



# Submodule codes as spherical codes in buildings

Mima Stanojkovski<sup>1</sup>

Received: 14 March 2022 / Revised: 27 October 2022 / Accepted: 25 February 2023 /  
Published online: 23 March 2023  
© The Author(s) 2023

## Abstract

We give a generalization of subspace codes by means of codes of modules over finite commutative chain rings. We define a new class of Sperner codes and use results from extremal combinatorics to prove the optimality of such codes in different cases. Moreover, we explain the connection with Bruhat–Tits buildings and show how our codes are the buildings’ analogue of spherical codes in the Euclidean sense.

**Keywords** Submodule codes · Subspace codes · Spherical codes · Chain rings · Sperner codes · Bruhat–Tits buildings · Sperner property · Balls in buildings

**Mathematics Subject Classification** 94B60 · 94B65 · 94B25 · 20E42 · 51E24 · 52B20

## 1 Introduction

The codes studied in this paper can be viewed as a bridge of generalization between two worlds, that of subspace codes and that of spherical codes. More specifically our codes consist of *equivalence classes* of modules over finite commutative *chain rings*, which can be interpreted at the same time as subsets of spheres in *Bruhat–Tits buildings*. In this introduction we will take a first glance at these connections and present the main questions that will be addressed in this document.

### 1.1 Spherical codes in the euclidean setting

Spherical codes in  $\mathbb{R}^d$ , equipped with the usual distance, are finite subsets of the unit sphere

$$B_1 = \{x = (x_1, \dots, x_d) \in \mathbb{R}^d \mid x_1^2 + \dots + x_d^2 = 1\}.$$

In this context, spherical codes can be constructed from sphere packings [14, Section 1.2.4] and find numerous applications in the field of telecommunication. In view of the applications,

---

Communicated by M. Lavrauw.

---

✉ Mima Stanojkovski  
mima.stanojkovski@unitn.it

<sup>1</sup> Dipartimento di Matematica, Università di Trento, Trento, Italy

it is desirable to produce sizable codes of large internal distance and small length. Optimal codes are thus codes with the “best possible” coexistence constraints on the last requirements. More precisely, it is greatly interesting to determine which spherical codes present the most favourable relationship between their *length*, *minimum distance*, and *cardinality*. Already for the small length value  $d = 3$ , however, the last problem turns out to be very hard and not all *optimal* codes are classified; cf. [21, Section 3.3]. For a broad overview of spherical codes in this setting we refer the interested reader to [21].

### 1.2 Chain rings in coding theory

Let  $R$  be a commutative ring, which we assume to be unital. The ring  $R$  is said to be a *chain ring* if all of its ideals form a chain, i.e. if  $I$  and  $J$  are ideals of  $R$ , then  $I \subseteq J$  or  $J \subseteq I$ . In this paper, only the case of commutative chain rings will be considered, though their definition extends also to the non-commutative case; cf. [26, Section 2]. Examples of finite commutative chain rings include

- (1)  $\mathbb{Z}/p^r\mathbb{Z}$ , where  $p$  is a prime number and  $r$  a positive integer, and
- (2)  $(\mathbb{Z}/p^m\mathbb{Z})[x]/(f(x))$ , where  $p$  is a prime number,  $m$  a positive integer, and  $f$  a monic polynomial that is irreducible modulo  $p$ .

For more on the classification of finite commutative chain rings we refer to [3, 12, 27]. In the present paper, we are mostly interested in viewing  $R$  as a quotient of a discrete valuation ring  $\mathcal{O}_K$  by a power  $\mathfrak{m}_K^r$  of its unique maximal ideal  $\mathfrak{m}_K$ , e.g.  $\mathcal{O}_K$  equals the  $p$ -adic integers  $\mathbb{Z}_p$  or the ring  $\mathbb{F}_q[[t]]$  of formal power series with nonnegative integer exponents and coefficients in the field  $\mathbb{F}_q$ . As can be found for instance in [26, Section 2], finite chain rings are local and their unique maximal ideal  $\mathfrak{m}$  is principal. Moreover, if  $\pi$  generates  $\mathfrak{m}$ , then every ideal of  $R$  is generated by a nonnegative power of  $\pi$ . Since  $R$  is finite, there exists a minimal positive integer  $r$ , called the nilpotency class of  $\mathfrak{m}$ , with the property that  $\mathfrak{m}^r = 0$ , equivalently that  $\pi^r = 0$ . In addition, an elementary divisor type theorem holds for finitely generated modules over chain rings. There are several applications of finite chain rings in coding theory including linear codes [8, 26, 33] and cyclic codes [11, 15, 24, 38], though to this author’s best knowledge the consideration of codes consisting of modules over finite chain rings does not appear anywhere in the literature.

### 1.3 Spherical codes of modules

Let  $R$  be a finite commutative chain ring and let  $r \geq 1$  be such that the unique maximal ideal  $\mathfrak{m}$  of  $R$  satisfies  $\mathfrak{m}^{r-1} \neq 0$  and  $\mathfrak{m}^r = 0$ . Let  $\pi \in R$  satisfy  $\mathfrak{m} = R\pi$  and let  $V_r$  be a free  $R$ -module of rank  $d \geq 2$ , that is  $V_r \cong R^d$ . Write  $\mathcal{L}(V_r)$  for the set of all  $R$ -submodules of  $V_r$  and  $\partial\mathcal{L}(V_r)$  for the *boundary* of  $\mathcal{L}(V_r)$ :

$$\partial\mathcal{L}(V_r) = \{U \in \mathcal{L}(V_r) \mid \pi^{r-1}V_r \not\subseteq U \not\subseteq \pi V_r\}.$$

Defining the map  $\text{dist} : \partial\mathcal{L}(V_r) \times \partial\mathcal{L}(V_r) \rightarrow \mathbb{Z}$  by

$$(U_1, U_2) \mapsto \text{dist}(U_1, U_2) = \min\{m \in \mathbb{Z}_{\geq 0} \mid \pi^m U_1 \subseteq U_2\} + \min\{n \in \mathbb{Z}_{\geq 0} \mid \pi^n U_2 \subseteq U_1\}$$

gives  $\partial\mathcal{L}(V_r)$  the additional structure of a metric space. The last distance can be extended to the whole of  $\mathcal{L}(V_r)$  modulo *homothety*; cf. Sect. 2. Moreover, for  $r = 1$ , one can see that  $\text{dist}$  does not coincide with the subspace metric or the injection metric on  $\mathcal{L}(V_1)$ ; cf. [30,

Section 1]. A *spherical code* in  $V_r$  is then a subset  $C$  of  $\partial\mathcal{L}(V_r)$  of cardinality at least 2 and its *minimum distance* is

$$\text{dist}(C) = \min\{\text{dist}(U_1, U_2) \mid U_1, U_2 \in C, U_1 \neq U_2\}.$$

Spherical codes in  $V_r$  are natural generalizations of subspace codes, though the attribute “spherical” comes from interpreting  $\partial\mathcal{L}(V_r)$  as a sphere of modules, cf. Proposition 2.6. In this manuscript, we address and give answers to the following question:

*For a given integer  $\psi$ , what are the largest spherical codes  $C$  in  $V_r$  with the property that  $\text{dist}(C) \geq \psi$ ?*

The largest codes associated to a given minimum distance are called *optimal*. If  $\psi = 1$ , then there is a unique optimal code of minimum distance 1, namely  $\partial\mathcal{L}(V_r)$ : we compute its cardinality in Sect. 8. In general, good candidates for optimal codes are the *Sperner codes* that we define in Sect. 4 using Grassmannians of  $R$ -modules. Such codes are defined starting from the parameters  $(d, R, \alpha)$  where  $\psi = 2\alpha$  is taken to be even. In Theorem 4.5, we compute the cardinality and minimum distance of a Sperner code with parameters  $(d, R, \alpha)$ , yielding general bounds on the maximal size of codes of minimum distance  $2\alpha$ ; cf. Corollary 4.6. In Sect. 5, we use results from extremal combinatorics to prove that Sperner codes are optimal when  $\alpha = r$  or  $d = 2$ ; cf. Theorems 5.4 and 5.6. We move on to the construction, in Sect. 6, of optimal codes in a subfamily of  $\partial\mathcal{L}(V_r)$  indexed by tuples of positive integers. More concretely, let  $\partial\mathcal{L}_e(V_r)$  denote the collection of boundary  $R$ -submodules of  $V_r$  that can be generated *compatibly* with a basis  $e = (e_1, \dots, e_d)$  of  $V_r$  over  $R$ , i.e. modules of the form

$$U = R\pi^{\delta_1}e_1 \oplus \dots \oplus R\pi^{\delta_d}e_d, \text{ where } 0 \leq \delta_i \leq r, \{0, r\} \subseteq \{\delta_1, \dots, \delta_d\}.$$

Generalizing [21, Chapter 4], a *permutation code* is a spherical code in  $V_r$  that is contained in  $\partial\mathcal{L}_e(V_r)$  and whose elements form one orbit under the natural action of the symmetric group  $\text{Sym}(d)$  on  $\partial\mathcal{L}_e(V_r)$ . In Theorem 6.9 we give bounds on minimum distance and cardinality of a permutation code in terms of its defining parameters.

### 1.4 The connection to Bruhat–tits buildings

Write  $R = \mathcal{O}_K/\mathfrak{m}_K^r$  and consider the natural projection  $\mathcal{O}_K^d \rightarrow R^d \cong V_r$ . Via the last map we identify every submodule of  $V_r$  with the unique maximal free  $\mathcal{O}_K$ -submodule of  $\mathcal{O}_K^d$  mapping to it. Such a module is called a *lattice* in  $K^d$ . The collection of lattices in  $K^d$ , considered up to *homothety*, forms the collection of 0-simplices of the *Bruhat–Tits Building*  $\mathcal{B}_d(K)$  of  $\text{SL}_d(K)$ . In this infinite simplicial complex,  $s$ -simplices are given by chains  $L_1 \supset L_2 \supset \dots \supset L_s \supset \pi L_1$  of lattices and maximal simplices all have size  $d$ . Transporting  $\text{dist}$  from the module setting to the buildings context (see Sect. 7.3) via the above projection, one can then interpret  $\partial\mathcal{L}(V_r)$  as a sphere  $\partial B_r$  in  $\mathcal{B}_d(K)$ , cf. Theorem 7.6, and thus spherical codes in  $V_r$  as spherical codes in  $B_r$ . To the best of our knowledge, this is the very first instance in which spherical codes in *affine* buildings are studied, adding yet another item to the already long list of applications of buildings; cf. Sect. 7. In our closing Sect. 8 we give formulas and asymptotics for the number of elements in a ball of radius  $r$  in  $\mathcal{B}_d(K)$ ; cf. Theorem 8.5. As a consequence, we derive densities of spherical codes in analogy to the ones found in [10] for linear codes over finite chain rings.

### 1.5 A note on the underlying geometry and combinatorics

Contrarily to what happens in the Euclidean context, a sphere in  $\mathcal{B}_d(K)$  is not a homogeneous space, but is rather to be thought of as the collection of boundary points of a lattice polytope and Sperner codes arise as strategically chosen subsets of the polytope’s vertices. As we deal with a discrete set, it is interesting and important to understand how the number of elements of  $\partial B_r$  depends on the size  $q$  of the residue field of  $K$ . This count and its asymptotic behaviour has been included in Sect. 8 as it seemed not to be explicitly available in the literature already. The count is much easier and independent of  $q$  when one restricts to the analogue  $\partial B_r \cap \mathcal{A}$  of  $\mathcal{L}_e(V_r)$  in the building. Indeed, in such case we are considering a slice of  $\partial B_r$  by an affine  $d$ -dimensional space resulting in a polytope that is both convex in the usual and in the tropical sense; cf. Sect. 6.

