# SUR CERTAINS DESIGNS SPHÉRIQUES LIÉS À DES RÉSEAUX ENTIERS

par Jacques MARTINET

RÉSUMÉ. On classe dans cette note les réseaux entiers de minimum $m \le 5$ dont l'ensemble des vecteurs minimaux constitue un $7$-design sphérique, étendant ainsi (sous une hypothèse plus restricitve) la classification de Venkov des $5$-designs obtenus à l'aide de réseaux de minimum $m \le 3$.

ABSTRACT. English title: Spherical designs and integral lattices.
In this note, we classify those integral lattices of minimum $m \le 5$ whose sets of minimal vectors are spherical $7$-designs. This classification extends (under a more restrictive hypothesis) Venkov's classification of $5$-designs provided by lattices of minimum $m \le 3$.

Rappelons d'abord un résultat de la théorie de Venkov exposée dans [Ven]. On dit qu'une partie finie *symétrique* $S$ d'une sphere $\boldsymbol{\Sigma}$ de rayon $\sqrt{m}$ centrée à l'origine d'un espace euclidien $E$ de dimension $n$ est un $(2\ell+1)$- (ou $2\ell$-, cela revient au même) *design sphérique* si l'intégrale sur $\boldsymbol{\Sigma}$ de tout polynôme homogène de degré au plus $2\ell+1$ s'obtient comme moyenne de ses valeurs aux points de $S$, ou, ce qui revient au même, si cette intégrale est nulle sur ceux de ces polynômes qui sont harmoniques et non constants. Dans la suite, nous n'utiliserons que la caractérisation suivante des $(2\ell+1)$-designs sphériques ([Ven], th. 3.2): on a

$$(*) \qquad \forall\, \alpha \in E\,, \sum_{x \in S/\{\pm 1\}} (x \,.\, \alpha)^{2t} = m^t\, N(\alpha)^t\, c_t$$

---

Laboratoire A2X, UPRES A 5465 C.N.R.S. — Université Bordeaux 1

Mots-clés : *Réseaux euclidiens, designs sphériques.*

Les trois premiers paragraphes de cette note ont été écrits pour l'essentiel pendant un séjour de deux semaines à Vienne au cours du mois de septembre 1998 au sein du *Erwin Schrödinger Institut*, que je remercie chaleureusement pour son hospitalité.

quel que soit $t = 1, \dots, \ell$, où, pour tout $t$, $c_t$ est une constante, qui vaut alors

$$c_t = s\, \frac{1.3 \dots (2t-1)}{n\,(n+2) \dots (n-2+2t)}\,,$$

où $s = \frac{1}{2}|S|$. Il suffirait en fait d'écrire la condition pour $t = \ell$, sa validité dans le cas des valeurs plus petites de $t$ s'en déduisant par le th. 3.2 de [Ven]. Toutefois, c'est l'utilisation des relations ci-dessus pour toutes les valeurs de $t$ qui permet d'avancer vers des résultats de classification, ce qui est notre but dans cette note.

Considérons le cas où $S$ est l'ensemble $S(\Lambda)$ des vecteurs d'un réseau $\Lambda$ entier de *norme* (ou *minimum*) $m$. Pour $x, y \in S$, les produits scalaires $x\,.\,y$ sont entiers. On a $|x\,.\,y| = m$ si $y = \pm x$, et $|x\,.\,y| \le \lfloor \frac{m}{2} \rfloor$ sinon, comme on le voit au moyen de l'inégalité $N(x \pm y) = N(x) + N(y) \pm 2x\,.\,y \ge m$, i.e. $|x\,.\,y| \le \frac{1}{2}N(y)$ qui s'applique quel que soit $x \in \Lambda$ minimal, et entraîne le résultat cherché lorsque $y$ est également minimal.

Soit $m' = \lfloor \frac{m}{2} \rfloor$. On pose $s = s(\Lambda) = \frac{1}{2}|S(\Lambda)|$, et, pour $y \in S(\Lambda)$ et $0 \le i \le m'$, on note $s_i$ le nombre d'éléments $x$ d'un demi-système de vecteurs minimaux de $\Lambda$ pour lesquels $x\,.\,y = \pm i$ :

$$s_i = |\{x \in S(\Lambda)/\{\pm 1\} \mid |x\,.\,y| = i\}|\,.$$

En toute rigueur, on devrait écrire $s_i(y)$ plutôt que $s_i$. Toutefois, dans les applications que nous avons en vue, $s_i(y)$ sera indépendant de $y$.

Si $S(\Lambda)$ est un $(2\ell+1)$-design, on a $\ell+1$ relations entre $s$ et les $s_i$, à savoir

$$s_0 + s_1 + \dots + s_{m'} = s - 1$$

et les $\ell$ relations provenant de $(*)$.

