ON PERMUTATION-INVARIANT CONSTRUCTION OF GLUED LATTICES

MARIA FERNANDA ZORDAN BONINI AND LENNY FUKSHANSKY

Abstract. Given a permutation τ on n letters, we consider lattices spanned by an orbit of one vector $\boldsymbol{x}$ in $\mathbb{R}^n$ under the action of τ by permutation of the coordinates. Such lattices generalize the important class of cyclic lattices and have previously been studied in [3], where a bound on their rank was established. We prove a sufficient condition on $\boldsymbol{x}$ for this bound to be achieved. We further investigate the structure of such permutation-invariant lattices, proving that they are glued by the permuted vector from the orthogonal cyclic blocks and giving a determinant formula for the lattice in terms of determinants of these blocks and the norm of the permuted vector. In the case $\boldsymbol{x}$ is an integer vector, these blocks are sublattices of the root lattices A_k in respective dimensions with root lattices themselves and their glued direct sums also realizable by this construction. We also exhibit a glued construction of permutation-invariant algebraic integral lattices from collections of cyclic number fields. Finally, we prove a strengthened version of a previous result of [4] on a related construction of well-rounded lattices spanned by sets of algebraic conjugates.

1. Introduction

Let $n \geq 2$ and write S_n for the permutation group on n letters. This group acts on $\mathbb{R}^n$ by permutation of the coordinates. Taking the standard representation of S_n in $\mathrm{GL}_n(\mathbb{Z})$ via permutation matrices, we can also view this action as left multiplication. Fix an element $\tau \in S_n$, then for each $\boldsymbol{x} \in \mathbb{R}^n$ we write $\tau(\boldsymbol{x})$ for the image of $\boldsymbol{x}$ under the action by τ. A lattice $L \subset \mathbb{R}^n$ (i.e., a discrete subgroup) is called *τ-invariant* if $\tau(L) = L$, which is equivalent to saying that τ is in $\mathrm{Aut}(L)$, the automorphism group of L, defined as

$$\mathrm{Aut}(L) = \left\{U \in \mathrm{GL}_n(\mathbb{Z}) : (U\boldsymbol{x})^\top (U\boldsymbol{y}) = \boldsymbol{x}^\top \boldsymbol{y},\ \forall\ \boldsymbol{x}, \boldsymbol{y} \in L\right\}.$$

We refer to all such lattices as *permutation-invariant*; they generalize the class of *cyclic* lattices, which are the τ-invariant lattices for $\tau = (1\ \ldots\ n)$. Cyclic lattices were introduced by D. Micciancio in the context of lattice cryptography [7], [8] and then studied by many other authors. Permutation-invariant lattices were studied in [3] with a special focus on lattices of the form

$$L_\tau(\boldsymbol{x}) = \mathrm{span}_{\mathbb{Z}} \left\{\tau^k(\boldsymbol{x}) : 0 \leq k \leq |\tau| - 1\right\},$$

where $\boldsymbol{x} \in \mathbb{R}^n$ and $|\tau|$ is the order of the element τ in the group S_n. We will call such lattices *simple τ-invariant*, generated by permutations of $\boldsymbol{x}$ under τ; this is a generalization of the *simple cyclic* lattices that were studied in [5]. Simple cyclic

2020 *Mathematics Subject Classification.* Primary: 11H06, 11H56, 11R04, 11R09.

Key words and phrases. permutation-invariant lattices, cyclic lattices, glued lattices, root lattices, number field lattices.

and, more generally, simple permutation-invariant lattices are especially useful for cryptographic applications due to their very compact description as orbits of just one vector under a given permutation. A just-announced breakthrough result by D. Wan [12] asserts that the Shortest Vector Problem (SVP) is NP-hard on cyclic (and hence, on permutation-invariant) lattices, establishing them as excellent candidates for secure crypto-scheme design. Further, cyclic lattices are naturally analogous to cyclic codes construction in coding theory (see, e.g. Chapters 7-8 of [6]); similarly, permutation-invariant lattices are analogous to the more recently introduced class of generalized quasi-cyclic codes (see, e.g, [10]). The goal of this paper is to study the structure of simple permutation-invariant lattices.

For each $\boldsymbol{x} \in \mathbb{R}^n$, the lattice $L_\tau(\boldsymbol{x})$ is τ-invariant by construction, however its rank can vary. Define

$$\mathrm{o}_\tau = \max\left\{\mathrm{rk}\, L_\tau(\boldsymbol{x}) : \boldsymbol{x} \in \mathbb{R}^n\right\},$$

then Lemma 2.1 of [3] asserts that $\mathrm{o}_\tau \leq n - \ell + 1$, where ℓ is the number of cycles in a disjoint cycle decomposition of τ; the bound is achieved if these cycles have pairwise relatively prime lengths. The first question we want to address is for which vectors $\boldsymbol{x} \in \mathbb{R}^n$ is $\mathrm{rk}\, L_\tau(\boldsymbol{x}) = \mathrm{o}_\tau$?

