# THE PERFECTION DEFAULT MODULE OF A EUCLIDEAN LATTICE

(AFTER A TALK IN LUMINY, SEPTEMBER 2000)

by J. MARTINET[1]

ABSTRACT. Following an idea of Roland Bacher, we discuss a notion of perfection over $\mathbb{Z}$ for a Euclidean lattice.
RÉSUMÉ. Suivant une idée de Roland Bacher, nous discutons une notion de perfection sur $\mathbb{Z}$ pour les réseaux euclidiens.
TITRE FRANÇAIS : Le module de défaut de perfection d'un réseau euclidien.

§ **1. Introduction.** Some time ago, Bacher ([Bc]) suggested that the property of perfection for a Euclidean lattice $L$, which can be defined using symmetric tensors of degree 2 (one requires that the tensors $x \otimes x$ for $x$ minimal in $L$ span the Symmetric square of the Euclidean space), could be considered over $\mathbb{Z}$, not only as usual over $\mathbb{Q}$ or $\mathbb{R}$. We can define in this way new invariants, which contain more information on the lattice that the mere perfection rank, as defined in [M], chapter III, section 2. To this end, we construct a finitely generated $\mathbb{Z}$-module (the *perfection default module*, see below, %) inside a convenient symmetric square, whose rank is the *perfection co-rank* (i.e., $\dim \operatorname{End}^s(E)$-perfection rank of $\Lambda$). The study of its torsion submodule is the object of this note.

The notion of a perfect lattice goes back to Korkine & Zolotareff and Voronoï (1873, 1908). Perfect lattices are precisely those which possess a finite perfection default module. They are the central object of our study.

Several years ago, for algorithmic reasons, Batut and myself considered perfection modulo a prime $p$: if the linear forms which define the perfection of a lattice have maximal rank modulo some prime $p$, then the lattice is certainly perfect. However, we were not able to assert conversely that a lattice which is not perfect modulo some conveniently chosen prime $p$ is indeed not perfect in the usual sense, since there may be a phenomenon of "bad reduction". Bacher's notion of a perfection default module might be an important tool to solve the question above: "good primes" are those which do not divide the order of its torsion submodule.

§ **2. Symmetric squares.** Let $R$ be a commutative ring and let $M$ be an $R$-module. Usually (e.g. in [Bou1], III, pp. 67 and 76), the symmetric algebra (as well as the exterior algebra) of $M$ is defined as a quotient of the tensor algebra $\bigotimes M$. In what follows, we need modify the definition of the symmetric algebra. We only need to consider the degree 2 part of the symmetric algebra.

*Key words and phrases.* Perfect lattices, symmetric squares. October, 2000.
[1]laboratoire A2X, UMR 5465 associée au C.N.R.S. – Université Bordeaux 1

**2.1. Definition.** The *symmetric square of $M$* denoted by $\mathrm{Sym}^2(M)$ (or $\mathrm{Sym}^2_R(M)$ if we need the ring $R$ in the notation) is the submodule of $\bigotimes^2 M$ generated by the symmetric tensors $x\otimes x$, $x\in M$.

[Note that the inclusion $\mathrm{Sym}^2(M)\hookrightarrow \bigotimes^2 M$ induces an isomorphism of $\mathrm{Sym}^2(M)$ onto the classical $\bigvee^2 M$ anytime the map $x\mapsto 2x$ is bijective, compare [Bou1], III, p. 68.]

In the applications to lattices, $M$ will be either a vector space over $\mathbb{Q}$ or $\mathbb{R}$, in which case the above map is bijective, or a finitely generated torsion free $\mathbb{Z}$-module, in which case it is not, except for $M=\{0\}$.

Let $T$ be a generating subset of $M$, endowed with an arbitrary total ordering. Then, the identity

$$\textbf{(2.2)}\qquad (\sum_{x\in T}\lambda_x x)\otimes(\sum_{y\in T}\lambda_y y)=\sum_{x\in T}\lambda_x\lambda_x\, x\otimes x+\sum_{x<y}\lambda_x\lambda_y(x\otimes y+y\otimes x)$$

shows that $\mathrm{Sym}^2(M)$ is generated by the split symmetric tensors $x\otimes x$, $x\in T$ on the one hand, and the tensors $(x\otimes y+y\otimes x)$, $x,y\in T$ on the other hand. The identities

$$\textbf{(2.3)}\qquad (x\pm y)\otimes(x\pm y)-x\otimes x-y\otimes y=\pm(x\otimes y+y\otimes x)$$

shows that we may replace for any pair $(x,y)\in T\times T$ the tensor $x\otimes y+y\otimes x$ by one of the tensors $(x+y)\otimes(x+y)$ or $(x-y)\otimes(x-y)$.

