Etude Algorithmique de Réseaux Construits avec la Forme Trace

Christine Bachoc et Christian Batut

TABLE DES MATIERES

On étudie les propriétés numériques de trois classes de réseaux construits à l'aide de la forme trace dans des corps de nombres cyclotomiques. Des algorithmes adaptés ont permis de calculer leur minimum, le nombre de vecteurs minimaux, et de déterminer s'ils sont parfaits ou eutactiques. Les réseaux considérés sont des réseaux unimodulaires pairs de minimum 4 construits par Eva Bayer en dimension 24 (Leech), 32 et 48, puis certains réseaux liés au réseau de Leech, et enfin les réseaux de Craig qui sont construits sur les puissances successives de l'idéal au-dessus de p dans le p-ième corps cyclotomique.

We study the numerical properties of three types of lattices constructed by means of the trace form in cyclotomic number fields. We calculate their minimum and minimal vectors, and determine whether or not they are perfect or eutactic. The lattices considered are: certain even unimodular lattices, constructed by Eva Bayer, of minimum 4 and dimension 24 (Leech lattice), 32 and 48 ; certain lattices related to the Leech lattice; and Craig's lattices, constructed using the successive powers of the ideal above p in the p-th cyclotomic field.

1. INTRODUCTION

Soit $K = \mathbf{Q}(\zeta_m)$ un corps cyclotomique. Soit I un idéal fractionnaire de K et a un élément de $F = K \cap \mathbf{R}$ totalement positif (c'est-à-dire dont tous les conjugués sont positifs). Alors le couple

$$(I, \mathrm{Trace}_{K/\mathbf{Q}}(ax\bar{x})), \tag{1.1}$$

où $x \mapsto \bar{x}$ désigne la conjugaison complexe, est un réseau euclidien lorsqu'on le plonge dans $\mathbf{R} \otimes_{\mathbf{Q}} K$. Le but de cet article est d'étudier les propriétés numériques de certains réseaux obtenus par ce procédé. Nous nous sommes intéressés en particulier à la valeur de leur minimum, au nombre de leurs vecteurs minimaux et à leur propriété de perfection et d'eutaxie ; pour ces calculs, nous avons utilisé les algorithmes fondamentaux décrits plus loin.

© AK Peters, Ltd.
1058-6458/92 $0.50 per page

Dans le paragraphe 2, on met en œuvre les résultats de Eva Bayer [Bayer-Fluckiger 1984], qui permettent de construire des réseaux unimodulaires, pairs, indécomposables et de minimum au moins 4 dans des corps cyclotomiques. On obtient ainsi une matrice de Gram agréable pour le réseau de Leech, un réseau en dimension 32 et deux réseaux en dimension 48 qui ont pour minimum 4 et sont parfaits.

Dans le paragraphe 3, on utilise la matrice précédemment trouvée pour le réseau de Leech pour étudier les propriétés de certains réseaux qui lui sont liés : ses sous-réseaux d'indice 2, le "réseau de Leech court" et le "réseau de Leech impair".

Le paragraphe 4 est consacré aux réseaux de Craig ; ce sont des réseaux entiers, de discriminant p^{2k+1}, et définis dans $\mathbf{Q}(\zeta_p)$ sur les puissances successives de l'idéal au-dessus de p.

Définitions et notations

Soit R un réseau d'un espace euclidien E de dimension n, dont le produit scalaire est noté $x.y$. Le réseau *dual* de R est $R^* = \{x \in E \mid x.R \subset \mathbf{Z}\}$. Par exemple, si R est de la forme (1.1), alors

$$R^* = a^{-1}\bar{I}^{-1}\mathcal{D}_K^{-1},$$

où $\mathcal{D}_K$ est la différente de K. On dit que R est *entier* si $R \subset R^*$, et dans ce cas son discriminant est $[R^* : R]$. On dit que R est *unimodulaire* si $R = R^*$. La *norme* de x est $N(x) = x.x$; on dit que R est *pair* si $N(x)$ est un entier pair pour tout x appartenant à R.