Let $\tau = c_1 \cdots c_\ell$ be the disjoint cycle decomposition for τ with $k_j = |c_j|$ for each $1 \leq j \leq \ell$, ordered so that $k_1 \leq \cdots \leq k_\ell$. Then $\sum_{j=1}^{\ell} k_j = n$, and for a vector $\boldsymbol{x} \in \mathbb{R}^n$ we write

$$\boldsymbol{x} = \begin{pmatrix} \boldsymbol{x}_1 \\ \vdots \\ \boldsymbol{x}_\ell \end{pmatrix}, \text{ so } \tau(\boldsymbol{x}) = \begin{pmatrix} c_1(\boldsymbol{x}_1) \\ \vdots \\ c_\ell(\boldsymbol{x}_\ell) \end{pmatrix},$$

where each block $\boldsymbol{x}_j = (x_{j1}, \ldots, x_{jk_j})^\top \in \mathbb{R}^{k_j}$. For each $1 \leq j \leq \ell$, define

$$d(\boldsymbol{x}_j) = \dim_{\mathbb{Q}} \mathrm{span}_{\mathbb{Q}}\{x_{j1}, \ldots, x_{jk_j}\},$$

and analogously for any vector with real coordinates. With this notation, we can state our first observation.

Proposition 1.1. *If $d(\boldsymbol{x}_j) \geq k_j$ for each $1 \leq j \leq \ell$, then* $\mathrm{rk}\, L_\tau(\boldsymbol{x}) = \mathrm{o}_\tau$.

We prove Proposition 1.1 in Section 2. The hypothesis of this proposition is a sufficient condition for $\mathrm{rk}\, L_\tau(\boldsymbol{x})$ to be equal to o_τ, however it is not necessary. In fact, some of the constructions of such lattices we show in Section 3 do not satisfy this condition. Our main result describes the structure of simple permutation-invariant lattices.

Theorem 1.2. *Let $2 \leq k_1 < \cdots < k_\ell$ be pairwise relatively prime integers, $n = \sum_{i=1}^{\ell} k_i$, and $\tau = c_1 \ldots c_\ell \in S_n$, where $c_1, \ldots, c_\ell$ are disjoint cycles of lengths $k_1, \ldots, k_\ell$, respectively. Let $\boldsymbol{x} \in \mathbb{R}^n$ be a vector such that* $\mathrm{rk}\, L_\tau(\boldsymbol{x}) = n - \ell + 1$. *Then*

$$L_\tau(\boldsymbol{x}) = \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{x}, \bigoplus_{i=1}^{\ell} M_i \right\}, \tag{1}$$

where each of the mutually orthogonal blocks M_i is a cyclic lattice in the corresponding space $\mathbb{R}^{k_i}$ embedded as the respective coordinate subspace of $\mathbb{R}^n$ and

$\boldsymbol{x} \notin \bigoplus_{i=1}^{\ell} M_i$. *Further,* $\operatorname{rk} M_i = k_i - 1$ *for each* $1 \le i \le \ell$ *and*

$$M_i \subset \mathbf{1}_{k_i}^{\perp} := \left\{ \boldsymbol{z} \in \mathbb{R}^{k_i} : \sum_{j=1}^{k_i} z_j = 0 \right\}.$$

Conversely, given a collection of simple cyclic lattices $M_i \subset \mathbf{1}_i^{\perp}$, $1 \le i \le \ell$ *with* $\operatorname{rk} M_i = k_i - 1$, *there exist infinitely many vectors* $\boldsymbol{x} \in \mathbb{R}^n$ *for which* (1) *holds so that* $\boldsymbol{x} \notin \bigoplus_{i=1}^{\ell} M_i$ *and* $\operatorname{rk} L_\tau(\boldsymbol{x}) = n - \ell + 1$.

We refer to $L_\tau(\boldsymbol{x})$ as the lattice *glued* from the blocks M_i with the *glue vector* $\boldsymbol{x}$ (see Section 4.3 of [1] for the details of gluing theory). Hence, the τ-permutation orbit of the glue vector $\boldsymbol{x}$ results in the glued lattice construction. We prove Theorem 1.2 in Section 3, where we also describe in details the construction of the blocks M_i from the glue vector $\boldsymbol{x}$. Further, we give a formula for the determinant of $L_\tau(\boldsymbol{x})$ in terms of the determinants of the blocks and norm of $\boldsymbol{x}$ as well as briefly discuss the successive minima of $L_\tau(\boldsymbol{x})$ in Remark 3.1. In the case when $\boldsymbol{x} \in \mathbb{Z}^n$, these blocks lie in the *root lattices*

$$A_{k_i-1} = \left\{ \boldsymbol{z} \in \mathbb{Z}^{k_i} : \sum_{j=1}^{k_i} z_j = 0 \right\},$$

which are generated by the *roots*, i.e., vectors of squared Euclidean norm 2. We demonstrate a specific example of a glue vector resulting in the blocks being equal to A_{k_i-1}, in which case the determinant and successive minima are particularly easy to compute.

