1. Introduction

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **40 (1994)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

L'Enseignement Mathématique, t. 40 (1994), p. 59-104

UNIMODULAR LATTICES WITH A COMPLETE ROOT SYSTEM

by Michel KERVAIRE

1. INTRODUCTION

Let $\mathbf{Q}^n$ be the n-dimensional euclidean space (over the field $\mathbf{Q}$ of rational numbers) endowed with the standard scalar product

$$(x, y) = \sum_{i=1}^{n} x_i y_i ,$$

where $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$.

A lattice $L \subset \mathbf{Q}^n$ is a $\mathbf{Z}$-submodule of rank n of $\mathbf{Q}^n$, i.e.

$$L = \{ \sum_{i=1}^{n} a_i v_i : a_i \in \mathbf{Z} \} ,$$

where $v_1, \ldots, v_n$ is some basis of $\mathbf{Q}^n$. We are interested in *integral* lattices, i.e. lattices L satisfying $(x, y) \in \mathbf{Z}$ for all $x, y \in L$.

An integral lattice L is said to be *unimodular* if

$$det(S) = \pm 1 ,$$

where S is the $n \times n$ matrix of scalar products

$$S = ((v_i, v_j)), \quad 1 \leqslant i, j \leqslant n ,$$

$v_1, \ldots, v_n$ being a $\mathbf{Z}$-basis of L. The number $det(S)$ is called the *determinant* of L and is denoted $det(L)$. It does not depend on the choice of the $\mathbf{Z}$-basis $v_1, \ldots, v_n$ of L.

If L is an integral lattice, the set

$$R = \{x \in L : (x, x) = 2\}$$

is a *root system*. (For the general notion of a root system see [B], p. 142.)

The author gratefully acknowledges partial support from the Fonds National Suisse de la Recherche Scientifique during the preparation of this paper. In particular the FNSRS provided the necessary computer.

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

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