Theorem 2.8. *If $C \in \mathcal{S}_i(R^n)$, then there exist $v_1, \ldots, v_i$ minimal generators of C with the property that*

$$V = \{e_j v_k \,:\, (j,k) \in [\ell] \times [i],\ e_j v_k \neq 0\}$$

is a minimal system of generators of C with $|V| \geqslant i$. Moreover,

$$M(C) = \max\{i \geqslant 0 \,:\, C \in \mathcal{S}_i(R^n)\}$$

and any minimal system of generators of C of cardinality $M(C)$ has the same form as V.

Proof. Let $w_1, \ldots, w_i$ be a minimal system of generators of $C = C_1 \times \cdots \times C_\ell$. Let $C_j' = 0 \times \cdots \times 0 \times C_j \times 0 \times \cdots \times 0 \subseteq C$. Observe that $e_j w_k \in C$ for all k and j and $w_k = e_1 w_k + \cdots + e_\ell w_k$ for all $k \in [i]$. This proves that the set $\{e_j w_k \,:\, (j,k) \in [\ell] \times [i],\ e_j w_k \neq 0\}$ generates C. Moreover, the set $\{e_j w_k \,:\, k \in [i],\ e_j w_k \neq 0\}$ generates C_j' for any $j \in [\ell]$.

Fix $j \in [\ell]$. If $e_j w_1, \ldots, e_j w_i$ do not form a minimal system of generators of C_j', then suppose up to reindexing that $e_j w_1, \ldots, e_j w_k$ do, for some $k < i$. For $h \in [i] \setminus [k]$, write $e_j w_h = r_{h,1} e_j w_1 + \cdots + r_{h,k} e_j w_k$ for some $r_{h,1}, \ldots, r_{h,k} \in R$. Let $v_h = w_h$ for $h \in [k]$, $v_h = w_h - r_{h,1} e_j w_1 - \cdots - r_{h,k} e_j w_k$ for $h \in [i] \setminus [k]$. Then $v_1, \ldots, v_i$ are a minimal system of generators of C with the property that $e_j v_1, \ldots, e_j v_k$ are a minimal system of generators of C_j' and $e_j v_{k+1} = \cdots = e_j v_i = 0$. Notice that only the jth coordinate of $v_1, \ldots, v_i$ was affected by this operation, hence $e_h w_k = e_h v_k$ for all $k \in [i]$ if $h \neq j$. Performing this operation for all $j \in [\ell]$ produces a minimal system of generators $v_1, \ldots, v_i$ of C with the property that the set $V = \{e_j v_k \,:\, (j,k) \in [\ell] \times [i],\ e_j v_k \neq 0\}$ is a minimal system of generators of C. Moreover, for $j \in [\ell]$, $\{e_j v_k \,:\, k \in [i],\ e_j v_k \neq 0\}$ is a minimal system of generators of C_j'. Since $v_1, \ldots, v_i \neq 0$, for each $k \in [i]$ there must be at least a $j \in [\ell]$ such that $e_j v_k \neq 0$. This proves that $|V| \geqslant i$.

To prove the last part of the statement, let $M = \max\{i \geqslant 0 \,:\, C \in \mathcal{S}_i(R^n)\}$. Since C has a minimal system of generators $v_1, \ldots, v_M$, by the first part of the statement $V = \{e_j v_k \,:\, (j,k) \in [\ell] \times [M],\ e_j v_k \neq 0\}$ is a minimal system of generators of C of $|V| = M$. Therefore, for each $k \in [M]$ there is exactly one $j \in [\ell]$ with $e_j v_k \neq 0$. Moreover, $\{v_k \,:\, k \in [M],\ e_j v_k \neq 0\}$ is a minimal system of generators of C_j' for $j \in [\ell]$, hence it has cardinality $\mu(C_j)$ by Theorem 2.5. It follows that $M = \mu(C_1) + \cdots + \mu(C_\ell) = M(C)$. □

We conclude the section with a few elementary properties of $M(C)$.

Proposition 2.9. *Let R be a finite commutative ring and let $D \subseteq C \subseteq 0 :_{R^n} J$ be codes. Then*

$$M(D) \leqslant M(C)$$

and equality holds if and only if $D = C$.

Proof. Write $C = C_1 \times \cdots \times C_\ell$ and $D = D_1 \times \cdots \times D_\ell$. Since $D \subseteq C$, we have $D_i \subseteq C_i \subseteq 0 :_{R_i^n} \mathfrak{M}_i$ for all $i \in [\ell]$. So C_i and D_i are $R_i/\mathfrak{M}_i$-vector spaces and $\mu(D_i) \leqslant \mu(C_i)$ for all $i \in [\ell]$ by Theorem 2.5. It follows that

$$M(D) = \mu(D_1) + \cdots + \mu(D_\ell) \leqslant \mu(C_1) + \cdots + \mu(C_\ell) = M(C).$$

Moreover, $M(D) = M(C)$ if and only if $\mu(D_i) = \mu(C_i)$ for all $i \in [\ell]$. In this case, C_i and D_i are $R_i/\mathfrak{M}_i$-vector spaces of the same dimension by Theorem 2.5. Hence they are equal, therefore $D = C$. □

Notice that one may have $D \subsetneq C \subseteq R^n$ with $M(D) = M(C)$. Some examples of this arise for instance from the fact that, over a principal ideal ring (**PIR** in the sequel), the value of $M(C)$ does not change when replacing C with its socle. We will use this fact repeatedly throughout the paper.

Proposition 2.10. *Let R be a finite PIR and let $C \subseteq R^n$ be a code. Then*

$$M(C) = M(0 :_C J).$$

Proof. We may assume without loss of generality that R is a finite chain ring. Indeed, if the result is true for finite chain rings, then write $R = R_1 \times \cdots \times R_\ell$ as a product of finite chain rings and $C = C_1 \times \cdots \times C_\ell$, where $C_i \subseteq R_i^n$ is a code for $i \in [\ell]$. We have

$$M(C) = \mu(C_1) + \cdots + \mu(C_\ell) = \mu(0 :_{C_1} \mathfrak{M}_1) + \cdots + \mu(0 :_{C_\ell} \mathfrak{M}_\ell) = M(0 :_C J),$$

where the last equality follows from

$$0 :_C J = (0 :_{C_1} \mathfrak{M}_1) \times \cdots \times (0 :_{C_\ell} \mathfrak{M}_\ell).$$

In order to prove that $\mu(C) = \mu(0 :_C J)$ for $C \subseteq R^n$ and R a finite chain ring, observe that $J = (\alpha)$ is principal and

$$\mu(C) = \dim_{R/(\alpha)}(C/\alpha C) = \dim_{R/(\alpha)}(0 :_C \alpha) = \mu(0 :_C \alpha), \tag{2.3}$$

where the first and last equalities follow from Theorem 2.5. The short exact sequence

$$0 \to 0 :_C \alpha \to C \to \alpha C \to 0$$

induces an isomorphism $C/\alpha C \cong 0 :_C \alpha$, which proves the central equality in (2.3). □

The statement of Proposition 2.10 also holds when $C = R^n$ and R is a product of finite Gorenstein local rings.

Example 2.11. Write $R = R_1 \times \cdots \times R_\ell$ and suppose that each R_i is a finite Gorenstein local ring. Suppose first that $\ell = 1$, i.e. R is a Gorenstein local ring with maximal ideal $\mathfrak{M}$. We have the following isomorphisms of $R/\mathfrak{M}$-vector spaces

$$R^n/\mathfrak{M}R^n \cong (R/\mathfrak{M}R)^n \cong (0 :_R \mathfrak{M})^n = 0 :_{R^n} \mathfrak{M},$$

where the central isomorphism follows from the definition of a Gorenstein local ring. Then $\mu(R^n) = \mu(0 :_{R^n} \mathfrak{M}) = n$ by Theorem 2.5.

For general ℓ, one has

$$M(R^n) = \mu(R_1^n) + \cdots + \mu(R_\ell^n).$$

Moreover, $0:_{R^n} J = \left(0:_{R_1^n} \mathfrak{M}_1\right) \times \cdots \times \left(0:_{R_\ell^n} \mathfrak{M}_\ell\right)$, hence

$$M(0:_{R^n} J) = \mu\left(0:_{R_1^n} \mathfrak{M}_1\right) + \cdots + \mu\left(0:_{R_\ell^n} \mathfrak{M}_\ell\right).$$

It follows from the previous case ($\ell = 1$) that

$$\mu(R_i^n) = \mu(0:_{R_i^n} \mathfrak{M}) = n$$

for all $i \in [\ell]$.

The argument of Example 2.11 also shows that, if the equality in Proposition 2.10 holds for $C = R^n$, for R a finite local ring, then R must be Gorenstein. However, Proposition 2.10 is not true in general over finite Gorenstein local rings. The next example was suggested to us by Maria Evelina Rossi.

Example 2.12. Let $R = \mathbb{F}_2[x,y]/(x^2,y^2)$. Then R is a finite local ring with maximal ideal $\mathfrak{M} = (x,y)$. Let $C = \mathfrak{M}$. Then $\mu(C) = 2$, but $\mu(0:_C \mathfrak{M}) = \mu(\langle xy\rangle) = 1$.

3. Supports and generalized weights

In this section we develop an algebraic theory of supports over a finite commutative ring R. We propose a general definition of support as a map $R^n \to \mathbb{N}^u$, which naturally induces a notion of generalized weights for codes $C \subseteq R^n$. This extends the notion of generalized Hamming weights for codes that are linear over a finite field $\mathbb{F}_q$. We establish some properties of support functions and generalized weights. We also define a family of supports, the *modular supports*, whose associated generalized weights will be studied in the next sections.

Notation 3.1. *In the sequel, $u \geqslant 1$ is an integer. For $s,t \in \mathbb{N}^u$ write $s \leqslant t$ if $s_i \leqslant t_i$ for all $i \in [u]$. Then $(\mathbb{N}^u, \leqslant)$ is a (poset) lattice. The* **meet** *of $s,t \in \mathbb{N}^u$ is the element $s \wedge t \in \mathbb{N}^u$ given by $(s \wedge t)_i = \min\{s_i, t_i\}$ for all $i \in [u]$. The* **join** *of $s,t \in \mathbb{N}^u$, denoted by $s \vee t$, is $(s \vee t)_i = \max\{s_i, t_i\}$ for all $i \in [u]$. For $s \in \mathbb{N}^u$, we let $|s| := s_1 + \cdots + s_u$.*

Definition 3.2. A **support** on R^n is a function $\sigma : R^n \to \mathbb{N}^u$ with the following properties.

(P1) $\sigma(v) = 0$ if and only if $v = 0$.

(P2) $\sigma(rv) \leqslant \sigma(v)$ for all $r \in R$ and $v \in R^n$.

(P3) $\sigma(v + w) \leqslant \sigma(v) \vee \sigma(w)$ for all $v, w \in R^n$.

A support function $\sigma : R^n \to \mathbb{N}^u$ satisfies the following additional properties.

Lemma 3.3. *Let $\sigma : R^n \to \mathbb{N}^u$ be a support. The following hold.*

(P4) If $v \in R^n$ and $r \in R$ is a unit, then $\sigma(rv) = \sigma(v)$.

(P5) If $v, w \in R^n$ and $i \in [u]$ satisfy $\sigma(v)_i = 0$ and $\sigma(w)_i \neq 0$, then $\sigma(w + v)_i \neq 0$.

(P6) If $v, w \in R^n$ and $i \in [u]$ satisfy $\sigma(v)_i = \sigma(w)_i = 0$, then $\sigma(w + v)_i = 0$.

Proof. The first claim easily follows from Property (P2). To see the second, suppose towards a contradiction that $\sigma(w+v)_i = 0$. Since $w = (w+v) + (-v)$, by (P3) and the first claim we have $\sigma(w) \leqslant \sigma(w+v) \vee \sigma(-v) = \sigma(w+v) \vee \sigma(v)$, from which $\sigma(w)_i = 0$, a contradiction. Finally, the third claim follows from Property (P3). □

A support $\sigma : R^n \to \mathbb{N}^u$ naturally induces a weight function $\mathrm{wt} : R^n \to \mathbb{N}$.