On the other hand, we can produce infinite families of simple permutation-invariant lattices satisfying the condition of Proposition 1.1. A lattice is called *integral* if the inner product of any two vectors in it is in $\mathbb{Z}$; a lattice is called *algebraic* if it is the image of a free $\mathbb{Z}$-module in a number field under the Minkowski embedding of this number field into a Euclidean space with the trace-induced Euclidean norm. In Section 4, we review the necessary number field notation and describe infinite families of integral simple permutation-invariant algebraic lattices satisfying the hypothesis of Proposition 1.1. They are also glued together from cyclic algebraic orthogonal blocks, as described in Theorem 1.2. Finally, in the Appendix (Section 5) we revisit the related construction of lattices spanned by full sets of algebraic conjugates, considered in [4] and prove a strengthening of the main result of [4]. We are now ready to proceed.

2. Permuting vectors with linearly independent coordinates

In this section, we prove Proposition 1.1. Let $m = \mathrm{o}_\tau$ and suppose that $\operatorname{rk} L_\tau(\boldsymbol{x})$ is smaller than m, then there exist integer coefficients $a_0, \dots, a_{m-1}$ such that

$$\sum_{k=0}^{m-1} a_k \tau^k(\boldsymbol{x}) = \mathbf{0},$$

meaning that

$$\sum_{k=0}^{m-1} a_k c_j^k(\boldsymbol{x}_j) = \mathbf{0}, \ \forall\ 1 \le j \le \ell. \tag{2}$$

Grouping together terms with the same coordinate x_{ji} for each $1 \le j \le \ell$, $1 \le i \le k_j$ in each equation of this linear system, we obtain a system of equations in x_{ji} with coefficients being sums of a_k's. Namely,

$$q_0 x_{j1} + q_1 x_{j2} + \cdots + q_{k_j - 1} x_{jk_j} = 0,$$

where $q_r = \sum_{t \equiv r \pmod{k_j}} a_t$ for each $0 \le r \le k_j - 1$. For example, if $\ell = 2$, $k_1 = 2$, $k_2 = 3$, our system becomes:

$$\begin{gathered}(a_0 + a_2)x_{11} + (a_1 + a_3)x_{12} = 0, (a_1 + a_3)x_{11} + (a_0 + a_2)x_{12} = 0,\\ (a_0 + a_3)x_{21} + a_1 x_{22} + a_2 x_{23} = 0, a_1 x_{21} + a_2 x_{22} + (a_0 + a_3)x_{23} = 0,\\ a_2 x_{21} + (a_0 + a_3)x_{22} + a_1 x_{23} = 0.\end{gathered}$$

Since $d(\boldsymbol{x}_j) \ge k_j$ for each $1 \le j \le \ell$, we must have all the coefficients (which are sums of a_k's independent of x_{ji}'s) in this system equal to 0. For instance, in the example above, it amounts to

$$a_0 + a_2 = 0,\ a_1 + a_3 = 0,\ a_0 + a_3 = 0,\ a_1 = 0,\ a_2 = 0.$$

This means that there exist integer coefficients $a_0, \dots, a_{m-1}$, not all zero, such that the corresponding linear system is identically zero for any choice of $\boldsymbol{x} \in \mathbb{R}^n$. This means that

$$\max\left\{\operatorname{rk} L_\tau(\boldsymbol{x}) : \boldsymbol{x} \in \mathbb{R}^n\right\} < m,$$

contradicting the definition of o_τ. Hence, we must have $\operatorname{rk} L_\tau(\boldsymbol{x}) = \mathrm{o}_\tau$ for each

$$\boldsymbol{x} = (\boldsymbol{x}_1, \dots, \boldsymbol{x}_\ell)^\top \in \mathbb{R}^{k_1} \times \cdots \times \mathbb{R}^{k_\ell}$$

with $d(\boldsymbol{x}_j) \ge k_j$.

3. Gluing construction

In this section we describe the structure of simple permutation-invariant lattices in $\mathbb{R}^n$, proving Theorem 1.2. Let $\tau = c_1 \cdots c_\ell \in S_n$ with $k_i = |c_i|$ for each $1 \le i \le \ell$ and $\gcd(k_i, k_j) = 1$ for $i \ne j$. Let

$$\boldsymbol{x} = (\boldsymbol{x}_1, \dots, \boldsymbol{x}_\ell)^\top \in \mathbb{R}^n \text{ with each } \boldsymbol{x}_i \in \mathbb{R}^{k_i}$$

be such that $\operatorname{rk} L_\tau(\boldsymbol{x}) = \mathrm{o}_\tau$. Since the cycle lengths are relatively prime, the Chinese Remainder Theorem implies that for each $1 \le i \le \ell$ and $1 \le t(i) \le k_i - 1$ there exists a power $0 \le m_{it(i)} < k_1 \cdots k_\ell = |\tau|$ such that $c_j^{m_{it(i)}} = c_j^{k_j}$ for all $j \ne i$ and $c_i^{m_{it(i)}} = c_i^{t(i)}$. This means that the vectors $\boldsymbol{x}$ and $\tau^{m_{it(i)}}(\boldsymbol{x})$ will have different coordinates only in the i-th block. Then define

$$\boldsymbol{z}_{it(i)} = \boldsymbol{x} - \tau^{m_{it(i)}}(\boldsymbol{x}) = \left(\mathbf{0}, \dots, \mathbf{0}, \boldsymbol{x}_i - c_i^{t(i)}(\boldsymbol{x}_i), \mathbf{0}, \dots, \mathbf{0}\right) \in L_\tau(\boldsymbol{x}). \tag{3}$$

