Bases of minimal vectors in lattices, I

Jacques Martinet

Abstract. We prove that a Euclidean lattice of dimension $n \le 8$ which is generated by its minimal vectors possesses a basis of minimal vectors.

Résumé. Nous montrons qu'un réseau euclidien de dimension $n \le 8$ engendré par ses vecteurs minimaux possède une base de vecteurs minimaux.
TITRE FRANÇAIS : Bases de vecteurs minimaux dans les réseaux, I.

Mathematics Subject Classification (2000). 11H55.

Keywords. Euclidean lattices, minimal vectors, bases.

1. Introduction

In their paper [1], Conway and Sloane constructed an 11-dimensional lattice generated by its minimal vectors having no basis of minimal vectors. We do not know whether such an example may exist in a lower dimension. However, the theorem below shows that if this occurs, then the lattice must have dimension at least 9:

Theorem 1.1. *A lattice of dimension $n \le 8$ which is generated by its minimal vectors has a basis of minimal vectors.*

We denote by E an n-dimensional Euclidean vector space. We say that a lattice $\Lambda \subset E$ is *well rounded* if its minimal vectors span E. Any system of n independent minimal vectors generates a sublattice Λ' of finite index in Λ. We denote by $\imath = \imath(\Lambda)$ the *maximal index* $[\Lambda : \Lambda']$ for sublattices Λ' generated by n independent minimal vectors of Λ.

The proof makes use of our knowledge of the possible values of $\imath$ and of the corresponding structure of the set of minimal vectors of Λ. Our basic reference for the index is [3], which relies on previous work of Watson, Ryshkov, and Zahareva. In particular, we shall make constant use of the results displayed in Table 11.1 of [3].

When $\imath$ is relatively small, we prove more, namely:

Travail effectué avec le soutien de l'Université Bordeaux 1 et du C.N.R.S. (UMR 5251).

Theorem 1.2. *A lattice of maximal index $\imath \leq 4$ and dimension $n \leq 10$ which is generated by its minimal vectors has a basis of minimal vectors.*

After having recalled in Section 2 a few results about the index, we prove Theorem 1.2 in Section 3; in particular, we obtain there a fairly precise description of lattices for which $\imath = 3$ and $n = 11$; Conway–Sloane's example is precisely a lattice of this type. Theorem 1.1 will result from Theorem 1.2 in dimensions $n \leq 7$. The case of dimension 8 is then solved in Section 4.

In the forthcoming paper [4], we shall prove the existence in low dimensions of small lower bounds s_0 for s ($2s$ is the *kissing number*) which ensure that a well rounded lattice with $s \geq s_0$ is indeed generated by its minimal vectors, hence possesses by Theorem 1.1 a basis of minimal vectors (such a problem was considered by Csóka in [2]). For this reason, ours proofs establish somewhat stronger assertions than what is strictly needed for the proof of Theorem 1.1 and 1.2. The late Louis Michel sent me in 1991 a preprint in which he claimed that Theorem 1.1 holds up to dimension 10 ([5]). However his proof only deals with lattices called in our language "of index at most 3", a result which is part of our Theorem 1.2.

Acknowledgements. I warmly thank Roland Bacher for his close look at a first draft of this paper and his numerous remarks which allowed me to greatly improve the original manuscript.

2. Index and bases

Let $\Lambda \subset E$ be an n-dimensional lattice and let $e_1, \dots, e_n$ be n independent minimal vectors. We denote by Λ' the lattice they generate. We attach to Λ the set of finite Abelian groups which occur by this construction as quotients Λ/Λ' and the finite list $\mathcal{L}$ of possible indices $[\Lambda : \Lambda']$. The existence of a basis of minimal vectors amounts to the inclusion $1 \in \mathcal{L}$.

