Reduction Modulo 2 and 3 of Euclidean Lattices, II

Jacques Martinet

Laboratoire A2X, UMR 5465 associée au C.N.R.S. & Université Bordeaux 1

Abstract. This paper is a continuation of *Reduction Modulo 2 and 3 of Euclidean Lattices* ([**7**], Journal of Algebra, 2002).

Résumé. *Reduction modulo 2 et 3 des réseaux euclidiens (II).* Cet article fait suite à l'article [**7**] *Reduction Modulo 2 and 3 of Euclidean Lattices*, paru en 2002 au Journal of Algebra.

1. Introduction.

Let E be an n-dimensional Euclidean space with scalar product $x \cdot y$, and let $\mathcal{L}$ be the set of lattices (discrete subgroups of rank n) in E. For a lattice $\Lambda \in \mathcal{L}$, we denote by $\min \Lambda$ its *minimal norm*: $\min \Lambda = \min_{x \in \Lambda \smallsetminus \{0\}} x \cdot x$, and by $\det \Lambda$ the determinant of the Gram matrix $(e_i \cdot e_j)$ of any $\mathbb{Z}$-basis $(e_1, e_2, \ldots, e_n)$ of Λ.

In this paper, we still study short representatives for classes modulo 2 and 3 of a given lattice, indeed only modulo 2 from Section 3 onwards. Section 2 is devoted to root lattices modulo 2 and 3 and Section 3 to laminated lattices modulo 2. In Section 4, we give a few complements which may apply to odd lattices. In Section 5, we show how to attach to classes modulo 2 containing not too large vectors a lattice of codimension 1 having a relatively large minimum. Notably, the Leech lattice produces the 23-dimensional "equiangular" integral lattice of minimum 5 described in [**9**] whose set of minimal vectors constitutes a spherical (tight) 5-design; see also [**1**].

We now recall some results which are proved in [**7**]. We denote by Λ a lattice, and we set $n = \dim \Lambda$, $m = \min \Lambda$, and for $t > 0$, we denote by S_t the set of norm t vectors in Λ and we set $s_t = \frac{1}{2}|S_t|$. We also denote by m' the norm of the second layer of Λ: $m' = \min_{N(x) > m} N(x)$.

1991 *Mathematics Subject Classification.* 11H55, 11H56.

Key words and phrases. Lattices, short vectors, reduction.

I thank the authors of the PARI system (H. Cohen et al.), and especially Christian Batut for his specific lattice programs.

For lattices modulo 2, the basic identity, involving non-zero vectors x and $y = x + 2z \equiv x \mod 2\Lambda$, is

$$N(y) + N(x) = 2\big(N(z) + N(x+z)\big)\,. \tag{1}$$

Provided that $y \neq \pm x$, this implies $N(y) + N(x) \geq 4m$, with equality if and only if z and $x + z = y - z$ are minimal.

PROPOSITION 1.1. *If $x \neq 0$ and $y \neq \pm x$, we have $N(y) + N(x) \geq 4m$, and equality holds if and only if z and $x + z = y - z$ are minimal. We then have $x \cdot z = -\frac{N(x)}{2}$, and x and y are orthogonal.*

PROOF. The first part is clear. If $N(z) = N(x+z) = m$, then

$$2\,x \cdot z + N(x) = 0 \text{ and } y \cdot x = N(x) + 2\,x \cdot z = 0\,.$$

□

A complete set T of shortest representatives for non-zero classes modulo 2 yields a weighted formula of the kind

$$\sum_{x \in T} \frac{1}{w(x)} = 2^n - 1 \tag{2}$$

where $w(x) = |\{y \in \Lambda \mid N(y) = N(x) \text{ and } y \equiv x \mod 2\Lambda\}|\,.$

In [**7**], we essentially considered vectors of norm $N \leq 2m$. The weight $w(x)$ is equal to 1 if $0 < N(x) < 2m$ and belongs to the interval $[1, n]$ if $N(x) = 2m$; some estimations for w beyond norm $2m$ will be proved in the next sections. This implies the inequality

$$\sum_{0<t<2m} s_t + \frac{s_{2m}}{n} \leq 2^n - 1$$

and various other inequalities of the same kind related to better bounds for w under various hypotheses.