### 1.6 Notation

Throughout the paper, let  $d \geq 2$  and  $r \geq 1$  denote two integers. Let  $R$  be a finite commutative chain ring with maximal ideal  $\mathfrak{m}$  generated by  $\pi$  and such that  $\pi^r = 0$ , but  $\pi^{r-1} \neq 0$ . Write  $q = |R/\mathfrak{m}|$  for the cardinality of the residue field of  $R$ . Let  $V_r$  denote a free  $R$ -module of rank  $d$  and fix  $\mathbf{e} = (e_1, \dots, e_d)$  to be a basis of  $V_r$  over  $R$ . If  $r = 1$ , then  $R$  is a field and we simply write  $V = V_1$ . Let  $\mathbf{1}$  denote the vector  $(1, \dots, 1) \in \mathbb{Z}^d$ , let  $\text{Sym}(d)$  denote the symmetric group on  $d$  letters, and let  $J_d$  denote the integral  $(d \times d)$ -matrix with 0’s on the diagonal and 1’s elsewhere. Set, additionally

$$\mathcal{E}_r^{(d)} = \{\varepsilon = (\varepsilon_1, \dots, \varepsilon_{d-1}, \varepsilon_d = 0) \in \mathbb{Z}^d \mid r \geq \varepsilon_1 \geq \dots \geq \varepsilon_{d-1} \geq 0\},$$

$$\partial \mathcal{E}_r^{(d)} = \{\varepsilon = (\varepsilon_1 = r, \varepsilon_2, \dots, \varepsilon_{d-1}, \varepsilon_d = 0) \in \mathbb{Z}^d \mid r \geq \varepsilon_2 \geq \dots \geq \varepsilon_{d-1} \geq 0\}.$$

In conclusion, for an indeterminate  $X$ , integers  $a \geq b \geq 0$ , and  $I = \{i_1, \dots, i_\ell\} \subseteq \mathbb{Z}_{\geq 0}$ , put

$$\binom{a}{b}_X = \prod_{i=0}^{b-1} \frac{1 - X^{a-i}}{1 - X^{b-i}} \quad \text{and} \quad \binom{d}{I}_X = \binom{d}{i_\ell}_X \binom{d}{i_{\ell-1}}_X \dots \binom{d}{i_1}_X.$$

## 2 The module distance

In this section we define an equivalence relation on the set  $\mathcal{L}(V_r)$  of all  $R$ -submodules of  $V_r$  and a distance on the collection of its equivalence classes.

**Definition 2.1** Let  $U$  be an element of  $\mathcal{L}(V_r)$ . Then  $m_U \in \{0, \dots, r\}$  is defined as

$$m_U = \max\{0 \leq m \leq r \mid U \subseteq \pi^m V_r\}.$$

Moreover,  $\tilde{U} \in \mathcal{L}(V_r)$  is defined to be the kernel of the map

$$V_r \longrightarrow V_r/U, \quad x \longmapsto \pi^{m_U} x + U.$$

Note that  $\tilde{U}$  is the unique maximal  $R$ -submodule of  $V_r$  with the property that  $\pi^{m_U} \tilde{U} = U$ . In particular, we have that  $U \subseteq \tilde{U}$  and, moreover,  $m_U = 0$  if and only if  $\tilde{U} = U$ . As a consequence, we have that

$$\partial \mathcal{L}(V_r) = \{U \in \mathcal{L}(V_r) \mid \pi^{r-1} V_r \not\subseteq U \not\subseteq \pi V_r\} \tag{2.1}$$

$$\subseteq \{U \in \mathcal{L}(V_r) \mid \tilde{U} = U\}. \tag{2.2}$$

**Definition 2.2** Modules  $U$  and  $U'$  in  $\mathcal{L}(V_r)$  are *homothetic* whenever  $\tilde{U} = \tilde{U}'$ .

Homothety defines an equivalence relation  $\sim$  on  $\mathcal{L}(V_r)$  and we write

$$\mathcal{L}^0(V_r) = \mathcal{L}(V_r)/\sim = \{[U] = \{U' \in \mathcal{L}(V_r) \mid \tilde{U} = \tilde{U}'\} \mid U \in \mathcal{L}(V_r)\}$$

for the collection of homothety classes of elements of  $\mathcal{L}(V_r)$ . Note that  $[V_r] = [0]$  has cardinality  $r + 1$  and the cardinality of each  $[U] \in \mathcal{L}^0(V_r) \setminus \{[0]\}$  is at most  $r$ . Moreover, it is not difficult to see that  $\partial\mathcal{L}(V_r)$  can be identified with the collection of equivalence classes in  $\mathcal{L}^0(V_r)$  with exactly one element. With a slight abuse of notation, we thus write

$$\partial\mathcal{L}(V_r) = \{[U] \in \mathcal{L}^0(V_r) \mid [U] = \{U\}\}. \tag{2.3}$$

We define a metric on  $\mathcal{L}^0(V_r)$ , which does not generalize the subspace or the injection metric; cf. [30, Section 1].

**Definition 2.3** Let  $[U], [U_1], [U_2] \in \mathcal{L}^0(V_r)$  denote homothety classes of modules. Define

$$n_{12} = \min\{m \in \mathbb{Z}_{\geq 0} \mid \pi^m \tilde{U}_1 \subseteq \tilde{U}_2\} \text{ and}$$

$$n_{21} = \min\{n \in \mathbb{Z}_{\geq 0} \mid \pi^n \tilde{U}_2 \subseteq \tilde{U}_1\}.$$

Then the *distance* between  $[U_1]$  and  $[U_2]$  is

$$\text{dist}([U_1], [U_2]) = n_{12} + n_{21}.$$

For a subset  $\mathcal{M} \subseteq \mathcal{L}^0(V_r)$ , put  $\text{dist}([U], \mathcal{M}) = \min\{\text{dist}([U], [U']) \mid [U'] \in \mathcal{M}\}$ .

The next result gives that  $\mathcal{L}^0(V_r)$  equipped with  $\text{dist}$  is a metric space.

**Lemma 2.4** *The map  $\text{dist} : \mathcal{L}^0(V_r) \times \mathcal{L}^0(V_r) \rightarrow \mathbb{Z}$  is a distance.*

**Proof** We only show that the triangle inequality holds, as the other defining properties are clear. For this, let  $[U_1], [U_2], [U_3] \in \mathcal{L}^0(V_r)$  and, for  $i, j = 1, 2, 3$ , let  $n_{ij}$  be as in Definition 2.3. It follows from their definitions that

$$\pi^{n_{13}} \tilde{U}_1 \subseteq \tilde{U}_3, \quad \pi^{n_{32}} \tilde{U}_3 \subseteq \tilde{U}_2, \quad \pi^{n_{23}} \tilde{U}_2 \subseteq \tilde{U}_3, \quad \pi^{n_{31}} \tilde{U}_3 \subseteq \tilde{U}_1,$$

and so the minimalities of  $n_{12}$  and  $n_{21}$  yield

$$n_{12} \leq n_{13} + n_{32} \text{ and } n_{21} \leq n_{23} + n_{31}.$$

It follows from Definition 2.3 that  $\text{dist}([U_1], [U_2]) \leq \text{dist}([U_1], [U_3]) + \text{dist}([U_2], [U_3])$ .  $\square$

We remark that every element in  $\mathcal{L}^0(V_r)$  has distance at most  $r$  from  $[V_r]$ , equivalently the set  $\mathcal{L}^0(V_r)$  can be interpreted as the *ball of radius  $r$  around  $[V_r]$* :

$$\mathcal{L}^0(V_r) = B_r([V_r]) = \{[U] \in \mathcal{L}^0(V_r) \mid \text{dist}([U], [V_r]) \leq r\}. \tag{2.4}$$

In general, for each  $\ell \in \{0, \dots, r\}$ , we set

$$B_\ell([V_r]) = \{[U] \in \mathcal{L}^0(V_r) \mid \text{dist}([U], [V_r]) \leq \ell\} \text{ and}$$

$$\partial B_\ell([V_r]) = \{[U] \in \mathcal{L}^0(V_r) \mid \text{dist}([U], [V_r]) = \ell\},$$

which we call the *ball of radius  $\ell$*  and the *sphere of radius  $\ell$*  around  $[V_r]$ , respectively.

**Example 2.5** Assume that  $R = \mathbb{Z}/32\mathbb{Z}$ , in which case the maximal ideal of  $R$  is generated by  $\pi = 2$  and  $r = 5$ . Figure 1 illustrates the elements of  $\mathcal{L}^0(V_5)$ : in this picture two elements are joined by an edge if they have distance 1. We look concretely at some of the elements of  $\mathcal{L}^0(V_5)$  and at the distances between them.

If  $U$  is the  $R$ -submodule generated by  $4e_1$  and  $8e_2$ , then  $m_U = 2$  and  $\tilde{U}$  is generated by  $e_1$  and  $2e_2$ . Writing  $(X)$  for the  $R$ -submodule of  $V_5$  generated by  $X \subseteq V_5$ , the tilde representatives of the classes in  $B_1(V_5)$  are

$$V_5, \quad U_1 = \langle e_1, 2e_2 \rangle, \quad U_2 = \langle 2e_1, e_2 \rangle, \quad U_3 = \langle e_1 + e_2, 2e_1 \rangle$$

while  $\partial B_1(V_5) = \{[U_1], [U_2], [U_3]\}$ . Note that  $\partial B_1(V_5)$  is in 1-to-1 correspondence with  $\mathbb{P}(V_5/2V_5)$ , i.e. the elements of  $\partial B_1(V_5)$  can be interpreted as lines in the 2-dimensional vector space  $V_5/2V_5$ . Setting now  $\ell = 2$ , we find the representatives of  $\partial B_2(V_5)$ :

$$U_{11} = \langle e_1, 4e_2 \rangle, \quad U_{12} = \langle e_1 + 2e_2, 4e_2 \rangle, \quad U_{21} = \langle e_2, 4e_1 \rangle, \quad U_{22} = \langle 2e_1 + e_2, 4e_1 \rangle, \\ U_{31} = \langle e_1 + e_2, 4e_1 \rangle, \quad U_{32} = \langle e_1 + 3e_2, 4e_1 \rangle.$$

In the following table we collect the distances within  $B_2(V_5)$ :

	1	2	3	11	12	21	22	31	32
1	0	2	2	1	1	3	3	3	3
2		0	2	3	3	1	1	3	3
3			0	3	3	3	3	1	1
11				0	2	4	4	4	4
12					0	4	4	4	4
21						0	2	4	4
22							0	4	4
31								0	2

The red dots in Fig. 1 denote the elements of  $\partial B_3(V_5)$ . Moreover, it turns out in this case that  $\text{dist}$  on  $\mathcal{L}^0(V_5)$  coincides with the graph distance on Fig. 1.

**Proposition 2.6** For each  $\ell \in \{0, \dots, r\}$ , the following hold:

- (1)  $\partial B_\ell([V_r]) = \{[U] \in \mathcal{L}^0(V_r) \mid |[U]| = r - \ell + 1\}$ ,
- (2)  $B_\ell([V_r]) = \{[U] \in \mathcal{L}^0(V_r) \mid |[U]| \geq r - \ell + 1\}$ .

Moreover, one has  $\partial \mathcal{L}(V_r) = \partial B_r([V_r])$ .

**Proof** Let  $\ell \in \{0, \dots, r\}$ . We start by showing (1). For this, let  $U \in \mathcal{L}(V_r)$  and assume without loss of generality that  $U = \tilde{U}$ . Then the following hold

$$\begin{aligned} \text{dist}([U], [V_r]) = \ell &\iff \ell = \min\{n \in \mathbb{Z}_{\geq 0} \mid \pi^n V_r \subseteq U\} \\ &\iff [U] = \{\pi^j U \mid j = 0, \dots, r - \ell\} \\ &\iff |[U]| = r - \ell + 1 \end{aligned}$$

and so (1) is proven. To show (2), we combine (1) to the observation that

$$B_\ell([V_r]) = \bigcup_{0 \leq j \leq \ell} \partial B_j([V_r]) = \bigcup_{r-\ell+1 \leq h \leq r+1} \{[U] \in \mathcal{L}^0(V_r) \mid |[U]| = h\}.$$

The proof of (1) also shows that  $\partial \mathcal{L}(V_r) = \partial B_r([V_r])$ . □

### 3 Spherical submodule codes

In this section we define spherical codes in  $V_r$  as codes of submodules and prove some initial results. For a comparison with subspace codes see for instance [30] while for a comparison with spherical codes in the Euclidean case, we refer to [21].

**Definition 3.1** Let  $\mathcal{C}$  be a subset of  $\mathcal{L}^0(V_r)$  with  $|\mathcal{C}| \geq 2$ . Then the *minimum distance* of  $\mathcal{C}$  is

$$\text{dist}(\mathcal{C}) = \min\{\text{dist}([U], [U']) \mid [U], [U'] \in \mathcal{C}, [U] \neq [U']\}.$$

Recall that  $\partial\mathcal{L}(V_r)$  is a metric space equipped with the metric  $\text{dist}$  from Sect. 2 via the identification in (2.3).

