AN EVEN EXTREMAL LATTICE OF RANK 64: COMPUTATIONAL DATA

ICHIRO SHIMADA

This note is an explanation of the computational data obtained in the paper [Paper]. These data are written in the `GAP` [GAP] format, and are available from the author's website

`http://www.math.sci.hiroshima-u.ac.jp/~shimada/lattice.html`.

The data is presented in 3 files:

`basiccompdata.txt`(6.1MB), `OLQ.txt.zip`(275.7MB), `ShortVectorsLQ.txt.zip`(77.7MB).

The zipped file of a folder `compdataL64` containing these 3 files is also available from the website above.

In the following, we use the notation fixed in [Paper].

1. Basis computational data

The file `basiccompdata.txt` contains the following data.

- `GramR` is the Gram matrix of R:

$$\texttt{GramR} = \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix}.$$

- `ORGenerators` is the generating set of $\mathrm{O}(R)$ consisting of the following matrices:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

- `projdiscR` is the 2×1 matrix

$$\begin{bmatrix} 175 \\ 35 \end{bmatrix},$$

which has the following property. The mapping

$$v \mapsto \bar{v} := v \cdot \texttt{projdiscR} \bmod 35$$

gives the natural projection $R^\vee \to D_R$, where $v \in R^\vee$ is written with respect to the standard basis e_1, e_2 of $R \otimes \mathbb{Q}$, and $\bar{v} \in D_R \cong \mathbb{Z}/35\mathbb{Z}$ is written with respect to the generator

$$u := \frac{1}{35}(34e_1 + 6e_2) \bmod R.$$

In the following, elements of $D_R \cong \mathbb{Z}/35\mathbb{Z}$ are written with respect to this generator u; that is, n means the element $nu \in D_R$, where n is an integer satisfying $0 \le n < 35$.

- `uDR` is the vector $[34/35, 6/35]$ that describes the generator u of D_R.
- `discR` is the 1×1 matrix $[[6/35]]$ that describes the finite quadratic form $q_R \colon D_R \to \mathbb{Q}/2\mathbb{Z}$ with respect to the generator u of D_R.
- `HR` is the list $[1, 6, 29, 34]$ of the elements of $H(R) = \mathrm{O}(q_R) \subset (\mathbb{Z}/35\mathbb{Z})^\times$.
- `GramR32` is the Gram matrix of R^{32}; that is, the block-diagonal matrix of size 64 whose diagonal matrices are 32 copies of `GramR`.
- `projdiscR32` is the 64×32 matrix which has the following property. The mapping

  $$v \mapsto \bar{v} := v \cdot \texttt{projdiscR32} \bmod 35$$

  gives the natural projection $(R^{32})^\vee = (R^\vee)^{32} \to D_{R^{32}} = (D_R)^{32}$; that is, `projdiscR32` is the block-diagonal matrix whose diagonal matrices are 32 copies of `projdiscR`.
- `discR32` is the 32×32 diagonal matrix with diagonal components $6/35 \in \mathbb{Q}/2\mathbb{Z}$. This matrix describes the finite quadratic form $q_{R^{32}} \colon D_{R^{32}} \to \mathbb{Q}/2\mathbb{Z}$.
- `lambdas` is the list of

  $$\lambda(n) := \min \ \{\ x^2 \ \mid \ x \in R^\vee,\ x \bmod R = n\ \},$$

  where $n \in D_R = \mathbb{Z}/35\mathbb{Z}$. For an integer n with $0 \le n < 35$, the $(n+1)$st entry of `lambdas` is $\lambda(n)$.
- `P1` is the list of points $P = [\alpha : \beta] = [\texttt{alpha}, \texttt{beta}]$ of $\mathbb{P}^1(\mathbb{F}_{31})$ sorted as

  $$[\,\infty, 0 \mid 1, 3^2, 3^4, \dots, 3^{28}, \mid 3, 3^3, 3^5, \dots, 3^{29}\,].$$

  The point ∞ is written as $[1:0]$, whereas the points in the finite part $\mathbb{F}_{31}$ are written in $[\nu : 1]$ $(0 \le \nu < 31)$.
- `PSLGenerators` is the list $[\xi, \eta, \zeta]$ of generators of $\mathrm{PSL}_2(31)$ embedded in $\mathfrak{S} = \mathfrak{S}(\mathbb{P}^1(\mathbb{F}_{31})) \cong \mathfrak{S}_{32}$. Each element is given by a 32×32 permutation matrix P such that $v \mapsto vP$ gives the permutation of components of a vector

v whose components are in one-to-one correspondence with the points of $\mathbb{P}^1(\mathbb{F}_{31})$ with the ordering fixed by the list `P1`.