Le *minimum* de R est

$$\operatorname{Min} R = \operatorname{Min}\{N(x) \mid x \in R\} \,;$$

les *vecteurs minimaux* de R sont les vecteurs de R dont la norme réalise $\operatorname{Min} R$. On note $S(R)$ l'ensemble des vecteurs minimaux de R et $s(R)$ la moitié du cardinal de $S(R)$.

A tout x appartenant à $S(R)$, on associe la projection orthogonale sur la droite $\mathbf{R}x$, notée p_x ; c'est un élément de l'espace $\operatorname{End}^s E$ des endomorphismes symétriques de E. On dit que le réseau R est *parfait* si la famille $\{p_x \mid x \in S(R)\}$ engendre $\operatorname{End}^s E$, et que R est *eutactique* s'il existe dans $\operatorname{End}^s E$ une relation de la forme

$$\mathrm{Id} = \sum_{x \in S(R)} \lambda_x p_x,$$

avec $\lambda_x > 0$ pour tout $x \in S(R)$ [Bergé et Martinet 1989].

Soit $\mathcal{B}$ une base de E, et soit X le vecteur des coordonnées de x dans cette base. La matrice de la projection p_x dans les bases $(\mathcal{B}, \mathcal{B}^*)$ est XX^t, où X^t désigne le vecteur transposé de X. On retrouve alors les définitions usuelles de la perfection et de l'eutaxie : le réseau est parfait si l'ensemble des XX^t lorsque x parcourt $S(R)$ est de rang $N = \frac{1}{2}n(n+1)$, et est eutactique s'il existe une relation de la forme $A^{-1} = \sum_{x \in S(R)} \lambda_X XX^t$.

L'intérêt de ces notions vient d'un théorème de Voronoï [1908] qui montre que les réseaux parfaits et eutactiques sont les réseaux extrêmes, c'est-à-dire ceux qui réalisent un maximum local de la fonction de densité.

Algorithmes utilisés

Soit R un réseau de E, et $A = (a_{i,j})_{1 \le i,j \le n}$ sa matrice de Gram dans une base $\mathcal{B}$.

Recherche des vecteurs minimaux. A partir d'une décomposition en carrés de la forme quadratique

$$q(x) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j,$$

un algorithme de "backtracking" [Pohst et Zassenhaus 1989, § 3.3] permet de trouver les vecteurs de $\mathbf{Z}^n$ tels que $q(x) \le C$.

Test de la perfection. On cherche le rang du système des XX^t en même temps que l'on trouve les vecteurs minimaux x de R. Lorsque la dimension est grande ($n > 24$), on fait les calculs modulo un nombre premier p (en général $p = 3$ suffit). En effet, si le rang est maximal sur $\mathbf{Z}/p\mathbf{Z}$, il est maximal sur $\mathbf{Z}$.

Test de l'eutaxie. Il est difficile en général de tester l'eutaxie. Cependant, si le groupe d'automorphismes est suffisamment transitif sur l'ensemble $S(R)$ des vecteurs minimaux, les coefficients d'eutaxie distincts sont en petit nombre (en effet, si le réseau est eutactique, il existe une relation d'eutaxie dont les coefficients λ_x sont constants sur les orbites de $S(R)$ sous l'action du groupe d'automorphismes). On a souvent de bonnes raisons de grouper certains vecteurs de $S(R)$ — par exemple, ceux qui sont orthogonaux à un vecteur donné — et on forme les sommes des XX^t sur ces parties de $S(R)$. Il est facile alors de trouver une relation de dépendance linéaire si elle existe entre les sommes obtenues et la matrice A^{-1}.

2. RESEAUX UNIMODULAIRES EN DIMENSION 24, 32 ET 48

Dans ce paragraphe, on construit explicitement certains réseaux unimodulaires mis en évidence par Eva Bayer dans [Bayer-Fluckiger 1984]. Soit Φ_m le m-ième polynôme cyclotomique et φ l'indicateur d'Euler. Bayer démontre que, si m n'est pas une puissance de 2, il existe un réseau unimodulaire ayant un automorphisme de polynôme caractéristique Φ_m si et seulement si m n'est pas de la forme p^r ou $2p^r$ et 8 divise $\varphi(m)$ [Bayer-Fluckiger, théorème 1.1]. De plus, un tel réseau est pair [ibid., lemme 1.4], indécomposable si m est sans facteurs carrés, et son minimum est supérieur ou égal à 4 si $\varphi(m) > 8$ [ibid., corollaire 2.2]. Ces réseaux sont, à isométrie près, de la forme (1.1) ; l'automorphisme de polynôme caractéristique Φ_m est la multiplication par ζ_m.