**Definition 3.2** A *spherical code* in  $V_r$  is a subset  $\mathcal{C}$  of  $\partial\mathcal{L}(V_r)$  with at least 2 elements.

The terminology ‘‘spherical’’ is motivated by Proposition 2.6, from which it follows in particular that each element  $[U]$  of a spherical code  $\mathcal{C}$  satisfies  $\text{dist}([U], [V_r]) = r$ . The proof of the next result is straightforward; compare also with the table in Example 2.5.

**Lemma 3.3** For each spherical code  $\mathcal{C}$  in  $V_r$ , one has  $\text{dist}(\mathcal{C}) \leq 2r$ .

A spherical code in  $V_r$  could in principle equal  $\partial\mathcal{L}(V_r)$ , so a universal yet weak bound on the cardinality of a spherical code is given by  $|\partial\mathcal{L}(V_r)|$ . For a precise count of the elements of  $\partial\mathcal{L}(V_r)$  or  $\mathcal{L}^0(V_r)$  we refer to Sect. 8 via Theorem 7.6. The most interesting bounds for spherical codes come from relating  $\text{dist}(\mathcal{C})$  and  $|\mathcal{C}|$ .

**Definition 3.4** Let  $\chi, \psi$  denote integers satisfying  $\chi \geq 2$  and  $\psi \geq 1$ . Define

- (1)  $\text{dist}(d; R; \chi) = \max\{\text{dist}(\mathcal{C}) \mid \mathcal{C} \subseteq \partial\mathcal{L}(V_r), |\mathcal{C}| \geq \chi\}$ ,
- (2)  $\text{card}(d; R; \psi) = \max\{|\mathcal{C}| \mid \mathcal{C} \subseteq \partial\mathcal{L}(V_r), \text{dist}(\mathcal{C}) \geq \psi\}$ .

Since (1) and (2) are somewhat dual to each other (see also the analogous definitions in the Euclidean case [21, Section 2.3]), we will mostly be focussing on (2).

**Example 3.5** The blue dots in Fig. 1 form a spherical code in  $V_5$  with minimum distance 6; cf. also Example 2.5. In particular this shows that  $\text{card}(2; \mathbb{Z}/32\mathbb{Z}; 6) \geq 12$  and  $\text{dist}(2; \mathbb{Z}/32\mathbb{Z}; 12) \geq 6$ .

**Definition 3.6** Let  $\mathcal{C} = \{[U_1], \dots, [U_s]\}$  denote an ordered spherical code in  $V_r$ . The *half-distance matrix* of  $\mathcal{C}$  is  $N(\mathcal{C}) = (n_{ij}) \in \mathbb{Z}^{s \times s}$  where

$$n_{ij} = \min\{\beta \in \mathbb{Z}_{\geq 0} \mid \pi^\beta \tilde{U}_i \subseteq \tilde{U}_j.\}$$

Note that, as a consequence of Proposition 2.6, if  $\text{dist}(\mathcal{C}) = 2r$ , then  $N(\mathcal{C}) = rJ_s$ .

**Remark 3.7** Let  $\mathcal{C} = \{[U_1], \dots, [U_s]\}$  be an ordered spherical code in  $V_r$ . The *distance matrix* of  $\mathcal{C}$  is

$$D(\mathcal{C}) = N(\mathcal{C}) + N(\mathcal{C})^t.$$

Then  $D(\mathcal{C}) = (\delta_{ij})$  is a symmetric matrix with the following properties:

- (1) for each pair  $(i, j)$ , one has  $\text{dist}([U_i], [U_j]) = \delta_{ij} = \delta_{ji}$ ,
- (2)  $\text{dist}(\mathcal{C}) = \min\{\delta_{ij} \mid \delta_{ij} \neq 0\}$ .

The following proposition is easily seen to hold as a consequence of Proposition 2.6.

**Proposition 3.8** Let  $[U_1], [U_2]$  be in  $\mathcal{L}^0(V_r)$ . Then the following are equivalent:

- (1)  $\text{dist}([U_1], [U_2]) = 2r$ .
- (2)  $[U_1], [U_2] \in \partial\mathcal{L}(V_r)$  and  $\pi^{r-1}U_1, \pi^{r-1}U_2 \not\subseteq U_1 \cap U_2$ .

### 4 Grassmannians and Sperner codes

In this section we build spherical codes in  $V_r$  starting from modules highlighted by the investigation of the Sperner property in finite abelian  $p$ -groups; cf. [41, 42, 45]. We call a subset  $\mathcal{K}$  of a poset  $\mathcal{P}$  a *chain* if any two of its elements are *comparable*, i.e.

$$a, b \in \mathcal{K} \implies a \preceq b \text{ or } b \preceq a.$$

On the contrary, an *antichain* is a subset  $\mathcal{A}$  of  $\mathcal{P}$  whose elements are pairwise *incomparable*, that is

$$a, b \in \mathcal{A} \implies a \not\preceq b \text{ and } b \not\preceq a.$$

Antichains play an important role in the construction of “big codes” in this paper.

#### 4.1 Grassmannians and sperner bounds

The content of this section could be presented in terms of the Sperner property, though we choose not to do so for the sake of brevity. For the purposes of this section,  $\mathcal{L}(V_r)$  is considered as the poset of all  $R$ -submodules of  $V_r$ , ordered by inclusion. Recall that, if  $U$  is a free  $R$ -submodule of  $V_r$ , then its *rank* equals the minimum cardinality of a generating set.

**Definition 4.1** Let  $n$  be an integer with  $1 \leq n \leq d - 1$ . The *Grassmannian*  $\text{Gr}(n, V_r)$  is the collection of all free  $R$ -submodules of  $V_r$  of rank  $n$ .

It is clear from its definition that, for each  $n$ , the Grassmannian  $\text{Gr}(n, V_r)$  is an antichain in  $\mathcal{L}(V_r)$  and is contained in  $\partial\mathcal{L}(V_r)$ . Moreover, when  $r = 1$ , the Grassmannian  $\text{Gr}(n, V)$  consists of the  $n$ -dimensional subspaces of  $V$ . For more on Grassmannians, we refer to [36, Chapter 5] and references therein. Generalizing the proof of [43, Proposition 1.3.18] to  $V_r$ , we have that

$$|\text{Gr}(n, V_r)| = \binom{d}{n}_{q^{-1}} q^{rn(d-n)}, \tag{4.1}$$

from which it follows that  $|\text{Gr}(n, V_r)| = |\text{Gr}(d - n, V_r)|$ . We remark that (4.1) also follows directly from the more general formulas from Sect. 8.

**Example 4.2** Assume that  $d = 2$  and  $R = \mathbb{Z}/32\mathbb{Z}$ , which implies that  $q = 2$ . We have seen in Example 2.5 that  $\partial B_1(V_5)$  has the same number of elements as  $\text{Gr}(1, V_5/2V_5)$ , where  $V_5/2V_5$  is viewed as a free  $R/2R$ -module. Indeed (4.1) ensures

$$|\text{Gr}(1, V_5/2V_5)| = \binom{2}{1}_{\frac{1}{2}} 2^1 = \frac{1 - (\frac{1}{2})^2}{1 - \frac{1}{2}} 2^1 = 3 = |\partial B_1(V_5)|.$$

The following is the main result of [45], which is there phrased to hold for  $r \geq 3$ . The case where  $r = 1$  can be found in [39, 41], while the case  $r = 2$  is given in [42, Theorem 2.7].

**Proposition 4.3** [45, Main Theorem] *Set  $e_- = (d - 1)/2$  and  $e = d/2$  and  $e_+ = (d + 1)/2$ . Let, moreover,  $n \in \{1, \dots, d - 1\}$ . Then  $\text{Gr}(n, V_r)$  is a maximal-sized antichain in  $\mathcal{L}(V_r)$  if and only if exactly one of the following holds:*

- (1)  $d$  is even and  $n = e$ ,
- (2)  $d$  is odd and  $n \in \{e_-, e_+\}$ .



### 4.2 Sperner codes

In this section we define spherical codes in  $V_r$  that will yield lower bounds to  $\text{card}(d; R; 2\alpha)$  for any choice of the integer  $1 \leq \alpha \leq r$ . To this end, we fix such an  $\alpha$  and define

$$m = r + 1 - \alpha \text{ and } e = \lceil d/2 \rceil = \begin{cases} d/2 & \text{if } d \text{ even,} \\ (d + 1)/2 & \text{if } d \text{ odd.} \end{cases} \tag{4.2}$$

We will define a family of codes  $\mathcal{C}$  that satisfy

$$\text{dist}(\mathcal{C}) \geq 2\alpha \text{ and } |\mathcal{C}| = |\text{Gr}(e, V_m)|, \tag{4.3}$$

cf. Definition 4.4. Write  $\text{Gr}(e, \pi^{\alpha-1}V_r)$  for the collection of free  $R/\mathfrak{m}^m$ -submodules of  $\pi^{\alpha-1}V_r$  of rank  $e$  and note that the elements of  $\text{Gr}(e, \pi^{\alpha-1}V_r)$  are incomparable. Moreover,  $\text{Gr}(e, \pi^{\alpha-1}V_r)$  is in bijection with  $\text{Gr}(e, V_m)$ , equivalently

$$|\text{Gr}(e, \pi^{\alpha-1}V_r)| = |\text{Gr}(e, V_m)| = \binom{d}{e}_{q^{-1}} q^{me(d-e)}.$$

**Definition 4.4** A Sperner code with parameters  $(d; R; \alpha)$  is a subset  $\mathcal{C}$  of  $\text{Gr}(e, V_r)$  such that the map

$$\mathcal{C} \longrightarrow \text{Gr}(e, \pi^{\alpha-1}V_r), \quad U \longmapsto \pi^{\alpha-1}U,$$

is a bijection.

We remark that a Sperner code with parameters  $(d; R; \alpha)$  is nothing else than a collection  $\mathcal{C}$  of free  $R$ -submodules of  $V_r$  with the property that  $\text{Gr}(e, V_r) = \{\pi^{\alpha-1}U \mid U \in \mathcal{C}\}$ . An example of a Sperner code when  $d = 2$  is given in Fig. 1 (see also Examples 2.5, and 3.5).

**Theorem 4.5** Let  $1 \leq \alpha \leq r$  be an integer and let  $\mathcal{C}$  be a Sperner code with parameters  $(d; R; \alpha)$ . Then the following are satisfied:

- (1)  $\mathcal{C}$  is a spherical code in  $V_r$ ,
- (2)  $\text{dist}(\mathcal{C}) \geq 2\alpha$ ,
- (3)  $|\mathcal{C}| = |\text{Gr}(\lceil d/2 \rceil, V_{r+1-\alpha})|$ .

**Proof** (1) and (3) are clear from the construction of Sperner codes, so we prove (2). For this, let  $U_1, U_2 \in \mathcal{C}$  be distinct: we claim that  $n_{12} \geq \alpha$ . For a contradiction, assume that this is not the case. It follows that  $\pi^{\alpha-1}U_1 \subseteq \pi^{n_{12}}U_1 \subseteq U_2$  and so

$$\pi^{\alpha-1}U_1 \subseteq U_2 \cap \pi^{\alpha-1}V_r = \pi^{\alpha-1}U_2,$$

which contradicts the bijectivity of the map  $\mathcal{C} \rightarrow \text{Gr}(e, \pi^{\alpha-1}V_r)$  from Definition 4.4. We have proven that  $n_{12} \geq \alpha$  and, the choice of  $U_1$  and  $U_2$  being arbitrary, we have that  $\text{dist}(\mathcal{C}) \geq 2\alpha$ .  $\square$

The following is an immediate corollary of the last result.

**Corollary 4.6** Let  $1 \leq \alpha \leq r$  be an integer and define  $e = \lceil d/2 \rceil$ . Then

$$\text{card}(d; R; 2\alpha) \geq \binom{d}{e}_{q^{-1}} q^{(r+1-\alpha)e(d-e)}.$$

As we will see in the next section, the inequality from Corollary 4.6 is an equality in some cases. We leave the following general question open.

**Question 4.7** Is the inequality from Corollary 4.6 always an equality?

## 5 Extremal cases

In this section we show that Question 4.7 has a positive answer when  $\alpha = r$  or  $d = 2$  by showing that, in these cases, Sperner codes are optimal codes with respect to the bound given in Corollary 4.6.