Notice that the coordinates of each $\boldsymbol{x}_i - c_i^{t(i)}(\boldsymbol{x}_i)$ (and hence, the coordinates of $\boldsymbol{z}_{it(i)}$) add up to 0. In particular, this means that for $\boldsymbol{x} \in \mathbb{Z}^n$, each $\boldsymbol{z}_{it(i)} \in A_{k_i - 1}$, the corresponding root lattice. All the vectors $\boldsymbol{z}_{it(i)}$ are linearly independent and there are a total of $\sum_{i=1}^{\ell}(k_i - 1) = n - \ell$ of them. Further,

$$\begin{aligned} L_\tau(\boldsymbol{x}) &= \operatorname{span}_{\mathbb{Z}}\left\{\boldsymbol{x}, \boldsymbol{z}_{it(i)} : 1 \le i \le \ell,\ 1 \le t(i) \le k_i - 1\right\} \\ &= \operatorname{span}_{\mathbb{Z}}\left\{\boldsymbol{x}, M_i : 1 \le i \le \ell\right\}, \end{aligned}$$

where $M_i = \operatorname{span}_{\mathbb{Z}} \left\{ \boldsymbol{z}_{it(i)} : 1 \le t(i) \le k_i - 1 \right\}$ for each $1 \le i \le \ell$ is invariant under the cyclic permutation c_i, and the blocks M_i, M_j are mutually orthogonal for all $i \neq j$. Thus

$$L_\tau(\boldsymbol{x}) = \operatorname{span}_{\mathbb{Z}} \left\{ \boldsymbol{x}, \bigoplus_{i=1}^{\ell} M_i \right\}. \tag{4}$$

In particular, if $\boldsymbol{x} \in \mathbb{Z}^n$, then

$$L_\tau(\boldsymbol{x}) \subseteq \operatorname{span}_{\mathbb{Z}} \left\{ \boldsymbol{x}, \bigoplus_{i=1}^{\ell} A_{k_i - 1} \right\}.$$

In the reverse direction, suppose that for each $1 \le i \le \ell$, $M_i \subset \mathbf{1}_i^{\perp} \subset \mathbb{R}^{k_i}$ is a cyclic lattice of rank $k_i - 1$ and let $\boldsymbol{z}_{i1}, \ldots, \boldsymbol{z}_{i(k_i-1)}$ be a basis for M_i. Let us construct a vector $\boldsymbol{x} \in \mathbb{R}^n$ so that (4) holds. Take any real numbers $\alpha_1, \ldots, \alpha_\ell$, and for each $1 \le i \le \ell$, define the i-th block of $\boldsymbol{x}$ to be

$$\boldsymbol{x}_i = \left(\alpha_i, \alpha_i + z_{i2}, \ldots, \alpha_i + \sum_{l=1}^{j} z_{il}, \ldots, \alpha_i - z_{i1} \right)^{\top},$$

and let $\boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_\ell)^{\top}$. Using Chinese Remainder Theorem same way as above, we obtain vectors $(\mathbf{0}, \ldots, \boldsymbol{z}_i, \ldots, \mathbf{0})$ for each $1 \le i \le \ell$ as difference vectors of $\boldsymbol{x}$ and its permutations by appropriate powers of τ. This gives (4).

Remark 3.1. One advantage of this family of simple permutation invariant lattices $L_\tau(\boldsymbol{x})$ is that some of their geometric invariants can be easy to compute. Recall that the *determinant* of $L_\tau(\boldsymbol{x})$ is the volume of its fundamental domain, which is equal to the absolute value of the determinant of any basis matrix, and the *successive minima* $0 < \lambda_1 \le \cdots \le \lambda_{n-\ell+1}$ of $L_\tau(\boldsymbol{x})$ are defined as

$$\lambda_i = \min \left\{ t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}} \left(\mathbb{B}_{n-\ell+1}(t) \cap L_\tau(\boldsymbol{x}) \right) \ge i \right\},$$

where $\mathbb{B}_{n-\ell+1}(t)$ is a ball of radius t centered at the origin in $\mathbb{R}^{n-\ell+1}$. Then determinant of $L_\tau(\boldsymbol{x})$ can be computed as the product of determinants of the cyclic orthogonal blocks times the norm of the projection of $\boldsymbol{x}$ in the direction orthogonal to the hyperplane V spanned by all those blocks, i.e.,

$$\det L_\tau(\boldsymbol{x}) = \left(\prod_{i=1}^{\ell} \det M_i \right) \|\boldsymbol{x}\| \sin\theta, \tag{5}$$

where θ is the angle $\boldsymbol{x}$ makes with V. Further, if $\theta \in [\pi/3, \pi/2]$ (a sufficient, not necessary condition), then the successive minima of $L_\tau(\boldsymbol{x})$ are the successive minima of the orthogonal blocks and $\|\boldsymbol{x}\|$.