For lattices modulo 3, the basic identity, involving non-zero vectors x and $y = x + 3z \equiv x \mod 3\Lambda$, is

$$N(y) + 2N(x) = 3\big(2N(z) + N(x+z)\big)\,, \tag{3\,a}$$

together with its companion identity obtained by exchanging x and y:

$$N(x) + 2N(y) = 3\big(2N(z) + N(y-z)\big)\,. \tag{3\,b}$$

We shall this time enumerate the classes modulo 3 up to sign (i.e., we now consider the set T of pairs $\pm\mathcal{C}$ of classes modulo 3). The weighted formula now takes the form

$$\sum_{x \in T} \frac{1}{w(x)} = \frac{3^n - 1}{2}\,. \tag{4}$$

In [**7**], Theorem 3.13, we proved for the weight the following results:
- $w(x) = 1$ if $0 < N(x) < m + m'$ or $m + m' < N(x) < 2m + m'$;
- $w(x) = 1$ or 3 if $N(x) = m + m'$;
- $1 \leq w(x) \leq n + 1$ if $N(x) = 2m + m'$.

[$w = 3$ (resp. $w = n + 1$) corresponds to a configuration $\mathbb{A}_2$ (resp. $\mathbb{A}^*_{n+1}$.)]

In the sequel, weighted formulae will be displayed in the following form: for norms N where the weight may take values larger than 1, an expression such as

$$\Big(\frac{(a_1 + a_2 + \cdots)}{w} + \frac{b_1 + b_2 + \cdots}{w'} + \cdots\Big)$$

means that $a_1, a_2, \ldots$ are the number of pairs of vectors in the various norm N orbits with weight w, etc.

As noticed in [**7**] (Proposition 2.9 and Table I), lattices having $\bmod 2$ representatives of norm $N < 2m$ constitute an open set in $\mathcal{L}$. The corresponding $\bmod 3$ result applies to lattices having representatives of norm $N < 2m + m'$; this results from [**7**], Propositions 3.7 and 3.8; it notably applies to $\mathbb{A}_n$ ($n \leq 3$) and $\mathbb{D}_4$; see next section. Finally, we shall essentially consider only *irreducible* lattices; indeed, the bound $2m$ for classes modulo 2 does not hold for reducible lattices to within the three exceptions $\mathbb{A}_1 \perp \mathbb{A}_1$, $\mathbb{A}_2 \perp \mathbb{A}_1$ and $\mathbb{A}_2 \perp \mathbb{A}_2$ (up to scale). It is easy to verify that the similar list for $\bmod 3$ lattices reduces to $\mathbb{A}_1 \perp \mathbb{A}_1$ and $\mathbb{A}_2 \perp \mathbb{A}_1$.

2. Root Lattices Modulo 2 and 3.

In this section, we consider irreducible root lattices, indeed lattices isometric to $\mathbb{A}_n$ ($n \geq 1$), $\mathbb{D}_n$ ($n \geq 4$) or $\mathbb{E}_n$ ($n = 6, 7, 8$). We have $m = 2$, and disregarding the trivial cases of $\mathbb{A}_1$ and $\mathbb{A}_2$, $m' = 4$, hence $2m + m' = 4m = 8$. We denote by $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n)$ (resp. $(\varepsilon_1, \ldots, \varepsilon_n)$) the canonical basis for $\mathbb{Z}^{n+1}$ (resp. $\mathbb{Z}^n$) and set

$$\mathbb{A}_n = \{x \in \mathbb{Z}^{n+1} \mid \textstyle\sum x_i = 0\} \quad \text{and} \quad \mathbb{D}_n = \{x \in \mathbb{Z}^n \mid \textstyle\sum x_i \equiv 0 \mod 2\}\,.$$

Proposition 2.1. *Up to signs, shortest representatives for classes modulo* 2 *or* 3 *of* $\mathbb{A}_n$ *or* $\mathbb{D}_n$ *are the vectors which are of one of the following forms:*

1. $\varepsilon_{i_1} \pm \varepsilon_{i_2} \pm \cdots \pm \varepsilon_{i_k}$*, of norm* $2k$*, for* $\mathbb{A}_n$ and $\mathbb{D}_n$*, modulo* 2 and 3*.*
2. $2\varepsilon_i$*, of norm* 4*, for* $\mathbb{D}_n$ *modulo* 2*.*
3. $2\varepsilon_{i_1} + \cdots + 2\varepsilon_{i_\ell} + \varepsilon_{i_{\ell+1}} + \cdots + \varepsilon_{i_{\ell+k}} - \varepsilon_{i_{\ell+k+1}} - \cdots - \varepsilon_{i_{3\ell+2k}}$ *($\ell > 0$), of norm* $6\ell + 2k$*, for* $\mathbb{A}_n$ *modulo* 3*.*
4. $2\varepsilon_{i_1} \pm \varepsilon_{i_2} \pm \cdots \pm \varepsilon_{i_k}$ *($k > 0$), of norm* $k + 4$*, for* $\mathbb{D}_n$ *modulo* 3*.*