- Dans le cas où $\ell = m'+1$, on vérifie qu'il s'agit d'un système de Cramer, d'où l'on déduit une unique possibilité pour l'ensemble $(s, s_0, \dots, s_{m'})$.
- Dans le cas $\ell \le m'$, les solutions se décrivent en fonction linéaire de $m' + 1 - \ell$ paramètres.
- Dans le cas $\ell > m' + 1$, on a un système sur-déterminé, qui peut conduire à de nouvelles impossibilités ou au contraire permettre de prouver (en appliquant le th. 8.1 de [Ven]) qu'il s'agit d'un design de paramètre supérieur .
- Remarquons que les relations écrites pour une norme $m$ s'appliquent aux normes $p < m$, à condition de poser $s_i = 0$ pour $i > \frac{p}{2}$.

Nous sommes maintenant en mesure d'énoncer notre résultat principal :

THÉORÈME. *Les réseaux $\Lambda$ entiers primitifs de norme $m \le 5$ tels que $S(\Lambda)$ soit un 7-design sont $\mathbb{Z}$, le réseau de racines $\mathbb{E}_8$, le réseau unimodulaire $O_{23}$ de minimum 3, les trois réseaux laminés $\Lambda_{16} = BW_{16}$ de Barnes-Wall, $\Lambda_{23}$ et le réseau de Leech $\Lambda_{24}$, et les réseaux unimodulaires pairs de dimension 32 et de minimum 4 (non classés à ce jour). En particulier, la norme 5 n'est pas possible.*

Grâce à Koch et Venkov ([K-V]) et à quelques continuateurs, on connaît de nombreux exemples de réseaux unimodulaires pairs de dimension 32 ; l'exemple le plus célèbre est celui du réseau de Barnes-Wall $BW_{32}$.

La démonstration va occuper les trois paragraphes suivants. On ne s'occupera que modérément du minimum 1, qui intervient seulement en dimension 1 : l'unique réseau est $\mathbb{Z}$, qui est un $t$-design quel que soit $t$, alors qu'il existe une borne pour $t$ dans toutes les autres dimensions. On se contentera de constater que les formules obtenues sont valables en dimension 1.

Les cas des minima 2 et 3 sont des conséquences des résultats de [Ven], §§5, 7. Toutefois, comme ils sont d'étude plus facile sous nos hypothèses, nous ne les laisserons pas de côté ici.

Après avoir explicité les relations $(*)$, on établit dans le §1 un certain nombre de propriétés générales de certains 7-designs, que l'on applique aux minima $m \le 3$. Le cas du minimum 4 est traité au §2 et celui du minimum 5 au §3. Nous édudions enfin au §4 la possibilité que ces designs soient de niveau plus élevé.

Il resterait à vérifier que ces réseaux sont tous effectivement des 7-designs. Le simple fait que nous connaissions le spectre $(s_0, s_1, s_2)$ de $S(\Lambda)$ permet de faire aisément cette vérification, en utilisant le th. 8.2 de [Ven] ; du reste, le résultat est acquis *a priori* pour des raisons modulaires dans presque tous les cas. De ce fait, ces vérifications seront laissées au lecteur, qui pourra en même temps démontrer :

PROPOSITION. *Les vecteurs minimaux des réseaux décrits dans le théorème ne constituent jamais un 8-design, sauf dans le cas du réseau de Leech, qui est un 11-design, mais non un 12-design.* □

Je remercie Christine Bachoc et Boris Venkov pour leurs interventions décisives dans la démonstration qui figure au paragraphe 3.

## 1. Designs associés à des réseaux entiers de petite norme

Appliquées à un vecteur minimal $\alpha$ de $\Lambda$, les formules $(*)$ prennent dans le cas des normes 4 et 5 la forme

$$\begin{aligned} & s_1 + 4s_2 + m^2 = m^2\,\frac{s}{n} \\ & s_1 + 4^2 s_2 + m^4 = m^4\,\frac{s}{n}\,\frac{3}{n+2} \\ (*_m) \qquad & s_1 + 4^3 s_2 + m^6 = m^6\,\frac{s}{n}\,\frac{3}{n+2}\,\frac{5}{n+4}\,. \end{aligned}$$