Given Λ as above, we can write $\Lambda = \langle \Lambda', f_1, \dots, f_k \rangle$ where each f_i is of the form $\frac{a_1 e_1 + \cdots + a_n e_n}{d}$ for integers $d > 1$ and $a_1, \dots, a_n$ globally prime to d. If a vector f of this form is minimal, any non-zero a_i is a divisor of an element in the list $\mathcal{L}$: for example, if $a_1 \neq 0$ then $-e_1 = \frac{-df + a_2 e_2 + \cdots + a_n e_n}{a_1}$, which shows that $|a_i|$ divides the order of the group Λ/Λ'' where Λ'' is the sublattice generated by the minimal elements $f, e_2, \dots, e_n$.

For the vectors f_j we can choose each coefficient a_i arbitrarily modulo d, for instance we may assume that $-\lfloor \frac{d}{2} \rfloor < a_i \leq \lfloor \frac{d}{2} \rfloor$. When $k = 1$, negating some e_i if necessary, we may assume that $a_i \geq 0$. Removing unnecessary zero-vectors and reordering the $e_1, \dots, e_n$ appropriately, we may write $\Lambda = \langle \Lambda', f \rangle$ where f is in a canonical form

$$f = \frac{a_1 e_1 + \cdots + a_p e_p}{d}\,,$$

with $p \leq n$ and $0 < a_1 \leq \cdots \leq a_p \leq \lfloor \frac{d}{2} \rfloor$.

With this notation, we have the following theorem; for a proof, see [3], *Théorème 2.9*:

Theorem 2.1. (Watson) *We have* $\sum_{i=1}^{p} |a_i| \geq 2d$ *and equality holds if and only if* $e - e_i$ *is minimal for every* i. $\square$

From Table 11.1 of [3], we see that we have $\imath \leq 4$ for all well rounded lattices of dimension $n \leq 7$, except for the 7-dimensional lattices which are similar to the root lattice $\mathbb{E}_7$. Since root lattices have bases of minimal vectors, Theorem 1.2 implies Theorem 1.1 for $n \leq 7$.

In the sequel, we consider a lattice Λ together with n independent minimal vectors $e_1, \dots, e_n$, which constitute a basis for a lattice Λ' of index $\imath$ in Λ. A necessary and sufficient condition for Λ to be generated by minimal vectors is that there exists minimal vectors $f_1, \dots, f_r$ in Λ which generate Λ over Λ'. If $[\Lambda : \Lambda']$ is a prime power, these vectors may be assumed to induce a minimal system of generators for Λ/Λ'. Otherwise, their number may be larger than the cardinality of a minimal system of generators. We shall have to consider this latter case when $[\Lambda : \Lambda'] = 6$. The condition is then that there exists in $S(\Lambda)$ either an f of order 6 modulo Λ', or vectors f_k, $k = 2, 3$ of order k modulo Λ'.

3. Lattices of small index

We now turn to the proof of Theorem 1.2. Of course, there is nothing to prove if $\imath = 1$. We consider first lattices with maximal index $\imath(\Lambda) = 2^r$ realised by a sublattice Λ' such that Λ/Λ' is 2-elementary. We consider next the case of lattices with maximal index $\imath = 3$ or $\imath = 4$, achieved by a cyclic group Λ/Λ'.

Lemma 3.1. *If the maximal index* $\imath(\Lambda)$ *of* Λ *is realised by a* 2*-elementary group* Λ/Λ' *of order* $2^r \leq 32$*, then* Λ *has a basis of minimal vectors.*