Definition 3.4. The **weight** of $v \in R^n$ is $\mathrm{wt}(v) := |\sigma(v)|$, where $|\sigma(v)| = \sum_{i=1}^{u} \sigma(v)_i$. The **minimum weight** and **maximum weight** of a code $0 \neq C \subseteq R^n$ are, respectively,

$$\min \mathrm{wt}(C) := \min\{\mathrm{wt}(v) \, : \, v \in C \setminus \{0\}\} \qquad \text{and} \qquad \max \mathrm{wt}(C) := \max\{\mathrm{wt}(v) \, : \, v \in C\}.$$

Notice that the function $\mathrm{wt} : R^n \to \mathbb{N}$ has indeed the properties of a weight, since $\mathrm{wt}(v) \geqslant 0$ for all v, $\mathrm{wt}(v) = 0$ if and only if $v = 0$, and $\mathrm{wt}(u+v) \leqslant \mathrm{wt}(u) + \mathrm{wt}(v)$ for all $u, v \in R^n$. In addition, the weight satisfies $\mathrm{wt}(rv) \leqslant \mathrm{wt}(v)$ for all $r \in R$ and $v \in R^n$ and $\mathrm{wt}(rv) = \mathrm{wt}(v)$ for $r \in R$ invertible and $v \in R^n$.

We give some examples of support functions. Many others can be obtained by applying Proposition 3.7 to these examples.

Example 3.5.

(1) The function $\sigma : \mathbb{F}_2^2 \to \{0,1,2\}^3$ defined by $\sigma(0,0) = (0,0,0)$, $\sigma(1,0) = (2,0,2)$, $\sigma(0,1) = (2,1,0)$, and $\sigma(1,1) = (0,1,2)$ is a support.

(2) Let R a be finite ring and let $0 = I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_{\epsilon-1} \subsetneq I_\epsilon = R$ be a chain of ideals of R. For $r \in R$, let $\sigma(r) := \min\{0 \leqslant i \leqslant \epsilon \, : \, r \in I_i\}$. Extend σ coordinatewise to $\sigma : R^n \to \{0, \dots, \epsilon\}^n$. It can be checked that σ is a support, called the **chain support** on R, see [Rav18, Example 26].

(3) Let R be a finite chain ring. The chain support associated to the full chain of ideals of R is the **chain ring support** on R.

(4) If $R = \mathbb{F}_q$ is a finite field, the chain ring support coincides with the **Hamming support** $\sigma^{\mathrm{H}} : \mathbb{F}_q^n \to \{0,1\}^n$, given by $\sigma^{\mathrm{H}}(v)_i = 1$ if $v_i \neq 0$ and $\sigma^{\mathrm{H}}(v)_i = 0$ if $v_i = 0$. See [MS77] for a general reference on Hamming-metric codes.

(5) In his master thesis [Gas20], written under the direction of J. Rosenthal and V. Weger, N. Gassner introduces the p-adic weight and distance on $\mathbb{Z}_{p^e}^n$, where p is prime and $e \geqslant 1$. The p-adic weight on $\mathbb{Z}_{p^e}$ induces the same partition as the weight associated to the chain ring support of $\mathbb{Z}_{p^e}$.

Not all the supports studied in the coding theory literature are supports according to Definition 3.2.

Example 3.6. The **Lee weight** $\mathrm{wt}^{\mathrm{L}} : \mathbb{Z}_4 \to \{0,1,2\}$ is defined by $\mathrm{wt}^{\mathrm{L}}(0) = 0$, $\mathrm{wt}^{\mathrm{L}}(1) = \mathrm{wt}^{\mathrm{L}}(3) = 1$ and $\mathrm{wt}^{\mathrm{L}}(2) = 2$. Its coordinatewise extension to $\mathbb{Z}_4^n$ is not a support in the sense of Definition 3.2. For instance, $\mathrm{wt}^{\mathrm{L}}(1+1) = 2 \not\leqslant \max\{\mathrm{wt}^{\mathrm{L}}(1), \mathrm{wt}^{\mathrm{L}}(1)\} = 1$, contradicting Property (P3).

In the next proposition we list some simple operations that allow one to construct new supports from known ones. The proof is straightforward and left to the reader.

Proposition 3.7. *(1) Let $\sigma : R^n \to \mathbb{N}^u$ be a function and let $s : \mathbb{N}^u \to \mathbb{N}^u$ be a permutation of the coordinates. Then σ is a support if and only if $s \circ \sigma$ is a support.*

(2) Let $\sigma_i : R^{n_i} \to \mathbb{N}^{u_i}$ be functions, $i \in [\ell]$. Let $n = n_1 + \cdots + n_\ell$ and $u = u_1 + \cdots + u_\ell$. Let

$$\sigma = \sigma_1 \times \cdots \times \sigma_\ell : R^n \to \mathbb{N}^u, \qquad (v_1, \ldots, v_\ell) \mapsto (\sigma_1(v_1), \ldots, \sigma_\ell(v_\ell)).$$

Then σ is a support if and only if $\sigma_1, \ldots, \sigma_\ell$ are supports.

(3) Let $\sigma : R^n \to \mathbb{N}^u$, $\sigma(v) = (\sigma_1(v), \ldots, \sigma_u(v))$, be a function. Let $i \in [u]$, $a \in \mathbb{N} \setminus \{0\}$, and define

$$\sigma_{i,a} : R^n \to \mathbb{N}^u, \qquad v \mapsto (\sigma_1(v), \ldots, \sigma_{i-1}(v), a\sigma_i(v), \sigma_{i+1}(v), \ldots, \sigma_u(v)).$$

Then σ is a support if and only if $\sigma_{i,a}$ is.

(4) Let $\sigma : R^n \to \mathbb{N}^u$, $\sigma(v) = (\sigma_1(v), \ldots, \sigma_u(v))$. For $i \in [u]$, let

$$\tilde{\sigma}_i : R^n \to \mathbb{N}^{u+1}, \qquad v \mapsto (\sigma_1(v), \ldots, \sigma_{i-1}(v), \sigma_i(v), \sigma_i(v), \sigma_{i+1}(v), \ldots, \sigma_u(v)).$$

Then σ is a support if and only if $\tilde{\sigma}_i$ is.

(5) Let $\sigma : R^n \to \mathbb{N}^u$, $\sigma(v) = (\sigma_1(v), \ldots, \sigma_u(v))$, be a support and let $i \in [u]$. Assume that there are no $a \in \mathbb{N} \setminus \{0\}$ and $v \in R^n$ such that $\sigma(v) = (0, \ldots, 0, a, 0, \ldots, 0)$, where a appears in the ith entry. Then

$$\hat{\sigma}_i : R^n \to \mathbb{N}^{u-1}, \qquad v \mapsto (\sigma_1(v), \ldots, \sigma_{i-1}(v), \sigma_{i+1}(v), \ldots, \sigma_u(v))$$

is a support.

(6) Let $\sigma : R^n \to \mathbb{N}^u$ be a function, $\sigma(v) = (\sigma_1(v), \ldots, \sigma_u(v))$. For $i \in [u]$, let

$$\breve{\sigma}_i : R^n \to \mathbb{N}^{u+1}, \qquad v \mapsto (\sigma_1(v), \ldots, \sigma_{i-1}(v), \sigma_i(v), 0, \sigma_{i+1}(v), \ldots, \sigma_u(v)).$$

Then σ is a support if and only if $\breve{\sigma}_i$ is.

(7) Let $\sigma : R^n \to \mathbb{N}^u$ be a support and let $f : R^k \to R^n$ be an injective R-linear map. Then $\sigma \circ f : R^k \to \mathbb{N}^u$ is a support.

(8) Let $\sigma_i : R^n \to \mathbb{N}^{u_i}$ be supports, $i \in [k]$. Then $\sigma = (\sigma_1, \ldots, \sigma_k) : R^n \to \mathbb{N}^{u_1+\cdots+u_k}$ is a support.

Similarly to the situation of linear codes endowed with the Hamming support, a support function over a finite commutative ring R induces a notion of support of a code. In turn, this allows us to define generalized weights for R-linear codes.

Definition 3.8. The **support** of a code $C \subseteq R^n$ is

$$\sigma(C) := \bigvee_{v \in C} \sigma(v) \in \mathbb{N}^u.$$

Notice that the support of a code is determined by the supports of the vectors in any system of generators. More precisely, let $C = \langle v_1, \dots, v_k \rangle \subseteq R^n$. Since, by Definition 3.2,

$$\sigma(r_1 v_1 + \cdots + r_k v_k) \leqslant \sigma(r_1 v_1) \vee \ldots \vee \sigma(r_k v_k) \leqslant \sigma(v_1) \vee \ldots \vee \sigma(v_k)$$

for any $r_1, \dots, r_k \in R$, we have

$$\sigma(C) = \bigvee_{i=1}^{k} \sigma(v_i). \tag{3.1}$$

Moreover, if $D \subseteq C$, then by definition $\sigma(D) \leqslant \sigma(C)$.

Definition 3.9. For $r \in [M(C)]$, the r-th **generalized weight** of C is the integer

$$d_r(C) := \min\{|\sigma(D)| \,:\, D \in \mathcal{S}_j(C) \text{ for some } j \geqslant r\}.$$

We also set

$$d_0(C) := 0.$$

It follows from Theorem 2.8 that for $r \in [M(C)]$ we have $\mathcal{S}_r(C) \neq \varnothing$. Hence $d_r(C)$ is well-defined.

Remark 3.10. For $r \in [M(C)]$ one has

$$d_r(C) = \min\{|\sigma(D)| \,:\, D \in \mathcal{S}_r(C)\}.$$

Indeed, let $j \geqslant r$ and let $D \in \mathcal{S}_j(C)$. Then there exists a $D' \subseteq D$ such that $D' \in \mathcal{S}_r(C)$ and $|\sigma(D')| \leqslant |\sigma(D)|$.

In the next lemma we collect a few easy consequences of Definition 3.9.

Lemma 3.11. *Let $D \subseteq C \subseteq R^n$ be codes. The following hold.*

(1) $d_1(C) = \min \text{wt}(C)$.

(2) $d_r(D) \geqslant d_r(C)$ *for* $r \in [\min\{M(D), M(C)\}]$.

(3) $d_{r+1}(C) \geqslant d_r(C)$ *for* $r \in [M(C) - 1]$.

(4) $d_r(C) = \min\{|\sigma(D)| \,:\, D \subseteq C,\ M(D) \geqslant r\}$ *for* $r \in [M(C)]$.

Proof. By Property (P2) one has $\sigma(\langle v \rangle) = \sigma(v)$ for any $v \in C$. Hence (1) follows, thanks to Remark 3.10. Part (2) holds since every subcode of D is also a subcode of C. Part (3) follows from observing that d_r is the minimum of the function $|\sigma(D)|$ for D ranging over the set $\mathcal{S}_r(C) \cup \ldots \cup \mathcal{S}_{M(C)}(C)$ and passing from r to $r+1$ we minimize over a subset. In order to prove (4), let $i \geqslant r$ and $D \in \mathcal{S}_i(C)$. Then $M(D) \geqslant i$ by Theorem 2.8. Therefore, if $D \in \mathcal{S}_i(C)$ for some $i \geqslant r$, then $D \in \mathcal{S}_{M(D)}(C)$ and $M(D) \geqslant r$. Since every $D \subseteq C$ belongs to $\mathcal{S}_{M(D)}(C)$, then $\{D \in \mathcal{S}_i(C) \text{ for some } i \geqslant r\} = \{D \subseteq C,\ M(D) \geqslant r\}$. Therefore

$$d_r(C) = \min\{|\sigma(D)| \,:\, D \in \mathcal{S}_i(C) \text{ for some } i \geqslant r\} = \min\{|\sigma(D)| \,:\, D \subseteq C,\ M(D) \geqslant r\}.$$

□

Equation (3.1) may not hold for supports studied in the coding theory literature which are not supports according to Definition 3.2. Moreover, failure of Equation (3.1) has as a consequence that $d_1(C)$ may not equal the minimum distance.

