Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 40 (1994)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: UNIMODULAR LATTICES WITH A COMPLETE ROOT SYSTEM

Autor: Kervaire, Michel

Kapitel: 2. Relationship with codes

DOI: https://doi.org/10.5169/seals-61105

The root system R will be said to be *complete* in L if the sublattice $N = \mathbf{Z}R$ of L generated by the roots R is a subgroup of finite index in L.

Our purpose is to study unimodular lattices with a complete root system.

It is well known that there are finitely many isomorphism classes of unimodular lattices $L \subset \mathbf{Q}^n$ for a given n. (See [MH], p. 18.)

The subcollection consisting of the lattices with a complete root system is particularly interesting, e.g. in view of the connection with the theory of error-correcting codes as we shall recall below.

We begin by setting up some necessary conditions that a root system must satisfy in order to be a complete root system in a unimodular lattice (Sections 3, 4 and 5).

We are particularly interested in even unimodular lattices, i.e. (x, x) is even for every $x \in L$. In this case, as is well known, the rank of L has to be divisible by 8. In dimensions 8, 16 and 24, where the classification of even unimodular lattices is available, it turns out that every such lattice has a complete root system, with the sole exception of the 24-dimensional Leech lattice. (History and relevant literature in e.g. [N], p. 142.)

In dimension 32, there are millions of even unimodular lattices. (See [Se], p. 95.) Among them as we shall see, only a small subcollection have a complete root system. In this paper, we endeavour to provide the complete list of such lattices.

There are 132 indecomposable even unimodular 32-dimensional lattices with a complete root system. In some cases several lattices happen to have the same root system. Thus, only a total number of 119 root systems correspond to these lattices. They are listed in Section 6.

The enumeration of the lattices and their root systems could only be completed using a computer, thanks to the generous help of Shalom Eliahou who patiently explained to me the use of mulisp programming language. Of course any mistake in the programs is my sole responsibility. It is a pleasure to express to him here my warmest gratitude.

I am also deeply indebted to Boris Venkov for very valuable discussions, in particular on the use of the notion of deficiency. (See Section 5.)

2. Relationship with codes

As is customary we shall use codes to describe lattices. We briefly recall how this can be done.

If $X \subset \mathbf{Q}^n$ is any finitely generated $\mathbf{Z}$-submodule of $\mathbf{Q}^n$, we set

$$X^{\#} = \{u \in \mathbf{Q}X : (u, x) \in \mathbf{Z} \text{ for all } x \in X\} .$$

Note that if $X_1, X_2 \subset \mathbf{Q}^n$ are mutually orthogonal finitely generated $\mathbf{Z}$-submodules of $\mathbf{Q}^n$, then

$$(X_1 \boxplus X_2)^\# = X_1^\# \boxplus X_2^\# ,$$

where we write the symbol $\boxplus$ to mean orthogonal (direct) sum.

Clearly, a lattice $L \subset \mathbf{Q}^n$ is integral if and only if $L \subset L^\#$, and L is unimodular precisely if $L = L^\#$. Indeed, if $v_1, \dots, v_n$ is a $\mathbf{Z}$-basis of L, and $w_1, \dots, w_n$ the dual basis of $L^\#$, where $(v_i, w_j) = \delta_{i,j}$, then $v_j = \sum_{k=1}^n t_{kj} w_k$ for some integral matrix $T = (t_{kj})$, and if S is the matrix of scalar products (v_i, v_j), then

$$(v_i, v_j) = (v_i, \sum_{k=1}^{n} t_{kj} w_k) = t_{ij} ,$$

and thus

$$[L^\# : L] = |\, det(T)\,| = |\, det(S)\,| .$$

Suppose now that L is an integral lattice in $\mathbf{Q}^n$ and that $N \subset L$ is a sublattice of finite index in L. Then, $N \subset L \subset L^\# \subset N^\#$ and the finite abelian group $T(N) = N^\# / N$ inherits a non-degenerate $\mathbf{Q}/\mathbf{Z}$-valued bilinear form

$$b : T(N) \times T(N) \to \mathbf{Q}/\mathbf{Z}$$

defined by

$$b(\xi, \eta) = (x, y) \quad mod\, \mathbf{Z} ,$$

where $x, y \in N^\#$ project on $\xi, \eta \in T(N) = N^\# / N$ respectively by the natural map $\pi : N^\# \to T(N)$.

The finite scalar product module $(T(N), b)$ is called the *discriminant form* of N.

Let $M = \pi(L)$. Then M is self-orthogonal, i.e. $M \subset M^\perp$, for the bilinear form b on $T(N)$. Thus M is a self-orthogonal code in $(T(N), b)$. Conversely, given a subgroup $M \subset T(N)$ such that $M \subset M^\perp$, we recapture the integral lattice L as $L = \pi^{-1}(M)$. Note that L is unimodular, i.e. $L = L^\#$ if and only if $M = M^\perp$. If T is a finite (abelian) group with a non-degenerate bilinear form $b : T \times T \to \mathbf{Q}/\mathbf{Z}$, and $M \subset T$ is a subgroup such that $M = M^\perp$, we say that M is a *metabolizer* for the scalar product module T. A metabolizer is the same object as a self-dual code.

Summarizing, one way of describing a unimodular lattice $L \subset \mathbf{Q}^n$ consists in giving the following data:

1) An integral lattice $N \subset \mathbf{Q}^n$;

2) A metabolizer $M \subset T(N)$, where $T(N) = N^{\#}/N$ is the discriminant form of N.