Nous nous sommes intéressés à des cas où on peut prendre pour $I = \mathbf{Z}[\zeta_m]$ l'anneau des entiers de K. Soit Ψ le polynôme minimal de $\eta = \zeta_m + \bar{\zeta}_m$ sur $\mathbf{Q}$. Alors on a

$$a = \frac{u}{\Psi'(\eta)},$$

où u est une unité de F de même signature que $\Psi'(\eta)$.

Dans chaque cas, on procède de la façon suivante : on cherche une unité u de F vérifiant (avec les notations de [Bayer-Fluckiger 1984, § 1])

$$\operatorname{sgn} u = \operatorname{sgn} \Psi'(\eta) = \sum_k g_{2k}^{-1},$$

et ayant la forme

$$u = \prod_{\substack{1 \le j \le m/2 \\ (j,m)=1}} \left(\frac{\zeta_m^j - \zeta_m^{-j}}{\zeta_m - \zeta_m^{-1}} \right)^{s_j},$$

ce qui conduit à la résolution d'un système linéaire modulo 2, dont on choisit une solution $s = (s_j)$.

Soit alors

$$\alpha_k = \operatorname{Trace}_{\mathbf{Q}(\zeta_m)/\mathbf{Q}} \left(\frac{u}{\Psi'(\eta)} \zeta_m^k \right),$$

pour $0 \le k \le \varphi(m) - 1$.

Comme on le verra ci-dessous, il est parfois utile de changer l'unité u en $uw\bar{w}$, où w est une unité de K, pour avoir un vecteur $\alpha = (\alpha_k)$ avec de petits coefficients. Un tel changement n'affecte pas la classe d'isométrie du réseau, car l'application $x \mapsto wx$ est une isométrie de

$$(I, \operatorname{Trace}_{\mathbf{Q}(\zeta_m)/\mathbf{Q}}(aw\bar{w}x\bar{x}))$$

sur $(I, \operatorname{Trace}_{\mathbf{Q}(\zeta_m)/\mathbf{Q}}(ax\bar{x}))$.

Proposition 2.1. *La matrice de* Gram *du réseau*

$$\left(\mathbf{Z}[\zeta_m], \operatorname{Trace}_{\mathbf{Q}(\zeta_m)/\mathbf{Q}} \left(\frac{u}{\Psi'(\eta)} x\bar{x} \right) \right)$$

dans la base $(\zeta_m^k)_{0 \le k \le \varphi(m)-1}$ *est*

$$A = (a_{i,j}), \quad \textit{avec } a_{i,j} = \alpha_{|i-j|}.$$

Cette matrice de Gram est obtenue par permutation circulaire de sa première ligne, qui est le vecteur α.

Résultats numériques

Dans chaque cas, nous avons testé la perfection du réseau par réduction modulo 3 de la matrice des xx^t ; en effet, à chaque fois, la réduction modulo 3 est de rang $N = \frac{1}{2}n(n+1)$, tandis que la réduction modulo 2 est de rang $N - 1$. Cette méthode ne permet malheureusement pas d'étudier l'eutaxie.

- $m = 35$, $n = \varphi(m) = 24$. Le réseau obtenu est isométrique au réseau de Leech, puisqu'il est pair, de dimension 24 et de minimum au moins égal à 4.

On peut choisir directement l'unité

$$u = (\zeta^3 + \zeta^{-3})(\zeta^6 + \zeta^{-6})(\zeta^9 + \zeta^{-9})(\zeta^{11} + \zeta^{-11}),$$

qui conduit au vecteur

$$\alpha = (4, 1, -1, 0, 0, 0, 1, -1, -2, -1, -1, -1, \\ 1, 1, -1, -1, 1, 2, 2, 1, -1, -1, 1, 1),$$

dont on déduit une matrice de Gram du réseau de Leech. Cette matrice sera utilisée dans le deuxième paragraphe. (La formule pour u qui se trouve dans [Bayer-Fluckiger, p. 529] n'est pas correcte.)