Let us consider a particular example. Let

$$\boldsymbol{x} = \left(\boldsymbol{e}_1^1, \ldots, \boldsymbol{e}_1^\ell \right)^{\top} \in \mathbb{Z}^n,$$

where $\boldsymbol{e}_1^i$ is the first standard basis vector in $\mathbb{R}^{k_i}$. Then the difference vector $\boldsymbol{z}_{it(i)}$ as in (3) has first coordinate in the i-th block equal to 1, $t(i)$-th coordinate in the i-th block equal to -1 and the rest of the coordinates equal to 0. For each $1 \le i \le \ell$,

the collection of i-th blocks of vectors $\boldsymbol{z}_{it(i)}$ spans the root lattice A_{k_i-1} with $\boldsymbol{z}_{it(i)}$ being the spanning roots, and so

$$L_\tau(\boldsymbol{x}) = \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{x}, \bigoplus_{i=1}^{\ell} A_{k_i-1} \right\} \tag{6}$$

is glued from the root lattice blocks by the glue vector $\boldsymbol{x}$. The situation is special when $\ell = 2$. In this case, the glue vector $\boldsymbol{x}$ is also a root, as it has two coordinates equal to 1 and the rest equal to 0. Thus, the resulting lattice generated by $n-1$ roots is $L_\tau(\boldsymbol{x}) = A_{n-1}$. Notice, in particular, that this last statement is independent of the lengths of the cycles c_1 and c_2. Hence, in the case $\ell = 2$, the geometric properties of $L_\tau(\boldsymbol{x})$ are well-understood. In the case $\ell > 2$, we can apply (5) to obtain

$$\det L_\tau(\boldsymbol{x}) = \left\{ \left(\prod_{i=1}^{\ell} k_i \right) \times \left(\sum_{i=1}^{\ell} \frac{1}{k_i} \right) \right\}^{1/2} = \left\{ \sum_{i=1}^{\ell} \left(\prod_{j=1, j\neq i}^{\ell} k_j \right) \right\}^{1/2},$$

since determinant of each block A_{k_i-1} is $\sqrt{k_i}$ and the norm of the projection of $\boldsymbol{x}$ in the direction orthogonal to the hyperplane V spanned by all those blocks is given by $\sqrt{\sum_{i=1}^{\ell} \frac{1}{k_i}}$. The first $n-\ell$ successive minima of $L_\tau(\boldsymbol{x})$ in this case are equal to $\sqrt{2}$, successive minima of the orthogonal blocks A_{k_i-1}, while the last one is $\sqrt{\ell} = \|\boldsymbol{x}\|$.

4. Gluing algebraic integral lattices

In this section, we use the gluing construction of Section 3 in the specific context of lattices coming from number fields, exhibiting a construction of algebraic integral permutation-invariant glued lattices. We start with some notation. Let $f(x) \in \mathbb{Z}[x]$ be an irreducible monic polynomial of degree n so that its Galois group $G(f) = \langle c \rangle \leq S_n$ is cyclic and $c = (1 \ \ldots \ n)$ is the standard generating n-cycle. Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be the roots of $f(x)$ ordered so that $\alpha_j = c^{j-1}(\alpha_1)$ for $1 \leq j \leq n$. Then $K(f) = \mathbb{Q}[x]/(f(x))$ is an extension of $\mathbb{Q}$ of degree n, thus it is the splitting field of $f(x)$. Let $\sigma_1, \ldots, \sigma_n : K(f) \to \mathbb{C}$ be the embeddings of $K(f)$ with r_1 of them real and $2r_2$ complex, coming in conjugate pairs, i.e., $n = r_1 + 2r_2$. We identify the roots of $f(x)$ with the images of α_1 under these embeddings, i.e., $\alpha_j = c^{j-1}(\alpha_1) = \sigma_j(\alpha_1)$ as a complex number, for all $1 \leq j \leq n$. The Minkowski embedding

$$\Sigma_{K(f)} = (\sigma_1, \ldots, \sigma_n) : K(f) \hookrightarrow \mathbb{C}^n$$

takes $K(f)$ into the space $K(f)_{\mathbb{R}} := K(f) \otimes_{\mathbb{Q}} \mathbb{R}$, which can be viewed as a subspace of

$$\left\{ (\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : y_{r_2+j} = \bar{y}_j \ \forall \ 1 \leq j \leq r_2 \right\} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \subset \mathbb{C}^n,$$

where in the last containment each copy of $\mathbb{R}$ is identified with the real part of the corresponding copy of $\mathbb{C}$. This is a Euclidean space where the Euclidean inner product is induced by the number field trace in the sense that

$$\left\langle \Sigma_{K(f)}(\beta), \Sigma_{K(f)}(\gamma) \right\rangle = \mathrm{Tr}_{K(f)}(\beta\bar{\gamma}) = \sum_{j=1}^{n} c^{j-1}(\beta\bar{\gamma}) \in \mathbb{Q},$$

for all $\beta, \gamma \in K(f)$. In particular, $\left\langle \Sigma_{K(f)}(\beta), \Sigma_{K(f)}(\gamma) \right\rangle \in \mathbb{Z}$ for all $\beta, \gamma \in \mathcal{O}_{K(f)}$.