**2.4. Definition.** For $S\subset M$, let $S^{(2)}=\{x\otimes x\mid x\in S\}$, and let $\mathrm{Perf}_S(M)$ be the submodule of $\mathrm{Sym}^2(S)$ generated by $S^{(2)}$. We call $\mathrm{Perf}_S(M)$ the *perfection module of $M$ ( with respect to $S$)*. We often write $\mathrm{Perf}(M)$ rather than $\mathrm{Perf}_S(M)$ when the reference to $S$ is clear from the context.

Since we are interested in the submodule of $\mathrm{Sym}^2(M)$ generated by $S^{(2)}$, we may assume that 0 does not belong to $S$ and that $S=-S$ (just replace if necessary $S$ by $S\cup -S$). Denote now by $S'$ a system of representatives of $S/\{\pm 1\}$. We then have $S=S'\cup(-S')$, $S\cap S'=\emptyset$, and of course $S^{(2)}={S'}^{(2)}$.

Let $N$ be a submodule of $M$ and let $P=M/N$. The embedding $N\hookrightarrow M$ induces maps $N\bigotimes N\to N\bigotimes M\to M\bigotimes M$, which are injective whenever $\mathrm{Tor}_1^R(P,N)=\mathrm{Tor}_1^R(P,M)=0$, whose product $N\bigotimes N\to M\bigotimes M$ is then also injective.

Take now $N=\langle S\rangle$. The quotient $\mathrm{Sym}^2(M)/\mathrm{Perf}(M)$ is an extension of the two modules $\mathrm{Sym}^2(N)/\mathrm{Perf}(M)=\mathrm{Sym}^2(N)/\mathrm{Perf}(N)$ and $\mathrm{Sym}^2(M)/\mathrm{Sym}^2(N)$. For this reason, we shall most of the time restrict ourselves to pairs $(M,S)$ where $S$ generates $M$. This hypothesis does not imply that $S^{(2)}$ generates $\mathrm{Sym}^2(M)$! In applications to lattices, such a circumstance is indeed rather scarce, see below, section %. Note for further use the following result, which easily follows from formulae 2.2 and 2.3:

**2.5. Proposition.** *If $S$ contains a generating system $\{e_1,\dots,e_r\}$ of $M$ together with all differences $e_j-e_k$, $j\neq k$, then* $\mathrm{Perf}(M)=\mathrm{Sym}^{(2)}(M)$. $\square$

**2.6. Definition.** The quotient

$$\mathrm{Dft}_S(M)=\mathrm{Sym}^2(M)/\mathrm{Perf}_S(M)$$

is called the *perfection default module* of $(M, S)$. We shall forget the index $S$ when the reference to $S$ is clear from the context.

**§ 3. Dedekind domains.** In this section, we suppose that $R$ is a Dedekind domain. We denote by $K$ is fraction field, by $M$ a finitely generated torsion free $R$-module, and by $V$ be the $K$-vector space $M \bigotimes_R K$. We still consider a symmetric subset $S$ of $M$ which does not contain 0.

Since $R$ is Dedekind, the torsion product $\operatorname{Tor}_1^R(M_1, M_2)$ is zero anytime at least one of the modules $M_1, M_2$ is torsion free (reduce by localization to the case when $R$ is a principal ideal domain, and apply [Bou1], X, p. 29, prop. 3.) Thus, for any submodule $N$ of $M$, $\operatorname{Sym}^2(N)$ can be identified with a submodule of $\operatorname{Sym}^2(M)$. In particular, the canonical map $x \mapsto x \otimes 1 : M \simeq M \bigotimes R \to V$ is injective. We use it to embed $M$ inside $V$. By making use of the composition of the maps $M \bigotimes M \to M \bigotimes V \to V \bigotimes V$, we obtain a canonical embedding

$$\operatorname{Sym}^2(M) \hookrightarrow \operatorname{Sym}^2(V)\,.$$

**3.1. Definition.** The rank $r$ of $S^{(2)}$ in $\operatorname{Sym}^2(V)$ is called the *perfection rank of* $S$, and the difference $\frac{n(n+1)}{2} - r = \dim \operatorname{Sym}^2(V) - r$ the *perfection co-rank of* $S$. We say that $M$ is *perfect (with respect to* $S$*)* if $r$ is maximum, i.e. if $S^{(2)}$ spans $\operatorname{Sym}^2(V)$.