Moreover, the weights of the vectors above are 1 *in case (1),* n *in case (2),* $\binom{3\ell+k}{\ell}$ *in case (3), and* k *in case (4).*

Proof. (Sketch.) If $x = \sum_j a_j\varepsilon_j \in \Lambda$ ($\Lambda = \mathbb{A}_n$ or $\mathbb{D}_n$) has some large component a_i, consider a transformation of the form $x \mapsto x \pm 2(\varepsilon_i - \varepsilon_j)$ or $x \mapsto x \pm 3(\varepsilon_i - \varepsilon_j)$ if $\Lambda = \mathbb{A}_n$, $x \mapsto x \pm 2(\varepsilon_i \pm \varepsilon_j)$ or $x \mapsto x \pm 3(\varepsilon_i \pm \varepsilon_j)$ if $\Lambda = \mathbb{D}_n$ (and then also $x \mapsto x \pm 4\varepsilon_i$ or $x \mapsto x \pm 6\varepsilon_i$ if x has a single component). That the vectors listed above are among the shortest representatives in their class is easy to verify; we leave to the reader the calculation of the weights. □

For exceptional lattices, we have:

Proposition 2.2. *For* $\mathbb{E}_6 \bmod 2$, $\mathbb{E}_7 \bmod 3$ *and* $\mathbb{E}_8 \bmod 2$ *and* 3*, all classes possess representatives of norm* $\leq 2m = 4$ *or* $2m + m' = 8$*. For* $\mathbb{E}_7 \bmod 2$ *(resp.* $\mathbb{E}_6 \bmod 3$*), there is one missing class, whose smallest representatives have norm* 6 *(resp.* 12*); this is the set of minimal vectors in* $2\,\mathbb{E}_7^*$ *(resp.* $3\,\mathbb{E}_6^*$*), of weight* 28 *(resp.* 27*).*

Proof. Modulo 2, we use the general bound $w \leq n$ and its refinement $w \leq n - 1$ (proved in [**7**] before Theorem 2.4) which applies to lattices such that $\frac{(2m)^n}{\det(\Lambda)}$ is not a square, together with the fact that the sum must not exceed $2^n - 1$. This immediately gives us the following three formulae for vectors of norm 2 and 4:

$$E_6 \bmod 2\text{:} \quad 36 + \frac{135}{5} = 63 = 2^6 - 1\,;$$

$$E_7 \mod 2: \quad 63 + \frac{378}{6} = 126 = (2^7 - 1) \text{ - } \mathbf{1};$$

$$E_8 \mod 2: \quad 120 + \frac{1080}{8} = 255 = 2^8 - 1.$$

The same device applies for classes modulo 3. For integral lattices, the bound $w \leq n+1$ can be refined to $w \leq n$ whenever the scaled copy of $\mathbb{A}_m^*$ to norm $2m+m'$ (here, 8) is not integral; this applies to $\mathbb{E}_6$ and $\mathbb{E}_7$. We also need the fact that norm 6 vectors in $\mathbb{E}_7$ share out among two orbits (in all other cases, *primitive* vectors of norm $N \leq 8$ constitute a single orbit). These two orbits have $s'_6 = 28$ and $s''_6 = 1008$ pairs of vectors; the first one is $2S(\mathbb{E}_7^*)$. These remarks show that the weighted formulae for vectors of norm $N \leq 8$ are:

$$E_6 \mod 3: \quad 36 + 135 + \frac{360}{3} + \frac{432}{6} = 363 = \frac{3^6 - 1}{2} \text{ - } \mathbf{1};$$

$$E_7 \mod 3: \quad 63 + 378 + \left(28 + \frac{1008}{3}\right) + \frac{2016}{7} = 1093 = \frac{3^7 - 1}{2};$$

$$E_8 \mod 3: \quad 120 + 1080 + \frac{3360}{3} + \frac{8640}{9} = 3280 = \frac{3^8 - 1}{2}.$$

There remains to characterize the two missing classes. For $\mathbb{E}_7 \mod 2$, consider $x \in 2S(\mathbb{E}_7^*)$. We have $N(x) = 2^2 \cdot \frac{3}{2} = 6$. Let $y \equiv x \mod 2$ in $\mathbb{E}_7$. We have $N(y) \equiv N(x) \equiv 2 \mod 4$. Hence if y were shorter than x, it would have norm 2. But pairs of norm 2 vectors in $\mathbb{E}_7$ constitute an orbit of $63 > 28$ different classes mod 2, a contradiction.