Proof. There exist vectors $(e'_1, \dots, e'_r) \in \Lambda$ whose images modulo Λ' form a basis of Λ/Λ' over $\mathbb{F}_2$, and such that each coset $e'_i + \Lambda'$ contains a minimal vector f_i of Λ. Each e'_i may be assumed to be of the form $\dfrac{e_{i_1} + \cdots + e_{i_s}}{2}$ with $i_s \geq 4$ by a theorem of Watson (Theorem 2.2 in [3]). Since each $L_i = \langle \Lambda', f_i \rangle$ is of index 2^{r-1} in Λ, each f_i is of the form $\dfrac{\pm e_{i_1} \pm \cdots \pm e_{i_k} \pm 2e_{j_1} \pm \cdots \pm 2e_{j_\ell}}{2}$. The images in $\mathbb{F}_2^n$ of the f_i constitute a basis $(w_1, \dots, w_r)$ for a binary code $\mathcal{C}$ of length n (and dimension r). We are faced with a problem in coding theory:
Question. *Can one choose* r *distinct indices* ℓ_i *with* ℓ_i *in the support of the word* w_i *?*
When the answer is positive, we immediately obtain a basis for Λ by replacing e_{ℓ_i} by f_i for $i = 1, \dots, r$. Now, the answer to the question above is obviously "yes" if $r \leq 4$, since $\mathcal{C}$ is of weight $w \geq 4$ again by Watson's theorem. If $r \leq 5$, and if $(\ell_1, \ell_2, \ell_3, \ell_4)$ is the word w_5 of $\mathcal{C}$, then w_1 certainly contains a non-zero coordinate ℓ'_1 at a place different from ℓ_2, ℓ_3, ℓ_4, and we can use the 5 indices $\ell'_1, \ell_1, \dots, \ell_4$. $\square$

Lemma 3.2. *If Λ has maximal index 3 and if $n \le 10$, then Λ has a basis of minimal vectors.*

Proof. Write $\Lambda = \Lambda' \cup \pm(\Lambda' + e)$ with $e = \frac{e_1+\cdots+e_p}{3}$. By a theorem of Watson (see [3], Example 3.6 and the five preceding lines), we have $p \ge 6$, and if $p = 6$, then the 6 vectors $e_i' = e - e_i$, $i = 1, \dots, 6$ are also minimal. In this case, $(e_1, e_1', e_3, \dots, e_n)$ is a basis for Λ. (Note that we did not make use of the hypothesis that $S(\Lambda)$ is generated by its minimal vectors.) Suppose now that $p \ge 7$. By hypothesis, there exists $f \in S(\Lambda) \cap (\Lambda' + e)$. Such a vector is of the form

$$f = \frac{a_1e_1 + \cdots + a_pe_p + b_1e_{p+1} + \cdots + b_qe_{p+q}}{3}$$

with $a_i = 1$ or -2, $b_j = \pm 3$ and $p + q \le n$. If, say, $a_1 = 1$, then $(f, e_2, \dots, e_n)$ is a basis for Λ. If $a_i = -2$ for $i = 1, \dots, p$, we have $f + e_{p+1} + \cdots + e_{p+q} \equiv 0 \mod 2\Lambda$. If $q \ge 4$, then $n \ge 11$. If $q \le 3$, then $q = 3$, and $f' = \frac{f \pm e_{p+1} \pm e_{p+2} \pm e_{p+3}}{2}$ is a minimal vector of Λ. Let $L \subset \Lambda$ be the lattice generated by the n vectors $f', e_2, \dots, e_n$. This contains $f = 2f' \mp e_{p+1} \mp e_{p+2} \mp e_{p+3}$ and $e_1 = 2f' - 3f - e_2 - \cdots - e_p$, hence $\langle \Lambda', f \rangle = \Lambda$. This shows that $\Lambda = L$, hence that $(f', e_2, \dots, e_n)$ is a basis for Λ. $\square$

Remark 3.3. The lower bound $n \ge 11$ in Lemma 3.2 for the existence of a lattice of maximal index 3 generated by its minimal vectors, but without a basis of minimal vectors, is the best possible, as shown by Conway and Sloane's example of [1], which is obtained taking $p = 7$ and $q = 4$, and giving only three values to the scalar products $e_i \cdot e_j$, $i < j$. (This is *a priori* possible, using the averaging argument of [3], Proposition 8.5.)