Clearly,

$$M \text{ is perfect } \iff V \text{ is perfect } \iff \operatorname{Dft}_S(M) \text{ is torsion.}$$

**3.2. Proposition.** *If $(M, S)$ is perfect, then $S$ spans $V$.*

*Proof.* Let $W$ be the span of $S$ in $V$. There exists a direct sum decomposition $V = W \bigoplus W'$, which shows that $\operatorname{Sym}^2(W')$ is a direct summand of $\operatorname{Sym}^2(V)$. Because of the inclusion $S^{(2)} \subset \operatorname{Sym}^2(W)$, $M$ cannot be perfect unless $\operatorname{Sym}^2(W') = 0$, which implies $W' = 0$, hence $W = V$. □

The rank of the perfection default module is the perfection co-rank of $M$. Its torsion submodule is a new invariant, that we shall investigate later, at least for perfect modules. In the applications, $K$ will be a number field. This implies that the torsion submodule of the perfection default module is finite, since all residue fields of $R$ are then finite.

**3.3. Proposition.** *If $\operatorname{Dft}_S(M) = 0$, then $S$ generates $M$.*

*Proof.* If $M = \{0\}$, there is nothing to prove. Otherwise, let $N$ be the submodule of $M$ generated by $S$, and let $P = M/N$. Since $M$ is perfect, we have $\dim N = \dim M = n \neq 0$. The commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N \bigotimes N & \longrightarrow & N \bigotimes M & \longrightarrow & N \bigotimes P & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M \bigotimes M & \longrightarrow & M \bigotimes M & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

yields via the snake lemma an injective map $N \bigotimes P \hookrightarrow M \bigotimes M/N \bigotimes N$. Now, we have the inclusions $\langle S \bigotimes S \rangle \subset N \bigotimes N \subset M \bigotimes M$. Since $\mathrm{Dft}(M) = 0$, we have $\langle S \bigotimes S \rangle = M \bigotimes M$, hence $N \bigotimes N = M \bigotimes M$, whence $N \bigotimes P = 0$. Since $N$ is projective and non-zero, this implies $P = 0$, i.e. $N = M$. $\square$

Recall that given a finitely generated torsion free $R$-module $P$ of rank $p$ and a submodule $Q$ of $P$ of rank $q$ ($q \le p$), there exist a $K$-basis $\mathcal{B} = (e_1, \dots, e_p)$ of $W = K \bigotimes P$ (we identify $P$ to a submodule of $W$, so that $W = KP$), fractional ideals $\mathfrak{b}_1, \dots, \mathfrak{b}_p$ of $R$ and integral ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_q$ of $R$ such that

(1) $P = \mathfrak{b}_1 e_1 \bigoplus \dots \bigoplus \mathfrak{b}_p e_p$ ;
(2) $Q = \mathfrak{a}_1 \mathfrak{b}_1 e_1 \bigoplus \dots \bigoplus \mathfrak{a}_q \mathfrak{b}_q e_q$ ;
(3) $\mathfrak{a}_1 \mid \mathfrak{a}_2, \dots, \mathfrak{a}_q \mid \mathfrak{a}_{q-1}$ .

Moreover, the integers $p$, $q$ and the sequence $\mathfrak{a}_1, \dots, \mathfrak{a}_q$ are invariants of the isomorphism class of the pair $(P, Q)$.

**3.4. Definition.** The ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_q$ are called the *elementary divisors* of the pair $(P, Q \subset P)$. The ordered set $(\mathfrak{a}_1, \dots, \mathfrak{a}_q)$, denoted $\mathrm{Smith}(P, Q)$, is called the *Smith invariant of* $(P, Q)$.

The torsion submodule of $P/Q$ is $P/(P \cap KQ)$, and we have a direct sum decomposition $P/Q = P/(P \cap KQ) \bigoplus P'$ where $P'$ is a projective $R$-module of rank $p - q$. The first term $\mathfrak{a}_1$ is the annihilator of $P/Q$. The last one $\mathfrak{a}_q$ is a "measure of imprimitivity" for the pair $(P, Q)$; it becomes trivial when we replace $Q$ by $Q' = \mathfrak{a}_q^{-1} Q$; note that when $\mathfrak{a}_q$ is principal, $Q'$ is isomorphic to $Q$. The product of the ideals $\mathfrak{a}_i$ is an "$R$-index": over $\mathbb{Z}$, it is simply the index $[P \cap KQ : Q]$. If $K$ is more generally a number field and if $R = \mathbb{Z}_K$ (the ring of integers of $K$), we have $[P \cap KQ : Q] = N_{K/\mathbb{Q}}(\mathfrak{a}_1) \dots N_{K/\mathbb{Q}}(\mathfrak{a}_q)$.