Similarly, the 27 pairs of vectors in $3S(\mathbb{E}_6^*)$, of norm $3^2\frac{4}{3} = 12$, cannot be congruent mod 3 to a shorter vector, for such a vector would have norm 6 (because $y \equiv x \mod 3\mathbb{E}_6 \Rightarrow N(y) \equiv N(x) \mod 3$), and norm 6 vectors constitute an orbit of $\frac{360}{2} = 120 > 27$ vectors. (Incidentally, this shows that all norm 10 vectors in $\mathbb{E}_6$ are congruent mod 3 to a norm 4 vector.) □

3. Laminated Lattices Modulo 2.

These lattices, that we shall consider only in the range $1 \leq n \leq 24$, were defined inductively by Conway and Sloane; see [**3**], Chapter 6 for a precise definition. They have minimum 4. There is one lattice in each dimension, denoted by Λ_n, except for $n = 11$, 12, 13 where there are two, three, and three lattices respectively, characterized by their kissing number, and denoted by an extra superscript min, mid or max. The aim of this section is to show that the list of laminated lattices for which it was proved in [**7**], Section 2, that all classes modulo 2 contain representatives of norm $N \leq 8$ is actually complete up to dimension 24.

THEOREM 3.1. *Laminated lattices of dimension $n \leq 24$ possessing representatives of norm $N \leq 8$ for all classes modulo 2 are those of dimension $n \leq 6$, $8 \leq n \leq 10$ and $n = 24$.*

Before proceeding to the proof, we state and prove a lemma:

LEMMA 3.2. *Let L be an integral lattice of minimum 3 and let $\Lambda = L_{even}$ be its even part. Assume that there exist in L two non-orthogonal pairs of minimal vectors. Then Λ has minimum 4 and contains a class modulo 2 of minimum 12.*

PROOF OF 3.2. We have $\min L_{even} \geq 4$, and if x, y are non-orthogonal, non-proportional minimal vectors in L, we have $x \cdot y = \pm 1$, hence $N(x \mp y) = 4$, whence $N(L_{even}) = 4$.

Let $e \in S(L)$ and let $f = 2e$. Since $[L : \Lambda] = 2$, we have $\Lambda = \langle L, e \rangle = \langle L, \frac{f}{2} \rangle$, hence

$$L \smallsetminus \Lambda = \left\{ \tfrac{x}{2} \mid x \equiv f \mod 2\Lambda \right\}.$$

Since $\min L = \min L \smallsetminus \Lambda = 3$, we have $N(x) \geq 12$ on the whole class of f modulo 2. Since $N(f) = 12$, this completes the proof of the lemma. □

PROOF OF THEOREM 3.1. In dimensions $n \leq 8$, the laminated lattices are scaled copies of root lattices, namely $\mathbb{A}_n$ ($n = 1, 2, 3$), $\mathbb{D}_n$ ($n = 4, 5$) and $\mathbb{E}_n$ ($n = 6, 7, 8$), and Theorem 3.1 follows from the results of Section 2. For $n = 24$, Λ_{24} is the Leech lattice, and the result is a theorem of Conway (see [**3**], Chapter 12). The case of dimensions 9 and 10 is dealt with in [**7**], Section 2, Table III. We are thus left with the 18 laminated lattices of dimension $n \in [11, 23]$. We now show how Lemma 3.2 can be used to deal with 16 of them.

Recall that O_{23} stands for the unimodular 23-dimensional lattice of minimum 3. The lattice $\mathbb{Z} \perp \mathrm{O}_{23}$ can be defined as a Kneser–neighbour of Λ_{24} through a norm 4 vector, which shows that $(\mathrm{O}_{23})_{even}$ is isometric to Λ_{23}. Now, it is shown in [**2**] that the *antilaminations* of O_{23} (the descending chain of the densest cross–sections) produce a unique lattice (denoted by O_n) in dimensions 23 to 14. Since the antilaminations of Λ_{23} also produce the Λ_n series in these dimensions, we have $(\mathrm{O}_n)_{even} \simeq \Lambda_n$ for $14 \leq n \leq 23$. Then we find two 13-dimensional lattices, which allows again to deal with $\Lambda_{13}^{\max}$ and $\Lambda_{13}^{\min}$ ($\Lambda_{13}^{\mathrm{mid}}$ is a dead–end for laminated lattices). We can even consider dimensions 12 and 11. Explicitly, in the notation of [**2**], we have $\Lambda_{13}^{\max} \simeq (\mathrm{O}_{13b})_{even}$, $\Lambda_{13}^{\min} \simeq (\mathrm{O}_{13a})_{even}$, $\Lambda_{12}^{\max} \simeq (\mathrm{O}_{12b})_{even}$, $\Lambda_{12}^{\mathrm{mid}} \simeq (\mathrm{O}_{12a})_{even}$, and $\Lambda_{11}^{\max} \simeq (\mathrm{O}_{11})_{even}$. As for $\Lambda_{13}^{\mathrm{mid}}$, it is also the even part of an integral norm 3 lattice, discovered by Plesken and Pohst ([**8**]), indeed the lattice with $s = 84$ of their list. Lemma 3.2 shows that all the sixteen lattices listed above contain a class of minimum 12.