En effectuant entre ces trois équations les combinaisons $(2)-(1)$ et $\frac{1}{4}((3)-(2))$, on obtient les deux équations

$$\begin{aligned} & 12\,s_2 + m^2(m^2-1) = m^2\,\frac{s}{n}\,\frac{3m^2-n-2}{n+2} \\ (*'_m) \qquad & 12\,s_2 + \frac{m^4(m^2-1)}{4} = \frac{m^4}{4}\,\frac{s}{n}\,\frac{3}{n+2}\,\frac{5m^2-n-4}{n+4}\,, \end{aligned}$$

d'où l'on tire $s$ par différence puis $s_2$, obtenant

$$(*''_m) \qquad \begin{aligned} s &= (m^2-1)\,(m^2-4)\,\frac{n(n+2)(n+4)}{4n^2-3(5m^2-8)n+15m^4-60m^2+32} \\ s_2 &= \frac{m^4(m^2-1)}{12}\,\frac{(n-1)(3m^2-4-n)}{4n^2-3(5m^2-8)n+15m^4-60m^2+32}\,, \end{aligned}$$

dont les expressions sous-entendent que le dénominateur ne doit pas s'annuler.

On tire ensuite $s_1$ de la première équation de $(*_m)$ et l'on a enfin $s_0 = s-1-s_1-s_2$. Il est inutile d'expliciter ces deux dernières formules.

Notons que l'inégalité $s_2 \geq 0$ entraîne la majoration $n < 3(m^2-1)$ dont l'existence a été signalée dans l'introduction.

Lemme 1.1. *Soit $\Lambda$ un réseau non unimodulaire de norme $m$ et soit $v \in \Lambda^* \smallsetminus \Lambda$ un vecteur qui est minimal dans sa classe modulo $\Lambda$. Alors, on a $|x\,.\,v| \leq \frac{1}{2}N(x)$ quel que soit $x \in \Lambda$, et en particulier $|x\,.\,v| \leq m' = \lfloor \frac{m}{2} \rfloor$ si $x \in S(\Lambda)$.*

*Démonstration.* En effet, on a $N(v \pm x) = N(v) + N(x) \pm 2v\,.\,x \geq N(v)$, d'où $\mp v\,.\,x \leq \frac{1}{2}N(x)$. $\square$

Dans l'énoncé suivant, on considère un réseau $\Lambda$ et un vecteur $v$ de son dual, et, pour tout entier $i \geq 0$, on pose

$$t_i = |\{x \in S(\Lambda)/\{\pm 1\} \mid |x \,.\, v| = i\}|\,.$$

[Noter que les produits scalaires $y \,.\, z$, $y \in \Lambda$, $z \in \Lambda^*$ sont entiers.]

Lemme 1.2. *Soit $\Lambda$ un réseau non unimodulaire de norme $m$ et soit $v \in \Lambda^* \smallsetminus \Lambda$ tel que $|v \,.\, x| \leq 2$ quel que soit $x \in S(\Lambda)$. Soit $t = N(v)$. Alors, $\dfrac{5(n+4)(28-n)}{3}$ est un carré, soit $\lambda^2$, et l'on a*

$$m\,t = \frac{(n+4)}{2} \pm \frac{\lambda}{10} \quad \text{et} \quad n \in \{1, 8, 16, 23, 26\}\,.$$

*En outre, les valeurs correspondantes pour $\lambda$, $m\,t$ et $\dfrac{t_2}{(s/n)}$ sont données par le tableau suivant :*

| $n$ | 1 | 8 | 16 | 23 | 26 |
|---|---|---|---|---|---|
| $\lambda$ | 15 | 20 | 20 | 15 | 10 |
| $m\,t$ | 1, 4 | 4, 8 | 8, 12 | 12. 15 | 14, 16 |
| $t_2/(s/n)$ | 0, 1 | $\frac{4}{5}$, $\frac{56}{5}$ | $\frac{8}{3}$, 12 | $\frac{132}{25}$, 12 | 7, $\frac{80}{7}$ |

*Démonstration.* Les relations $(*)$ appliquées avec $\alpha = v$ s'écrivent

$$\begin{aligned} t_1 + 4t_2 &= m\,t\,\frac{s}{n} \\ t_1 + 16t_2 &= m^2t^2\,\frac{s}{n}\,\frac{3}{n+2} \\ t_1 + 64t_2 &= m^3t^3\,\frac{s}{n}\,\frac{3}{n+2}\,\frac{5}{n+4}\,. \end{aligned}$$

Les combinaisons $(2) - (1)$ et $\frac{1}{4}((3) - (2))$ entraînent la double égalité

$$12t_2 = m\,t\,\frac{s}{n}\,\frac{3m\,t - n - 2}{n+2} = \frac{m^2t^2}{4}\,\frac{s}{n}\,\frac{3}{n+2}\,\frac{5m\,t - n - 4}{n+4}\,.$$

En comparant les deux valeurs trouvées pour $t_2$, on obtient après simplification l'équation $5m^2t^2 - 5m(n+4)t + \dfrac{4(n+2)(n+4)}{3}$, dont le discriminant se met sous la forme

$$\Delta = \frac{5m^2(n+4)(28-n)}{3}\,.$$

On trouve donc la condition $\Delta = \lambda^2$ (qui est indépendante de $m$), et le reste du lemme en résulte. $\square$