### 5.1 Codes of maximal distance

This section is devoted to the case  $\alpha = r$ .

**Proposition 5.1** *Let  $\mathcal{C}$  be a spherical code in  $V_r$  with  $\text{dist } \mathcal{C} = 2r$ . Then there exists a spherical code  $\mathcal{C}'$  in  $V_r$  such that the following hold:*

- (1)  $|\mathcal{C}| = |\mathcal{C}'|$  and  $\text{dist}(\mathcal{C}') = 2r$ ,
- (2) for each  $U \in \mathcal{C}'$ , one has  $\pi U = U \cap \pi V_r$ .

**Proof** Define  $\mathcal{C}_F$  to be the collection of all  $U \in \mathcal{C}$  such that  $\pi U = U \cap \pi V_r$ . We prove, by induction on  $n = |\mathcal{C} \setminus \mathcal{C}_F|$ , that there exists  $\mathcal{C}'$  satisfying (1) and (2). If  $n = 0$ , then  $\mathcal{C}$  already satisfies (2) and we set  $\mathcal{C}' = \mathcal{C}$ . Assume now that  $n > 0$  and that the claim is satisfied for  $n - 1$ . Let  $U \in \mathcal{C}$  be such that  $\pi U \neq U \cap \pi V_r$ , that is  $U$  is not a free  $R$ -submodule of  $V_r$ . In view of this, let  $X$  and  $H$  be submodules of  $U$  satisfying

$$U = X \oplus H, \quad \pi H = H \cap \pi V_r, \quad \pi^{r-1} X = 0.$$

In particular,  $H$  is isomorphic to the free part (as  $R$ -submodule) of  $U$  and both  $H$  and  $X$  are non-trivial. Set now  $\mathcal{C}'' = (\mathcal{C} \setminus \{U\}) \cup \{H\}$ . It follows from  $\pi^{r-1} U = \pi^{r-1} H$  and Proposition 3.8 that  $\mathcal{C}''$  is a spherical code of minimal distance  $2r$ . Moreover, we have  $\mathcal{C}''_F = \mathcal{C}_F \cup \{H\}$  and  $\mathcal{C}$  and  $\mathcal{C}''$  have the same cardinality. We are now done thanks to the induction hypothesis. □

Thanks to Proposition 5.1, to compute the maximal cardinality of spherical codes of maximal distance in  $V_r$  it suffices to look at free  $R$ -submodules of  $V_r$ , equivalently at subsets of the sets of vertices of the ball  $B_r$  as a lattice polytope; cf. Definition 7.4 and Sects. 6.1 and 7.

**Definition 5.2** A spherical code  $\mathcal{C}$  in  $V_r$  is called *free* if it satisfies Proposition 5.1(2).

The next result follows in a straightforward way from Proposition 3.8.

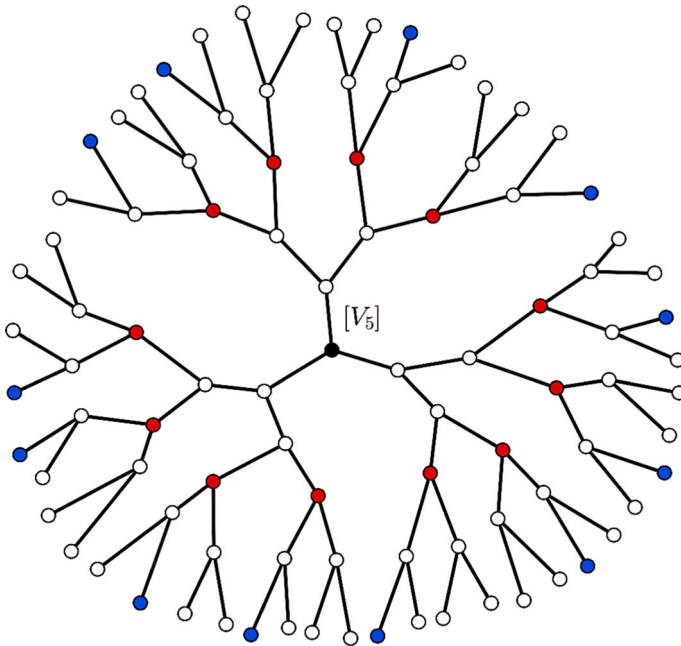
**Lemma 5.3** *Let  $\mathcal{C}$  be a free spherical code in  $V_r$  and let  $U_1, U_2 \in \mathcal{C}$ . Then the following are equivalent:*

- (1)  $\text{dist}([U_1], [U_2]) = 2r$ ,
- (2)  $\pi^{r-1} U_1$  and  $\pi^{r-1} U_2$  are incomparable.

**Theorem 5.4** *Let  $e = \lceil d/2 \rceil$  be as defined in (4.2). Then the following holds:*

$$\text{card}(d; R; 2r) = \binom{d}{e}_{q^{-1}} q^{e(d-e)}.$$

**Proof** Let  $\mathcal{C}$  be a spherical code in  $V_r$  of maximal cardinality satisfying  $\text{dist}(\mathcal{C}) = 2r$ . Thanks to Proposition 5.1, we assume without loss of generality that  $\mathcal{C}$  is free. Then Lemma 5.3 yields that the elements of  $\mathcal{C}$  are in bijection with a collection of maximal size of incomparable subspaces of  $\pi^{r-1} V_r \cong V$ . We are now done thanks to Proposition 4.3 and (4.1). □



**Fig. 1** The vertices of this graph denote the elements of  $\mathcal{L}^0(V_5)$  and  $([U], [U'])$  is an edge if  $\pi \tilde{U} \subset \tilde{U}' \subset \tilde{U}$  or  $\pi \tilde{U}' \subset \tilde{U} \subset \tilde{U}'$ . The red points are the elements of  $\partial B_3([V_5])$ , which are represented by the elements of  $\text{Gr}(1, \pi^2 V_5)$  from Sect. 4.1. A Sperner code with parameters  $(2; \mathbb{Z}/32\mathbb{Z}; 3)$  and thus minimum distance 6 is given in blue (Color figure online)

### 5.2 Codes in small dimension

In this section we answer Question 4.7 when  $d = 2$ , which we assume throughout Sect. 5.2.

**Remark 5.5** There is a number of properties that spherical codes satisfy when  $d = 2$ , which do not generally hold for every spherical code. For instance, each element of  $\partial \mathcal{L}(V_r)$  is a free  $R$ -submodule of  $V_r$  and, for every  $1 \leq \alpha \leq r$ , the family  $\text{Gr}(1, \pi^{\alpha-1} V_r)$  from Sect. 4.1 forms a set of representatives for the classes in  $\partial B_{r+1-\alpha}([V_r])$ ; cf. Fig. 1. Write now  $\text{Gr}(1, \pi^{\alpha-1} V_r) = \{S_1, \dots, S_t\}$  and, for each  $k \in \{1, \dots, t\}$ , define

$$\partial_\alpha^k \mathcal{L}(V_r) = \{U \in \partial \mathcal{L}(V_r) \mid \text{dist}([U], [S_k]) = \alpha - 1\}.$$

Then  $\partial \mathcal{L}(V_r)$  equals the disjoint union of the  $\partial_\alpha^k \mathcal{L}(V_r)$ 's and defining a Sperner code with parameters  $(2; R; \alpha)$  is the same as choosing one element in each  $\partial_\alpha^k \mathcal{L}(V_r)$ ; cf. Fig. 1.

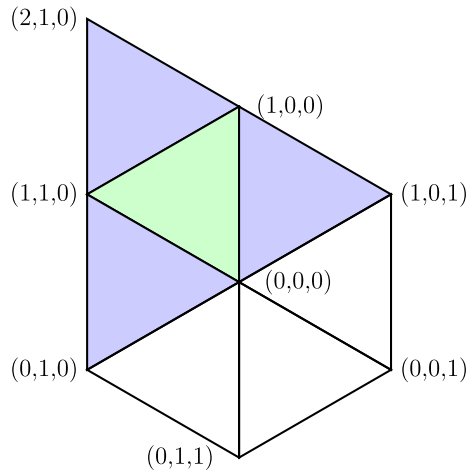
**Theorem 5.6** *Let  $1 \leq \alpha \leq r$  be an integer. Then the following holds:*

$$\text{card}(2; R; 2\alpha) = (q + 1)q^{r-\alpha}.$$

**Proof** Thanks to Corollary 4.6, we have that

$$\text{card}(2; R; 2\alpha) \geq |\text{Gr}(1, V_{r+1-\alpha})| = \binom{2}{1}_{q^{-1}} q^{r+1-\alpha} = (q + 1)q^{r-\alpha},$$

**Fig. 2** A local picture of  $\mathcal{L}_{\mathbf{e}}^0$  when  $d = 3$  (Color figure online)



so we prove the other inequality. With the notation from Remark 5.5, we have, for any  $k \in \{1, \dots, t\}$  and  $U, U' \in \partial_{\alpha}^k \mathcal{L}(V_r)$ , that

$$\text{dist}([U], [U']) \leq \text{dist}([U], [S_k]) + \text{dist}([U'], [S_k]) = 2(\alpha - 1) < 2\alpha.$$

The choice of  $k$  being arbitrary, this shows that any spherical code in  $V_r$  with  $\text{dist}(C) \geq 2\alpha$ , can contain at most one representative from each  $\partial_{\alpha}^k \mathcal{L}(V_r)$ . This concludes the proof.  $\square$

### 6 Permutation codes

In this section, we give a possible generalization of permutation codes, as defined in [21, Chapter 4], by means of  $\text{Sym}(d)$ -orbits of  $R$ -modules with compatible generating sets. For the fixed  $R$ -basis  $\mathbf{e} = (e_1, \dots, e_d)$  of  $V_r$ , we define  $\mathcal{L}_{\mathbf{e}}(V_r)$  to be the family of  $R$ -submodules of  $V_r$  that can be generated *compatibly with  $\mathbf{e}$* , in other words modules of the form

$$U_{\delta} = R\pi^{\delta_1} e_1 \oplus \dots \oplus R\pi^{\delta_d} e_d, \text{ where } 0 \leq \delta_i \leq r.$$

The homothety relation from Sect. 2 respects base compatibility and so we define  $\mathcal{L}_{\mathbf{e}}^0(V_r)$  to be the subfamily of  $\mathcal{L}^0(V_r)$  with representatives in  $\mathcal{L}_{\mathbf{e}}(V_r)$ . In particular, we can model all elements of  $\mathcal{L}_{\mathbf{e}}^0(V_r)$  in terms of the  $\text{Sym}(d)$ -orbits of the set  $\mathcal{E}_r^{(d)}$  in  $\mathbb{Z}^d$  and  $\partial \mathcal{L}_{\mathbf{e}}(V_r) = \partial \mathcal{L}(V_r) \cap \mathcal{L}_{\mathbf{e}}(V_r)$  is defined by permutations of elements of  $\partial \mathcal{E}_r^{(d)}$ .

**Example 6.1** Assume that  $d = 3$  and  $R = \mathbb{Z}/25\mathbb{Z}$ , yielding  $r = 2$  and  $q = 5$ . Then  $U_{(0,0,0)}$  is the same as  $V_2$  and the modules  $U_{(1,1,0)} \subset U_{(1,0,0)} \subset U_{(0,0,0)}$  are pairwise at distance 1 from each other. Moreover,  $U_{(2,1,0)}$  is an element of  $\partial \mathcal{L}_{\mathbf{e}}(V_2)$ . Note that, while  $|\partial \mathcal{L}_{\mathbf{e}}(V_2)| = 12$ , the cardinality of  $\partial \mathcal{L}(V_2)$  is equal to 1860; cf. Sect. 8. If we compared the spheres of radius 1 around  $[V_2]$ , we would get 6 elements in the compatible case, against the 62 without basis restrictions (see Fig. 2).