We write

$$\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)^\top \in K(f)_{\mathbb{R}}$$

for the image of α_1 under $\Sigma_{K(f)}$ and let the n-cycle c act on $\boldsymbol{\alpha}$ by permutation of the coordinates. Notice that, due to the ordering of the conjugates of α_1 we chose,

$$\left\langle \boldsymbol{\alpha}, c^{j-1}(\boldsymbol{\alpha}) \right\rangle = \mathrm{Tr}_{K(f)}(\alpha_1 \bar{\alpha_j}) \in \mathbb{Z},$$

for all $1 \leq j \leq n$. This implies that the inner product of any two integer linear combinations of vectors $c^{j-1}(\boldsymbol{\alpha})$, $1 \leq j \leq n$ is integral. Thus, we have an integral algebraic lattice $\Sigma_K(\mathcal{M}_f)$, where $\mathcal{M}_f = \mathrm{span}_{\mathbb{Z}}\{\alpha_1, \dots, \alpha_n\} \subset K$ is a free $\mathbb{Z}$-module spanned by the roots of $f(x)$ in K. This observation suggests the following construction.

Let $\tau \in S_n$ be a permutation, given by the disjoint cycle decomposition

$$\tau = c_1 \dots c_\ell,$$

where each c_i is a k_i-cycle, so that $\sum_{i=1}^{\ell} k_i = n$, and $\gcd(k_i, k_j) = 1$ for all $i \neq j$. For each $1 \leq i \leq \ell$, let $f_i(x) \in \mathbb{Z}[x]$ be an irreducible monic polynomial of degree k_i such that $G(f_i) = \langle c_i \rangle$ and its roots $\alpha_{i1}, \dots, \alpha_{ik_i}$ are $\mathbb{Q}$-linearly independent. Notice that for every $k_i \geq 2$ there exist infinitely such polynomials. Write $\boldsymbol{\alpha}_i = (\alpha_{i1}, \dots, \alpha_{ik_i})^\top \in K(f_i)_{\mathbb{R}}$, and let

$$\boldsymbol{x} = (\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_\ell) \in K(f_1)_{\mathbb{R}} \times \dots \times K(f_\ell)_{\mathbb{R}}.$$

Since $\boldsymbol{x}$ satisfies the hypothesis of Proposition 1.1, the lattice $L_\tau(\boldsymbol{x})$ has rank $\mathrm{o}_\tau = n - \ell + 1$ in the n-dimensional space Euclidean space $K(f_1)_{\mathbb{R}} \times \dots \times K(f_\ell)_{\mathbb{R}}$, it is integral and consists of orthogonal cyclic blocks glued by the vector $\boldsymbol{x}$, as described in Theorem 1.2.

Let us consider an example of this algebraic lattice construction. Let $\tau = (1\ 2)(3\ 4\ 5)$ and take

$$f_1(x) = x^2 + x - 1,\ f_2(x) = x^3 - 3x - 1.$$

Both of these polynomials have cyclic Galois groups of orders 2 and 3, respectively, and the roots of these polynomials are

$$\alpha_{11} = \frac{-1+\sqrt{5}}{2},\ \alpha_{12} = \frac{-1-\sqrt{5}}{2},$$

and

$$\alpha_{21} = 2\cos\left(\frac{\pi}{9}\right),\ \alpha_{22} = -2\cos\left(\frac{2\pi}{9}\right),\ \alpha_{23} = -2\cos\left(\frac{4\pi}{9}\right),$$

respectively. Taking the glue vector

$$\boldsymbol{x} = \left(\frac{-1+\sqrt{5}}{2}, \frac{-1-\sqrt{5}}{2}, 2\cos\left(\frac{\pi}{9}\right), -2\cos\left(\frac{2\pi}{9}\right), -2\cos\left(\frac{4\pi}{9}\right)\right)$$

in the space $\left(\mathbb{Q}(\sqrt{5}) \otimes_{\mathbb{Q}} \mathbb{R}\right) \times \left(\mathbb{Q}\left(\cos\left(\frac{\pi}{9}\right)\right) \otimes_{\mathbb{Q}} \mathbb{R}\right) \cong \mathbb{R}^5$, we obtain the lattice $L_\tau(\boldsymbol{x}) \subset \mathbb{R}^5$ of rank 4 with basis matrix $B = \left(\boldsymbol{x}\ \tau(\boldsymbol{x})\ \tau^2(\boldsymbol{x})\ \tau^3(\boldsymbol{x})\right)$ and the corresponding integral Gram matrix

$$C = B^\top B = \begin{pmatrix} 9 & -5 & 0 & 4 \\ -5 & 9 & -5 & 0 \\ 0 & -5 & 9 & -5 \\ 4 & 0 & -5 & 9 \end{pmatrix}.$$