We now apply the definition above to $P = \mathrm{Sym}^2(M)$ and $Q = \mathrm{Perf}_S(M)$ (i.e., $Q = \langle \mathrm{Sym}_2(S) \rangle \subset \mathrm{Sym}_2(M)$).

**3.5. Definition.** We denote by $\mathrm{Smith}^{(2)}_S(M)$, or simply by $\mathrm{Smith}^{(2)}(M)$, the Smith invariant of $(\mathrm{Sym}^2(M), \mathrm{Perf}(M))$.

If $\mathfrak{a}_1, \dots, \mathfrak{a}_q$ are the elementary divisors of the pair $(\mathrm{Sym}^2(M), \mathrm{Perf}(M))$, then $\mathrm{Dft}(M)$ is isometric to the direct sum $R/\mathfrak{a}_1 \bigoplus \dots \bigoplus R/\mathfrak{a}_q \bigoplus R^{q-p}$. When $\mathbb{R} = \mathbb{Z}$ and $\mathrm{Dft}(M)$ is a finite group, then $\mathfrak{a}_i = (a_i)$ for a well defined integer $a_i \ge 1$. We shall use the notation $\mathrm{Smith}^{(2)}(M) = (b_1^{\beta_1}, \dots, b_r^{\beta_r})$ to say that $a_1 = \dots = a_{\beta_1} = b_1$, $a_{\beta_1+1} = \dots = a_{\beta_1+\beta_2} = b_2$, $\dots$, $\dots = a_p = b_{\beta_r}$.

**3.6. Remark.** When $W$ is endowed with a symmetric bilinear form taking values in $R$ on $M$ (we then say that $M$ is *integral*), $M$ is contained in its dual $M^* = \{x \in V \mid \forall y \in M, x.y \in R\}$, so that we can define the *Smith invariant* $\mathrm{Smith}(M)$ *of* $M$, namely the Smith invariant of the pair $(M^*, M)$. Experimental data indicate that $\mathrm{Smith}^{(2)}(M)$ has essentially nothing to do with $\mathrm{Smith}(M)$.

**§ 4. Symmetric endomorphisms and matrices.** Let $W$ be a vector space of finite dimension $n$ over some field $C$. The map

$$(e, \varphi) \mapsto \big(x \mapsto \varphi(x)\, e\big) : W \times W^* \to \mathrm{End}(W)$$

($W^*$ is the dual $\mathcal{L}(W,C)$ of $W$) induces a canonical isomorphism $W \bigotimes W^* \simeq \mathrm{End}(W)$. (This homomorphism is easily seen to be surjective, and both sides have the same dimension). Suppose now that $W$ is endowed with a non-degenerate symmetric bilinear form $(x,y) \mapsto x \cdot y$. We can then identify $W$ and $W^*$ (by $f \mapsto \varphi = (x \mapsto f \cdot x)$), obtaining in this way an isomorphism $W \bigotimes W \simeq \mathrm{End}(W)$, which is characterized by the condition

$$\forall x \in W\,,\ (e \otimes f)\,(x) = (f \cdot x)\,e\,.$$

Recall that $u \in \mathrm{End}(W)$ is *symmetric* if it satisfies the identity $u(x) \cdot y = x \cdot u(y)$ ; We denote by $\mathrm{End}^s(W)$ the vector space of symmetric endomorphisms of $W$. Among symmetric endomorphisms, orthogonal projections onto non-isotropic lines $D$ play a crucial rôle. Given a non-zero $e \in D$, this projection is defined by the formula $p_D(x)\ \big(= p_e(x)\big) = \dfrac{x \cdot e}{e \cdot e}\, e$. The endomorphism $x \mapsto (f \cdot x)\, e$ is symmetric if and only if $f$ and $e$ are collinear, and if $e \cdot e \neq 0$, the image of $e \otimes e$ in $\mathrm{End}^s(W)$ is $(e \cdot e)\, p_e$.