Example 3.12. Equation (3.1) does not hold for the Lee weight $\mathrm{wt}^{\mathrm{L}} : \mathbb{Z}_4 \to \{0,1,2\}$, nor for its coordinatewise extension to $\mathbb{Z}_4^n$. For example, $\mathrm{wt}^{\mathrm{L}}(\langle 1\rangle) = 2 > 1 = \mathrm{wt}^{\mathrm{L}}(1)$ and

$$d_1(\langle 1\rangle) = \mathrm{wt}^{\mathrm{L}}(\langle 1\rangle) = 2 > 1 = \min \mathrm{wt}^{\mathrm{L}}(\langle 1\rangle).$$

We now show how the structure of supports relate to the decomposition of R in (2.1).

Proposition 3.13. *Let $\sigma : R^n \to \mathbb{N}^u$ be a support. Then for any $v = (v_1,\dots,v_\ell) \in R^n = R_1^n \times \cdots \times R_\ell^n$ we have*

$$\sigma(v) = \sigma_1(v_1) \vee \ldots \vee \sigma_\ell(v_\ell),$$

where $\sigma_i : R_i^n \to \mathbb{N}^u$ is as support defined via $\sigma_i(v_i) := \sigma(e_i v)$ for all $i \in [\ell]$.

Proof. It is easy to check that σ_i is well-defined and is a support for all $i \in [\ell]$. One has $\sigma_i(v_i) = \sigma(e_i v) \leqslant \sigma(v)$, hence $\sigma_1(v_1) \vee \ldots \vee \sigma_\ell(v_\ell) \leqslant \sigma(v)$. Furthermore,

$$\sigma(v) = \sigma\left(\sum_{i=1}^{\ell} e_i v\right) \leqslant \bigvee_{i=1}^{\ell} \sigma(e_i v) = \bigvee_{i=1}^{\ell} \sigma_i(v_i).$$

It follows that $\sigma(v) = \sigma_1(v_1) \vee \ldots \vee \sigma_\ell(v_\ell)$, as desired. □

Remark 3.14. When R is a finite chain ring, support functions on R have a simple description. To see this, let α be a generator of the maximal ideal of R and let $\epsilon = \min\{i > 0 : \alpha^i = 0\}$. Let $\sigma, \tau : R \to \mathbb{N}^u$ be supports. Then $\sigma = \tau$ if and only if $\sigma(\alpha^i) = \tau(\alpha^i)$ for $0 \leqslant i \leqslant \epsilon - 1$. Indeed, every element of $R \setminus \{0\}$ is of the form $r\alpha^i$ where r is a unit and $0 \leqslant i \leqslant \epsilon - 1$, and $\sigma(r\alpha^i) = \sigma(\alpha^i)$. Therefore, a support $\sigma : R \to \mathbb{N}^u$ corresponds to a set of vectors $a^{(0)}, a^{(1)}, \dots, a^{(\epsilon-1)} \in \mathbb{N}^u$ with the property that $a^{(0)} \geqslant a^{(1)} \geqslant \ldots \geqslant a^{(\epsilon-1)}$. The correspondence is determined by setting $\sigma(\alpha^i) = a^{(i)}$ for all $i \in \{0,\dots,\epsilon-1\}$. In particular, any support on R induces the same partition as a chain support.

3.1. Modular supports

In this subsection we define and study a class of supports whose structure is closely related to the R-module structure of R^n, and that we therefore call *modular*. This paper is primarily devoted to the study of generalized weights associated to modular supports.

Definition 3.15. A support σ is **modular** if it satisfies the following:

(P$\star$) If $v, w \in R^n$ and $i \in [u]$ satisfy $0 \neq \sigma(v)_i \leqslant \sigma(w)_i$, then there exists $r \in R$ such that $\sigma(v + rw)_i < \sigma(v)_i$.

Remark 3.16. By repeatedly applying Property (P$\star$), one obtains the following equivalent property: If $v, w \in R^n$ and $i \in [u]$ satisfy $0 \neq \sigma(v)_i \leqslant \sigma(w)_i$, then there exists $r \in R$ such that $\sigma(v + rw)_i = 0$.

As for supports, one can easily produce new modular supports from known ones.

Proposition 3.17. *Let $\sigma : R^n \to \mathbb{N}^u$ be a support. Following the notation and numbering of Proposition 3.7, we have:*

(1) σ is modular if and only if $s \circ \sigma$ is modular;

(2) $\sigma_1, \ldots, \sigma_\ell$ are modular if and only if σ is modular;

(3) σ is modular if and only if $\sigma_{i,a}$ is modular;

(4) σ is modular if and only if $\tilde{\sigma}_i$ is modular;

(5) if σ is modular, then $\hat{\sigma}_i$ is modular;

(6) σ is modular if and only if $\breve{\sigma}_i$ is modular;

(7) if σ is modular, then $\sigma \circ f$ is modular;

(8) if $\sigma_1, \ldots, \sigma_k$ are modular, then $\sigma = (\sigma_1, \ldots, \sigma_k)$ is modular.

Several, but not all, of the supports that we have encountered so far are modular.

Example 3.18. Support (1) of Example 3.5 is modular, while an arbitrary chain support is not. Over a finite chain ring, the only modular chain support is the chain ring support. For example, the chain support on $\mathbb{Z}_4$ associated with the chain $0 \subsetneq \mathbb{Z}_4$ is not modular. Indeed, $\sigma(2) = \sigma(4) = 1$, but there is no $r \in \mathbb{Z}_4$ with $2 - 4r = 0$.

The Hamming support is an example of modular support.

Example 3.19. It is easy to check that the chain ring support of Example 3.5(3) is modular. Hence a product of chain ring supports is modular by Proposition 3.7 and Proposition 3.17(2). In particular, the Hamming support is modular.

Example 3.20. The supports of Remark 3.14 are modular if and only if $(a^{(j)})_i \neq (a^{(k)})_i$ for all $j, k \in \{0, \ldots, \epsilon - 1\}$ distinct and $i \in [u]$.

We now give more examples of supports which are not modular.

Example 3.21. Let $R = \mathbb{F}_2$ and let $\sigma : \mathbb{F}_2^2 \to \{0,1\}^2$ be defined by

$$\sigma(0,0) = (0,0), \quad \sigma(1,0) = (1,1), \quad \sigma(0,1) = (0,1), \quad \sigma(1,1) = (1,1).$$

Then σ is a support which is not modular.

Example 3.22. The chain support on $\mathbb{Z}_6$ associated with the chain $(0) \subsetneq (2) \subsetneq \mathbb{Z}_6$ is not modular. Indeed, $\sigma(2) = 1$ and $\sigma(3) = 2$, but there is no $r \in \mathbb{Z}_6$ with $2 - 3r = 0$.

The next result shows that every modular support over a finite commutative ring decomposes as a product of modular supports over finite local rings.

Theorem 3.23. *Let R be a finite commutative ring and let $\sigma : R^n \to \mathbb{N}^u$ be a modular support. Up to a permutation of the coordinates of $\mathbb{N}^u$ we have $\sigma = \sigma_1 \times \cdots \times \sigma_\ell$ where $\sigma_i : R_i^n \to \mathbb{N}^{u_i}$ for $i \in [\ell]$ and $u_1, \dots, u_\ell$ are integers with $u_1 + \cdots + u_\ell = u$. Moreover, σ_i is a modular support for all $i \in [\ell]$.*

Proof. For $v \in R^n$, write $v = (v_1, \dots, v_\ell)$ with $v_i \in R_i^n$. By Proposition 3.13 we have

$$\sigma(v_1, \dots, v_\ell) = \sigma_1(v_1) \vee \ldots \vee \sigma_\ell(v_\ell),$$

where $\sigma_i : R_i^n \to \mathbb{N}^u$ is a support defined via $\sigma_i(v_i) := \sigma(e_i v)$, $i \in [\ell]$. We claim that for each $x \in [u]$ there is at most one $i \in [\ell]$ such that $\sigma_i(v_i)_x \neq 0$ for some $v \in R^n$. Indeed, assume towards a contradiction that there exist $i \neq j$ and $v, w \in R^n$ such that $\sigma_i(v_i)_x, \sigma_j(w_j)_x \neq 0$. Without loss of generality we may assume that $0 < \sigma_i(v_i)_x \leqslant \sigma_j(w_j)_x$. By Property (P⋆) there exists $r = (r_1, \dots, r_\ell) \in R$ such that

$$\sigma(e_i v)_x > \sigma(e_i v + e_j r w)_x = [\sigma_i(v_i) \vee \sigma_j(r_j w_j)]_x \geqslant \sigma_i(v_i)_x,$$

where the equality follows from Proposition 3.13. This a contradiction, establishing the claim.

We have shown that for each $x \in [u]$ there exists at most one $i \in [\ell]$ for which $(\sigma_i)_x$ is not the zero function. In other words, the supports of the images of the functions σ_i are disjoint. Up to permuting the coordinates of $\mathbb{N}^u$, one may assume that σ_1 is supported on the first u_1 coordinates, σ_2 on the next u_2,..., and σ_ℓ on the last u_ℓ. Therefore one may regard each σ_i as a function which takes values in $\mathbb{N}^{u_i}$. Then $\sigma = \sigma_1 \times \cdots \times \sigma_\ell$ and each σ_i is a modular support by Proposition 3.7(2) and Proposition 3.17(2). □

By combining Remark 3.14 with Theorem 3.23, support functions on a principal ideal ring R can be easily characterized as follows.

Corollary 3.24. *Let R be a finite principal ideal ring and let $\sigma : R \to \mathbb{N}^u$ be a modular support. By the Zariski–Samuel Theorem, $R = R_1 \times \cdots \times R_\ell$ where $R_1, \dots, R_\ell$ are finite chain rings. For each i, let α_i be a generator of the maximal ideal of R_i and let $\epsilon_i := \min\{j : \alpha_i^j = 0\}$. Then there exist $u_1, \dots, u_\ell$ such that $u_1 + \cdots + u_\ell = u$ and $\sigma = \sigma_1 \times \cdots \times \sigma_\ell$, where $\sigma_i : R_i \to \mathbb{N}^{u_i}$ for $i \in [\ell]$. Let $\sigma_i(\alpha_i^j) = a^{(i,j)} \in \mathbb{N}^{u_i}$ for $i \in [\ell]$ and $j \in \{0, \dots, \epsilon_i - 1\}$. Then $(a^{(i,j-1)})_k > (a^{(i,j)})_k$ for $j \in [\epsilon_i - 1]$, $i \in [\ell]$, $k \in [u_i]$.*

Conversely, any set of vectors $a^{(i,j)} \in \mathbb{N}^{u_i}$ such that $a^{(i,j-1)} \geqslant a^{(i,j)}$ for $j \in [\epsilon_i - 1]$ and $i \in [\ell]$ defines a support $\sigma = \sigma_1 \times \cdots \times \sigma_\ell$ on R via $\sigma_i(r\alpha_i^j) = a^{(i,j)}$ for $i \in [\ell], j \in \{0, \dots, \epsilon_i - 1\}$, and $r \in R_i$ invertible. Moreover, if $(a^{(i,j-1)})_k > (a^{(i,j)})_k$ for $j \in [\epsilon_i - 1]$, $i \in [\ell]$, and $k \in [u_i]$, then σ is modular.

The following is a reformulation of Property (P⋆) for elements of $0 :_{R^n} J$.

Corollary 3.25. *Assume that σ is modular. If $v, w \in 0 :_{R^n} J$ and $i \in [u]$ satisfy $\sigma(v)_i \neq 0$ and $\sigma(w)_i \neq 0$, then there exists a unit $r \in R$ with $\sigma(v - rw)_i = 0$.*

Proof. By Theorem 3.23 we may assume without loss of generality that R is a finite local ring. Indeed, let $j \in [\ell]$ be such that $(\sigma_j)_i$ is not identically zero and suppose that $\sigma_j(v_j - r_j w_j)_i = 0$ for some $r_j \in R_j$ invertible, then $r = (1, \dots, 1, r_j, 1, \dots, 1) \in R$ is invertible and satisfies $\sigma(v - rw)_i = 0$.