To complete the proof of Theorem 3.1, it suffices to consider the two lattices $\Lambda_{11}^{\min}$ and $\Lambda_{12}^{\min}$. We have shown using PARI-GP that vectors of norm $N \leq 8$ do not represent all classes. For the sake of completeness, we display below the weighted formulae for vectors of norm $N \leq 8$ for the four lattices Λ_9, Λ_{10}, $\Lambda_{11}^{\min}$ and $\Lambda_{12}^{\min}$. The notation is that of section 2. The first two numbers are s_4 and s_6; we then give for each weight the numbers of vectors in a given orbit with this weight. (Note that two congruent vectors may belong to different orbits.)

$$\Lambda_9 \quad : 136 + 128 + \frac{1+8}{9} + \frac{560+512}{8} + \frac{448}{4} = 511\,.$$

$$\Lambda_{10} \quad : 168 + 384 + \frac{3+24}{9} + \frac{768+288}{8} + \frac{48+192}{5} + \frac{1152}{4} = 1023\,.$$

$$\Lambda_{11}^{\min} : 216 + 816 + \frac{54}{9} + \frac{1032}{8} + \frac{960}{5} + \frac{1920}{4} + \frac{384}{3} = 1967\,.$$

$$\Lambda_{12}^{\mathrm{mid}} : 312 + 1728 + \frac{12+96}{9} + \frac{768+192+24}{8} + \frac{768+3072}{5} + \frac{1536+2304}{4} = 3903\,.$$

We observe that there are $(2^{11}-1)-1967=80$ missing classes in the case of $\Lambda_{11}^{\min}$ and $(2^{12}-1)-3903=192$ in the case of $\Lambda_{12}^{\min}$. □

4. Odd Lattices Modulo 2.

In this section, we consider as previously a lattice Λ of dimension n and minimum m. Our aim is to study the contribution of norm $2m+1$ vectors. Such vectors of course do not exist if Λ is even. In the proposition below, the rôle of the dual of an $\mathbb{A}_k$ lattice resembles the one it plays for norm $2m+m'$ vectors with respect to Λ mod 3.

THEOREM 4.1. *Let Λ be integral.*

(1) *Vectors of norm $2m+1$ (if any) are minimal in their class modulo 2.*
(2) *If $\min\Lambda$ is odd, each class contains at most $2m+2$ pairs of such vectors, and when this bound is attained, their configuration is that of $S(\mathbb{A}_{2m+1}^*)$.*

PROOF. Let $x\in S_{2m+1}(\Lambda)$, and let $y\equiv x \mod 2\Lambda$, say, $y=x+2z$. By Proposition 1.1, we have $N(y)\geq 2m-1$. Since $y\equiv x \mod 2 \Longrightarrow N(y)\equiv N(x) \mod 4$, we must have $N(y)\geq N(x)$, which proves the first part of Theorem 4.1.

Suppose now that $N(y)=N(x)=2m+1$. Writing $-y=x-2(x+z)$, we see that changing y into $-y$ amounts to exchanging z and $-(x+z)$. In the sequel, we shall assume that $N(z)=m+1$ and $N(x+z)=m$. With this choice we have $x\cdot z=-(m+1)$, hence $x\cdot y=2m+1-2(m+1)=-1$.