Let $\mathcal{B} = (e_1, \dots, e_n)$ be a basis of $L$. For $x \in W$, let $X$ be the column vector of the components of $x$ on $\mathcal{B}$, and let $e \in W$. For the endomorphism $u_e : x \mapsto (e \cdot x)\, e$, we have the matrix representation $\mathrm{Mat}(u_e, \mathcal{B}^*, \mathcal{B}) = X^t X$. We can thus pass from symmetric squares to matrix rings by the correspondence

$$x \otimes x \in \mathrm{Sym}^2(W) \longleftrightarrow X^t X \in \mathrm{Sym}_n(C)\,.$$

We can now recover the usual definition of perfection for Euclidean lattices. The traditional definition of perfection (in terms of quadratic forms) is that $q$ is *perfect* if the rank-1 $n \times n$ matrices $X^t X$, $X \in S(q)$ span the space $\mathrm{Sym}_n(\mathbb{R})$ of real symmetric matrices; we pass from lattices to quadratic forms by taking for $\mathcal{B}$ a basis of the lattice and considering the quadratic form $q(x) = {}^t X A X$ where $A = (e_i \cdot e_j)$ is the *Gram matrix* $\mathrm{Gram}(\mathcal{B})$ *of* $\mathcal{B}$.

Applying the definitions of the previous sections with $R = \mathbb{Z}$, $K = \mathbb{Q}$, and $C = \mathbb{R}$, choosing for $W$ a Euclidean space $E$, for $M$ a lattice $\Lambda \subset E$, and for $S$ the set $S(\Lambda)$ of minimal vectors of $\Lambda$, we see immediately that $\Lambda$ is perfect in the sense of definition 3.1 if and only if the projections $p_e$, $e \in S$ span $\mathrm{End}^s(E)$, and this is precisely one of the possible definitions for the perfection of $\Lambda$ as a Euclidean lattice, see [M], chapter III, definitions 2.2 and 2.7. We have thus proved:

**4.1. Proposition.** *A Euclidean lattice $\Lambda$ is perfect if and only if the pair $\big(\Lambda, S(\Lambda)\big)$ is perfect in the sense of definition 2.6.* □

Let us come back to the $C$-vector space $W$. We define the *norm of* $x \in W$ by the formula $N(x) = x \cdot x$. (This extends the definition currently used in the theory of lattices, where this norm is the square of the Euclidean norm $x \mapsto \|x\|$.) The bilinear map

$$(x,y) \mapsto x \cdot y : W \times W \to C$$

induces a linear map from $W \bigotimes W$ onto $C$ which is well defined by the condition that it takes the value $x \cdot y$ on the split tensors $x \otimes y$. By restriction, we obtain a linear map $N : \mathrm{Sym}^2(W) \to C$ which is well defined by the condition

$$\forall x \in W,\ N(x \otimes x) = N(x)\,. \tag{4.2}$$

We have the formula

$$N(x\otimes y+y\otimes x)=N\big((x+y)\otimes(x+y)\big)-N(x\otimes x)-N(y\otimes y)=2\,x\cdot y\,.$$

**4.3. Definition.** The map $N$ from $\mathrm{Sym}^2(W)$ onto $C$ defined above is called the *norm map*.

Let $S=S'\cup -S'$ ($S'\cap -S'=\emptyset$) be a symmetric subset of $W$ and let $t$ be a symmetric tensor belonging to the span of $S^{(2)}$ in $\mathrm{Sym}^2(W)$. Choose a representation

$$t=\sum_{x\in S'}\lambda_x(t)\,x\otimes x$$

of $t$ on $S^{(2)}$ and let

$$\lambda(t)=\sum_{x\in S'}\lambda_x(t)\,.$$

**4.4. Proposition.** *Suppose that all the vectors of $S$ have the same non-zero norm, that we denote by $N(S)$. Then, we have*

$$\lambda(t)=\frac{N(t)}{N(S)}\,.$$

*In particular, $\lambda(t)$ does not depend on the representation of $t$ on $S^{(2)}$.*

*Proof.* By the linearity of the norm map, we have $N(t)=\sum\lambda_x(t)\,N(x\otimes x)$. □

**4.5. Corollary.** *If $t=y\otimes y$, then $\lambda(t)=\dfrac{N(y)}{N(S)}$.* □

§ **5. Euclidean lattices.** We again apply the previous sections taking $R=\mathbb{Z}$, $K=\mathbb{Q}$, $C=\mathbb{R}$, $M$, now denoted $\Lambda$, being a lattice in $W$, now denoted $E$, endowed with a Euclidean structure. We denote by $S$ the sets of its minimal vectors, and by $S'$ a half system of minimal vectors. The *norm of* $x\in E$ is $N(x)=x\cdot x$, and the *norm* (or *minimum*) *of* $\Lambda$ is the common norm of its minimal vectors.

For any similarity $u$ of $E$, we have $S(u(\Lambda))=u(S(\Lambda))$. Hence, the perfection default module of $\Lambda$ only depends on the similarity class of $\Lambda$. Now, by an old result of Korkine and Zolotareff (see [M], chapter III, proposition 2.11), a perfect lattice is proportional to an integral lattice, so that its similarity class contains an integral primitive lattice, well defined up to isometry.