Lemma 3.4. *If Λ has maximal index 4, if Λ/Λ' is cyclic, and if $n \le 10$, then Λ has a basis of minimal vectors.*

Proof. Let Λ/Λ' be cyclic, say $\Lambda = \langle \Lambda', e \rangle$, with

$$e = \frac{e_1 + \cdots + e_p + 2e_{p+1} + \cdots + 2e_{p+q}}{4} = \frac{e' + e_{p+1} + \cdots + e_{p+q}}{2},$$

$p + q \le n$, and $e' = \frac{e_1+\cdots+e_p}{2}$.

Watson's theorem (Théorème 3.2 in [3]) implies that we must have $p \ge 4$, and that when equality holds, e' is minimal. Then, if $q = 3$, e is minimal, and $(e', e_2, \dots, e_6, e, e_8, \dots, e_n)$ is a basis of minimal vectors for Λ. (Such an unconditional result also holds if $p = 6, q = 1$ or $p = 8, q = 0$.)

From now on, we suppose that $p \ge 5$. Since $S(\Lambda)$ is a generating set for Λ, there exists $f \in (e + \Lambda) \cap S(\Lambda)$, say

$$f = \frac{a_1e_1+\cdots+a_pe_p+b_1e_{p+1}+\cdots+b_qe_{p+q}+c_1e_{p+q+1}+\cdots+c_re_{p+q+r}}{4},$$

with $a_i \in \{-3, 1\}$, $b_j = \pm 2$, $c_k = \pm 4$, and $p + q + r \le n$, and we even may assume that $b_j = +2$ and $c_k = -4$ (by negating some e_j or e_k). If one of the a_i is equal to 1, we are done. Otherwise,

$$f' = \frac{f + e_{p+1} + \cdots + e_{p+q} + e_{p+q+1} + \cdots + e_{p+q+r}}{3}$$

is a vector of Λ. If $q+r\geq 6$, we have $n\geq p+6\geq 11$. If $q+r\leq 5$, then equality holds in Watson's theorem and the vector $f''=f'-e_{p+1}$ is minimal. Replacing f by its explicit expression on $e_1,\dots,e_n$, we obtain

$$f''=\frac{-e_1-\cdots-e_p-2e_{p+1}+2e_{p+2}+\cdots+2e_{p+q}}{4}\,,$$

which shows that $(f'',e_2,\dots,e_n)$ is a basis for Λ whose elements lie in $S(\Lambda)$. $\square$

Proof of Theorem 1.2. Putting together the three lemmas above, we immediately obtain Theorem 1.2. [Note that the existence of a basis of minimal vectors for lattices of 2-elementary type could be proved for dimensions far beyond dimension 11.] $\square$

4. Lattices in dimension 8

In this section, we consider lattices of dimension $n=8$. From [3], Table 11.1, we see that Λ contains a lattice Λ' generated by n independent minimal vectors $e_1,\dots,e_n$ such that one of the following conditions holds:
- $[\Lambda:\Lambda']\leq 6$;
- $[\Lambda:\Lambda']=8$ and Λ/Λ' is not cyclic;
- $[\Lambda:\Lambda']=9$ or 16, and Λ is similar to $\mathbb{E}_8$.

Using Theorem 1.2 together with the fact that $\mathbb{E}_8$ has a basis of minimal vectors, we see that the proof of Theorem 1.1 reduces to a study of 8-dimensional lattices of maximal index 5, 6, or 8.

Table 11.1 of [3] displays 3, 6, and 6 possible types (in the sense of [3]) for each index 5, 6, and 8, that we denote by $5a$ to $5c$, $6a$ to $6f$, and $8a$ to $8f$ respectively, in the order they occur in the table. In all but two cases, we shall prove a stronger result, namely that there exists a basis of minimal vectors without making use of the hypothesis that $S(\Lambda)$ should generate Λ, for example:

Proposition 4.1. *Let Λ be an 8-dimensional lattice, containing a sublattice Λ' generated by minimal vectors. If $\Lambda/\Lambda'\simeq\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, then Λ has a basis of minimal vectors.*