LEMMA 4.2. *Let $\pm x_1,\dots,\pm x_r$, $r\geq 2$ be a system of norm $2m+1$ vectors in Λ belonging to the same class modulo $2\,\Lambda$. Then for a convenient choice of the x_i among $x_i,-x_i$, the scalar products $x_i\cdot x_j$, $j\neq i$ all have the same value, namely $+1$ if m is even, and -1 if m is odd.*

PROOF OF 4.2. For $i=2,\dots,r$, define z_i by $x_i=x_1+2z_i$. Taking $x=x_1$ and $y=x_i$ in the calculation we made in the course of the proof of Theorem 4.1, we see that we may choose the signs of the x_i so that $x_1\cdot x_i=-1$ for all $i\geq 2$. We then have

$$x_i\cdot x_j=(x_1+2z_i)\cdot(x_1+2z_j)=2m+1-4(m+1)+4\,z_i\cdot z_j$$

hence

$$z_i\cdot z_j=\frac{2m+3+x_i\cdot x_j}{4}$$

for $2\leq i<j\leq r$. We must have $x_i\cdot x_j+2m+3\equiv 0 \mod 4$, whence the result for $2\leq i<j\leq n$. Negating x_1 if m is even yields the desired result in all cases. □

END OF PROOF OF 4.1. Since m is odd, we may assume by Lemma 4.2 that $x_i\cdot x_j=-1$ for all pairs (i,j) with $j\neq i$. Since

$$N(x_1+\cdots+x_r)=r(2m+1)-2\binom{r}{2}=r\,(2m+2-r)\geq 0\,,$$

we have $r\leq 2m+2$, and $x_1,\dots,x_r$ generate a canonical section of $\mathbb{A}_{2m+1}^*$ scaled to norm $2m+1$. Since the vectors $\frac{x_i+x_j}{2}$ belong to Λ, we are done. □

EXAMPLE 4.3. Let Λ be $\mathbb{E}_7^*$ scaled to minimum 3. This is an integral lattice, whose norms are the positive integers congruent to 0 or -1 modulo 4. We have $s_3=28$, $s_4=63$ and $s_7=288$, hence

$$s_3+s_4+\frac{s_7}{8}=28+63+36=127=2^7-1\,.$$

Theorem 4.1 hence shows that the shortest vectors in classes modulo 2 of Λ are those of norm 3, 4, and 7.

5. Lattices of Codimension 1.

In this section, we assume that Λ is integral. We explain how to construct lattices of dimension $n-1$ from a vector $e \in \Lambda$ of norm μ in the range $m \le \mu < 2m$. (Everything also works if $\mu = 2m$, but the configuration of minimal vectors of the lattices we are going to construct are then uninteresting orthogonal configurations.) We denote by $\mathcal{C}$ the class of e modulo 2.

LEMMA 5.1. *Let e be as above and let $x \equiv e \mod 2\Lambda$. Then one of the following conditions holds:*

(1) *x is proportional to e.*
(2) *$N(x) > 4m - \mu$.*
(3) *$N(x) = 4m - \mu$ and x is orthogonal to e.*

PROOF. Write $x = e + 2z$. Proposition 1.1 shows that if x is not proportional to e, then $N(x) \ge 4m - N(e)$, and that if equality holds, then $e \cdot z = -\frac{N(e)}{2}$, which implies $e \cdot x = e \cdot (e + 2z) = 0$. □

LEMMA 5.2. *$L = \mathcal{C} \cup 2\Lambda$ is a lattice of determinant $2^{2n-2} \det(\Lambda)$.*

PROOF. We have $\mathcal{C} \cup 2\Lambda = 2\Lambda \cup (e + 2\Lambda)$. Hence L is a lattice containing 2Λ to index 2, which shows that $\det(L) = 2^{-2} \det(2\Lambda)$. □

By Lemma 5.1, $\min L = \mu$ and $S(L) = \{\pm e\}$. To obtain a lattice with a larger minimum, we consider $L_e = (\mathbb{R}\, e)^\perp \cap L$.

PROPOSITION 5.3. *$L_e = (\mathbb{R}\, e)^\perp \cap L$ is an $(n-1)$-dimensional lattice of minimum $M \ge 4m - \mu$ and determinant $2^{2n-2}\mu \det(\Lambda)$ if μ is even, and $2^{2n}\mu \det(\Lambda)$ if μ is odd.*

PROOF. Only the last assertion needs a proof. Given a primitive vector $e' \in L^*$, the determinant of $L' = L \cap (\mathbb{R}\, e')^\perp$ is $\det(L') = \det(L)\, N(e')$ (see [**6**], Proposition 1.3.4; $N(e')$ is the determinant of the 1-dimensional lattice $(\mathbb{R}\, e') \cap L^*$). Here we must determine a generator e' of $\mathbb{R}\, e \cap L^*$. We have $L = \langle 2\Lambda, e\rangle$ and $(2\Lambda)^* = \frac{1}{2}\Lambda^*$, hence

$$L^* = \left\{ \frac{y}{2} \,\middle|\, y \in \Lambda^*,\ y \cdot e \equiv 0 \mod 2 \right\}.$$