Assume now that $(R, \mathfrak{M})$ is a finite local ring. If $\sigma(v)_i \leqslant \sigma(w)_i$, then by Property (P$\star$) there is $r \in R$ such that $\sigma(v - rw)_i = 0$. If $r \in \mathfrak{M}$, then $rw = 0$, hence $\sigma(v)_i = 0$, contradicting the assumption in the statement. Therefore r is invertible. Similarly, if $\sigma(w)_i \leqslant \sigma(v)_i$, then there exists $s \in R$ invertible such that $0 = \sigma(w - sv)_i = \sigma(v - s^{-1}w)_i$. □

4. Codewords and subcodes of minimal support

In this section we study the codewords and subcodes of minimal support of an R-linear code endowed with a modular support. In particular, we establish some properties of the systems of generators of subcodes of minimal support. This allows us to derive properties of the generalized weights, such as monotonicity and a generalization of the Singleton bound.

In the sequel, we follow the notation of the previous sections and let $\sigma : R^n \to \mathbb{N}^u$ be a modular support. The minimal codewords of a code play a central role in our work. They are defined as follows.

Definition 4.1. Let $C \subseteq R^n$ be a code. We say that $v \in C \setminus \{0\}$ is **minimal** in C if its support is minimal among the supports of the elements of $C \setminus \{0\}$. We denote by $\mathrm{Min}(C)$ the set of minimal codewords of C.

Remark 4.2. By definition, $C = 0$ has no minimal codewords, i.e., $\mathrm{Min}(0) = \varnothing$.

We start by observing that a modular support $\sigma : R^n \to \mathbb{N}^u$ that takes values in $\{0, 1\}^u$ allows us to associate a matroid to a code C. More precisely, the minimal ones among the supports of the codewords of C are the circuits of a matroid. This generalizes the well-known fact that one may associate to a linear block-code the matroid represented by its parity-check matrix, whose circuits correspond to the minimal supports of the nonzero codewords of C with respect to the Hamming weight. We refer the reader to [Oxl06, Section 1.1] for the definition of matroids via their circuits or their independent sets, and for the equivalence of the two definitions.

Theorem 4.3. *Let R be a finite commutative ring and let $\sigma : R^n \to \{0, 1\}^u$ be a modular support. Let $0 \neq C \subseteq R^n$ be a code. Then the elements of the set*

$$\mathcal{C} := \{\sigma(v) : v \in \mathrm{Min}(C)\}$$

are the circuits of a matroid.

Proof. If a support σ takes values in $\{0, 1\}^u$, then the support of a vector can be naturally identified with a subset of $[u]$. In order to show that $\mathcal{C}$ is the set of circuits of a matroid, we check the circuit axioms as stated in [Oxl06, page 9].

Properties (C1) and (C2) are immediate to verify. To see that Property (C3) holds, suppose that $\sigma(v), \sigma(w) \in \mathcal{C}$, that $\sigma(v) \neq \sigma(w)$, and that $(\sigma(v) \wedge \sigma(w))_i \neq 0$. By repeatedly applying Property (P$\star$) and up to exchanging the role of v and w, one sees that there exists $r \in R$

with $\sigma(v-rw)_i = 0$. We claim that $v - rw \neq 0$. Indeed, if $v = rw$ then we would have $\sigma(v) = \sigma(rw) \leqslant \sigma(w)$. Since $\sigma(w)$ is minimal by assumption and $v \neq 0$, it must be that $\sigma(v) = \sigma(w)$, a contradiction.

Since $v - rw \neq 0$, we have $\sigma(v-rw) \neq 0$. Fix $z \in C$ with $\sigma(z) \in \mathcal{C}$, $\sigma(z) \leqslant \sigma(v-rw)$. We have

$$\sigma(z) \leqslant \sigma(v-rw) \leqslant \sigma(v) \vee \sigma(-rw) \leqslant \sigma(v) \vee \sigma(w). \tag{4.1}$$

Moreover, $0 = \sigma(v-rw)_i \geqslant \sigma(z)_i$. This establishes Property (C3). □

We start our study of the minimal codewords by showing that the minimal codewords of a code C coincide with those of its socle. We also show that the minimal codewords of a given code are determined by their support, up to multiplication by a unit.

Theorem 4.4. *Let $C \subseteq R^n$ be a code and assume that σ is modular. The following hold.*

(1) The set of minimal codewords of C is

$$\begin{aligned}\mathrm{Min}(C) &= \bigcup_{i=1}^{\ell}(0 \times \cdots \times 0 \times \mathrm{Min}(C_i) \times 0 \times \cdots \times 0)\\ &\subseteq \bigcup_{i=1}^{\ell}(0 \times \cdots \times 0 \times (0 :_{C_i} \mathfrak{M}_i) \times 0 \times \cdots \times 0) \quad \subseteq \quad 0 :_C J.\end{aligned}$$

(2) In particular,

$$\mathrm{Min}(C) = \mathrm{Min}(0 :_C J).$$

(3) If $v, w \in \mathrm{Min}(C)$ are minimal codewords with $\sigma(v) = \sigma(w)$, then $v = rw$ for some invertible $r \in R$.

Proof. (1) By Theorem 3.23, up to a permutation of the coordinates of $\mathbb{N}^u$, σ decomposes as a product $\sigma = \sigma_1 \times \cdots \times \sigma_\ell$, where each σ_i is a modular support. Let $i \in [\ell]$ and $v = (v_1, \ldots, v_\ell) \in \mathrm{Min}(C)$ with $v_i \neq 0$. Then $0 \neq \sigma(e_i v) \leqslant \sigma(v)$, hence $\sigma(e_i v) = \sigma(v)$. In particular, $\sigma_j(v_j) = 0$ for all $j \neq i$, hence $v_j = 0$ for all $j \neq i$. Therefore, $v = e_i v$ and $v_i \in \mathrm{Min}(C_i)$. This proves the equality in the statement.

Suppose now that $(R, \mathfrak{M})$ is a finite local ring and $v \in \mathrm{Min}(C)$. If $r \in R$ is such that $rv \neq 0$, then $\sigma(v) = \sigma(rv)$. Since σ is modular, there exists $s \in R$ such that $\sigma(v - srv) < \sigma(v)$, hence $v - srv = 0$ by the minimality of $\sigma(v)$. Hence $1 - sr \in 0 :_R v \subseteq \mathfrak{M}$. This shows that $sr \notin \mathfrak{M}$, hence $r \notin \mathfrak{M}$. Therefore, $v \in 0 :_C \mathfrak{M}$, which proves the first inclusion.

The second inclusion follows from the fact that $0 :_C J = (0 :_{C_1} \mathfrak{M}_1) \times \cdots \times (0 :_{C_\ell} \mathfrak{M}_\ell)$.

(2) This follows from part (1), since $0 :_C J \subseteq C$ implies

$$\mathrm{Min}(0 :_C J) \supseteq \mathrm{Min}(C) \cap (0 :_C J) = \mathrm{Min}(C),$$

where the equality follows from part (1). Conversely, if $v \in \mathrm{Min}(0 :_C J)$, then there exists $w \in \mathrm{Min}(C)$ such that $\sigma(w) \leqslant \sigma(v)$. Since $w \in 0 :_C J$ by part (1), then $\sigma(w) = \sigma(v)$ and $v \in \mathrm{Min}(C)$.

(3) Since σ is modular, there exists $r \in R$ such that $\sigma(v - rw) < \sigma(v)$. By the minimality of $\sigma(v)$, $v - rw = 0$, hence $v = rw$. Exchanging the roles of v and w one sees that there exists $s \in R$ such that $w = sv$. Therefore, $(1 - rs)v = 0$, so $1 - rs \in 0 :_R v$. By part (1), $v = e_i v$ for some $i \in [\ell]$ and $0 :_R v = R_1 \times \cdots \times R_{i-1} \times \mathfrak{M}_i \times R_{i+1} \times \cdots \times R_\ell$. Since $1 - s_i r_i \in \mathfrak{M}_i$, then $r_i \notin \mathfrak{M}_i$, hence r_i is invertible. Let $\overline{r} = (1, \dots, 1, r_i, 1, \dots, 1)$. Then $v = \overline{r}w$ and $\overline{r} \in R$ is invertible. □

Theorem 4.4 implies that a code generated by its minimal codewords must be a subcode of $0 :_{R^n} J$. In the next theorem we prove that every subcode of $0 :_{R^n} J$ is generated by its minimal codewords.

Theorem 4.5. *Let $0 \neq C \subseteq R^n$ be a code and assume that σ is modular. Then $0 :_C J$ has a minimal system of generators consisting of codewords that are minimal in C. Moreover, every minimal system of generators of $0 :_C J$ consisting of minimal codewords has the same cardinality $M(0 :_C J)$. In particular, C has a minimal system of generators consisting of minimal codewords if and only if $C \subseteq 0 :_{R^n} J$. If this is the case, then every such minimal system of generators has cardinality $M(C)$.*

Proof. By Theorem 4.4(2) we have $\mathrm{Min}(C) = \mathrm{Min}(0 :_C J)$. Let $D = 0 :_C J$. Since every system of generators of D contains a minimal one, in order to show that D has a minimal system of generators consisting of minimal codewords, it suffices to show that the elements of $\mathrm{Min}(D)$ generate D.

Let $v \in D$ and suppose by contradiction that v is a codeword of minimal support among those in the set $D \setminus \langle \mathrm{Min}(D) \rangle$. Since $v \notin \mathrm{Min}(D)$, then there is a $w \in \mathrm{Min}(D)$ such that $\sigma(w) < \sigma(v)$. Let $i \in [u]$ such that $\sigma(w)_i \neq 0$. By Theorem 4.4(1), $w = e_j w$ for some $j \in [\ell]$ and $w_j \mathfrak{M}_j = 0$. By Property (P$\star$) there exists $r \in R$ such that $\sigma(w - rv)_i = 0$. Since

$$0 = \sigma(w - rv)_i = \sigma(e_j w - e_j rv)_i < \sigma(e_j w)_i = \sigma(w)_i, \tag{4.2}$$

then $r_j \notin \mathfrak{M}_j$. Indeed, $v \in 0 :_C J$ implies that $v_j \in 0 :_{C_j} \mathfrak{M}_j$. Hence, if $r_j \in \mathfrak{M}_j$, then $e_j w - e_j rv = e_j w$, contradictiong equation (4.2). Let $s = (1, \dots, 1, r_j, 1, \dots, 1) \in R$. Then $s \in R$ is invertible and

$$\sigma(w - sv)_i = \sigma(e_j w - e_j sv)_i = \sigma(e_j w - e_j rv)_i = \sigma(w - rv)_i = 0.$$

Then $\sigma(w - sv) < \sigma(v)$, hence by the minimality of $\sigma(v)$ among the supports of elements of $D \setminus \langle \mathrm{Min}(D) \rangle$ we have that $w - sv \in \langle \mathrm{Min}(D) \rangle$. Since s is invertible, this implies that $v \in \langle \mathrm{Min}(D) \rangle$, which contradicts the assumption that $v \in D \setminus \langle \mathrm{Min}(D) \rangle$.

In order to prove that every minimal system of generators of D consisting of minimal codewords has cardinality $M(D)$, write $D = D_1 \times \cdots \times D_\ell$. By Theorem 4.4(1), every minimal codeword v of D satisfies $v = e_i v$ for some $i \in [\ell]$. Therefore, each minimal system of generators of D consisting of minimal codewords is the union for $i \in [\ell]$ of minimal systems of generators of $0 \times \cdots \times 0 \times D_i \times 0 \times \cdots \times 0$. Since R_i is a finite local ring, the cardinality of any minimal system of generators of $0 \times \cdots \times 0 \times D_i \times 0 \times \cdots \times 0$ is $\mu(D_i)$ by Theorem 2.5. Therefore, the cardinality of a minimal system of generators of D consisting of minimal codewords is $\mu(D_1) = \cdots + \mu(D_\ell) = M(D)$. □

We stress that not every minimal system of generators of a code $C \subseteq 0 :_{R^n} J$ consists of minimal codewords.

Example 4.6. The element $(2,3)$ is not an element of minimal support in $C = \langle (2,3) \rangle \subseteq \mathbb{Z}_6^2$. However, $(2,0), (0,3)$ are elements of minimal support that generate C. Here $C_1 = \langle (2,0) \rangle \subseteq \mathbb{Z}_3^2$, $C_2 = \langle (0,1) \rangle \subseteq \mathbb{Z}_2^2$, and $M(C) = \mu(C_1) + \mu(C_2) = 2$.