Le cas des minima 2 et 3 est maintenant facile. On a vu que $s_2$ doit être nul. En utilisant sa valeur donnée dans $*''_m$ (et en écartant le cas trivial de la dimension $1$), on voit que $m = 2$ (resp. $m = 3$) n'est possible que pour $n = 8$ (resp. $n = 23$), et le lemme 1.2 montre que les réseaux correspondants doivent être unimodulaires. Ils doivent donc être respectivement isométriques à $\mathbb{E}_8$ et à $O_{23}$.

## 2. Les réseaux de minimum 4

Dans le cas du minimum $4$, les formules $(*''_m)$ se simplifient en

$$s = \frac{45n(n+2)(n+4)}{(n-26)(n-28)}$$

$$(*''_4) \qquad s_2 = \frac{80(n-1)(44-n)}{(n-26)(n-28)}\,.$$

Le signe de $s_2$ limite le choix de $n$ à la réunion des deux intervalles $[1,25]$ et $[29,44]$.

Si $\Lambda$ n'est pas unimodulaire, les lemmes 1.1 et 1.2 montrent que $n$ ne peut prendre que l'une des valeurs $1, 8, 16, 23$. Si au contraire $\Lambda$ est unimodulaire, le fait qu'il soit de minimum $4$ entraîne la minoration $n \geq 24$ ([C-S], ch. 16). Un tel réseau doit donc être pair, car le réseau pair qui lui serait attaché dans le cas contraire définirait encore un $7$-design (parce que les deux réseaux auraient même ensemble de vecteurs minimaux) qui, n'étant pas unimodulaire, ne pourrait avoir que l'une des dimensions $1, 8, 16, 23, 26$ prévues par le lemme 1.2. D'après un théorème de Hecke, on a alors $n \equiv 0 \mod 8$, donc $n = 24$, $n = 32$ ou $n = 40$, et l'on doit exclure la dimension $40$, car $s_2$ n'est pas entier dans ce cas.

Les assertions du théorème sont donc complètement démontrées dans le cas des réseaux unimodulaires de norme $4$, et nous passons maintenant au cas où $\Lambda$ *n'est pas* unimodulaire en examinant successivement les cas $n = 8$, $n = 16$ et $n = 23$.

$\underline{n = 8.}$ On trouve $s = 120$ et $s_2 = 56$, d'où l'on déduit $s_1 = 0$ par $(*_m)$. On a donc $\Lambda \simeq \sqrt{2}\,\Lambda'$ pour un certain réseau entier de norme $2$, d'où $\Lambda \simeq \sqrt{2}\,\mathbb{E}_8$.

$\underline{n = 16}$.

LEMME 2.1. *Soit $\Lambda$ un réseau entier, soit $T$ un système de représentants des classes de $\Lambda^*$ modulo $\Lambda$, et soit $L$ un réseau de la forme $L = \Lambda \cup \big(\bigcup_{v \in T'} (v + \Lambda)\big)$ où $T' \subset \frac{1}{2}\Lambda$ est une partie de $T$ dont les normes des éléments sont entières. Alors, le réseau $L = \langle \Lambda, T' \rangle$ est demi-entier, et il est même entier si $T'$ est réduit à un élément. En outre, quelque soit $T'$, $\sqrt{2}\,L$ est un réseau pair.*

*Démonstration.* Les éléments de $L \smallsetminus \Lambda$ sont de la forme $v+x$, $v \in T'$, $x \in \Lambda$, et l'on a $N(v+x) = N(v) + 2v\,.\,x + N(x) \in \mathbb{Z}$. Donc, si $y = v + x$ et $z = v' + x'$ $(v, v' \in T',\ x, x' \in \Lambda)$ sont deux éléments de $L$, $y\,.\,z = \frac{1}{2}[N(y+z) - N(y) - N(z)]$ est demi-entier. Si $T'$ est réduit à un élément $v$, on doit prendre $v' = v$ dans le calcul ci-dessus, et l'on a alors $y\,.\,z = (v+x)\,.\,(v+x') = N(v) + v\,.\,x + v'\,.\,x + x\,.\,x' \in \mathbb{Z}$. Enfin, $N(\sqrt{2}(v+x))$ est clairement un entier pair. $\square$