### 6.1 Tropical operations and polytropes

For the sake of conciseness and in adherence to the references cited below we introduce here some more notation, coming from tropical geometry. For real elements  $a$  and  $b$  we set

$$a \underline{\oplus} b = \min\{a, b\}, \quad a \overline{\oplus} b = \max\{a, b\}, \quad a \odot b = a + b$$

and remark that the last operations can be extended to  $\mathbb{R}^d$  componentwise. For each matrix  $M \in \mathbb{R}^{d \times d}$  with 0's on the diagonal, we define moreover

$$Q(M) = \{u \in \mathbb{R}^d / \mathbb{R}\mathbf{1} : u_i - u_j \leq m_{ij} \text{ for } 1 \leq i, j \leq d\}, \tag{6.1}$$

which is a convex polytope in  $\mathbb{R}^d / \mathbb{R}\mathbf{1}$  and is called a *polytrope* in tropical geometry. For more on polytropes, we refer the interested reader to [17, 28, 29, 34]. In this paper, we will only deal with polytropes like the ones in the next example. As we mention in [17, Example 13], such polytropes are called *pyropes* in [29] and can be seen as balls of radius  $r$  in the tropical metric [13, Section 3.3]. Recall that  $J_d$  denotes the matrix in  $\mathbb{Z}^{d \times d}$  with 0's on the diagonal and off-diagonal entries all equal to 1.

**Example 6.2** Let  $[\delta] \in Q(rJ_d)$  be such that  $\delta$  has integral coordinates. Then there exists  $\tilde{\delta} \in [\delta]$  all of whose coordinates  $\tilde{\delta}_i$  are integral and satisfy  $0 \leq \tilde{\delta}_i \leq r$ . Then  $U_{\tilde{\delta}}$  belongs to  $\mathcal{L}_e(V_r)$  and, any other  $\tilde{\delta}'$  such that

$$\tilde{\delta}' \in \tilde{\delta} + \mathbb{Z}\mathbf{1} \text{ and } 0 \leq \tilde{\delta}'_i \leq r$$

yields  $[U_{\tilde{\delta}}] = [U_{\tilde{\delta}'}]$ . More precisely, using the language of buildings, one can show that there is a one-to-one correspondence between the integral points of  $Q(rJ_d)$  and the elements of  $\mathcal{L}_e^0(V_r)$ ; cf. Theorem 7.6 and [19, Theorem 5.2].

Identifying  $\mathbb{R}^d / \mathbb{R}\mathbf{1}$  with  $\{u \in \mathbb{R}^d \mid u_d = 0\}$ , it is not difficult to see from Equation 6.1 that the coordinates of vertices of the polytope  $Q(rJ_d)$  are in  $\{0, r\}^d \cup \{0, -r\}^d$ . As mentioned in the Introduction, this has a nice interpretation in terms of free  $R$ -submodules of  $V_r$ .

### 6.2 Permutation codes

In this section we define permutation codes and give examples of such codes in connection with the theory of polytropes. In Theorem 6.9 we give sharp bounds on the minimum distance and cardinality of permutation codes in terms of their defining parameters.

**Definition 6.3** An *e-permutation code* in  $V_r$  is a code of the form

$$C = \{[U_\delta] \mid \delta \in \text{Sym}(d) \cdot \varepsilon\}, \text{ where } \varepsilon \in \partial\mathcal{E}_r^{(d)}. \tag{6.2}$$

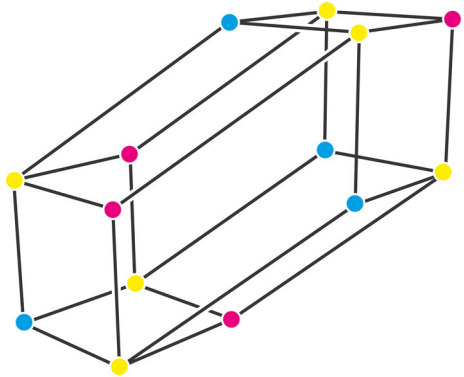
To lighten the notation, we will often write  $C = \text{Sym}(d) \cdot \varepsilon$  for a code as in (6.2).

**Remark 6.4** Let  $\delta, \varepsilon \in \{0, \dots, r\}^d$ . Then the distance between  $[U_\delta]$  and  $[U_\varepsilon]$  is given by

$$\text{dist}([U_\delta], [U_\varepsilon]) = \max_{i=1, \dots, d} \{\delta_i - \varepsilon_i\} - \min_{i=1, \dots, d} \{\delta_i - \varepsilon_i\}.$$

This can be proven by direct computation or relying on Theorem 7.6 and [19, Remark 3.3].

**Fig. 3** A representation in  $\mathbb{R}^4/\mathbb{R}\mathbf{1}$  of  $Q(J_4)$ . The yellow dots constitute an e-permutation code of maximal size having distance 2; cf. Theorem 6.9



**Remark 6.5** One could replace  $\text{Sym}(d)$  with  $\text{Aut}(V_r)$  and study codes of the form  $\text{Aut}(V_r) \cdot \varepsilon$ , that is maximal codes consisting of pairwise isomorphic  $R$ -modules. However, one can already see for  $d = 2$  that these codes are not particularly interesting in terms of general bounds. More precisely, if  $d = 2$ , one has  $\partial\mathcal{L}(V_r) = \text{Aut}(V_r) \cdot (r, 0) = \mathcal{C}$  and so  $\text{dist}(\mathcal{C}) = 2$  while  $|\mathcal{C}| = |\text{Gr}(1, V_r)| = (q + 1)q^{r-1}$ .

Of particular interest are codes that are derived from vertices of the polytope  $Q(rJ_d)$ ; cf. Example 6.2. Such vertices are given by permutations of elements  $\varepsilon$  of  $\mathcal{E}_r^{(d)}$  whose entries satisfy  $\{0, r\} = \{\varepsilon_1, \dots, \varepsilon_d\}$ , in other words they correspond to the free  $R$ -submodules of  $V_r$ . For each  $n \in \{1, \dots, d - 1\}$ , we set

$$\mathcal{F}_r^n = \text{Sym}(d) \cdot \underbrace{(r, \dots, r, 0, \dots, 0)}_{d-n}$$

describing the collection of all free  $R$ -submodules of  $V_r$  that belong to  $\mathcal{L}_\varepsilon(V_r)$ . Note that, by its definition, each  $\mathcal{F}_r^n$  is contained in  $\partial\mathcal{L}(V_r)$  and the cardinality of  $\mathcal{F}_r^n$  is equal to

$$|\mathcal{F}_r^n| = \binom{d}{n} = \frac{d!}{n!(d - n)!}.$$

**Example 6.6** In Fig. 3, the 14 regular vertices of the polytope  $Q(J_4)$  are so divided:

- the red vertices describe  $\mathcal{F}_1^1$ ,
- the blue vertices describe  $\mathcal{F}_1^3$ ,
- all other vertices, i.e. the yellow ones, are the elements of  $\mathcal{F}_1^2$ .

Moreover, in the language of tropical geometry, the red and blue vertices are the min- resp. max-vertices of the polytope  $Q(J_4)$ ; cf. [17, Example 1, Theorem 16].

In the following results we compute cardinality and minimal distance of permutation codes. For this, We fix  $\varepsilon \in \partial\mathcal{E}_r^{(d)}$  and write

- $\ell = -1 + |\{\varepsilon_1, \dots, \varepsilon_d\}| \geq 0$ ,
- $\{\varepsilon_1, \dots, \varepsilon_d\} = \{\tilde{\varepsilon}_1 > \dots > \tilde{\varepsilon}_{\ell+1} = 0\}$ .

For each  $s \in \{1, \dots, \ell + 1\}$ , we define moreover  $m_s = |\{i \in \{1, \dots, d\} \mid \varepsilon_i = \tilde{\varepsilon}_s\}|$  and note that  $m_1 + \dots + m_{\ell+1} = d$ .

**Proposition 6.7** For  $\mathcal{C} = \text{Sym}(d) \cdot \varepsilon$ , the following hold:

$$|\mathcal{C}| = \frac{d!}{m_1!m_2! \cdots m_{\ell+1}!} \text{ and } \text{dist}(\mathcal{C}) = 2 \bigoplus_{1 \leq j < i \leq \ell+1} \tilde{\varepsilon}_i - \tilde{\varepsilon}_j.$$

**Proof** The first equality follows straightforward from the definition, so we prove the second. To this end, write  $\mathcal{C} = \text{Sym}(d) \cdot \varepsilon$  and set  $\text{Set}[U_1] = [U_\varepsilon]$ . Let, moreover,  $[U_2] \in \mathcal{C}$ . In view of Remark 6.4, to minimize  $\text{dist}([U_1], [U_2])$  we pick indices  $h, k \in \{1, \dots, d\}$  such that

$$\varepsilon_h - \varepsilon_k = \bigoplus_{1 \leq j < i \leq \ell+1} \tilde{\varepsilon}_i - \tilde{\varepsilon}_j$$

and define  $\sigma$  to be the transposition in  $\text{Sym}(d)$  interchanging  $h$  and  $k$ . Choosing  $[U_2]$  to correspond to  $\sigma \cdot \varepsilon$ , we get from Remark 6.4 that

$$\text{dist}(\mathcal{C}) = \text{dist}([U_1], [U_2]) = 2(\varepsilon_h - \varepsilon_k) = 2 \bigoplus_{1 \leq j < i \leq \ell+1} \tilde{\varepsilon}_i - \tilde{\varepsilon}_j.$$

□

**Corollary 6.8** Let  $n \in \{1, \dots, d - 1\}$ . Then  $\mathcal{F}_r^n$  is a spherical code in  $V_r$  of minimal distance  $2r$ .

In the following result, we provide sharp bounds for minimum distance and cardinality when cardinality and minimum distance are given, respectively.

**Theorem 6.9** Let  $1 \leq \alpha \leq r$  be an integer and write  $\mathcal{C} = \text{Sym}(d) \cdot \varepsilon$ . Then the following are satisfied:

(1) If  $r = \delta\ell + Z$  with  $\delta, Z$  non-negative integers satisfying  $Z < \ell$ , then

$$\text{dist}(\mathcal{C}) \leq 2\delta.$$

(2) Write  $r = \alpha X + Y$  and  $d = \beta X + \gamma$ , for  $X, Y, \beta, \gamma$  non-negative integers satisfying  $Y < \alpha$  and  $\gamma < X$ . If  $\text{dist}(\mathcal{C}) = 2\alpha$ , then

$$|\mathcal{C}| \leq \frac{d!}{(\beta!)^{X+1}(\beta + 1)^\gamma}.$$

**Proof** We start by proving (1). For this, write  $r = \delta\ell + Z$  and assume without loss of generality that  $\varepsilon$  is such that  $\text{dist}(\mathcal{C})$  is maximal. Thanks to Proposition 6.7, maximizing the minimum distance of  $\mathcal{C}$  is the same as maximizing the minimum  $\eta$  of the set  $\{\tilde{\varepsilon}_i - \tilde{\varepsilon}_j \mid i > j\}$ . This is clearly achieved for  $\eta = \delta$ . We now prove (2). To this end, assume that  $\text{dist}(\mathcal{C}) = 2\alpha$ . Thanks to Proposition 6.7, we know that  $\min\{\tilde{\varepsilon}_i - \tilde{\varepsilon}_j \mid i > j\} = \alpha$  and we now need to determine  $\varepsilon$  for which

$$|\mathcal{C}| = \frac{d!}{m_1!m_2! \cdots m_{\ell+1}!}$$

is maximal, i.e. for which  $m_1!m_2! \cdots m_{\ell+1}!$  is minimal. This happens when  $\ell$  is as large as possible and the  $m_i$ 's are all roughly the same (i.e. the same or differing by 1). In view of this,  $\ell = X$  and  $\{m_1, \dots, m_{X+1}\} \subseteq \{\beta, \beta + 1\}$ . More precisely, the number of  $m_i$ 's that are equal to  $\beta + 1$  is  $\gamma$  and so Proposition 6.7 yields

$$|\mathcal{C}| \leq \frac{d!}{(\beta!)^{X+1-\gamma}((\beta + 1)!)^\gamma} = \frac{d!}{(\beta!)^{X+1}(\beta + 1)^\gamma}.$$

This concludes the proof.

□

It is not difficult to see, from the proof of Theorem 6.9, how one can build optimal codes in this context, i.e. permutation codes achieving the bounds from Theorem 6.9. As for the case of regular spherical codes, optimal permutation codes are not unique; cf. Sect. 4.2. Another thing that is worth mentioning is that optimal permutation codes are far from being optimal in the sense of Corollary 4.6. We remark that, similar bounds to those of Theorem 6.9 are proven for a different type of permutation codes in [37].

**Question 6.10** Are there other interesting generalizations of permutation codes in the context of buildings? What about group codes; cf. [21, Chapter 8]?

In the following remark we stress how, in terms of storage and decoding, permutation codes stand out among spherical codes (in accordance with the Euclidean setting).