We will presently make use of this: If L is a unimodular lattice with a complete root system R, then $N = \mathbf{Z}R \subset L$ is a lattice of finite index in L, and by the above, L can be encoded by the data of the root system R which determines $N = \mathbf{Z}R \subset \mathbf{Q}^n$, $N^{\#}$ and $T(R) = N^{\#}/N$ with its non-degenerate form $b : T(R) \times T(R) \to \mathbf{Q}/\mathbf{Z}$, together with a metabolizer $M = M^{\perp} \subset T(R)$.

Note however that if we start with a root system $R \subset \mathbf{Q}^n$ and construct L as $L = \pi^{-1}(M)$, where M is a metabolizer in $T(R)$, then $R' = \{a \in L : (a, a) = 2\}$ will contain R but may possibly be strictly larger.

We shall say that M is an *admissible* metabolizer if indeed we have $R = \{a \in L : (a, a) = 2\}$, where $L = \pi^{-1}(M)$.

Thus, the problem of deciding whether there exists a unimodular lattice $L \subset \mathbf{Q}^n$ with given root system R such that $\mathbf{Q}R = \mathbf{Q}^n$ is equivalent to the question: Does the finite scalar product module $(T(R), b)$ possess an admissible metabolizer?

If $R \subset \mathbf{Q}^n$ is a root system and $N = \mathbf{Z}R \subset N^{\#}$ is the lattice generated by R, we define the *norm*

$$\mathbf{n} : T(R) \to \mathbf{Q}$$

by $\mathbf{n}(\xi) = min\{(x, x) : \pi(x) = \xi\}$, where the minimum of (x, x) is taken over all the elements $x \in N^{\#}$ representing $\xi \in T(R) = N^{\#}/N$.

We say that ξ is *admissible* if $\mathbf{n}(\xi) = 0$, or $\mathbf{n}(\xi)$ is an integer > 2. It is easy to see that a metabolizer $M \subset T(R)$ is admissible if and only if every $\xi \in M$ is admissible. (Note that if R is a complete root system in L, then L cannot contain any vector u with $(u, u) = 1$.)

If an *even* unimodular lattice L is required with a prescribed root system R, then the metabolizer $M \subset T(R)$ will have to satisfy the additional condition: For all non-zero $\xi \in M$, the norm $\mathbf{n}(\xi)$ must be an even integer $\geqslant 4$. Depending on the context, we occasionally change the meaning of "admissible" to include this stronger condition, e.g. in Section 6, when setting up the tables of even unimodular lattices in dimension 32.

The classification of root systems is well known. (See [B], p. 197.) We recall the facts which are relevant to us in the next section, following mostly the notations of [N]. The possible lattices $N = \mathbf{Z}R$ are thus easily described as well as the finite scalar product modules $T(R) = N^{\#}/N$.

The existence of a mere metabolizer for $(T(R), b)$, perhaps not admissible, is already a strong restriction on R. We study this condition in the next Section 3.

We give some necessary conditions for the existence of an admissible metabolizer using coding theory in Section 4.

In Section 6, after explaining the notations used in the tables, we list the even unimodular lattices with complete root systems in dimension 32.

3. The Witt class associated with a root system

Recall the Witt group $W(\mathbf{Q}/\mathbf{Z})$ of finite scalar product modules: If T and T' are two finite abelian groups with non-degenerate bilinear forms $b : T \times T \to \mathbf{Q}/\mathbf{Z}$, $b' : T' \times T' \to \mathbf{Q}/\mathbf{Z}$, then T and T' are said to be Witt equivalent if there exist finite scalar product modules H, H' each with a metabolizer $M = M^{\perp} \subset H$, $M' = M'^{\perp} \subset H'$ such that $T \boxplus H$ and $T' \boxplus H'$ are isometric. The Witt equivalence classes of finite scalar product modules form an abelian group $W(\mathbf{Q}/\mathbf{Z})$ under the operation induced by orthogonal direct sum $\boxplus$.

We recall below the explicit determination of $W(\mathbf{Q}/\mathbf{Z})$.

Let $R \subset \mathbf{Q}^n$ be a root system. As before, we denote by $T(R)$ the associated finite scalar product module. As a group, $T(R) = (\mathbf{Z}R)^{\#}/\mathbf{Z}R$, where

$$(\mathbf{Z}R)^{\#} = \{v \in \mathbf{Q}R = \mathbf{Q}^n : (v, R) \subset \mathbf{Z}\} .$$

The bilinear form $b : T(R) \times T(R) \to \mathbf{Q}/\mathbf{Z}$ is induced from the scalar product in $\mathbf{Q}^n$, restricted to $(\mathbf{Z}R)^{\#}$.

The Witt class of $(T(R), b)$ is an element of $W(\mathbf{Q}/\mathbf{Z})$ which we call the Witt class associated with the root system R and denote by $w(R) \in W(\mathbf{Q}/\mathbf{Z})$.

As we saw in Section 2, if R is the root system of a unimodular lattice $L \subset \mathbf{Q}^n$, and R is complete in L, i.e. $\mathbf{Q}R = \mathbf{Q}L = \mathbf{Q}^n$, then $(T(R), b)$ possesses a metabolizer and therefore $w(R)$ must be 0 in $W(\mathbf{Q}/\mathbf{Z})$.

If $R = R_1 \boxplus R_2$ is an orthogonal decomposition of the root system R, i.e. if R is the disjoint union $R_1 \sqcup R_2$ of two mutually orthogonal root systems R_1, R_2, then

$$w(R) = w(R_1) + w(R_2) .$$

Indeed,

$$(\mathbf{Z}R)^{\#} = (\mathbf{Z}R_1)^{\#} \boxplus (\mathbf{Z}R_2)^{\#} ,$$