Scharlau et Venkov ([S-V]) ont classé les réseaux $\Lambda$ de dimension 16 qui sont 2-élémentaires (i.e., on a $2\Lambda^* \subset \Lambda$) et tels que $\Lambda$ et $\sqrt{2}\,\Lambda^*$ sont tous les deux pairs. Ils démontrent en particulier que ceux pour lesquels $\Lambda$ et $\sqrt{2}\,\Lambda^*$ sont tous deux de minimum 4 sont isométriques au réseau de Barnes-Wall $BW_{16} = \Lambda_{16}$. Le tableau du lemme 1.2 montre que $\Lambda$ satisfait les hypothèses du lemme 2.1. (Noter que les vecteurs courts des classes de $\Lambda^*/\Lambda \smallsetminus \Lambda$ sont de norme 2 ou 3 et que $\Lambda$ est bien 2-élémentaire, car si $y = v + x$ avec $N(v) = 2$ ou $N(v) = 3$ et $x \in \Lambda$, $2y$ n'est pas de de cette forme, et est donc dans $\Lambda$.)

Si donc $\Lambda$ est pair, on a $\Lambda \simeq \Lambda_{16}$.

Supposons maintenant $\Lambda$ impair, et notons $\Lambda'$ le réseau pair qui lui est associé. On peut écrire $\Lambda = \langle \Lambda', v \rangle$ pour un vecteur convenable $v \in \Lambda'^*$ de norme impaire. Comme $S(\Lambda') = S(\Lambda)$, on peut appliquer le lemme 1.2 à $\Lambda'$ : on doit avoir $N(v) = 2$ ou $N(v) = 3$, en fait $N(v) = 3$, et donc $N(\Lambda) = 3$, contrairement à l'hypothèse.

[ En prenant $N(v) = 3$, on obtient le réseau appelé $O_{16}$ dans [Ven], déf. 7.3.]

$\underline{n = 23}$. Faute de disposer d'un résultat analogue pour la dimension 23, l'étude de ce dernier cas va nécessiter quelques développements. *Nous supposons d'abord que $\Lambda$ est un réseau pair.*

Choisissons dans chaque classe non nulle de $\Lambda^*/\Lambda$ un vecteur de norme minimale. Les lemmes 1.1 et 1.2 montrent que ces vecteurs se répartissent en deux ensembles $T_1$ et $T_2$ tels que $N(v)=3$ si $v\in T_1$ et $N(v)=\frac{15}{4}$ si $v\in T_2$. Posons $L=\langle\Lambda,T_1\rangle$.

Lemme 2.2. *On a* $2L\subset\Lambda$, $2\Lambda^*\subset L$ *et* $4\Lambda^*\subset\Lambda$. *En outre,* $L=\frac{1}{2}\Lambda\cap\Lambda^*$.

*Démonstration.* Si $y=v+x$ $(v\in T_1,\ x\in\Lambda)$ est dans $L$, $2y$ n'est pas de la forme $w+x'$ avec $w\in T_1\cup T_2$ et $x'\in L$. C'est donc un élément de $\Lambda$.

Si $y=v+x$, $v\in T_2$, $x\in\Lambda$ est dans $\Lambda^*\smallsetminus L$, comme $2v$ est de norme impaire, $2y$ ne peut être que de la forme $w+x'$ avec $w\in T_1$ et $x'\in\Lambda$. On a donc $2y\in L\smallsetminus\Lambda$, et en particulier $2\Lambda^*\subset L$ et par conséquent $4\Lambda^*\subset\Lambda$. La dernière assertion du lemme est immédiate. □

Lemme 2.3. *Soient* $u\in T_1$ *et* $v\in T_1\cup T_2$ *avec* $v\neq u$ *si* $v\in T_1$. *Alors, on a* $u\,.\,v\equiv\frac{1}{2}\mod\mathbb{Z}$.

*Démonstration.* Il est clair que $u+v$ n'est pas dans $\Lambda$. On peut donc écrire $u+v=w+x$ avec $w\in T_1\cup T_2$ et $x\in\Lambda$. Si $v\in T_2$ (resp. $v\in T_1$), alors $u+v$ est d'ordre 4 (resp. 2) modulo $\Lambda$, et il en est donc de même de $w$. Par conséquent, $v$ et $w$ ont même norme. L'égalité $N(u+v)=N(w+x)$ s'écrit $3+2u\,.\,v+N(v)=N(w)+2w\,.\,x+N(x)$, i.e. $u\,.\,v=-\frac{3}{2}+w\,.\,x+N(x)$. □

Lemme 2.4. *On a* $\det(\Lambda)=4$.