If μ is even, $e \in L^*$; if μ is odd, $2e \in L^*$. Since e is primitive in Λ (because $N(e) < 4m$), a congruence $e \cdot y \equiv 0 \bmod a$ may not hold on Λ^* for an integer $a > 1$. This shows that if μ is even (resp. odd), e (resp. $2e$) is primitive in L^*. This completes the proof of the proposition. □

PROPOSITION 5.4. *Let $\Lambda_e = L_e$ if $\mu \equiv 1 \mod 2$, $\Lambda_e = \frac{1}{\sqrt{2}} L_e$ if $\mu \equiv 2 \mod 4$, and $\Lambda_e = \frac{1}{2} L_e$ if $\mu \equiv 0 \mod 4$. Then Λ_e is an integral lattice, and we have $\det(\Lambda_e) = 2^{2n}\mu \det(\Lambda)$ if $\mu \equiv 1 \mod 2$, $\det(\Lambda_e) = 2^{n-2}\mu \det(\Lambda)$ if $\mu \equiv 2 \mod 4$, and $\det(\Lambda_e) = \frac{\mu}{4} \det(\Lambda)$ if $\mu \equiv 0 \mod 4$.*

PROOF. The assertions concerning the determinant of Λ_e follow immediately from Proposition 5.3. It thus suffices to prove that $x, y \in L_e \Longrightarrow x \cdot y \equiv 0 \mod (4, \mu)$. Write $x = 2z$ (resp. $x = e + 2z$) if $x \in 2\Lambda$ (resp. $x \notin 2\Lambda$), and similarly $y = 2t$ or $y = e + 2t$. If both x and y belong to 2Λ, then $x \cdot y \equiv 0 \mod 4$. If, say,

$x \in 2\Lambda$ and $y \notin 2\Lambda$, we again have $x \cdot y = 2(z \cdot e) + 4\, z \cdot t = 4\, z \cdot t \equiv 0 \mod 4$. Finally, in the remaining case, we have

$$x \cdot y = \mu + 2e \cdot z + 2e \cdot t + 4\, z \cdot t \text{ and } 2(e \cdot z) \equiv 2(e \cdot t) \equiv -\mu \mod 4\,,$$

hence $x \cdot y \equiv -\mu \mod 4$. □

We now give some examples. In all cases we shall consider, the minimum of Λ_e is equal to the lower bound given in Proposition 5.3.

If $m = 2$ and if Λ is even, the only possible choice is $\mu = 2$. Take for Λ an irreducible root lattice of dimension $n \geq 2$. Then norm 6 vectors in Λ belong to one or two classes modulo 2, and exactly one such class $\mathcal{C}$ contains a norm 2 vector e. When Λ is isometric to $\mathbb{A}_n$ ($n \geq 2$), $\mathbb{D}_n$ ($n \geq 4$), $\mathbb{E}_6$, $\mathbb{E}_7$, and $\mathbb{E}_8$, Λ_e has minimum 3, and $s(\Lambda_e)$ is equal to $n-1$, $2(n-2)$, 10, 16, and 28 respectively. The lattice corresponding to $\mathbb{E}_8$ is a scaled copy of $\mathbb{E}_7^*$, and $\mathbb{E}_7$ and $\mathbb{E}_6$ yield lattices similar to Coxeter's $\mathbb{D}_6^+$ and $\mathbb{A}_5^2$.

If $m = 4$, we may choose $\mu = 4$ or $\mu = 6$, obtaining in general a lattice Λ_e of minimum $M_e = 3$ if $\mu = 4$ and $M_e = 5$ if $\mu = 6$ (and no other value if Λ is even).

THEOREM 5.5. *Let Λ be an integral lattice of minimum 4.*

(1) *If $\mu = 4$, then $\min \Lambda_e \geq 3$ and $\det(\Lambda_e) = \det(\Lambda)$.*
(2) *If $\mu = 6$, Λ_e is an integral lattice whose norm 5 vectors have mutual scalar products ± 1. In particular, directions of norm 5 vectors constitute an equiangular family of lines.*

PROOF. If $\mu = 4$, the result is an immediate consequence of Proposition 5.4. Let now $\mu = 6$, and let $x = e + 2z$ and $y = e + 2t$ ($y \neq \pm x$) be two norm 10 vectors in L_e. We have $x \cdot y = -6 + 4\, z \cdot t$ (see the proof of Proposition 5.4). Since z and t are minimal in Λ, we have $z \cdot t \in \{4, 2, 1, 0, -1, -2, -4\}$. Since $y \neq \pm x$, we have $|x \cdot y| \leq 5$, which implies $z \cdot t = 2$ or 1, hence $x \cdot y = \pm 2$. This proves that non-proportional norm 5 vectors in Λ_e have scalar product ± 1, hence that they generate an equiangular family of lines. □

We now consider the important special case of $\Lambda = \Lambda_{24}$ (the Leech lattice).