Proof. Quotients Λ/Λ' of type $(4,2)$ correspond to types $8a$ to $8c$, and are described in Theorem 10.5 of [3] as Cases (a), (b), and (c). The third type corresponds to lattices similar to $\mathbb{E}_8$. The second one also corresponds to known lattices, which when rescaled to minimum 2, contain a cross-section Λ_0 isometric to $\mathbb{E}_7$. The high density of $\mathbb{E}_7$ implies at any minimal vector in $S(\Lambda)\smallsetminus\Lambda_0$ can be used to extend a basis for Λ_0 to a basis for Λ. To deal with the first case, we make use of the discussion which follows the proof of Theorem 10.5 in [3]. It shows that Λ is generated over Λ' by two explicitly given vectors e and f such that both cosets $\Lambda'+e$ and $\Lambda'+f$ contain minimal vectors e',f' and $(e',f',e_3,\dots,e_8)$ is a basis for Λ. $\square$

Proof of Theorem 1.1. Lemma 3.1 and Proposition 4.1 (together with the non-existence of a cyclic group $\Lambda/\Lambda'\simeq\mathbb{Z}/8\mathbb{Z}$ in dimension 8; see Table 1.1 in [3]) show the existence of a basis of minimal vectors for $\imath = 8$. We now successively consider lattices of maximal index 5 and 6, for which we refer to Section 9 of [3].

Index 5. We can write $\Lambda = \langle \Lambda', e = \dfrac{a_1e_1 + \cdots + a_8e_8}{5} \rangle$, where $a_i = 1$ for $1 \leq i \leq p$ and $a_i = 2$ for $p+1 \leq i \leq 8$, with $p = 4$, 5, or 6. Type $5c$ corresponds to $p = 6$ and gives rise to equality in Watson's theorem. This implies that $e - e_7$ is minimal and shows that $(e - e_7, e_2, \dots, e_8)$ is a basis for Λ. For type $5a$ corresponding to $p = 4$, there also exist several indices i such that $e - e_i$ is minimal. Taking $i > 1$, we see that $(e - e_i, e_2, \dots, e_8)$ is a basis for Λ.

To deal with type $5b$, we must use explicitly the hypothesis that Λ is generated by its minimal vectors, i.e. that there exists a minimal vector $f = \dfrac{a_1e_1 + \cdots + a_8e_8}{5}$ in at least one of the cosets $e + \Lambda$, $2e + \Lambda$.

In the first case, we have $a_i \in \{1, -4\}$ if $i \leq 5$ and $a_i \in \{2, -3\}$ if $i \geq 6$. If, say, $a_1 = 1$, then $(f, e_2, \dots, e_8)$ is a basis of minimal vectors. If $a_i = -4$ for $i = 1, \dots, 5$ then the sublattice L generated by f, e_6, e_7, e_8 is of maximal index $\imath \geq 4$ in the 4-dimensional lattice $\Lambda \cap (L \bigotimes \mathbb{Q})$ which is impossible.

Similarly, in the second case, we may choose

$$f \in e' + \Lambda' \quad \text{with} \quad e' = \frac{e_6 + e_7 + e_8 - 2e_1 - \cdots - 2e_5}{5}\,,$$

and we produce in the same way a 6-dimensional lattice of maximal index 4 of cyclic type, which is again impossible.

Index 6. For 5 out of the 6 types (as for types $5a$, $5c$, $8a$, $8b$, $8c$ above), we prove the existence of a basis of minimal vectors for Λ without using the fact that Λ is generated by its minimal vectors. Indeed, we can easily deduce from the data of [3], Section 9, that $e'_1 = e$ for types $6c$, $6d$, $6f$, and $e'_1 = e - e_4$ for type $6a$ is minimal, so that $(e'_1, e_2, \dots, e_8)$ is a basis of minimal vectors for Λ. (In case $6c$ this is because equality holds in Watson's theorem.) The same argument may be applied to type $6b$ with $e'_1 = e - e_5$; this can be seen on the Gram matrix given in [3], which yields generic components for the minimal vectors of *all* lattices of type $6b$.