The following property of minimal codewords will be needed in the next proposition.

Lemma 4.7. *Let σ be a modular support on R^n. Let $C \subseteq 0 :_{R^n} J$ be a code and let $v \in C$ with $\sigma(v)_i \neq 0$. Then there exists $w \in \mathrm{Min}(C)$ with $\sigma(w) \leqslant \sigma(v)$ and $\sigma(w)_i \neq 0$.*

Proof. Write $C = C_1 \times \cdots \times C_\ell$. By Theorem 3.23, we may assume without loss of generality that $(R, \mathfrak{M})$ is a finite local ring. Indeed, if $\sigma = \sigma_1 \times \cdots \sigma_\ell$ and $\sigma(v)_i = \sigma_k(v_k)_i$ for some $k \in [\ell]$, then $e_k v \in 0 \times \cdots \times 0 \times R_k \times 0 \times \cdots \times 0$ has $\sigma(e_k v) \leqslant \sigma(v)$ and $\sigma(e_k v)_i \neq 0$. If $w_k \in \mathrm{Min}(C_k)$ and $\sigma_k(w_k)_i \neq 0$, then $\sigma_k(w_k) \leqslant \sigma_k(v_k)$, therefore

$$\sigma(0, \ldots, 0, w_k, 0, \ldots, 0) \leqslant \sigma(e_k v) \leqslant \sigma(v)$$

and $\sigma(0, \ldots, 0, w_k, 0, \ldots, 0)_i = \sigma_k(w_k)_i \neq 0$. Moreover, $(0, \ldots, 0, w_k, 0, \ldots, 0) \in \mathrm{Min}(C)$ as $w_k \in \mathrm{Min}(C_k)$.

Proceed by induction on $|\sigma(v)|$. Let $v' \in \mathrm{Min}(C)$ with $\sigma(v') \leqslant \sigma(v)$. If $\sigma(v')_i \neq 0$ then let $w = v'$, else fix $j \in [u]$ with $\sigma(v')_j \neq 0$. By Corollary 3.25 there exists $r \in R$ invertible such that $\sigma(v' - rv)_j = 0$. Hence $\sigma(v' - rv) < \sigma(v)$ and $\sigma(v' - rv)_i \neq 0$, by Lemma 3.3(P5). So we may apply the induction hypothesis to $v' - rv$ and obtain $w \in \mathrm{Min}(C)$ such that $\sigma(w) \leqslant \sigma(v' - rv) \leqslant \sigma(v)$ and $\sigma(w)_i \neq 0$. □

We now prove that modularity allows us to produce minimal systems of generators of submodules of $0 :_{R^n} J$, whose supports have a shape which is reminiscent of the rows of a matrix in reduced row-echelon form.

Proposition 4.8. *Let $j \geqslant 1$ and let $C \in \mathcal{S}_j(0 :_{R^n} J)$. If σ is modular, then C has a minimal system of generators $\{v_1, \ldots, v_j\}$ such that for all $i \in [j]$ there exists $k_i \in [u]$ with $\sigma(v_i)_{k_i} \neq 0$ and $\sigma(v_h)_{k_i} = 0$ for all $h \neq i$.*

Proof. Any system of generators with the required property is minimal, since for all $i \in [j]$

$$\sigma(v_i) \not\leqslant \bigvee_{h \neq i} \sigma(v_h).$$

We prove that C has such a system of generators by induction on j. The statement is trivial if $j = 1$. Hence assume $j \geqslant 2$ and fix a minimal system of generators $\{w_1, \ldots, w_j\}$ of C. Up to permuting the entries in the supports, we may assume without loss of generality that $\sigma(w_1)_1 \neq 0$. By Corollary 3.25 there exist $r_2, \ldots, r_j \in R$ with $\sigma(w_i - r_i w_1)_1 = 0$ for all $i \in \{2, \ldots, j\}$. Let $w_i' := w_i - r_i w_1$ for $i \in \{2, \ldots, j\}$ and observe that C is generated by $\{w_1, w_2', \ldots, w_j'\}$. Moreover, $\sigma(v)_1 = 0$ for all $v \in C' = \langle w_2', \ldots, w_j' \rangle$ by Lemma 3.3(P6). We apply the induction hypothesis to the code $C' = \langle w_2', \ldots, w_j' \rangle$, obtaining a system of generators $\{v_2, \ldots, v_j\}$

of C' such that for all $i \in \{2,\dots,j\}$ there exists k_i with $\sigma(v_i)_{k_i} \neq 0$ and $\sigma(v_h)_{k_i} = 0$ for $h \in \{2,\dots,j\} \setminus \{i\}$. By Corollary 3.25 we find $r'_2,\dots,r'_j \in R$ with $\sigma(w_1 - r'_i v_i)_{k_i} = 0$ for $i \in \{2,\dots,j\}$. Finally, let $v_1 := w_1 - \sum_{i=2}^{j} r'_i v_i$ and set $k_1 = 1$. By parts (P5) and (P6) of Lemma 3.3 we have $\sigma(v_1)_{k_1} \neq 0$ and $\sigma(v_1)_{k_i} = 0$ for $i \in \{2,\dots,j\}$. In addition, $\{v_1,\dots,v_j\}$ is a system of generators of C, since $\{w_1, v_2, \dots, v_j\}$ is. □

The proposition also implies that the codomain of a modular support cannot be too small.

Corollary 4.9. *If $\sigma : R^n \to \mathbb{N}^u$ is modular, then $u \geqslant M(0 :_{R^n} J)$. In particular, if R is a PIR or $JR^n = 0$, then $u \geqslant \ell n$.*

Proof. Proposition 4.8 for $C = 0 :_{R^n} J$ and $j = M(0 :_{R^n} J)$ implies that $u \geqslant M(0 :_{R^n} J)$. If $JR^n = 0$, then $R^n = 0 :_{R^n} J$, hence $M(0 :_{R^n} J) = M(R^n)$. If R is a PIR, then $M(0 :_{R^n} J) = M(R^n)$ by Proposition 2.10. In both cases, one has that $M(0 :_{R^n} J) = \ell n$. □

Understanding the subcodes of C generated by minimal codewords allows us to prove that the generalized weights of C are attained by subcodes of $0 :_C J$. In particular, C and its socle have the same generalized weights.

Proposition 4.10. *Let R be a PIR. Suppose that σ is modular and let $C \subseteq R^n$ be a code. Let $r \in [M(C)]$ and $D \in \mathcal{S}_j(C)$, $j \geqslant r$, be such that $d_r(C) = |\sigma(D)|$. Then $0 :_D J \in \mathcal{S}_i(C)$ for some $i \geqslant r$ and $d_r(C) = |\sigma(0 :_D J)|$. In particular,*

$$d_r(C) = d_r(0 :_C J).$$

Proof. By Proposition 2.10 and Theorem 4.5, $0 :_D J \subseteq D$ is minimally generated by a set of $M(0 :_D J) = M(D)$ codewords. Therefore $0 :_D J \in \mathcal{S}_{M(D)}(C)$ and $M(D) \geqslant r$. Moreover

$$|\sigma(0 :_D J)| \leqslant |\sigma(D)| = d_r(C),$$

hence equality holds. Since $0 :_D J \subseteq 0 :_C J$, then

$$d_r(0 :_C J) \leqslant |\sigma(0 :_D J)| = d_r(C).$$

The reverse inequality follows from the inclusion $0 :_C J \subseteq C$. □

In particular, this allows us to determine the last generalized weight of C.

Corollary 4.11. *Let $C \subseteq R^n$ be a code and σ be a modular support. Assume that either $C \subseteq 0 :_{R^n} J$ or R is a PIR. Then*

$$d_{M(C)}(C) = |\sigma(0 :_C J)|.$$

Proof. We claim that $M(C) = M(0 :_C J)$ and $d_{M(C)}(C) = d_{M(C)}(0 :_C J)$. This is clear if $C \subseteq 0 :_{R^n} J$, since $C = 0 :_C J$. If R is a PIR, the claim follows from Proposition 2.10 and Proposition 4.10.

By Proposition 2.9, $M(D) \leqslant M(C)$ for every $D \subseteq 0 :_C J$ and the only subcode $D \subseteq 0 :_C J$ with $M(D) = M(C)$ is $D = 0 :_C J$. Therefore

$$d_{M(C)}(C) = |\sigma(0 :_C J)|.$$

□

For a given code, we can produce subcodes that attain its generalized weights and that are minimally generated by a set of minimal codewords, whose supports have the same reduced shape as in Proposition 4.8. This technical result plays a crucial role in the proof of Theorem 5.4.

Theorem 4.12. *Let $C \subseteq R^n$ be a code and let σ be a modular support. Assume that either $C \subseteq 0 :_{R^n} J$ or R is a PIR. Then, for all $r \in [M(C)]$, there exists a subcode $D \subseteq C$ such that:*

(1) $d_r(C) = |\sigma(D)|$,

(2) *D has a minimal system of generators $\{v_1, \dots, v_r\}$ such that $v_i \in \mathrm{Min}(C)$ for all $i \in [r]$. Moreover*
$$\sigma(v_i) \nleqslant \bigvee_{j \neq i} \sigma(v_j).$$

Proof. If $C \subseteq 0 :_{R^n} J$, then let $D' \subseteq C$ such that $D' \in \mathcal{S}_j(C)$, $j \geqslant r$, and $d_r(C) = |\sigma(D')|$. If R is a PIR, then by Proposition 4.10 there exist $j \geqslant r$ and $D' \subseteq 0 :_C J$ such that $D' \in \mathcal{S}_j(C)$ and $d_r(C) = |\sigma(D')|$. In both cases, by Proposition 4.8, D' has a minimal system of generators $w_1, \dots, w_j$ with the following property: For all $i \in [j]$ there exists $k_i \in [u]$ with $\sigma(w_i)_{k_i} \neq 0$ and $\sigma(w_h)_{k_i} = 0$ for $h \neq i$. By Lemma 4.7, for all $i \in [j]$ there exists $v_i \in \mathrm{Min}(C)$ with $\sigma(v_i) \leqslant \sigma(w_i)$ and $\sigma(v_i)_{k_i} \neq 0$. In particular, $\sigma(v_i) \nleqslant \vee_{h \neq i} \sigma(v_h)$ for $i \in [j]$. Let $D = \langle v_1, \dots, v_r \rangle$. Notice that $D \in \mathcal{S}_r(C)$, since $v_h \notin \langle v_k : k \in [r], k \neq h \rangle$ for all $h \in [r]$. Moreover,
$$|\sigma(D)| = \bigvee_{i=1}^{r} \sigma(v_i) \leqslant \bigvee_{i=1}^{j} \sigma(w_i) = |\sigma(D')|.$$
Therefore $|\sigma(D)| = |\sigma(D')| = d_r(C)$. □

Notation 4.13. *Let $C \subseteq R^n$ be a code and let $j \in [M(C)]$. We let*
$$\mathcal{M}_j(C) := \{D \subseteq C \,:\, D \text{ has a minimal system of generators of } j \text{ minimal codewords}\}.$$

Theorem 4.12 shows that for all $r \in [M(C)]$ there exists $D \in \mathcal{M}_r(C)$ such that $d_r(C) = |\sigma(D)|$. In particular, we have shown the following.

Corollary 4.14. *Let $C \subseteq R^n$ be a code and let σ be a modular support. Assume that either $C \subseteq 0 :_{R^n} J$ or R is a PIR. The following quantities are equal to the r-th generalized weight $d_r(C)$, for any $r \in [M(C)]$:*

(1) $\min\{|\sigma(D)| \,:\, D \in \mathcal{S}_j(C)$ *for some* $j \geqslant r\}$,

(2) $\min\{|\sigma(D)| \,:\, D \in \mathcal{S}_r(C)\}$,

(3) $\min\{|\sigma(D)| \,:\, D \in \mathcal{M}_j(C)$ *for some* $j \geqslant r\}$,

(4) $\min\{|\sigma(D)| \,:\, D \in \mathcal{M}_r(C)\}$.