**5.1. Theorem** (A.-M. Bergé). *Let $\Lambda$ be an integral and primitive perfect lattice, of norm $m$. Then, the annihilator of the torsion submodule of the perfection default module of $\Lambda$ is divisible by $\frac{m}{2}$ if $m$ is even, and by $m$ if $m$ is odd.*

*Proof.* Let $\alpha\in\mathbb{Z}$ be the annihilator of the perfection default module of $\Lambda$ (which is a finite group because $\Lambda$ is perfect). It is the smallest integer such that, for all $y\in\Lambda$, there is a relation

$$\alpha\,y\otimes y=\sum_{x\in S'}\lambda_x(y)\,x\otimes x$$

with $\lambda_x(y) \in \mathbb{Z}$. By Corollary 3.5, we have

$$\alpha\, N(y) = \Big(\sum_{x\in S'} \lambda_x(y)\Big)\, m\,.$$

This proves that $m$ divides the product $\alpha \times \text{g.c.d.}\big(N(y),\, y \in \Lambda\big)$, whence the result since the g.c.d. of the norms on $\Lambda$ is 2 when $\Lambda$ is even and 1 when $\Lambda$ is odd. □

We shall now use this theorem to characterize lattices whose perfection default module is trivial. Recall that a *root* in a lattice $\Lambda$ is a non-zero primitive vector $e$ of $\Lambda$ such that $\Lambda$ is invariant under the reflection $\sigma_e$ with respect to the hyperplane orthogonal to $e$. A lattice generated by its roots is called a *root lattice*. It is easy to see that the roots of a lattice constitute a root system in the space they span, and the classification of root systems (see [Bou2], VI) shows that a root lattice is isometric to an orthogonal sum of irreducible root lattices, each of which is similar to one of the integral primitive lattices $\mathbb{Z}$, $\mathbb{A}_n$, $n \geq 2$, $\mathbb{D}_n$, $n \geq 4$, $\mathbb{E}_6$, $\mathbb{E}_7$, or $\mathbb{E}_8$ (see [M], chapter IV,sections 1–5 for the definitions). Finally, we see ("Witt's theorem") that integral lattices generated by vectors of norm 1 or 2 are root lattices and are isometric to direct sums of copies of $\mathbb{Z}$, $\mathbb{A}_n$, $n \geq 1$, $\mathbb{D}_n$, $n \geq 4$, or $\mathbb{E}_n$, $n = 6, 7, 8$, which are pairwise non-isometric.

**5.2. Theorem.** *A lattice $\Lambda$ has a trivial perfection default module if and only if it is similar to one of the irreducible root lattices $\mathbb{Z}$, $\mathbb{A}_n$, $n \geq 2$, $\mathbb{D}_n$, $n \geq 4$, $\mathbb{E}_6$, $\mathbb{E}_7$, or $\mathbb{E}_8$.*

*Proof.* If $\text{Dft}(\Lambda) = \{0\}$, $\Lambda$ is perfect, hence irreducible and proportional to an integral primitive lattice, which is unique up to isometry. Let $m = N(\Lambda)$. By Theorem 5.1, $m$ divides 2. By proposition 3.3, $S$ generates $\Lambda$. By Witt's theorem, $\Lambda$ is one of the lattices which are listed in the theorem we want to prove,

Conversely, we must show that irreducible integral primitive root lattices have trivial perfection default modules, a result which was known to Bacher. This is clear if $m = 1$, where $\Lambda = \mathbb{Z}$. We may thus restrict ourselves to lattices with $m = 2$ and $n \geq 2$. For such a lattice, we make use of bases of type "Korkine-Zolotareff" in the sense of [M], chapter IV. These are bases whose Gram matrix $A = (a_{i,j})$ fulfils the conditions $a_{i,i} = 2$ and $a_{i,j} = 1$ for $i \neq j$ except for $\{i,j\} = \{1,2\}$ in the case of $\mathbb{D}_n$ and $\{i,j\} = \{1,2\}$ or $\{1,3\}$ if the case of $\mathbb{E}_n$, where $a_{i,j} = 0$. Clearly, $S^{(2)}$ contains all tensors $e_i \otimes e_i$. We shall show that it also contains all tensors $e_i \otimes e_j + e_j \otimes e_i$ for $1 \leq i < j \leq n$, ; By formula 2.3, we may replace any such tensor by $(e_i - e_j) \otimes (e_i - e_j)$.