We are finally left with type $6d$, for which

$$\Lambda = \langle \Lambda', e \rangle \quad \text{with} \quad e = \frac{e_1 + e_2 + e_3 + 2e_4 + 2e_5 + 2e_6 + 3e_7 + 3e_8}{6}\,.$$

Up to sign, non-trivial representatives for Λ modulo Λ' are e,

$$e' = \frac{e_1 + e_2 + e_3 - e_4 - e_5 - e_6}{3} \equiv 2e$$

which satisfies equality in Watson's theorem and

$$e'' = \frac{e_1 + e_2 + e_3 + e_6 + e_7}{2} \equiv 3e\,.$$

As we explained at the end of Section 2, we consider two cases, according to whether there exists or not a minimal vector in $e + \Lambda'$.

In the first case, Λ contains a minimal vector

$$f = \frac{a_1 e_1 + \cdots + a_8 e_8}{6}$$

with $|a_i| \leq 6$ for all i, with $d = 6$ or $d = 2$, and all coefficients a_i congruent modulo 6 to the corresponding coefficient of e. If $a_1 = a_2 = a_3 = -5$, the 6-dimensional lattice L generated by $f, e_4, \ldots, e_8$ is of index $\imath \geq 5$ in the lattice $\Lambda \cap (L \bigotimes \mathbb{Q})$ and this is impossible. Hence we have $a_i = 1$ for say $i = 1$ and $(f, e_2, \ldots, e_8)$ is a basis for Λ.

In the second case, Λ contains necessarily a minimal vector

$$f = \frac{a_1 e_1 + \cdots + a_8 e_8}{2} \in e'' + \Lambda'$$

whose class, together with the class of the vector e', generates the quotient group Λ/Λ'. We have $|a_i| \leq 6$ and $a_i \equiv 1 \mod 2$ for $i \in \{1, 2, 3, 7, 8\}$.

No two e_i can be equal to ± 5 for the other e_i together with f would generate a 7-dimensional lattice of index $\imath \geq 5$ in $\Lambda \cap (L \bigotimes \mathbb{Q})$. Similarly, no four a_i can be equal to 3, since otherwise there would exist 5-dimensional lattice of maximal index $\imath \geq 3$. Hence, we have $a_{i_0} = \pm 1$ for at least one index $i_0 \in \{1, 2, 3, 7, 8\}$.

Now, $e', e_2, \ldots, e_6$ generate a 6-dimensional lattice of maximal index 3. This implies that $e' - e_i$ $(i = 1, 2, 3)$ and $e' + e_j$ $(j = 4, 5, 6)$ are minimal in Λ. Replacing e_{i_0} by f and e_4 by $e' + e_4$ in the basis $(e_1, \ldots, e_8)$ for Λ', we obtain a basis of minimal vectors for Λ. This completes the proof of Theorem 1.1. $\square$

References

[1] J.H. Conway, N.J.A. Sloane, *A Lattice Without a Basis of Minimal Vectors*, Mathematika **42** (1995), 175–177.

[2] G. Csóka, *There exists a basis of minimal vectors in every $n \leq 7$ dimensional perfect lattice*, Ann. Univ. Sc. Budapest Eőtvős, Sect. Math. **30** (1987), 245–258.

[3] J. Martinet. *Sur l'indice d'un sous-réseau*, in "Réseaux euclidiens, designs sphériques et formes modulaires", J. Martinet éditeur, Monographie Ens. Math. **37**, Genève (2001), 165–213.

[4] J. Martinet. *Bases of minimal vectors in lattices, II*, preprint.

[5] L. Michel. *Lattice with no basis in the generating set s of shortest vectors*, private communication (1992).

Jacques Martinet
Institut de Mathématiques
351, cours de la Libération
33405 Talence cedex
France
e-mail: `Jacques.Martinet@math.u-bordeaux1.fr`