Proof. Equality between $d_r(C)$ and (1) holds by definition. Equality between $d_r(C)$ and (4) follows directly from Theorem 4.12. Equality between $d_r(C)$ and (3) then follows from the chain of inclusions

$$\mathcal{M}_r(C) \subseteq \cup_{j \geqslant r} \mathcal{M}_j(C) \subseteq \cup_{j \geqslant r} \mathcal{S}_j(C).$$

Similarly, equality between $d_r(C)$ and (2) follows from the chain of inclusions

$$\mathcal{M}_r(C) \subseteq \mathcal{S}_r(C) \subseteq \cup_{j \geqslant r} \mathcal{S}_j(C). \qquad \square$$

Remark 4.15. Theorem 4.5 and Corollary 4.14 are in general false for supports that are not modular. For instance, the support of Example 3.21 violates both results taking $C = \mathbb{F}_2^2$.

We can now prove that the generalized weights form a strictly increasing sequence. This extends a classical result by Wei [Wei91].

Theorem 4.16. *Let $C \subseteq R^n$ be a code and let σ be a modular support. Assume that either $C \subseteq 0 :_{R^n} J$ or R is a PIR. Then*

$$\min \text{wt}(C) = d_1(C) < d_2(C) < \ldots < d_{M(C)}(C) = |\sigma(0 :_C J)|.$$

Proof. By Corollary 4.14 and Theorem 4.4(1) we may assume without loss of generality that $C \subseteq 0 :_{R^n} J$. Let $r \in [M(C) - 1]$ and let $D \subseteq C$ be such that $|\sigma(D)| = d_{r+1}(C)$. We may assume that D has a minimal system of generators $\{v_1, \ldots, v_{j+1}\}$ as in Proposition 4.8 with $j \geqslant r$. Then $D' := \langle v_1, \ldots, v_j \rangle \in \mathcal{S}_j(D)$. We have $\sigma(D') \leqslant \sigma(D)$ and $\sigma(D')_{k_{j+1}} = 0 < \sigma(D)_{k_{j+1}}$, hence $|\sigma(D')| < |\sigma(D)|$. In particular,

$$d_r(C) \leqslant |\sigma(D')| < |\sigma(D)| = d_{r+1}(C).$$

The two equalities in the statement follow from Lemma 3.11(1) and Corollary 4.11. $\square$

As an application of Theorem 4.16, we extend the generalized Singleton bound [Wei91, Corollary 1] to every code over a PIR and some codes over finite commutative rings.

Corollary 4.17. *Let $C \subseteq R^n$ be a code and let σ be a modular support. Assume that either $C \subseteq 0 :_{R^n} J$ or R is a PIR. Then*

$$\min \text{wt}(C) + r - 1 \leqslant d_r(C) \leqslant |\sigma(0 :_{R^n} J)| - M(C) + r$$

for all $r \in [M(C)]$. In particular,

$$\min \text{wt}(C) \leqslant |\sigma(0 :_{R^n} J)| - M(C) + 1.$$

Proof. The result follows by combining Theorem 4.16 with

$$d_M(C) = |\sigma(0 :_C J)| \leqslant |\sigma(0 :_{R^n} J)|,$$

where the equality on the left hand side follows from Corollary 4.11. $\square$

The next corollary proves that, for modular supports, any subcode D of C with $d_r(C) = |\sigma(D)|$ has a minimal system of generators consisting of r elements, and no minimal system of generators of larger cardinality. This result allows us to restrict to such subcodes when studying the generalized weights of C.

Corollary 4.18. *Let $C \subseteq R^n$ be a code and let σ be a modular support. Assume that either $C \subseteq 0 :_{R^n} J$ or R is a PIR. Let $r \in [M(C)]$ and $D \in \mathcal{S}_j(C)$, $j \geqslant r$, be such that $d_r(C) = |\sigma(D)|$. Then $r = j = M(D)$.*

Proof. Since $D \in \mathcal{S}_j(C)$, then $r \leqslant j \leqslant M(D)$ and $D \in \mathcal{S}_{M(D)}(C)$ by Proposition 2.8. Then

$$|\sigma(D)| \geqslant d_{M(D)}(C) \geqslant d_r(C) = |\sigma(D)|,$$

where the first inequality follows from $D \in \mathcal{S}_{M(D)}(C)$ and the second from Lemma 3.11(3). Therefore the inequalities are equalities and $r = j = M(D)$ by Theorem 4.16. □

In the next theorem, we establish some additional properties of the subcodes of C that realize the generalized weights of C.

Theorem 4.19. *Let $C \subseteq R^n$ be a code and let σ be a modular support. Assume that either $C \subseteq 0 :_{R^n} J$ or R is a PIR. Let $r \in [M(C)]$ and $D \in \mathcal{S}_r(C)$ be such that $d_r(C) = |\sigma(D)|$. The following hold.*

(1) If $v \in \mathrm{Min}(C)$ satisfies $\sigma(v) \leqslant \sigma(D)$, then $v \in D$. In particular, $\mathrm{Min}(D) = \mathrm{Min}(C) \cap D$.

(2) $0 :_D J = \langle v \in C \,:\, v \in \mathrm{Min}(C),\, \sigma(v) \leqslant \sigma(D)\rangle$.

In particular, if $D \in \mathcal{M}_r(C)$, then $D = \langle v \in C \,:\, v \in \mathrm{Min}(C),\, \sigma(v) \leqslant \sigma(D)\rangle$.

Proof. (1) If $C \subseteq 0 :_{R^n} J$, then also $D \subseteq 0 :_{R^n} J$. If R is a PIR, then $0 :_D J \subseteq D$ has $\sigma(0 :_D J) = \sigma(D)$ by Proposition 4.10. In both cases, it suffices to prove the thesis under the assumption that $D \subseteq 0 :_{R^n} J$.

If $v \notin D$, consider $D \subsetneq D' = D + \langle v\rangle \subseteq 0 :_{R^n} J$. We have

$$r = M(D) < M(D') \leqslant M(D) + 1 = r + 1,$$

where the equalities follows from Corollary 4.18 and the first inequality follows from Proposition 2.9. The second inequality follows from observing that, if $D = D_1 \times \cdots \times D_\ell$ and $v = e_j v$, then

$$D' = D_1 \times \cdots \times D_{j-1} \times (D_j + \langle v_j\rangle) \times D_{j+1} \times \cdots \times D_\ell.$$

Since $v_j \notin D_j$ and $0 :_{R_j} \mathfrak{M}_j \supseteq D_j \cup \{v_j\}$, then

$$\mu(D_j + \langle v_j\rangle) = \dim_{R_j/\mathfrak{M}_j}(D_j + \langle v_j\rangle) = \dim_{R_j/\mathfrak{M}_j}(D_j) + 1 = \mu(D_j) + 1.$$

Therefore $M(D') = r + 1$. Since $\sigma(D') = \sigma(v) \vee \sigma(D) = \sigma(D)$, then $d_{r+1}(C) \leqslant |\sigma(D)| = d_r(C)$, contradicting Theorem 4.16. It follows that $v \in D$, as desired.

In order to prove that $\mathrm{Min}(D) = \mathrm{Min}(C) \cap D$, it suffices to prove that $\mathrm{Min}(D) \subseteq \mathrm{Min}(C)$. Let $w \in \mathrm{Min}(D) \subseteq C$, then there is a $v \in \mathrm{Min}(C)$ such that $\sigma(v) \leqslant \sigma(w) \leqslant \sigma(D)$, where the second inequality follows from $w \in D$. By the first part of the proof, $v \in D$. Therefore $\sigma(w) = \sigma(v)$ and $w \in \mathrm{Min}(C)$.

(2) By Theorem 4.4(2) and Theorem 4.5 and part (1),

$$0 :_D J = \langle v \in \mathrm{Min}(D)\rangle = \langle v \in \mathrm{Min}(C) \cap D\rangle = \langle v \in \mathrm{Min}(C) \, : \, \sigma(v) \leqslant \sigma(D)\rangle. \qquad \square$$

The next result relates the generalized weights of C with those of its factors.

Corollary 4.20. *Let $C = C_1 \times \cdots \times C_\ell \subseteq R^n$ be a code and let σ be a modular support. Assume that either $C \subseteq 0 :_{R^n} J$ or R is a PIR. Then*

$$d_r(C) = \min\left\{ \sum_{j=1}^{\ell} d_{r_j}(C_j) \, : \, r_1 + \cdots + r_\ell = r, \; r_j \in \{0, \ldots, \mu(C_j)\} \right\}$$

for all $r \in [M(C)]$.

Proof. By Theorem 3.23, up to a permutation of the coordinates of $\mathbb{N}^u$ we can write $\sigma = \sigma_1 \times \cdots \times \sigma_\ell$, where $\sigma_j : R_j^n \to \mathbb{N}^{u_j}$ is a modular support for $j \in [\ell]$ and $u = u_1 + \cdots + u_\ell$. Fix $r \in [M(C)]$ and $r_1, \ldots, r_\ell$ such that $r = r_1 + \cdots + r_\ell$ and $r_j \in \{0, \ldots, \mu(C_j)\}$. For $j \in [\ell]$, let $D_j \in \mathcal{M}_{r_j}(C_j)$ be such that $|\sigma_j(D_j)| = d_{r_j}(C_j)$. Let $D = D_1 \times \cdots \times D_\ell$. Then $D \in \mathcal{M}_r(C)$ has $|\sigma(D)| = d_{r_1}(C_1) + \cdots + d_{r_\ell}(C_\ell)$, proving that

$$d_r(C) \leqslant \min\left\{ \sum_{j=1}^{\ell} d_{r_j}(C_j) \, : \, r_1 + \cdots + r_\ell = r, \; r_j \in \{0, \ldots, \mu(C_j)\} \right\}.$$

To prove the reverse inequality, let $D = D_1 \times \cdots \times D_\ell \in \mathcal{M}_r(C)$. By Theorem 4.4(1) each of the minimal codewords of C, say $v_1, \ldots, v_r$, that minimally generate D belongs to $0 \times \cdots \times 0 \times D_j \times 0 \times \cdots \times 0$ for some $j \in [\ell]$. Let

$$r_j = |\{v_1, \ldots, v_r\} \cap (0 \times \cdots \times 0 \times D_j \times 0 \times \cdots \times 0)|.$$

Then $r = r_1 + \cdots + r_\ell$ and $0 \leqslant r_j \leqslant \mu(D_j) \leqslant \mu(C_j)$ for $j \in [\ell]$. Moreover,

$$|\sigma(D)| = \sum_{j=1}^{\ell} |\sigma_j(D_j)| \geqslant \sum_{j=1}^{\ell} d_{r_j}(C_j),$$

where the last inequality follows from the fact that $D_j \in \mathcal{M}_{r_j}(C_j)$. By Corollary 4.18

$$\begin{aligned} d_r(C) &= \min\{|\sigma(D)| \, : \, D \in \mathcal{M}_r(C)\} \\ &\geqslant \min\left\{ \sum_{j=1}^{\ell} d_{r_j}(C_j) \, : \, r = r_1 + \cdots + r_\ell, \, r_j \in \{0, \ldots, \mu(C_j)\} \right\}. \end{aligned} \qquad \square$$

5. Codes, supports, and monomial ideals

In this section, we prove that the generalized weights of an R-linear code endowed with a modular support are determined by the graded Betti numbers of a monomial ideal associated to the code. We follow the notation of the previous sections.

Notation 5.1. *In the sequel we work in the multivariate polynomial ring $S = K[x_1, \dots, x_u]$, where K is an arbitrary field. A* ***monomial*** *of S is a polynomial of the form $x_1^{a_1} \cdots x_u^{a_u}$, where $(a_1, \dots, a_u) \in \mathbb{N}^u$. In particular, we assume that monomials are monic. A* **monomial ideal** *is an ideal which has a system of generators consisting of monomials.*

We fix a modular support σ on R^n. The support σ can be used to associate a monomial ideal to a subcode of R^n as follows.