The case of $\mathbb{A}_n$ is now a consequence of proposition 2.5.

For $\mathbb{D}_n$, we must show that $e_1 \otimes e_2 + e_2 \otimes e_1$ is a linear combination of vectors belonging to $S \bigotimes S$. This is achieved by making use of the minimal vector $e_1 + e_2 - e_3$.

A similar argument applies to $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$, using the minimal vectors $e_1 + e_2 - e_4$ and $e_1 + e_3 - e_4$. □

§ **6. Numerical results.** We account here for some calculations of Smith$^{(2)}$ which have been done using the PARI package together with some more specific programs written by Batut.

We have first considered the 48 perfect lattices of dimension $n \le 7$ and the 10916 known perfect lattices (at the date this paper is written, [B-M]) with $n = 8$. All these lattices are even, except the root lattice $\mathbb{Z}$ and the lattice $P_7^2 \simeq \mathbb{E}_7^*$, of norm 3. For the 10962 even known perfect lattices of dimension up to 8, the following facts have been observed:

**6.1. Facts.**

(1) The components of $\mathrm{Smith}^{(2)}$ of rank $r > n$ are trivial;
(2) The first component of $\mathrm{Smith}^{(2)}$ (i.e., the annihilator of the perfection default module) is equal to $\frac{m}{2}$ or to $m$.
(3) For $m = 4$, $\mathrm{Smith}^{(2)}$ reduces to its first component, which is always equal to $\frac{m}{2} = 2$.

Note that all these lattices possess a basis of minimal vectors. This is no more true in dimensions $n \le 10$, and the remark we have made in section 2 about lattices which are not generated by their minimal vectors shows that the facts 2 and 3 above cannot be true when $S$ does not generate $\Lambda$.

For instance, the lattices $\mathbb{D}_n^+$, when scaled to a primitive integral lattice, have norm 2 if $n \equiv 0 \mod 4$ and 4 if $n \equiv 2 \mod 4$. For all (even) $n$, we have $\mathrm{Smith}^{(2)}(\mathbb{D}_n^+) = 4 \cdot 2^{n-1}$.

Consider now the Coxeter lattices $\mathbb{A}_n^r$, $r \mid n+1$, the sublattices of $\mathbb{A}_n^*$ which contain $\mathbb{A}_n$ to the index $r$. Results similar to that we obtained for $\mathbb{D}_n^+$ hold for $2 \le r \le \frac{n+1}{3}$ (exactly the same one for $r = 2$). However, the "exotic" perfect lattices $\mathbb{A}_n^{(n+1)/2}$ produce original examples. When rescaled to an integral primitive lattice, $\mathbb{A}_n^{(n+1)/2}$ is even with minimum $n-1$ if $n \equiv 1 \mod 4$ and odd with minimum $\frac{n-1}{2}$ if $n \equiv 3 \mod 4$, in all cases generated by their minimal vectors. However, for all $n \ge 5$ odd, we likely have

$$\mathrm{Smith}^{(2)}(\mathbb{A}_n^{(n+1)/2}) = \left( \frac{(n-1)\,(n-3)}{4}, \left(\frac{n-3}{2}\right)^{n-1} \right).$$

The ratio $\dfrac{a_1}{m}$, equal to $\dfrac{n-3}{4}$ or $\dfrac{n-3}{2}$, tends to infinity with $n$. This shows that the second experimental fact verified for known perfect lattices up to dimension 8 is not general. However, no bad prime $p > n$ occur.

I have no counter-examples to facts 1 and 3. However, since the value of $\mathrm{Smith}^{(2)}$ depends on subtle linear relations over $\mathbb{Z}$ between minimal vectors, it does not seem reasonable to conjecture that fact 3 holds for all norm 4 lattices generated by their minimal vectors.

**§ 7. Relative perfection over Z.** We still denote by $\Lambda$ a lattice in the $n$-dimensional Euclidean space $E$. Let $F$ be a hyperplane of $E$ such that $M = \Lambda \cap F$ is a lattice in $F$. It was proved by Barnes (see [M], chapter XII, theorem 3.5) that if $M$ is perfect, then $\Lambda$ is perfect whenever there exists a set of $n$ independent minimal vectors in $L \smallsetminus M$. The following statement is a kind of enlargement of Barnes's theorem:

**7.1. Theorem.** *Suppose that there exists $e \in \Lambda \smallsetminus M$ and generators $e_1, \dots, e_r$ of $M$ such that*

(1) $e, e+e_1, \dots, e+e_r \in S(\Lambda)$.
(2) $e, e_1, \dots, e_r$ *generate* $\Lambda$.