*Démonstration.* L'inclusion $4\Lambda^*\subset\Lambda$ montre que $\det(\Lambda)$ est une puissance de 2, qui n'est pas triviale, car $\Lambda$ n'est pas unimodulaire. On n'a pas non plus $\det(\Lambda)=2$, car alors $\Lambda^*$ serait entier par le lemme 2.1, donc unimodulaire à cause des deux inclusions $\Lambda\subset\Lambda^*$ et $\Lambda^*\subset\Lambda$. Ainsi, $\det(\Lambda)$ est un multiple de 4, et il nous suffit maintenant de montrer que $\Lambda^*/\Lambda$ ne contient pas de sous-groupe de l'un des types $(2,2,2)$ ou $(4,2)$.

Dans le premier cas, $\Lambda^*$ contiendrait un réseau de la forme $M=\langle\Lambda,v_1,v_2,v_3\rangle$, les $v_i$ étant d'ordre 2 modulo $\Lambda$, donc de norme 3. Leur somme étant aussi d'odre 2, on a une relation de la forme $v_1+v_2+v_3=v+x$ avec $v\in T_1$ et $x\in\Lambda$. En prenant les normes des deux membres, on obtient $v_1\,.\,v_2+v_1\,.\,v_3+v_2\,.\,v_3=-3+v\,.\,x+\frac{1}{2}N(x)$, égalité impossible car le membre de droite est entier et celui de gauche ne l'est pas.

Le second cas est analogue. On représente le sous-groupe de type $(4,2)$ par un couple $(u,v)\in T_1\times T_2$. Alors, $2u+v$ est d'ordre 2 modulo $\Lambda$, d'où une égalité $2u + v = w + x$ avec $w \in T_1$ et $x \in \Lambda$. En prenant les normes des deux membres, on obtient $3 + 4u \,.\, v + 15 = 3 + 2w \,.\, x + N(x)$, égalité dont les deux membres sont de parité différente. $\square$

Il est maintenant facile de caractériser $\Lambda$, *toujours supposé pair*, dans le cas de la dimension $n = 23$. Comme $\Lambda^*/\Lambda$ est d'ordre $4$, il existe un réseau $M$ vérifiant les inclusions $\Lambda \subset M \subset \Lambda^*$, chacune avec l'indice $2$. On a donc $\det(M) = 1$. Par ailleurs, $M$ est de la forme $\langle \Lambda, v\rangle$ avec $v \in T_1$. Il est donc entier et de minimum $3$, donc isométrique à $O_{23}$, et le réseau pair $M'$ qui lui est associé est par conséquent isométrique à $\Lambda_{23}$. Comme $\Lambda$ est pair et inclus dans $M$, il est inclus dans $M'$. Comme $\det(\Lambda) = \det(M')$, on a $\Lambda = M'$,

Si $\Lambda$ est était impair, on pourrait appliquer le résultat précédent au réseau pair $\Lambda'$ qui lui est associé. On aurait $\det(\Lambda') = 4$, donc $\det(\Lambda) = 1$, et $\Lambda$ serait un réseau unimodulaire de norme $4$ et de dimension $23$, ce qui est impossible.

Cela achève la démonstration du théorème de l'introduction dans le cas des réseaux de minimum $4$.

## 3. Les réseaux de minimum 5

Dans le cas du minimum $5$, les formules $(*''_m)$ prennent la forme

$$(*''_5) \qquad \begin{aligned} s &= \frac{504n(n+2)(n+4)}{4n^2 - 351n + 7907} \\ s_2 &= \frac{1250(n-1)(71-n)}{4n^2 - 351n + 7907}\,. \end{aligned}$$

Le calcul explicite de $s$ et de $s_2$ montre que ces deux quantités sont entières si et seulement si $n = 43$, $n = 46$ ou $n = 71$. Le lemme 1.2 entraîne donc qu'un tel réseau doit être unimodulaire. Un théorème récent Rains et Sloane ([R-S]) affirme que le minimum des réseaux unimodulaires de dimension $n \neq 23$ est borné par $2\lfloor \frac{n}{24} \rfloor + 2$, donc que les réseaux de dimension 43 et 46 n'existent pas; je remercie Christine Bachoc de m'avoir signalé cette référence.

La démonstration du fait qu'il n'existe pas de réseau en dimension 71 est due à Venkov, dont nous reproduisons l'argument ci-dessous.

Soit $c$ un vecteur de parité (ou vecteur caractéristique) de $\Lambda$, c'est-à-dire un vecteur $c$ tel que l'on ait $x \,.\, x \equiv c \,.\, x \mod 2$ pour tout $x \in \Lambda$, que l'on suppose en outre être de longueur minimale parmi les vecteurs de parité de $\Lambda$. Pour tout $x \in S(\Lambda)$, $c\,.\,x$ est impair (puisque $x\,.\,x = 5$), $c{+}2x$ et $c - 2x$ sont encore des vecteurs de parité, et l'on a $(c \pm 2x)\,.\,(c \pm 2x) = c\,.\,c \pm 4c\,.\,x + 4\,.\,5 \geq c\,.\,c$, donc $|c\,.\,x| \leq \frac{20}{4} = 5$, i.e. $c\,.\,x \in \{\pm 1, \pm 3, \pm 5\}$.