Definition 5.2. For any $v \in R^n \setminus \{0\}$, let

$$m_v := x^{\sigma(v)} := x_1^{\sigma(v)_1} \cdots x_u^{\sigma(v)_u} \in S.$$

For $0 \neq C \subseteq R^n$, let

$$I_C := (m_v \,:\, v \in C \setminus \{0\}) \subseteq S.$$

Notice that not every monomial $m \in I_C$ corresponds to the support of a codeword $v \in C \setminus \{0\}$. However, every monomial $m \in I_C$ is of the form $m = m_v \cdot m'$ for some $v \in C \setminus \{0\}$ and some monomial $m' \in S$.

Proposition 5.3. *Let $0 \neq C \subseteq R^n$ be a code. Then*

$$I_C = I_{0:_C J} = (m_v \,:\, v \in \mathrm{Min}(C))$$

and $\{m_v \,:\, v \in \mathrm{Min}(C))\}$ is a minimal system of generators of I_C.

The next theorem is the main result of this paper. We prove that the graded Betti numbers of the monomial ideal associated to a code determine its generalized weights.

Theorem 5.4. *Let σ be a modular support and let $C \subseteq R^n$ be a code. Assume that either $C \subseteq 0 :_{R^n} J$ or R is a PIR. Let $I_C \subseteq S$ be the monomial ideal associated to C and let $r \in [M(C)]$. Then $M(C)$ is the projective dimension of S/I_C and $d_r(C)$ is the minimum shift (i.e., the minimum degree of a nonzero element) in the r-th free module in a minimal free resolution of S/I_C. In particular, the graded Betti numbers of S/I_C determine $M(C)$ and the generalized weights of C.*

Proof. Let $I_C = (m_1, \dots, m_t)$ where $m_1, \dots, m_t$ are a minimal system of monomial generators of I_C. By Theorem 4.4(3) $\langle v \rangle = \langle w \rangle$ if and only if $\sigma(v) = \sigma(w)$ for $v, w \in \mathrm{Min}(C)$. By Theorem 4.5, $0 :_C J$ has a minimal system of generators consisting of minimal codewords, hence $t \geqslant M(0 :_C J) = M(C)$ by Proposition 2.10. For each $i \in [t]$ let $v_i \in \mathrm{Min}(C)$ such that $m_{v_i} = m_i$. For any $A \subseteq [t]$ let

$$m_A = \mathrm{lcm}\{m_i \,:\, i \in A\} = x^{\sigma(\langle v_i \,:\, i \in A \rangle)}.$$

A graded free resolution of S/I_C is given by the Taylor complex [HH11, Section 7.1]

$$0 \longrightarrow \mathbb{F}_t \xrightarrow{f_t} \mathbb{F}_{t-1} \xrightarrow{f_{t-1}} \cdots \xrightarrow{f_2} \mathbb{F}_1 \xrightarrow{f_1} S \longrightarrow S/I_C \longrightarrow 0,$$

where

$$\mathbb{F}_r = \bigoplus_{A \subseteq [t],\ |A|=r} S(-\deg(m_A))$$

with basis $\{e_A \,:\, A \subseteq [t],\ |A| = r\}$ and

$$f_r(e_A) = \sum_{k=1}^{r} (-1)^{k+1} \frac{m_A}{m_{A\setminus\{i_k\}}} e_{A\setminus\{i_k\}} \ \text{ for } \ A = \{i_1, \ldots, i_r\} \subseteq [t].$$

The Taylor resolution is in general not minimal: A cancellation occurs between the modules $S(-\deg(m_A)) \subseteq \mathbb{F}_r$ and $S(-\deg(m_B)) \subseteq \mathbb{F}_{r-1}$ if and only if $B = A \setminus \{k\}$ for some $k \in A$ and $m_A = m_B$. Notice that $m_A = m_B$ if and only if $m_k \mid \operatorname{lcm}\{m_i \,:\, i \in B\}$, that is, if and only if $\sigma(v_k) \leqslant \vee_{i\in B}\sigma(v_i)$.

Let

$$0 \longrightarrow \mathbb{G}_p \xrightarrow{g_p} \mathbb{G}_{p-1} \xrightarrow{g_{p-1}} \cdots \xrightarrow{g_2} \mathbb{G}_1 \xrightarrow{g_1} S \longrightarrow S/I_C \longrightarrow 0 \tag{5.1}$$

be a minimal free resolution obtained from the Taylor resolution after making all the possible cancellations. In particular, p is the projective dimension of S/I_C.

For $A \subseteq [t]$ with $|A| = r$, let

$$C_A = \langle v_i \,:\, i \in A \rangle \subseteq C.$$

Notice that, if $v_k \in \langle v_i \,:\, i \in A \setminus \{k\} \rangle$ for some $k \in A$, then $S(-\deg(m_A))$ cancels with $S(-\deg(m_{A\setminus\{k\}}))$ while passing from the Taylor resolution to resolution (5.1). Therefore, the direct summands $S(-\deg(m_A))$ appearing in (5.1) come from subcodes $C_A \in \mathcal{M}_r(C)$. Since $\mathcal{M}_i(C) = 0$ for $i > M(C)$, then $p \leqslant M(C)$.

For $r \in [M(C)]$, let b_r be the smallest shift appearing in the r-th module of a minimal graded free resolution of S/I_C, i.e. b_r is the smallest degree of a nonzero element of $\mathbb{G}_r$. In particular, b_1 is the smallest degree of a minimal generator of I_C, hence

$$b_1 = d_1(C).$$

We claim that $b_r = d_r(C)$ for all $r \in [M(C)]$. Fix a value of r and choose $A \subseteq [t]$ with $|A| = r$ such that $b_r = \deg(m_A)$. Then $\sigma(C_A) = \vee_{i\in A}\sigma(v_i) = b_r$. Since $C_A \in \mathcal{M}_r(C)$, then

$$d_r(C) \leqslant b_r \tag{5.2}$$

by Theorem 4.14.

To prove the reverse inequality of (5.2), we start by observing that

$$d_r(C) = \min\{|\sigma(C_A)| \,:\, |A| = r,\ C_A \in \mathcal{M}_r(C)\}$$

by Theorem 4.14 and Theorem 4.4(3). Hence $d_r(C)$ is one of the shifts appearing in the r-th free module of the Taylor resolution of S/I_C. In order to complete the proof, it suffices to prove the following

Claim 5.5. *$\mathbb{G}_r$ contains at least one direct summand $S(-d_r(C))$.*

To prove the claim, suppose that we have made all the possible cancellations until the $(r-1)$-st step of the resolution. Therefore we have a free resolution of the form

$$0 \longrightarrow \mathbb{F}_t \xrightarrow{f_t} \cdots \xrightarrow{f_{r+2}} \mathbb{F}_{r+1} \xrightarrow{h_{r+1}} \mathbb{H}_r \xrightarrow{h_r} \mathbb{G}_{r-1} \xrightarrow{g_{r-1}} \cdots \xrightarrow{g_2} \mathbb{G}_1 \xrightarrow{g_1} S \longrightarrow S/I_C \longrightarrow 0.$$

By Theorem 4.12 and Corollary 4.18, $\mathbb{H}_r$ contains a direct summand $S(-d_r(C))$. Consider now the possible cancellations between $\mathbb{F}_{r+1}$ and $\mathbb{H}_r$. The map

$$\mathbb{H}_r \xrightarrow{h_r} \mathrm{Syz}_{r-1}(I_C) \tag{5.3}$$

is surjective and corresponds to a choice of generators of the $(r-1)$-st syzygy module $\mathrm{Syz}_{r-1}(I_C)$ of I_C. A cancellation between $\mathbb{F}_{r+1}$ and $\mathbb{H}_r$ comes from an element in the kernel of h_r which has an invertible entry, hence it corresponds to eliminating a non-minimal generator of $\mathrm{Syz}_{r-1}(I_C)$. Claim 5.5 amounts to showing that, among all direct summands $S(-d_r(C))$ of $\mathbb{H}_r$, there is at least one which does not cancel with a direct summand of $\mathbb{F}_{r+1}$. If they all cancel, however, $\mathrm{Syz}_{r-1}(I_C)$ has no elements in degree $d_r(C)$. However this is not possible, since the map in (5.3) is surjective and no component of h_r is the zero map, hence the image of h_r contains a nonzero element of degree $d_r(C)$. In particular, $\mathbb{G}_p = S(-|\sigma(0 :_C J)|)^s$ for some $s \geqslant 1$ and $p = M(C)$. □

Since minimal free resolutions of monomial ideals are easy to compute, Theorem 5.4 gives a way to efficiently compute the generalized weights of a code, if one knows the supports of its minimal codewords. Notice however that the problem of computing the supports of the minimal codewords (or just the minimum distance) of a code is NP-hard, even for the special case of binary linear codes endowed with the Hamming distance, see [Var97].

We conclude the section with some examples.

Example 5.6. Let $R = \mathbb{Z}_6$ and consider the support $\omega : \mathbb{Z}_6 \to \mathbb{N}^2$ defined as follows:

$$\omega(0) = (0,0), \quad \omega(1) = (2,1), \quad \omega(2) = (0,1),$$
$$\omega(3) = (2,0), \quad \omega(4) = (0,1), \quad \omega(5) = (2,1).$$

It can be checked that ω is modular. We extend ω componentwise to a function $\omega : \mathbb{Z}_6^3 \to \mathbb{N}^6$ and compose it with the $\mathbb{Z}_6$-linear map defined by the invertible matrix

$$A = \begin{pmatrix} 3 & 4 & 1 \\ 5 & 3 & 3 \\ 2 & 4 & 5 \end{pmatrix}.$$

In other words, we define $\sigma : \mathbb{Z}_6^3 \to \mathbb{N}^6$ by $\sigma(v) = (\omega((Av)_1), \omega((Av)_2), \omega((Av)_3))$ for all $v \in \mathbb{Z}_6^3$. Then σ is modular by Proposition 3.17(7). Let $C = \langle (3,1,2), (2,4,3) \rangle \subseteq \mathbb{Z}_6^3$.

Then C has the following six minimal codewords and supports:

$$\begin{array}{ll}
(3,3,3) & (0,0,2,0,2,0), \\
(0,4,2) & (0,0,0,0,0,1), \\
(2,0,4) & (0,1,0,1,0,0), \\
(3,3,0) & (2,0,0,0,0,0), \\
(0,2,4) & (0,0,0,0,0,1), \\
(4,0,2) & (0,1,0,1,0,0).
\end{array}$$

In particular, the ideal associated to C is

$$I_C = (x_1^2, x_2x_4, x_3^2x_5^2, x_6).$$

Notice that the generators of I_C form a regular sequence, therefore a minimal free resolution of S/I_C is given by the Koszul complex. In other words, there is no cancellation in the Taylor complex

$$0 \longrightarrow S(-9) \longrightarrow \begin{array}{c} S(-8) \\ \oplus \\ S(-7)^2 \\ \oplus \\ S(-5) \end{array} \longrightarrow \begin{array}{c} S(-6)^2 \\ \oplus \\ S(-5)^2 \\ \oplus \\ S(-4) \\ \oplus \\ S(-3)^2 \end{array} \longrightarrow \begin{array}{c} S(-4) \\ \oplus \\ S(-2)^2 \\ \oplus \\ S(-1) \end{array} \longrightarrow S \longrightarrow S/I_C \longrightarrow 0.$$

Therefore one has $M(C) = 4$, $d_1(C) = 1$, $d_2(C) = 3$, $d_3(C) = 5$, and $d_4(C) = 9$. Looking at the maps in the minimal free resolutions, one sees that

$$\begin{aligned}
d_1(C) &= |\sigma(\langle(0,2,4)\rangle)| = |(0,0,0,0,0,1)| = 1, \\
d_2(C) &= |\sigma(\langle(0,2,4),(3,3,0)\rangle)| = |\sigma(\langle(0,2,4),(2,0,4)\rangle)| = |(2,0,0,0,0,1)| \\
&= |(0,1,0,1,0,1)| = 3, \\
d_3(C) &= |\sigma(\langle(0,2,4),(3,3,0),(2,0,4)\rangle)| = |(2,1,0,1,0,1)| = 5, \\
d_4(C) &= |\sigma(\langle(0,2,4),(3,3,0),(2,0,4),(3,3,3)\rangle)| = |(2,1,2,1,2,1)| = 9.
\end{aligned}$$

In the next example, we show that all the cancellations discussed in the proof of Theorem 5.4 can actually occur.