Define the mutually orthogonal blocks $M_1 = \mathrm{span}_{\mathbb{Z}} \left\{ \left(\sqrt{5}, -\sqrt{5}, 0, 0, 0\right)^\top \right\} \subset \mathbf{1}_2^\top \times \mathbb{R}^3$ and $M_2 =$

$$= \mathrm{span}_{\mathbb{Z}} \left\{ \begin{pmatrix} 0 \\ 0 \\ 2\cos\left(\frac{\pi}{9}\right) + 2\cos\left(\frac{4\pi}{9}\right) \\ -2\cos\left(\frac{2\pi}{9}\right) - 2\cos\left(\frac{\pi}{9}\right) \\ -2\cos\left(\frac{4\pi}{9}\right) + 2\cos\left(\frac{2\pi}{9}\right) \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2\cos\left(\frac{\pi}{9}\right) + 2\cos\left(\frac{2\pi}{9}\right) \\ -2\cos\left(\frac{2\pi}{9}\right) + 2\cos\left(\frac{4\pi}{9}\right) \\ -2\cos\left(\frac{4\pi}{9}\right) - 2\cos\left(\frac{\pi}{9}\right) \end{pmatrix} \right\} \subset \mathbb{R}^2 \times \mathbf{1}_3^\top,$$

then $L_\tau(\boldsymbol{x}) = \mathrm{span}_{\mathbb{Z}} \{\boldsymbol{x}, M_1 \oplus M_2\}$ with $\det L_\tau(\boldsymbol{x}) = 9\sqrt{15}$ and successive minima $\lambda_1 = \lambda_2 = \sqrt{7}$, $\lambda_3 = \lambda_4 = 2\sqrt{2}$.

5. Appendix: lattices spanned by algebraic conjugates

In this appendix, we want to revisit a construction of algebraic lattices described in [4]. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be a monic irreducible polynomial of degree $n \geq 2$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. Let K be its splitting field and G its Galois group over $\mathbb{Q}$. Then

$$d := [K : \mathbb{Q}] = |G| \leq n!.$$

Write $G = \{\sigma_1, \ldots, \sigma_d\}$, then for each $1 \leq i \leq n$ and $1 \leq j \leq d$, $\sigma_j(\alpha_i) = \alpha_{i_j}$ for some corresponding $1 \leq i_j \leq n$. Then

$$-a_{n-1} = \alpha_1 + \cdots + \alpha_n \in \mathbb{Z}, \tag{7}$$

and

$$\mathcal{M}_f = \mathrm{span}_{\mathbb{Z}} \{\alpha_1, \ldots, \alpha_n\} \subset K$$

is a $\mathbb{Z}$-module of rank $\leq n$ generated by all the conjugates of α. The module $\mathcal{M}_f$ is closed under the action of G, since automorphisms of the Galois extension $K/\mathbb{Q}$ simply permute the roots of an irreducible polynomial. Identifying elements of G with the embeddings as in Section 4 above, we have the Minkowski embedding

$$\Sigma_K = (\sigma_1, \ldots, \sigma_d) : K \hookrightarrow K_{\mathbb{R}}.$$

Writing $\boldsymbol{\alpha}$ for the image $\Sigma_K(\alpha) \in K_{\mathbb{R}}$ of $\alpha \in K$, we define the angle θ between $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ is given by

$$\theta = \cos^{-1}\left(\frac{\langle \boldsymbol{\alpha}, \boldsymbol{\beta} \rangle}{\|\boldsymbol{\alpha}\| \|\boldsymbol{\beta}\|}\right),$$

for each pair $\alpha, \beta \in K$, where $\| \boldsymbol{\alpha}\| = \langle \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle$ is the Euclidean norm.

Define $L_f := \Sigma_K(\mathcal{M}_f)$, which is a Euclidean lattice in $K_{\mathbb{R}}$. Then

$$L_f = \mathrm{span}_{\mathbb{Z}} \{\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n\}.$$

Let $m = \mathrm{rk}\, L_f$. The *minimal norm* of this lattice is $|L_f| := \min\{\|\boldsymbol{\beta}\| : \mathbf{0} \neq \boldsymbol{\beta} \in L_f\}$, which is the same as the first successive minimum, and the *minimal vectors* are vectors with this minimal norm. We say that L_f is *well-rounded* (WR) if it has m $\mathbb{R}$-linearly independent minimal vectors. Further, L_f is *generic WR* (GWR) if it is WR and the number of minimal vectors is precisely $2m$. Further, let $\mathcal{B} = \{\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_m\}$ be an ordered basis for L_f, and define a sequence of angles $\theta_1, \ldots, \theta_{n-1}$ as follows: each θ_i is the angle between $\boldsymbol{\beta}_{i+1}$ and the subspace

$$\mathrm{span}_{\mathbb{R}}\{\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_i\}.$$

Then each $\theta_i \in [0, \pi/2]$ and we say that $\mathcal{B}$ is a *weakly nearly orthogonal* basis if $\theta_i \geq \pi/3$ for each $1 \leq i \leq n-1$. A basis $\mathcal{B}$ is called *nearly orthogonal* if every ordering of it is weakly nearly orthogonal. If L_f has such a basis, we say that L_f is a nearly orthogonal lattice. The following result is Theorem 1.5 of [4].