*Then, the canonical map* $\mathrm{Dft}(M) \to \mathrm{Dft}(\Lambda)$ *is surjective.*

*Proof.* Set $e_0 = 0$ and $e_i' = e + e_i$ for $0 \le i \le n$. Then, $\{e_0', e_1', \dots, e_n'\}$ is a generating set for $\Lambda$. Hence, $\mathrm{Sym}^{(2)}(\Lambda)$ is generated by the symmetric tensors $e_i' \otimes e_i'$, $0 \le i \le n$, which belong to $\mathrm{Perf}_{S(\Lambda)}(\Lambda)$, and $e_i' \otimes e_j' + e_j' \otimes e_i'$, $0 \le i < j \le n$, for which we write

$$\begin{aligned} e_i' \otimes e_j' + e_j' \otimes e_i' &= e_i' \otimes e_i' + e_j' \otimes e_j' - (e_j' - e_i') \otimes (e_j' - e_i') \\ &= e_i' \otimes e_i' + e_j' \otimes e_j' - (e_j - e_i) \otimes (e_j - e_i) \\ &\in \mathrm{Perf}_{S(\Lambda)}(\Lambda) + \mathrm{Sym}^{(2)}(M)\,. \quad \square \end{aligned}$$

The theorem above could have been used to prove that irreducible root lattices have trivial perfection default modules, using the inclusions $\mathbb{A}_{n-1} \subset \mathbb{A}_n$ $(n \ge 2)$, $\mathbb{D}_{n-1} \subset \mathbb{D}_n$ $(n \ge 4)$, and $\mathbb{E}_{n-1} \subset \mathbb{E}_n$ $(n \ge 6)$, together with the standard isometries $\mathbb{D}_3 \simeq \mathbb{A}_3$ and $\mathbb{E}_5 \simeq \mathbb{D}_5$. Consider now the ascending sequence of laminated lattices

$$\Lambda_0 = \{0\} \subset \Lambda_1 \subset \cdots \subset \Lambda_n \subset \dots$$

These are norm 4 lattices, integral for $n \le 24$, uniquely defined up to isometry in the ranges $0 \le n \le 10$ and $14 \le n \le 24$, which are scaled copies of root lattices for $n \le 8$ ([C-S], chapter 6). Hence, the corresponding perfection default modules are trivial up to $n = 8$. For $n \ge 9$, they are not, because primitive integral scaled copies have a norm $N > 2$ $(N = 4$ if $9 \le n \le 24)$. We have actually $\mathrm{Dft}(\Lambda_9) \simeq \mathbb{Z}/2\mathbb{Z}$. (Proof: note that $\Lambda_9$ is a scaled copy of $\mathbb{E}_8 + \mathbb{D}_9$, see [M], chapter 5, section 5.) I have verified that Theorem 7.1 applies up to $n = 16$ ($\Lambda_{16}$ is the Barnes-Wall lattice $BW_{16}$). I have also verified in the same way that $\mathrm{Dft}(K_n)$ is also cyclic of order 2 for $n = 9, 10, 11, 12$.

Theorem 7.1 also allows to prove that $\mathrm{Dft}(L) \simeq \mathbb{Z}/2\mathbb{Z}$ for lattices $L$ belonging to some classical infinite series. This is for instance easily verified for the Barnes lattices $L_n^r$, $n \ge 5$, $r \ge 2$, on the definition given in [M], chapter V, section 4.

ACKNOWLEDGMENTS. I thank Anne-Marie BERGÉ, with whom I had numerous helpful discussions. I also thank the authors of the *PARI* system, and in particular Christian BATUT, whose various programs on lattices have been very useful in many instances.

## REFERENCES

[Bc] R. Bacher, Private communication, 1998.

[Bt-M] C. Batut, J. Martinet, Martinet's WEB page, http://www.math.u-bordeaux.fr/˜martinet.

[Bou1] N. Bourbaki, *Algèbre, ch. I–X*, Hermann, Masson, Paris, 1970, 1980.

[Bou2] N. Bourbaki, *Groupes et algèbres de Lie, chapitres IV, V, VI*, Masson, Paris, 1981.

[C-S] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, Grundlehren nu. 290, Heidelberg, 1988.

[M] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, Masson, Paris, 1996.

JACQUES MARTINET
A2X, INSTITUT DE MATHÉMATIQUES
UNIVERSITÉ BORDEAUX 1
351, COURS DE LA LIBÉRATION
F–33405 TALENCE CEDEX

E-mail: martinet@math.u-bordeaux.fr