Notons $n_i$ $(i = 1, 3, 5)$ le nombre de vecteurs $x$ d'un demi-système de vecteurs minimaux de $\Lambda$ tels que $c\,.\,x = \pm i$. En appliquant avec $\alpha = c$ la propriété $(*)$, on obtient le système

$$\begin{aligned} n_1 + n_3 + n_5 &= 2^2.3.71.73 \\ n_1 + 3^2 n_3 + 5^2 n_5 &= 2^2.3.5.73\, c\,.\,c \\ n_1 + 3^4 n_2 + 5^4 n_5 &= 2^2.3^2.5^2\,(c\,.\,c)^2 \\ n_1 + 3^6 n_2 + 5^6 n_5 &= 2^2.3.5^2\,(c\,.\,c)^3\,. \end{aligned}$$

En écrivant que son déterminant bordé par la colonne des seconds membres est nul, on voit que $c\,.\,c$ doit être racine du polynôme

$$5X^3 - 3^2.5.7.X^2 + 7.37.73X - 3^2.5.71.73$$

dont on vérifie qu'il ne possède aucune racine rationnelle. Ceci achève la démonstration du théorème énoncé dans l'introduction.

Remarque 3.1. Le même raisonnement s'applique aux dimensions 43 (avec $s = 218268$) et 46 (avec $s = 247296$), ce qui évite de recourir au difficile théorème de Rains et Sloane.

## 4. Sur l'existence de designs supérieurs

Comme on l'a signalé dans [Ven], § 16, la série $\Theta$ d'un réseau unimodulaire extrémal de dimension donnée $n$ multiple de 8 (lorsqu'un tel réseau existe) ne dépend que de l'entier $n$. En fait, toute référence aux réseaux est inutile : cette fonction est l'unique forme modulaire de poids $\varpi = \frac{n}{2}$ pour le groupe modulaire $\mathrm{PSL}\,2(\mathbb{Z})$ tout entier dont le développement soit de la forme

$$\Theta_n(q) = 1 + \sum_{k=k_0}^{\infty} a(k) q^k$$

avec $k_0 \geq 2\lfloor \frac{n}{24} \rfloor + 2$ ; on a alors $k_0 = 2\lfloor \frac{n}{24} \rfloor + 2$ et le coefficient $a_{k_0}$ est non nul. Nous posons $a_{k_0} = 2s(n)$ ; c'est le *kissing number* commun à tous les éventuels réseaux extrémaux de dimension $n$, dont la norme est $m = k_0$.

Posons comme dans [Ven] $n = 24k + \varepsilon$ avec $\varepsilon = 0$, $8$ ou $16$, et $\ell = 5$, $\ell = 3$ ou $\ell = 1$ selon que l'on a $\varepsilon = 0$, $\varepsilon = 8$ ou $\varepsilon = 16$. Le théorème 16.4 de [Ven] entraîne que les coefficients autres que le premier de la forme modulaire $\Theta_n$ vérifient certaines propriétés de divisibilité, en particulier que le nombre

$$\varphi(n) = m^{2\ell}\, s(n) \frac{1.3 \dots (2\ell+1)}{n\,(n+2) \dots (n-2+2\ell)}$$

est entier. La question se pose de savoir si l'ensemble $S(n)$ des vecteurs minimaux des réseaux extrémaux peut être un design sphérique de niveau supérieur à $2\ell + 1$.

PROPOSITION 4.1. *Pour $8 \le n \le 80$ (et $n$ multiple de $8$), $S$ n'est pas un $2\ell + 2$-design sphérique.*

*Démonstration.* Le cas de la dimension $16$ (pour lequel $2s = 480$) est immédiat : les systèmes de racines de rang $r > 8$ ne sont pas des $4$-designs ; le cas de la dimension $8$ est traité dans [Ven], § 5.