Example 5.7. Let σ be the Hamming weight and let $C \subseteq \mathbb{F}_2^4$ be the even weight code, i.e., the code consisting of all vectors of even weight. The minimal codewords of C are all vectors of weight 2 of $\mathbb{F}_2^4$, therefore the associated ideal I_C is the ideal generated by all squarefree monomials of degree 2 in 4 variables. A minimal free resolution of S/I_C is well-known and has the form

$$0 \longrightarrow S(-4)^2 \longrightarrow S(-3)^8 \longrightarrow S(-2)^6 \longrightarrow S \longrightarrow S/I_C \longrightarrow 0.$$

The Taylor complex associated to S/I_C is as follows

$$0 \longrightarrow S(-4) \longrightarrow S(-4)^6 \longrightarrow S(-4)^{15} \longrightarrow \begin{matrix} S(-4)^{16} \\ \oplus \\ S(-3)^4 \end{matrix} \longrightarrow \begin{matrix} S(-4)^{3} \\ \oplus \\ S(-3)^{12} \end{matrix} \longrightarrow S(-2)^6 \longrightarrow S \longrightarrow S/I_C \longrightarrow 0.$$

We use the notation of the proof of Theorem 5.4 when referring to the free modules in the resolutions above. By comparing the two free resolutions, one sees that the modules $\mathbb{F}_4$, $\mathbb{F}_5$ and $\mathbb{F}_6$ in the Taylor complex completely cancel. Moreover, the free summand $S(-3)^4$ of $\mathbb{F}_3$, corresponding to the minimal shift in its homological degree, cancels, as well as the direct summand $S(-4)^{14}$. Finally, the direct summands $S(-3)^4$ and $S(-4)^3$ of $\mathbb{F}_2$ cancel.

It is easy to find examples of functions that are not supports according to Definition 3.2, and for which the result of Theorem 5.4 does not hold.

Example 5.8. Let $R = \mathbb{Z}_4$. Let wt^{L} denote the Lee weight and let σ^{L} be its coordinatewise extension to $\mathbb{Z}_4^3$. In Example 3.6 we observed that σ^{L} is not a support according to Definition 3.2. Consider the code $C = \langle (1,1,0),(3,2,1)\rangle \subseteq \mathbb{Z}_4^3$. Then

$$\mathrm{Min}(C) = \{(1,1,0),(3,3,0),(0,1,3),(0,3,1),(1,0,1),(3,0,3)\}$$

and $I_C = (xy, xz, yz) \subseteq S = K[x,y,z]$. The graded Betti numbers of a minimal free resolution of S/I_C are

$$0 \longrightarrow S(-3)^2 \longrightarrow S(-2)^3 \longrightarrow S \longrightarrow S/I_C \longrightarrow 0.$$

In particular, $b_1 = 2$ and $b_2 = 3$. One can check that $d_1(C) = 4$ and $d_2(C) = 6$.

Notice that Theorem 5.4 does not hold in general for supports that are not modular, even for linear codes over fields.

Example 5.9. Let $C = \mathbb{F}_2^2$ with the support σ defined in Example 3.21. The associated monomial ideal is $I_{\mathbb{F}_2^2} = (y) \subseteq K[x,y]$, whose minimal free resolution is

$$0 \longrightarrow S(-1) \longrightarrow S \longrightarrow S/(y) \longrightarrow 0.$$

We have $\mu(\mathbb{F}_2^2) = 2$, while the projective dimension of $S/(y)$ is 1. In particular, the second free module in a minimal free resolution of $S/(y)$ is 0 and it does not determine $d_2(\mathbb{F}_2^2) = |\sigma(\mathbb{F}_2^2)| = 2$.

6. The Hamming support

In this section we let $R = \mathbb{F}_q$ and make some observations on the Hamming support $\sigma^{\mathrm{H}} : \mathbb{F}_q^n \to \{0,1\}^n$, see Example 3.5. For $v \in \mathbb{F}_q^n$, we identify $\sigma^{\mathrm{H}}(v)$ with a subset of $[n]$.

Let $C \subseteq \mathbb{F}_q^n$ be a code. Several authors study the matroid M_C associated to a parity-check matrix H of C. This is the matroid on the ground set $[n]$, whose independent sets are the sets $\{j_1,\dots,j_t\} \subseteq [n]$ such that columns $j_1,\dots,j_t$ of H are linearly independent, see e.g. [Bar97, JV13]. Denote by $\mathcal{I}(M_C) \subseteq 2^{[n]}$ the set of independent sets of M_C. It is easy to check that M_C does not depend on the choice of H. The code C, the matroid M_C, and the corresponding Stanley–Reisner ideal I_C relate as follows:

(1) Let $A \subseteq [n]$. Then $A \in \mathcal{I}(M_C)$ if and only if there is no $v \in C \setminus \{0\}$ with $\sigma^{\mathrm{H}}(v) \subseteq A$.

(2) The squarefree monomials in I_C are exactly those of the form x^A, where $A \notin \mathcal{I}(M_C)$.

(3) The circuits of M_C are the supports of the minimal codewords of C.

(4) The minimal monomial generators of I_C are in one-to-one correspondence with the circuits of the matroid M_C.

Therefore,

$$\mathcal{I}(M_C) = 2^{[n]} \setminus \{A \subseteq [n] \, : \, A \supseteq \sigma^H(v) \text{ for some } v \in C \setminus \{0\}\} = 2^{[n]} \setminus \{A \subseteq [n] \, : \, x^A \in I_C\}. \tag{6.1}$$

The resolutions of the ideals associated to various classes of codes (most notably, MDS codes, one/two weight codes, Reed–Muller codes) have been studied in [GS20, GL21].

The main result of [JV13] is Theorem 2, which shows that the generalized Hamming weights of a code $C \subseteq \mathbb{F}_q^n$ are determined by the graded Betti numbers of I_C. Our Theorem 5.4 generalizes [JV13, Theorem 2] with a different and stand-alone proof strategy that does not rely on any matroid theory results.

A known fact about codes $C \subseteq \mathbb{F}_q^n$ endowed with the Hamming metric is that they are generated by their minimal codewords [AB98, Lemma 2.1.4]. This is a special case of Theorem 4.5 in this paper.

Corollary 6.1. *Every code $0 \neq C \subseteq \mathbb{F}_q^n$ is generated by its minimal codewords.*

It is natural to ask whether a code $C \subseteq \mathbb{F}_q^n$ is also generated by its codewords of maximal support. The answer to this question is negative in general, as the following simple example shows.

Example 6.2. Let $C = \mathbb{F}_2^2$. The only codeword of maximal support is $(1, 1)$ and $\langle(1, 1)\rangle \subsetneq C$.

Although codes $C \subseteq \mathbb{F}_q^n$ are in general not generated by their maximal codewords, for q sufficiently large most codes are.

Proposition 6.3. *Let $1 \leqslant k \leqslant n$. The proportion of codes in $\mathbb{F}_q^n$, within the k-dimensional ones, generated by their maximal codewords is at least*

$$\frac{(q-1)^n\,(q^k-1) - (q^n-1)q^{k-1}}{(q^n-1)(q^k-q^{k-1}-1)},$$

and the above fraction approaches 1 as $q \to +\infty$.

Proof. We obtain the result by bounding from below the number of k-dimensional codes C with $|C \cap A_n| > q^{k-1}$, where A_n is the set of vectors in $\mathbb{F}_q^n$ of weight n. To obtain such a lower bound, denote by $\mathcal{F}$ the set of k-dimensional codes in $\mathbb{F}_q^n$ and consider the sum

$$S := \sum_{C \in \mathcal{F}} |C \cap A_n|.$$

We have

$$|\mathcal{F}| = \begin{bmatrix} n \\ k \end{bmatrix}_q .$$

We write $\mathcal{F}$ as a disjoint union $\mathcal{F} = \mathcal{F}' \cup \mathcal{F}''$, where $\mathcal{F}'$ is the set of codes $C \in \mathcal{F}$ with $|C \cap A_n| > q^{k-1}$ and $\mathcal{F}''$ the set of codes $C \in \mathcal{F}$ with $|C \cap A_n| \leqslant q^{k-1}$. We then have

$$\begin{aligned} S &= \sum_{C \in \mathcal{F}'} |C \cap A_n| + \sum_{C \in \mathcal{F}''} |C \cap A_n| \\ &\leqslant |\mathcal{F}'| \, (q^k - 1) + (|\mathcal{F}| - |\mathcal{F}'|) \, q^{k-1} \\ &= |\mathcal{F}'| \, (q^k - q^{k-1} - 1) + |\mathcal{F}| \, q^{k-1}. \end{aligned} \tag{6.2}$$

On the other hand, we can rewrite S as

$$S = \sum_{v \in A_n} |\{C \in \mathcal{F} \, : \, C \ni v\}| = |A_n| \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q . \tag{6.3}$$

Combining (6.2) with (6.3), and using the definition of q-binomial coefficient, we obtain

$$|\mathcal{F}'|/|\mathcal{F}| \geqslant |A_n| \frac{q^k - 1}{(q^n - 1)(q^k - q^{k-1} - 1)} - \frac{q^{k-1}}{q^k - q^{k-1} - 1},$$

which is the desired estimate, since $|A_n| = (q-1)^n$. □

Acknowledgements

We are grateful to Maria Evelina Rossi for suggesting Example 2.12.

References

[AB98] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, 1998. doi:10.1109/18.705584.

[Bar97] A. Barg. The matroid of supports of a linear code. *Applicable Algebra in Engineering, Communication and Computing*, 8(2):165–172, 1997. doi:10.1007/s002000050060.

[Bri07] T. Britz. Higher support matroids. *Discrete Mathematics*, 307(17-18):2300–2308, 2007. doi:10.1016/j.disc.2006.12.001.

[Bri10] T. Britz. Code enumerators and Tutte polynomials. *IEEE Transactions on Information Theory*, 56(9):4350–4358, 2010. doi:10.1109/tit.2010.2054654.

[Gas20] N. Gassner. *Weight-induced distance functions on $\mathbb{Z}/p^s\mathbb{Z}$-codes*. Master Thesis (University of Zurich), 2020. Supervisors: J. Rosenthal and V. Weger.

[GL21] S. R. Ghorpade and R. Ludhani. On the purity of resolutions of Stanley-Reisner rings associated to Reed-Muller codes. 2021. `arXiv:2102.00308`.

[Gre76] C. Greene. Weight enumeration and the geometry of linear codes. *Studies in Applied Mathematics*, 55(2):119–128, 1976. `doi:10.1002/sapm1976552119`.

[GS20] S. R. Ghorpade and P. Singh. Pure resolutions, linear codes, and Betti numbers. *Journal of Pure and Applied Algebra*, 224(10):106385, 2020. `doi:10.1016/j.jpaa.2020.106385`.

[HH11] J. Herzog and T. Hibi. *Monomial Ideals*. Springer, 2011.

[JP13] R. Jurrius and R. Pellikaan. Codes, arrangements and matroids. In *Algebraic Geometry Modeling in Information Theory*, pages 219–325. World Scientific, 2013.

[JV13] T. Johnsen and H. Verdure. Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids. *Applicable Algebra in Engineering, Communication and Computing*, 24(1):73–93, 2013. `doi:10.1007/s00200-012-0183-7`.

[Mat89] H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1989.

[MS77] J. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library, 1977.

[Oxl06] J. G Oxley. *Matroid Theory*. Oxford University Press, 2006.

[Rav18] Alberto Ravagnani. Duality of codes supported on regular lattices, with an application to enumerative combinatorics. *Designs, Codes and Cryptography*, 86(9):2035–2063, 2018. `doi:10.1007/s10623-017-0436-3`.

[Var97] A. Vardy. The intractability of computing the minimum distance of a code. *IEEE Transactions on Information Theory*, 43(6):1757–1766, 1997. `doi:10.1109/18.641542`.

[Wei91] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Transactions on Information Theory*, 37(5):1412–1418, 1991. `doi:10.1109/18.133259`.