**Remark 6.11** (A note on storage and decoding) Let  $\mathcal{C}$  be any spherical code in  $V_r$ . Then the elements of  $\mathcal{C}$  can be encoded in a vector of  $(d \times d)$ -matrices with coefficients in  $R$  where the row-span of each matrix identifies an element  $[U]$  of  $\mathcal{C}$  via returning its  $\tilde{U}$  representative. A convenient choice would be to communicate these matrices in row echelon form. In the special case when  $\mathcal{C}$  is a permutation code, it however suffices to store an element of  $\partial\mathcal{E}_r^{(d)}$  to give full information on the code  $\mathcal{C}$ .

For what concerns decoding, the lack of additional structure makes it difficult to give a straightforward algorithm for the decoding of general spherical codes of modules, even in the case where they are known to be Sperner codes. However, thanks to Remark 6.4 and in agreement with the Euclidean case, the decoding of e-permutation codes is relatively simple. To illustrate this, we fix a permutation code  $\mathcal{C}$  and a vector  $\eta = (\eta_1, \dots, \eta_d) \in \mathcal{E}_r^{(d)}$  (note that actually  $\eta$  can be taken in  $\mathbb{Z}^d$  as the following algorithm allows us also to work in balls of larger radius; cf. Sect. 7.3). We want to find  $\varepsilon^* \in \partial\mathcal{E}_r^{(d)}$  such that  $U_{\varepsilon^*} \in \mathcal{C}$  and  $\text{dist}([U_\eta], [U_{\varepsilon^*}]) = \text{dist}([U_\eta], \mathcal{C})$ . We follow the steps below:

- (1) Let  $\eta' \in \mathbb{Z}^d$  and  $\sigma \in \text{Sym}(d)$  be such that  $\eta'_1 \geq \dots \geq \eta'_d$  and  $\eta' = \sigma \cdot \eta$ .
- (2) Define  $\tilde{\eta} = \eta' - \eta'_d \mathbf{1}$ .
- (3) Choose  $\varepsilon \in \mathcal{C}$  and identify  $h, k \in \{1, \dots, d\}$  such that  $\varepsilon_h = 0$  and  $\varepsilon_k = r$ .
- (4) Define  $\varepsilon'$  and  $\tau \in \text{Sym}(d)$  to satisfy  $\varepsilon' = \tau \cdot \varepsilon$  and  $\varepsilon'_1 = 0$  and  $\varepsilon'_d = r$ .
- (5) Set  $\varepsilon^* = \sigma^{-1} \cdot \varepsilon'$ .

We see from its construction that the element  $\varepsilon^*$  might not be unique. It is, however, not difficult to design an algorithm avoiding choices, once  $\mathcal{C}$  is given.

### 7 Spherical codes in Bruhat–Tits buildings

In this section we rephrase the results of this paper in terms of buildings. As we will see, Bruhat–Tits buildings are a way of talking about lattices and via these objects we can consider balls (in the sense of Sect. 2) “of any radius” at the same time. Moreover, it is worth mentioning that, on top of their central role in the theory of reductive groups, buildings have many different applications, for instance in optimization [9, 25], statistics [16, 20], and coding theory [32]. Though the employment of buildings in the study and construction of codes is not new, this seems to be the first time spherical codes in buildings are considered. In the applications of flags to network coding, spherical buildings are used. Such strategy, first introduced in [32], has found further developments in [4–6, 31] and variations in [22]. Moreover, Bruhat–Tits buildings also make their appearance in the study of holographic codes [35] as well as in the study of valued rank-metric codes [18].



### 7.1 From chain rings to valued fields

We choose a discretely valued field  $(K, \text{val})$ , with valuation ring  $\mathcal{O}_K$ , uniformizer  $\pi$ , and unique maximal ideal  $\mathfrak{m}_K = \mathcal{O}_K\pi \neq 0$ , in such a way that  $R \cong \mathcal{O}_K/\mathfrak{m}_K^r$ ; cf. [3, §1]. With a slight abuse of notation, we set  $\mathbf{e} = (e_1, \dots, e_d)$  to be the standard basis of  $K^d$  and we write  $\mathcal{O}_K^d$  for the free  $\mathcal{O}_K$ -module  $\mathcal{O}_K^d = \mathcal{O}_K e_1 \oplus \dots \oplus \mathcal{O}_K e_d$ . We will use the bar notation for the subobjects of  $V_r$ : if  $L \subseteq \mathcal{O}_K^d$ , then  $\bar{L}$  denotes the image of  $L$  in  $V_r$  under the natural projection  $\mathcal{O}_K^d \rightarrow V_r$ . Up to very small variations, our notation is compatible with the one from [19].

### 7.2 Lattices and buildings

An  $\mathcal{O}_K$ -lattice (or simply lattice) in  $K^d$  is a free  $\mathcal{O}_K$ -submodule of maximal rank  $d$ . The (homothety) class of a lattice  $L$  in  $K^d$  is

$$[L] = \{cL \mid c \in K \setminus \{0\}\} = \{\pi^n L \mid n \in \mathbb{Z}\},$$

while  $\text{End}_{\mathcal{O}_K}(L)$  denotes the endomorphism ring of  $L$  as an  $\mathcal{O}_K$ -submodule of  $K^d$ , i.e. the collection of  $\mathcal{O}_K$ -linear maps  $K^d \rightarrow K^d$  that stabilize  $L$ . Note that any two homothetic lattices have the same endomorphism ring. Moreover, lattices in  $K^d$  form one orbit under the natural action of  $\text{GL}_d(K)$  and so it will often not be restrictive to assume (up to base change) that a given lattice  $L$  is equal to  $\mathcal{O}_K^d$ . Additionally, each element of  $\mathcal{L}(V_r)$  can be obtained from a lattice  $\pi^r \mathcal{O}_K^d \subseteq L \subseteq \mathcal{O}_K^d$ , via projecting  $L$  to  $V_r$ :

$$\mathcal{O}_K^d \supseteq L \longmapsto \bar{L} = U_L \subseteq V_r. \tag{7.1}$$

We stress that the notions of equivalence for lattices and modules are compatible by means of the last projection. In line with the content of this paper, we define the affine building of  $\text{SL}_d(K)$  via its lattice class model [2, 23] and refer the interested reader to [1] for the more general description.

**Definition 7.1** The affine building  $\mathcal{B}_d(K)$  is an infinite simplicial complex such that

- (1) the vertex set is  $\mathcal{B}_d^0 = \{[L] \mid L \text{ is an } \mathcal{O}_K\text{-lattice in } K^d\}$ .
- (2)  $\{[L_1], \dots, [L_s]\}$  is a simplex in  $\mathcal{B}_d(K)$  if and only if, up to permutation of the indices and choice of representatives, one has  $L_1 \supset L_2 \supset \dots \supset L_s \supset \pi L_1$ .

The standard apartment of  $\mathcal{B}_d(K)$  is the subset  $\mathcal{A}$  of  $\mathcal{B}_d^0(K)$  of all lattice classes with representatives of the form

$$L_u = \mathcal{O}_K \pi^{u_1} e_1 \oplus \dots \oplus \mathcal{O}_K \pi^{u_d} e_d, \text{ where } u = (u_1, \dots, u_d) \in \mathbb{Z}^d.$$

More generally, one could define an apartment for any frame choice in  $K^d$ , cf. [19, Section 2]. Since (7.1) respects homothety classes, the new terminology allows us to consider the codes from Sect. 6 as one-apartment codes in buildings.

**Example 7.2** The rings from Examples 2.5 and 6.1 can both be expressed as quotients of a  $p$ -adic ring: in the first case  $R \cong \mathcal{O}_K/\mathfrak{m}_K^r = \mathbb{Z}_2/(2\mathbb{Z}_2)^5$  while in the second case  $R \cong \mathcal{O}_K/\mathfrak{m}_K^r = \mathbb{Z}_5/(5\mathbb{Z}_5)^2$ . When  $d = 2$  or  $d = 3$ , local pictures of  $\mathcal{B}_d(\mathbb{Q}_2)$  can be found in [7, Figures 2-5].

### 7.3 Distance and balls

The following distance was introduced in [19, Definition 3.1]. In view of Theorem 7.6, we use the same notation as in Definition 2.3.

**Definition 7.3** Let  $[L_1], [L_2] \in \mathcal{B}_d^0(K)$  be two homothety classes of lattices. Then

$$\text{dist}([L_1], [L_2]) = \min\{s \mid \text{there are } L'_1 \in [L_1], L'_2 \in [L_2] \text{ with } \pi^s L'_1 \subseteq L'_2 \subseteq L'_1\}.$$

As proven in [19, Lemma 3.2], the map  $\text{dist} : \mathcal{B}_d^0(K) \times \mathcal{B}_d^0(K) \rightarrow \mathbb{Z}$  defines a distance on  $\mathcal{B}_d^0(K)$ . In view of this, it makes sense to define balls in  $\mathcal{B}_d^0(K)$ .

**Definition 7.4** Let  $[L]$  be a lattice class in  $\mathcal{B}_d^0(K)$ . Then the (closed) ball of radius  $r$  and center  $[L]$  is

$$B_r([L]) = \{[L'] \in \mathcal{B}_d^0(K) \mid \text{dist}([L], [L']) \leq r\}$$

and its boundary is

$$\partial B_r([L]) = B_r([L]) \setminus B_{r-1}([L]) = \{[L'] \in \mathcal{B}_d^0(K) \mid \text{dist}([L'], [L]) = r\}.$$

If  $[L] = [\mathcal{O}_K^d]$ , we write simply  $B_r$  and  $\partial B_r$  for  $B_r([\mathcal{O}_K^d])$  and  $\partial B_r([\mathcal{O}_K^d])$ , respectively.

**Example 7.5** Assume  $d = 2$ . Then  $\mathcal{B}_2(K)$  is a  $(q + 1)$ -regular tree and  $\text{dist}$  equals the graph distance on  $\mathcal{B}_2(K)$ . Figure 1 represents  $B_5$  as a subset of  $\mathcal{B}_2(\mathbb{Q}_2)$ . In the same figure, the red points constitute  $\partial B_3$ . For more on buildings as trees, see for instance [40].

Balls in the affine building  $\mathcal{B}_d(K)$  naturally arise as the collections of stable lattice classes of ball orders [19, Section 5] and can be modeled by means of the submodules of  $V_r$ .

**Theorem 7.6** *The following are isometric:*

- (1)  $\mathcal{L}^0(V_r)$  and  $B_r$ ,
- (2)  $\partial \mathcal{L}(V_r)$  and  $\partial B_r$ ,
- (3)  $\mathcal{L}_e^0(V_r)$  and  $B_r \cap A$ ,
- (4)  $\partial \mathcal{L}_e(V_r)$  and  $\partial B_r \cap A$ .

**Proof** We show (1). To this end, we start by observing that  $[L] \in B_r$  if and only if there exists a representative  $L' \in [L]$  such that  $\pi^r \mathcal{O}_K \subseteq L' \subseteq \mathcal{O}_K^d$ . Since Equation 7.1 respects homothety, it is clear that  $B_r$  and  $\mathcal{L}^0(V_r)$  are in bijection via  $\mathcal{O}_K^d \rightarrow V_r$ . We show that the distances are also compatible. For this, let  $\pi^r \mathcal{O}_K \subseteq L_1, L_2 \subseteq \mathcal{O}_K^d$  be lattices and write  $U_1 = \overline{L_1}$  and  $U_2 = \overline{L_2}$ . Assume without loss of generality that  $U_1 = \tilde{U}_1$  and  $U_2 = \tilde{U}_2$ . Set  $\alpha = \text{dist}([L_1], [L_2])$  and let  $n_{12}$  and  $n_{21}$  be as in Definition 2.3. It follows from the definitions of  $U_1$  and  $U_2$  that  $L_1 \supseteq \pi^{n_{21}} L_2 \supseteq \pi^{n_{21}} (\pi^{n_{12}} L_1) = \pi^{n_{21}+n_{12}} L_1$  and in particular  $\alpha \leq n_{12} + n_{21}$ . Without loss of generality, let now  $m$  be a non-negative integer such that  $L_1 \supseteq \pi^m L_2 \supseteq \pi^\alpha L_1$ . Then it follows from the definitions of  $n_{21}$  and  $n_{21}$  that  $m \geq n_{21}$  and  $\alpha - m \geq n_{12}$ . Moreover, we have

$$\pi^{n_{12}+n_{21}} L_1 \subseteq \pi^\alpha L_1 \subseteq \pi^m L_2,$$

which in turn yields that  $\pi^{n_{12}+n_{21}-m} L_1 \subseteq L_2$ . It follows from the definition of  $n_{12}$  that  $m = n_{21}$  and thus we derive that  $\alpha \geq n_{12} + n_{21}$ . This proves (1) and so, as a consequence, also (2),(3), and (4). □

In view of the last theorem, we transport Definitions 3.1 and 3.2 to the framework of Bruhat–Tits buildings (see Fig. 4).