Pour toutes les autres dimensions, on conclut en exhibant un nombre premier $p > 2\ell + 3$ qui divise $n + 2\ell$ mais ne divise pas $s(n)$. Voici les valeurs de $s(n)$ et de $p$ qui permettent de conclure (nous avons calculé $s(n)$ en écrivant $\Theta_n$ comme combinaison linéaire de séries d'Eisenstein $E_4^x E_6^y$ avec $3x + 2y = \frac{n}{2}$) :

| | | | |
|---|---|---|---|
| $n = 24$ | $s = 98\,280$ | $\ell = 5$ | $p = 17 \mid 34$ |
| $n = 32$ | $s = 73\,440$ | $\ell = 3$ | $p = 19 \mid 38$ |
| $n = 40$ | $s = 19\,800$ | $\ell = 1$ | $p = 7 \mid 42$ |
| $n = 48$ | $s = 2\,620\,800$ | $\ell = 5$ | $p = 29 \mid 58$ |
| $n = 56$ | $s = 7\,795\,200$ | $\ell = 3$ | $p = 31 \mid 62$ |
| $n = 64$ | $s = 1\,305\,100$ | $\ell = 1$ | $p = 11 \mid 66$ |
| $n = 72$ | $s = 31\,090\,878\,000$ | $\ell = 5$ | $p = 41 \mid 82$ |
| $n = 80$ | $s = 625\,086\,600$ | $\ell = 3$ | $p = 43 \mid 86$ |

□

On voit donc en particulier que les réseaux extrémaux de dimension $n = 40$ ne sont pas fortement parfaits, un résultat démontré antérieurement par Bachoc à l'aide de formes modulaires de Siegel de genre 2. Cela n'empêche pas que certains d'entre eux soient parfaits au sens usuel de Voronoï. En dimension 16, il y a deux réseaux, à savoir $\mathbb{D}_{16}^+$ et $\mathbb{E}_8 \perp \mathbb{E}_8$. Le premier est parfait, le second ne l'est pas. Des exemples de réseaux extrémaux parfaits de dimension 40 ont été trouvés par Bachoc et Batut ([Bc-Bt]).

La dimension suivante est $n = 88$, à partir de laquelle (comme dans le cas $n = 72$) aucun réseau extrémal n'est connu. Le procédé utilisé pour démontrer la proposition précédente montre que $S$ n'est pas un 8-design. Rien n'empêche *a priori* qu'il soit un 5-design et peut-être même un 7-design. Toutefois, nous conjecturons que le théorème de Venkov est optimal.

Grâce à un programme de Henri Cohen (reposant sur une méthode de Siegel), j'ai pu constater que le procédé ci-dessus s'applique à de nombreux autres exemples au-delà de la dimension 88, et en particulier aux trois dimensions 96, 104, 112 pour lesquelles les réseaux extrémaux doivent être de norme 10.

Il n'y a pas de raison de se limiter aux réseaux unimodulaires. Un exemple intéressant est celui des réseaux 2-modulaires de dimension 32 et de norme 6, pour lesquels $s = 130510 = 2^9.3.5.17$ n'est pas divisible par le facteur premier 19 de $n+6 = 38$. Dans ce cas, $S$ est un 7-design d'après un théorème de Bachoc et Venkov ([Bc-V]), mais n'est pas un 8-design.

Il résulte de l'article [Ven] de Boris Venkov que le niveau d'un design sphérique formé par les vecteurs minimaux d'un réseau peut prendre l'une des valeurs 1, 3, 5, 7, 11. Les résultats de notre article, joints à ceux de [Ven] et de Bachoc–Venkov ([Bc-V]) soulèvent les questions suivantes relatives aux designs de cette forme :

Questions.

(1) Le niveau 9 est-il possible ?

(2) Un niveau $\ell \geq 13$ est-il possible ?

(3) Existe-t-il des exemples de 11-designs en-dehors des réseaux unimodulaires pairs extrémaux de dimension multiple de 24 ?

## BIBLIOGRAPHIE


[Bc-Bt] BACHOC, C. et BATUT, C. Étude algorithmique de réseaux construits avec la forme trace, *J. Exp. Math. 1* (1992), 183–190.

[Bc-V] BACHOC, C. et VENKOV, B. Modular forms, lattices and spherical designs, *Ce volume.*

[C-S] CONWAY, J. H. et SLOANE, N. J. A. *Sphere Packings, Lattices and Groups.* Grundlehren no. 290, Springer-Verlag (Heidelberg), 1993. (Troisième édition : 1999.)

[K-V] KOCH, H. et VENKOV, B. B. Über ganzzahlige unimodulare euklidische Gitter. *J. reine angew. Math. 398* (1989), 144–168.

[R-S] RAINS, E.M. et SLOANE, N. J. A. The Shadow Theory of Modular and Unimodular Lattices. *J. Number Theory 73* (1998), 359–389.

[S-V] SCHARLAU, R. et VENKOV, B. B. The genus of the Barnes-Wall lattice. *Comment. Math. Helvet. l69* (1994), 322–333.

[Ven] VENKOV, B. B. Réseaux et "designs" sphériques. Notes par J. Martinet. *Ce volume.*



Jacques Martinet

A2X, Institut de Mathématiques
Université Bordeaux 1
351, cours de la Libération
33405 Talence cedex
France
*e-mail :* martinet@math.u-bordeaux.fr