COROLLARY 5.6. *Let Λ be the Leech lattice Λ_{24}.*

(1) *If $\mu = 4$, Λ_e is the unimodular lattice O_{23} ($\min = 3$, $s = 2300$).*
(2) *If $\mu = 6$, Λ_e is the integral lattice of minimum 5 with $s = 276\, (= \frac{23 \cdot 24}{2})$ which is dual (up to scale) to the lattice $M_{23}[2]$ of [**9**], Table 19.2.*

PROOF. If $\mu = 4$, Λ_e is a unimodular lattice of minimum $M \geq 3$, hence isometric to O_{23} ([**3**], Table 16.7).

If $\mu = 6$, we use the fact that Λ_e has minimum 5 and kissing number $\dfrac{|a_{10}|}{|a_6|} = 276$, where we denote as in [**7**] by a_6 (resp. a_{10}) the unique orbit of vectors of norm 6 (resp. 10) in Λ_{24}. Theorem 9.1 of [**9**] (and the results of [**5**] on equiangular families of lines) now shows that Λ_e, as an integral lattice of minimum 5 with equiangular directions of minimal vectors and maximal possible value of s, is similar to $M_{23}[2]^*$. [For $\mu = 4$, since $\dfrac{|b_{12}|}{|a_4|} = 2300$ (notation of [**7**]), we recover the equality $s(\mathrm{O}_{23}) = 2300$.] □

REMARK 5.7. The integral scaled copies L of $M_{23}[2]^*$ (of minimum 5) and L' of M_{23}^* (of minimum 15) which occur in Table 19.2 of [**9**] have the same configurations of minimal vectors. Indeed, L' contains to index 2 a lattice isometric to $\sqrt{3}\,L$. The successive layers of L (resp. L') have norms $5, 8, 9, 12, \dots$ (resp. $15, 20, 24, \dots$). This shows that L contains a class modulo 3 of minimum 60, which produces vectors of norm $3 \cdot \frac{60}{9} = 20$ in L'.

Similarly, using the parity class of O_{23} (of minimum 15; see [**4**], where Elkies proves a much more general result), we obtain after rescaling an integral lattice of minimum 12. This lattice is indeed proportional to Λ_{23}^*.

References

[1] E. Bannai, A. Munemasa, B. Venkov, *The Nonexistence of Certain Tight Spherical Designs (with an appendix by Y.-F. S. Peterman)*, preprint.

[2] C. Batut, J. Martinet, *A Catalogue of Perfect Lattices*, http://www.math.u-bordeaux.fr/~martinet .

[3] J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren **290**, Springer-Verlag, Heidelberg (1988). Third edition: 1993.

[4] N. Elkies, *Lattices and codes with long shadows*, Math. Res. Lett. **2** (1995), 643–651.

[5] P. W. H. Lemmens, J. J. Seidel, *Equiangular lines*, J. Algebra **24** (1973), 494–512.

[6] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Grundlehren **327**, Springer-Verlag, Heidelberg (2003). (English corrected and updated edition of a French version, Masson (now Dunod), Paris, 1996.)

[7] J. Martinet, *Reduction Modulo* 2 *and* 3 *of Euclidean Lattices*, J. Algebra **251** (2002), 864–887.

[8] W. Plesken, M. Pohst, *Constructing integral lattices with prescribed minimum. I*, Math. Comp. **45** (1985), 209–221 and S5–S16.

[9] B. Venkov, *Réseaux et "designs" sphériques* (Notes by J. Martinet), in Réseaux euclidiens, designs sphériques et groupes, L'Ens. Math., Monographie **37**, J. Martinet, ed., Genève (2001), 10–86.

J. MARTINET
A2X, INSTITUT DE MATHÉMATIQUES
UNIVERSITÉ BORDEAUX 1
351, COURS DE LA LIBÉRATION
F–33405 TALENCE CEDEX
E-mail address: martinet@math.u-bordeaux.fr