- `T` is the template matrix T of generalized quadratic residue codes of length 32. The rows and columns of T are indexed by $\mathbb{P}^1(\mathbb{F}_{31})$ with the ordering fixed by `P1`. Components of `T` are strings `"a"`, `"b"`, `"d"`, `"s"`, `"t"`, `"e"`
- `abdste` $= [0, 0, 1, 7, 3, 2]$ is the parameter of the generalized quadratic residue code $\mathcal{Q}$.
- `QGenerators` is the list of the generators $\boldsymbol{v}_\infty, \boldsymbol{v}_0, \boldsymbol{v}_1, \dots, \boldsymbol{v}_{30} \in (\mathbb{Z}/35\mathbb{Z})^{32}$ of $\mathcal{Q}$. The list `QGenerators` is obtained from the template matrix `T` by substituting [`"a"`, `"b"`, `"d"`, `"s"`, `"t"`, `"e"`] with `abdste` $= [0, 0, 1, 7, 3, 2]$.
- `QBasis` is the basis of $\mathcal{Q}$ written is the form $[\, I_{16} \mid B\,]$, where B is the 16×16 matrix given in Table 1.1 of [Paper].
- `AutQGenerators` is a finite generating set of $\mathrm{Aut}_{H(R)}(\mathcal{Q})$. Each element of this list is given as a 32×32 matrix M such that $v \mapsto vM \bmod 35$ gives an automorphism of $\mathcal{Q}$.
- `embR32L` is the matrix of the embedding $R^{32} \hookrightarrow L_{\mathcal{Q}}$. This matrix fixes a basis $b_1, \dots, b_{64}$ of $L_{\mathcal{Q}}$ in the following sense: the row vectors of the inverse matrix $\texttt{embLR32}^{-1}$ are the vector representations of $b_1, \dots, b_{64}$ with respect to the standard basis $E = \{e_1^{(1)}, e_2^{(1)}, \dots, e_1^{(32)}, e_2^{(32)}\}$ of $R^{32} \otimes \mathbb{Q}$.
- `embR32Linv` is the inverse matrix of `embR32L`.
- `GramLQ` is the Gram matrix of $L_{\mathcal{Q}}$ with respect to the basis $b_1, \dots, b_{64}$ fixed above.
- `GammaLQGenerators` is a finite generating set of $\Gamma_{\mathcal{Q}} \subset \mathrm{O}(L_{\mathcal{Q}})$. Each member is written in the form of a 64×64 matrix with respect to the basis $b_1, \dots, b_{64}$ of $L_{\mathcal{Q}}$. This list is sorted according to `AutQGenerators`; that is, the ith member of `GammaLQGenerators` is the unique lift of the ith member of `AutQGenerators`.
- `Taus` is the list of the triples [`tau`, `size`, `indices`] of a type $\tau =$ `tau` of vectors in $\mathcal{S}$, the size of $\mathcal{S}_\tau$, and the list of indices i such that $o_i \subset \mathcal{S}_\tau$, where $o_i \subset \mathcal{S}$ is the orbit under the action of $\Gamma_{\mathcal{Q}}$ that appears at the ith position of the list `ShortVectorsLQ` below.
- `S0` is the list $\mathcal{S}_0$ of vectors in $\mathcal{S}$ with type $[\ 1377392,\ 578256,\ 38343,\ 304,\ 1\ ]$. The size of $\mathcal{S}_0$ is 23808, and $\mathcal{S}_0$ is the disjoint union of the two orbits o_7 and o_9. The elements in the first half of S_0 form o_7, and the elements in the second half form o_9.

- `NewBasisV0` is the list $V_0 = [v_1, \dots, v_{64}]$ of vectors in $\mathcal{S}_0$. The vectors v_i are written with respect to the basis $b_1, \dots, b_{64}$ of $L_{\mathcal{Q}}$.
- `GramLQV0` is the Gram matrix of $L_{\mathcal{Q}}$ with respect to the basis V_0.
- `TenVs` is the list $[V_1, \dots, V_{10}]$ of lists V_i of vectors of $\mathcal{S}_0$.
- `TenOLQGenerators` is the list $[g_1, \dots, g_{10}]$ of elements g_i of $\mathrm{O}(L_{\mathcal{Q}})$ such that $V_0^{g_i} = V_i$. These isometries g_i are written with respect to the basis $b_1, \dots, b_{64}$ of $L_{\mathcal{Q}}$.
- `smallms` is the list $[m_a, m_b, m_d, m_s, m_t, m_e]$ of the 2×2 matrices.
- `Mrho` is the matrix representation M_ρ of $\rho \otimes \mathbb{Q} \in \mathrm{O}(R^{32} \otimes \mathbb{Q})$ with respect to the standard basis E of $R^{32} \otimes \mathbb{Q}$.
- `GramNebe` is a Gram matrix of Nebe's lattice N_{64}. This matrix is copied from the website [NS].
- `GammaNebeGenerators` is a finite generating set of Nebe's subgroup of $\mathrm{O}(N_{64})$ with order 587520. This list is copied from the website [NS].

2. Big data

- The file `OLQ.txt` contains the list `OLQ` of elements of $\mathrm{O}(L_{\mathcal{Q}})$. This list `OLQ` consists of two lists. The first is the list of elements of the subgroup $\Gamma_{\mathcal{Q}} \subset \mathrm{O}(L_{\mathcal{Q}})$. The second is the list of elements of $\mathrm{O}(L_{\mathcal{Q}}) \setminus \Gamma_{\mathcal{Q}}$.
- The file `ShortVectorsLQ.txt` contains the list `ShortVectorsLQ` that describes the orbit decomposition of the set $\mathcal{S}$ of vectors in $L_{\mathcal{Q}}$ of square-norm 6. The vectors are written with respect to the basis $b_1, \dots, b_{64}$ of $L_{\mathcal{Q}}$ fixed by `embR32L`. This list is decomposed into 56 orbits by the action of $\Gamma_{\mathcal{Q}}$. The first orbit is o_1 and the second orbit is o_2.

References

[GAP] The GAP Group. GAP - Groups, Algorithms, and Programming. Version 4.8.6; 2016 (http://www.gap-system.org).

[NS] Gabriele Nebe and Neil Sloane. A Catalogue of Lattices. `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/`. Accessed: 2017-09-16.

[Paper] Ichiro Shimada. An even extremal lattice of rank 64. preprint. `http://www.math.sci.hiroshima-u.ac.jp/~shimada/preprints.html`.

Department of Mathematics, Graduate School of Science, Hiroshima University, 1-3-1 Kagamiyama, Higashi-Hiroshima, 739-8526 JAPAN

E-mail address: `ichiro-shimada@hiroshima-u.ac.jp`