**Definition 7.7** A spherical code in  $B_r$  is a subset  $\mathcal{C}$  of  $B_r$  with  $|\mathcal{C}| \geq 2$ . The minimum distance of  $\mathcal{C}$  is

$$\text{dist}(\mathcal{C}) = \min\{\text{dist}([L_1], [L_2]) \mid [L_1], [L_2] \in \mathcal{C}, [L_1] \neq [L_2]\}.$$

The results from Sects. 4, 5, and 6 can now be also stated in terms of spherical codes in buildings. We close this section with a connection to an earlier paper. The following is the same as [19, Definition 5.5].

**Definition 7.8** A star configuration  $\star_r([L])$  with center  $[L]$  and radius  $r$  is a set

$$\star_r([L]) = \{[L_1], \dots, [L_d], [L_{d+1}]\}$$

such that the following hold:

- (1)  $\pi^r L \subseteq L_1, \dots, L_{d+1} \subseteq L$ ,
- (2) for each  $i \in \{1, \dots, d + 1\}$ , one has  $L_i/\pi^r L \cong R$ ,
- (3) for each  $i \in \{1, \dots, d + 1\}$ , one has  $L = \sum_{j \neq i} L_j$ .

**Proposition 7.9** A star configuration  $\star([\mathcal{O}_K^d])$  with center  $[\mathcal{O}_K^d]$  and radius  $r$  is a spherical code with  $\text{dist}(\star([\mathcal{O}_K^d])) = 2r$ .

**Proof** Write  $\star([\mathcal{O}_K^d]) = \{[L_1], \dots, [L_{d+1}]\}$ . In view of conditions (1)-(2)-(3) above, up to a convenient base change, we assume without loss of generality that

$$L_i = \begin{cases} \mathcal{O}_K e_i + \pi^r \mathcal{O}_K^d & \text{if } 1 \leq i \leq d, \\ \mathcal{O}_K(e_1 + \dots + e_d) + \pi^r \mathcal{O}_K^d & \text{if } i = d + 1. \end{cases}$$

It is clear that  $\star([\mathcal{O}_K^d])$  is a spherical code in  $B_r$ . Fix now  $i \neq j$ . Then Theorem 7.6 and Proposition 3.8 yield  $\text{dist}([L_i], [L_j]) = 2r$  and, the choice of  $i, j$  being arbitrary, it follows that  $\text{dist}(\star([L])) = 2r$ . □

The next corollary follows in a straightforward way from Definition 3.4, with the combination of Lemma 3.3, Theorem 7.6, and Proposition 7.9.

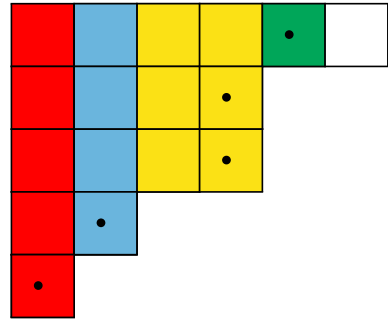
**Corollary 7.10** One has  $\text{dist}(d; R; d + 1) = 2r$ .

### 8 Counting elements of balls

This section is meant to add to the understanding of balls of modules, resp. balls in buildings in terms of their elements’ count. The results of this section are self contained and do not explicitly extend results from previous sections though they call for some new observations and questions; cf. Remarks 8.6 and 8.7.

We work here under the assumption of Sect. 7.1, though we do not necessarily assume that the residue field of  $K$  is finite. We leverage on results from [44], in particular its Sect. 3, to give a polynomial counting the lattice classes in the ball  $B_r$ . More precisely, we define  $b_r^{(d)}(X) \in \mathbb{Z}[X]$  such that, if  $q = |\mathcal{O}_K/\mathfrak{m}_K|$  is finite, then  $|B_r| = b_r^{(d)}(q)$ . We do so by writing  $b_r^{(d)}(X) = \sum_{\varepsilon \in \mathcal{E}_r^{(d)}} b_\varepsilon(X)$  where, contrarily to what is done in Sect. 6, here  $\mathcal{E}_r^{(d)}$  parametrizes

**Fig. 4** In this figure  $\varepsilon = (5, 4, 3, 3, 1, 0)$ . The different colors represent the different  $\tilde{\varepsilon}_j$ 's. The horizontal shifts represent the  $i_j$ 's while the vertical dots represent the  $r_{i_j}$ 's. Concretely,  $\ell = 4$  and  $(i_1, i_2, i_3, i_4) = (1, 2, 4, 5)$  and  $(r_{i_1}, r_{i_2}, r_{i_3}, r_{i_4}) = (1, 1, 2, 1)$



the elementary divisor types of lattices  $\pi^r \mathcal{O}_K^d \subset L \subseteq \mathcal{O}_K^d$  up to homothety. The role of the polynomial  $b_\varepsilon$  will be to count all lattice classes with the same elementary divisors. We fix  $\varepsilon \in \mathcal{E}_r^{(d)}$  and proceed to define  $b_\varepsilon(X)$ . For this, write  $\ell = -1 + |\{\varepsilon_1, \dots, \varepsilon_d\}| \geq 0$  and  $\{\varepsilon_1, \dots, \varepsilon_d\} = \{\tilde{\varepsilon}_1 > \dots > \tilde{\varepsilon}_{\ell+1} = 0\}$ : for an example see Fig. 4. Now, for each  $s \in \{1, \dots, \ell\}$ , define

$$i_s = |\{i \in \{1, \dots, d\} \mid \varepsilon_i \geq \tilde{\varepsilon}_s\}| \text{ and } r_{i_s} = \tilde{\varepsilon}_s - \tilde{\varepsilon}_{s+1}.$$

We set, moreover  $\Lambda_\varepsilon = \mathcal{O}_K^{d \times d} \cap \text{End}_{\mathcal{O}_K}(L_\varepsilon)$  and  $I = I(\varepsilon) = \{i_1 < \dots < i_\ell\}$ . In terms of these parameters, the endomorphism ring  $\text{End}_{\mathcal{O}_K}(L_\varepsilon)$  is denoted  $\Gamma_{I, \mathbf{r}}$  in [44] and is explicitly described in [44, Section 3.1]. In accordance with [44, Section 3], we finally define

$$b_\varepsilon(X) = \binom{d}{I}_{X^{-1}} X^{\sum_{i \in I} r_i \iota(d-i)}.$$

The next result is a direct consequence of the work in [44, Section 3]; cf. in particular [44, Equation (26)].

**Proposition 8.1** [44, Section 3] *Let  $[L] \in \mathcal{B}_d^0(K)$ . Then the following hold:*

(1) *for each  $\varepsilon \in \mathcal{E}_r^{(d)}$ , one has that  $b_\varepsilon(X)$  is a monic integral polynomial of degree*

$$\deg b_\varepsilon(X) = \sum_{i \in I(\varepsilon)} r_i \iota(d-i) = |\mathcal{O}_K^{d \times d} : \Lambda_\varepsilon|.$$

(2) *one has  $|\mathbf{B}_r([L])| = b_r^{(d)}(q) = \sum_{\varepsilon \in \mathcal{E}_r^{(d)}} b_\varepsilon(q)$ .*

**Example 8.2** For  $[L] \in \mathcal{B}_3^0(K)$ , we have

$$\begin{aligned} |\mathbf{B}_2([L])| &= b_2^{(3)}(q) \\ &= b_{(0,0,0)}(q) + b_{(1,0,0)}(q) + b_{(1,1,0)}(q) + b_{(2,0,0)}(q) + b_{(2,1,0)}(q) + b_{(2,2,0)}(q) \\ &= 1 + 2(q^2 + q + 1) + (2(q^4 + q^3 + q^2) + (q^4 + 2q^3 + 2q^2 + q)) \\ &= 3q^4 + 4q^3 + 6q^2 + 3q + 3. \end{aligned}$$

**Definition 8.3** Let  $\text{rev} : \mathbb{Z}^d \rightarrow \mathbb{Z}^d$  be the involution defined by

$$\varepsilon = (\varepsilon_1, \dots, \varepsilon_d) \mapsto \text{rev}(\varepsilon) = (\varepsilon_d, \dots, \varepsilon_1).$$

**Lemma 8.4** *Let  $\lambda$  be a non-negative integer and let  $\varepsilon, \varepsilon' \in \mathcal{E}_r^{(d)}$ . The following hold:*

(1) If  $\varepsilon + \text{rev } \varepsilon' = \lambda \mathbf{1}$ , then  $\text{deg } b_\varepsilon(X) = \text{deg } b_{\varepsilon'}(X)$ .

(2) If  $k \in \{1, \dots, d\}$  is such that

$$\varepsilon - \varepsilon' = (\delta_{ik}\lambda)_{i=1, \dots, d}$$

then  $\text{deg } b_\varepsilon(X) = \text{deg } b_{\varepsilon'}(X) + (d + 1 - 2k)\lambda$ .

**Proof** (1) Assume that  $\varepsilon + \text{rev } \varepsilon' = \lambda \mathbf{1}$ , equivalently, for all  $i \in \{1, \dots, d\}$ , one has  $\varepsilon_i = \lambda - \varepsilon_{d-i+1}$ . It follows from Proposition 8.1 (1) that

$$\begin{aligned} \text{deg } b_\varepsilon(X) &= |\mathcal{O}_K^{d \times d} : \Lambda_\varepsilon| = \sum_{1 \leq i < j \leq d} \varepsilon_i - \varepsilon_j = \sum_{1 \leq i < j \leq d} \varepsilon'_{d-j+1} - \varepsilon'_{d-i+1} \\ &= \sum_{1 \leq s < t \leq d} \varepsilon'_s - \varepsilon'_t = |\mathcal{O}_K^{d \times d} : \Lambda_{\varepsilon'}| = \text{deg } b_{\varepsilon'}(X). \end{aligned}$$

(2) Let  $k \in \{1, \dots, k\}$  be such that

$$\varepsilon_s = \begin{cases} \varepsilon'_s & \text{if } s \neq k, \\ \varepsilon'_s + \lambda & \text{if } s = k. \end{cases}$$

It follows from Proposition 8.1(1) that

$$\begin{aligned} \text{deg } b_\varepsilon(X) &= |\mathcal{O}_K^{d \times d} : \Lambda_\varepsilon| = \sum_{1 \leq i < j \leq d} \varepsilon_i - \varepsilon_j \\ &= \sum_{\substack{1 \leq i < j \leq d \\ i, j \neq k}} \varepsilon'_i - \varepsilon'_j + \sum_{k < j \leq d} (\varepsilon'_k + \lambda - \varepsilon'_j) + \sum_{1 \leq i < k} (\varepsilon'_i - \varepsilon'_j - \lambda) \\ &= \sum_{1 \leq s < t \leq d} \varepsilon'_s - \varepsilon'_t + (d + 1 - 2k)\lambda \\ &= |\mathcal{O}_K^{d \times d} : \Lambda_{\varepsilon'}| + (d + 1 - 2k)\lambda = \text{deg } b_{\varepsilon'}(X) + (d + 1 - 2k)\lambda. \end{aligned}$$

□

The proof of the next result shows that the asymptotics of  $|\text{B}_r([L])|$  is dominated by  $|\partial \text{B}_r([L])|$ , i.e. the dominating summands in  $b_r^{(d)}(X)$  correspond to elements of  $\partial \mathcal{E}_r^{(d)}$ .

**Theorem 8.5** *The following hold:*

(1) If  $d$  is even, then the leading term of  $b_r^{(d)}(X)$  is  $X^{d^2 r/4}$ .

(2) If  $d$  is odd, then the leading term of  $b_r^{(d)}(X)$  is  $(r + 1)X^{(d^2 - 1)r/4}$ .