Theorem 5.1. *Let $n \geq 3$ be prime. There exist infinitely many polynomials $f(x) \in \mathbb{Z}[x]$ of degree n so that L_f is a GWR nearly orthogonal lattice of rank n in $K_{\mathbb{R}}$, where K is the splitting field of $f(x)$; further, L_f contains a basis consisting of minimal vectors. For example, we can take $f(x) = x^n + a_{n-1}x^{n-1} + a_0$, where*

$$|a_0| > \frac{8(n-1)n!}{\sqrt{(n-2)^2 + 16(n-1)} - (n-2)} \tag{8}$$

and $|a_{n-1}| > |a_0| + 1$ are integers.

Here, we prove the following strengthening of this theorem.

Corollary 5.2. *Let $n \geq 3$, not necessarily prime, and let the rest of the notation be as in Theorem 5.1. There exist infinitely many trinomials $f(x) = x^n + a_{n-1}x^{n-1} + a_0$ satisfying conditions* (8) *and $|a_{n-1}| > |a_0| + 1$ as in Theorem 5.1 such that L_f is GWR nearly orthogonal with a basis of minimal vectors.*

Proof. The proof is the same as the proof of Theorem 1.5 of [4] with one important modification. The only reason the assumption that n is prime was needed was to ensure that rank of L_f is equal to n, i.e., that the conjugates $\alpha_1, \ldots, \alpha_n$ are $\mathbb{Q}$-linearly independent. For this, [4] used a theorem of Dubickas (Theorem 1 of [2]) that guarantees this linear independence under the conditions $a_{n-1} \neq 0$ and n being prime. The condition $a_{n-1} \neq 0$ is clearly necessary, however n being prime can be replaced by a weaker condition. Specifically, if $a_{n-1} \neq 0$ and $G = S_n$, then a result of C. J. Smyth (Lemma 1 of [11]) implies that the conjugates $\alpha_1, \ldots, \alpha_n$ are $\mathbb{Q}$-linearly independent, and hence our lattice L_f has rank n in $n!$-dimensional Euclidean space $K_{\mathbb{R}}$. Now, the fact that there exist infinitely many integer trinomials $f(x) = x^n + a_{n-1}x^{n-1} + a_0$ satisfying conditions (8) and $|a_{n-1}| > |a_0| + 1$ as in Theorem 5.1 with Galois group equal to S_n follows, for instance, from [9]. □

References

[1] J. H. Conway and N. J. A. Sloane. Sphere packings, lattices and groups, 3rd edition, Springer-Verlag, 1999.

[2] A. Dubickas. On the degree of a linear form in conjugates of an algebraic number. *Illinois J. Math.*, 46(2):571–585, 2002.

[3] L. Fukshansky, S. R. Garcia and X. Sun. Permutation invariant lattices. *Discrete Math.*, 338(8):1536–1541, 2015.

[4] L. Fukshansky and E. Knight. On lattices generated by algebraic conjugates of prime degree. *Illinois J. Math.*, 70(1):193–211, 2026.

[5] L. Fukshansky and D. Kogan. Cyclic and well-rounded lattices. *Mosc. J. Comb. Number Theory*, 11(1):79–96, 2022.

[6] F. J. MacWilliams and N. J. A. Sloane. The theory of error-correcting codes., North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[7] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. *FOCS, IEEE Computer Society*, pages 356–365, 2002.

[8] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput. Complexity*, 16(4):365–411, 2007.
[9] H. Osada. The Galois groups of the polynomials $X^n + aX^l + b$. *J. Number Theory*, 25(2):230–238, 1987.
[10] I. Siap and N. Kulhan. The structure of generalized quasi cyclic codes. *Appl. Math. E-Notes*, 5:24–30, 2005.
[11] C. J. Smyth. Additive and multiplicative relations connecting conjugate algebraic numbers. *J. Number Theory*, 23(2):243–254, 1986.
[12] D. Wan. Euclidean SVP is NP-hard for Cyclic Lattices. *arXiv:2609.16711v1*, 2026.

Departamento de Matemática, São Paulo State University, R. Cristóvão Colombo, 2265 - Jardim Nazareth, São José do Rio Preto, 15054-000, Brazil
Email address: maria.bonini@unesp.br

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711, USA
Email address: lenny@cmc.edu