**Proof** We prove (2). To this end, write  $d = 2k + 1$  and define the subset  $\mathcal{S}$  of  $\mathcal{E}_r^{(d)}$  to consist of all elements  $\varepsilon$  satisfying

$$\varepsilon_i = \begin{cases} r & \text{if } i < k + 1, \\ 0 & \text{if } i > k + 1. \end{cases}$$

Then  $\mathcal{S}$  has cardinality  $r + 1$ . Let moreover,  $\mathcal{S}_-$  and  $\mathcal{S}_+$  denote the subsets of  $\mathcal{E}_r^{(d)}$  of those elements that are smaller resp. bigger than elements in  $\mathcal{S}$ , with respect to the lexicographic order. Then  $\mathcal{E}_r^{(d)}$  equals the disjoint union  $\mathcal{S}_- \cup \mathcal{S} \cup \mathcal{S}_+$ . Let now  $\varepsilon \in \mathcal{E}_r^{(d)}$  and  $\varepsilon^* \in \mathcal{S}$ . If  $\varepsilon \in \mathcal{S}_-$ , then Lemma 8.4(2) yields that  $\text{deg } b_\varepsilon(X) < \text{deg } b_{\varepsilon^*}(X)$ . Moreover, Lemma 8.4(2) also ensures that, if  $\varepsilon \in \mathcal{S}$ , then  $\text{deg } b_\varepsilon(X) = \text{deg } b_{\varepsilon^*}(X)$ . Assume now that  $\varepsilon \in \mathcal{S}_+$ : we claim

that  $\deg b_\varepsilon(X) > \deg b_{\varepsilon^*}(X)$ . To this end, define  $\varepsilon' = \text{rev}(r\mathbf{1} - \varepsilon)$  and note that  $\varepsilon' \in \mathcal{S}_-$ . Now  $\deg b_\varepsilon(X) > \deg b_{\varepsilon^*}(X)$  thanks to Lemma 8.4(1) and so we conclude thanks to Proposition 8.1(1).

To prove (1), one can proceed in an analogous way by defining  $\mathcal{S}$  to be the singleton consisting of the vector whose first  $d/2$  entries are equal to  $r$  and all others are 0. □

**Remark 8.6** (Asymptotic of balls against Sperner codes) We have seen in Sect. 4.2 that, if  $\mathcal{C}$  is a Sperner code with parameters  $(d; R; \alpha)$  and  $e = \lceil d/2 \rceil$ , then the cardinality of  $\mathcal{C}$  is the same as that of  $\text{Gr}(e, V_{r+\alpha-1})$ . In particular, thanks to Proposition 8.1(1), we know that the leading term of the polynomial describing  $|\mathcal{C}|$  is equal to  $q^{(r+1-\alpha)e(d-e)}$ . Rewriting thus compactly the degree of the leading terms from Theorem 8.5 as  $re(d - e)$ , we get that the density of a Sperner code on  $\partial B_r$  is asymptotically equivalent (as  $q \rightarrow \infty$ ) to

$$q^{(1-\alpha)e(d-e)} \cdot \begin{cases} 1 & \text{if } d \text{ is even,} \\ (r + 1)^{-1} & \text{otherwise.} \end{cases}$$

**Remark 8.7** (Analogue of sphere packing bounds for odd distances) Let  $\mathcal{C}$  be a spherical code in  $B_r$ , as defined in Definition 7.7, of odd minimum distance  $2\alpha + 1$ . In this case, it is clear that any two elements  $[L]$  and  $[L']$  of  $\mathcal{C}$  satisfy  $B_\alpha([L]) \cap B_\alpha([L']) = \emptyset$ . It follows therefore that a very loose sphere packing bound on the cardinality of  $\mathcal{C}$  is given by

$$|\mathcal{C}| \leq \frac{|B_{r+\alpha}| - |B_{r-\alpha}|}{|B_\alpha| - 1},$$

which indeed, thanks to Theorem 8.5, is asymptotically no better than the known trivial bound given by  $|\partial B_r|$ . For a better asymptotic bound one should compute, for  $[L] \in \partial B_r$  the size of  $B_\alpha([L]) \cap \partial B_r$  yielding the tighter

$$|\mathcal{C}| \leq \frac{|\partial B_r|}{|B_\alpha([L]) \cap \partial B_r|};$$

compare with [21, Theorem 1.6.1]. What is the asymptotic behaviour of the right term of the last inequality as  $q \rightarrow \infty$ ?

**Acknowledgements** I wish to thank Gabriele Nebe for suggesting the investigation of spherical codes in the context of buildings and for her precious feedback on the content of this paper. In addition, I am thankful to Christopher Voll for pointing out and illustrating the results from [44]. I am grateful to Yassine El Maazouz, Alessandro Neri, Bernd Sturmfels, and Christopher Voll for their very helpful comments on an early version of this manuscript. I thank the two anonymous referees for their valuable reports, which helped improve the exposition of this paper. This project was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Project-ID 286237555 – TRR 195.

**Funding** Open access funding provided by Università degli Studi di Trento within the CRUI-CARE Agreement.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

## References

1. Abramenko P., Brown K.S.: Buildings: Theory and Applications, vol. 248. Graduate Texts in Mathematics. Springer, New York (2008).
2. Abramenko P., Nebe G.: Lattice chain models for affine buildings of classical type. *Math. Ann.* **322**(3), 537–562 (2002).
3. Alabiad S., Alkhamees Y.: On classification of finite commutative chain rings. *AIMS Math.* **7**(2), 1742–1757 (2022).
4. Alonso-González C., Navarro-Pérez M.A.: Cyclic orbit flag codes. *Des. Codes Cryptogr.* **89**(10), 2331–2356 (2021).
5. Alonso-González C., Navarro-Pérez M.A., Soler-Escrivà X.: Flag codes from planar spreads in network coding. *Finite Fields Appl.* **68**(101745), 20 (2020).
6. Alonso-González C., Navarro-Pérez M.A., Soler-Escrivà X.: Optimum distance flag codes from spreads via perfect matchings in graphs. *J. Algebraic Combin.* **54**(4), 1279–1297 (2021).
7. Bekker B., Solleveld M.: The buildings gallery: visualizing buildings. *J. Math. Arts* **16**(1–2), 11–28 (2022).
8. Blake I.F.: Codes over integer residue rings. *Inf. Control* **29**(4), 295–300 (1975).
9. Bürgisser P., Franks C., Garg A., Oliveira R., Walter M., Wigderson A.: Towards a theory of non-commutative optimization: geodesic 1st and 2nd order methods for moment maps and polytopes. In: 2019 IEEE 60th Annual Symposium on Foundations of Computer Science, pp. 845–861. IEEE Comput. Soc. Press, Los Alamitos, CA (2019).
10. Byrne E., Horlemann A.-L., Khathuria K., Weger V.: Density of free modules over finite chain rings. (2022). [arXiv:2106.09403](https://arxiv.org/abs/2106.09403).
11. Calderbank A.R., Sloane N.J.A.: Modular and  $p$ -adic cyclic codes. *Des. Codes Cryptogr.* **6**(1), 21–35 (1995).
12. Clark W.E., Liang J.J.: Enumeration of finite commutative chain rings. *J. Algebra* **27**, 445–453 (1973).
13. Cohen G., Gaubert S., Quadrat J.-P.: Duality and separation theorems in idempotent semimodules. *Linear Algebra Appl.* **379**, 395–422 (2004) **Tenth Conference of the International Linear Algebra Society**.
14. Conway J.H., Sloane N.J.A.: Sphere packings, lattices and groups, volume 290 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, 2nd edn. Springer, New York (1993). With additional contributions by E. Bannai, R.E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.
15. Dinh H.Q., López-Permouth S.R.: Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inf. Theory* **50**(8), 1728–1744 (2004).
16. El Maazouz Y.: The Gaussian entropy map in valued fields. [arXiv:2101.00767](https://arxiv.org/abs/2101.00767) (2021).
17. El Maazouz Y., Hahn M.A., Nebe G., Stanojkovski M., Sturmfels B.: Orders and polytropes: matrix algebras from valuations. *Beitr. Algebra Geom.* **63**(3), 515–531 (2022).
18. El Maazouz Y., Hahn M.A., Neri A., Stanojkovski M.: Valued rank-metric codes. 2021. [arXiv:2104.03216](https://arxiv.org/abs/2104.03216).
19. El Maazouz Y., Nebe G., Stanojkovski M.: Bolytrope orders. *Int. J. Number Theory* (2022). <https://www.worldscientific.com/doi/10.1142/S1793042123500471>.
20. El Maazouz Y., Tran N.M.: Statistics of Gaussians on local fields and their tropicalizations. (2019). [arXiv:1909.00559](https://arxiv.org/abs/1909.00559).
21. Ericson T., Zinoviev V.: Codes on Euclidean Spheres, vol. 63. North-Holland Mathematical Library. North-Holland Publishing Co., Amsterdam (2001).
22. Fourier G., Nebe G.: Degenerate flag varieties in network coding. *Adv. Math. Commun.* (2021). <https://www.aims-science.org/article/doi/10.3934/amc.2021027>.
23. Garrett P.: Buildings and Classical Groups. Chapman & Hall, London (1997).
24. Greferath M.: Cyclic codes over finite rings. *Discret. Math.* **177**(1–3), 273–277 (1997).
25. Hamada M., Hirai H.: Computing the nc-rank via discrete convex optimization on CAT(0) spaces. *SIAM J. Appl. Algebra Geom.* **5**(3), 455–478 (2021).
26. Honold T., Landjev I.: Linear codes over finite chain rings. *Electron. J. Comb.* **7**, 1–22 (2000) (**Research Paper 11**).
27. Hou X.-D.: Finite commutative chain rings. *Finite Fields Appl.* **7**(3), 382–396 (2001).
28. Joswig M.: Essentials of Tropical Combinatorics. Graduate Studies in Mathematics, vol. 219. American Mathematical Society, Providence, RI (2021).
29. Joswig M., Kulas K.: Tropical and ordinary convexity combined. *Adv. Geom.* **10**(2), 333–352 (2010).
30. Khaleghi A., Silva D., Kschischang F.R.L.: Subspace codes. In: *Cryptography and Coding*, volume 5921 of *Lecture Notes in Comput. Sci.*, pp. 1–21. Springer, Berlin (2009).
31. Kurz S.: Bounds for flag codes. *Des. Codes Cryptogr.* **89**(12), 2759–2785 (2021).

32. Liebhold D., Nebe G., Vazquez-Castro A.: Network coding with flags. *Des. Codes Cryptogr.* **86**(2), 269–284 (2018).
33. Liu X., Liu H.: LCD codes over finite chain rings. *Finite Fields Appl.* **34**, 1–19 (2015).
34. Maclagan D., Sturmfels B.: *Introduction to Tropical Geometry*. Graduate Studies in Mathematics, vol. 161. American Mathematical Society, Providence, RI (2015).
35. Marcolli M.: Holographic codes on Bruhat–Tits buildings and Drinfeld symmetric spaces. (2018). [arXiv:1801.09623](https://arxiv.org/abs/1801.09623).
36. Michałek M., Sturmfels B.: *Invitation to Nonlinear Algebra*. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI (2021).
37. Micheli G., Neri A.: New lower bounds for permutation codes using linear block codes. *IEEE Trans. Inf. Theory* **66**(7), 4019–4025 (2020).
38. Norton G.H., Sălăgean A.: On the structure of linear and cyclic codes over a finite chain ring. *Appl. Algebra Eng. Commun. Comput.* **10**(6), 489–506 (2000).
39. Rota G.-C., Harper L.H.: Matching theory, an introduction. In: *Advances in Probability and Related Topics*, vol. 1, pp. 169–215. Dekker, New York (1971).
40. Serre J.-P.: *Trees*. Springer Monographs in Mathematics. Springer, Berlin (2003). Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation.
41. Sperner E.: Ein Satz über Untermengen einer endlichen Menge. *Math. Z.* **27**(1), 544–548 (1928).
42. Stanley R.P.: Some applications of algebra to combinatorics, vol. 34, pp. 241–277. (1991). *Combinatorics and theoretical computer science* (Washington, DC, 1989).
43. Stanley R.P.: *Enumerative combinatorics*. Vol. 1, vol 49 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge (1997). With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.
44. Voll C.: Functional equations for zeta functions of groups and rings. *Ann. Math. (2)* **172**(2), 1181–1218 (2010).
45. Wang J.: Proof of a conjecture on the Sperner property of the subgroup lattice of an abelian  $p$ -group. *Ann. Comb.* **2**(1), 85–101 (1998).

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.