- $m = 51$, $n = \varphi(m) = 32$. Dans ce cas le calcul conduit à

$$s = (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0),$$

qui fournit une matrice du réseau à gros coefficients. On cherche alors des éléments w de K de petite norme. Par l'algorithme LLL [Lenstra et al. 1982], on trouve que l'unité $w = (1 - \zeta)^3$ est de norme 4. On remplace alors l'unité u par $vw\bar{w}$. On obtient finalement

$$\alpha = (4, 2, 1, -1, -1, -1, 0, 0, 1, 0, 0, -1, 0, 1, 2, 1, \\ 0, -2, -2, -2, -1, 0, 1, 1, 0, -1, -1, 0, 1, 1, 0, -1).$$

Ce réseau est parfait et possède 73440 paires de vecteurs minimaux, conformément à ce que prédit la théorie des fonctions thêta.

- $m = 65$, $n = \varphi(m) = 48$. Comme précédemment, on trouve d'abord l'unité correspondant au vecteur

$$s = (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, \\ 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0).$$

Une réduction par l'algorithme LLL conduit à l'unité $v = (1 - \zeta^2)^4(1 - \zeta^{22})$, qui donne le vecteur

$$\alpha = (4, 0, -1, 1, 1, -1, -1, 1, 1, 0, -1, 1, 1, -2, -1, 1, 0, \\ -1, 0, 1, 0, -1, -1, 1, 0, -2, 0, 2, -1, -1, 1, 1, -1, \\ -1, 1, 1, -1, -1, 2, 0, -2, 0, 1, -1, -1, 0, 1, 0).$$

Ce réseau est parfait et possède 4680 paires de vecteurs minimaux.

- $m = 105$, $n = \varphi(m) = 48$. On trouve d'abord l'unité correspondant au vecteur

$$s = (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, \\ 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0).$$

L'algorithme LLL conduit à l'unité

$$v = \zeta^3(\zeta^2 - 1)^4 \left(\zeta^{36} + 1 - \zeta^3 \frac{\zeta^{32} - 1}{\zeta^2 - 1}\right),$$

qui donne le vecteur

$$\alpha = (4, 0, 1, 1, 1, 2, 0, 2, 0, 1, 2, 0, 1, 0, 2, 0, 0, 1, 0, \\ 1, 0, 0, 0, 0, 1, -1, 0, 0, 0, 0, -1, 0, -1, 0, 0, -2, 0, \\ -1, 0, -1, -1, 0, -2, 0, -1, -1, -1, -1).$$

Ce réseau est parfait et possède 15120 paires de vecteurs minimaux.

3. CERTAINS RESEAUX LIES AU RESEAU DE LEECH

Les résultats de ce paragraphe sont résumés dans le tableau 1.

Réseau	det	min	s	parfait?	eutactique?
Λ_4	4	4	51176	oui	oui
Λ_6	4	4	49128	oui	oui
Λ_8	4	4	49128	oui	oui
O_{23}	1	3	2300	oui	oui
O_{24}	1	3	2048	non	oui

TABLE 1. Propriétés des sous-réseaux d'indice 2 du réseau de Leech (Λ_4, Λ_6, Λ_8), du réseau de Leech court (O_{23}) et du réseau de Leech impair (O_{24}).

Les sous-réseaux d'indice 2 du réseau de Leech

Soit R un réseau entier. Tout sous-réseau de R d'indice 2 dans R est de la forme

$$R_v = \{x \in R \mid x.v \equiv 0 \pmod 2\},$$

avec $v \in R^*$ et $v \notin 2R^*$. Le réseau R_v ainsi défini ne dépend que de la classe de v dans le quotient $R^*/2R^*$. De plus, si les classes de deux vecteurs dans ce quotient sont dans la même orbite sous l'action du groupe des isométries de R, les réseaux R_v correspondants sont évidemment isométriques.

Soit Λ le réseau de Leech. On rappelle le résultat suivant :

Proposition 3.1. *Soit C l'ensemble des vecteurs de Λ de norme inférieure ou égale à* 8.

(*a*) *Toute classe non nulle de $\Lambda/2\Lambda$ contient au moins une paire $\{\pm x\}$ de vecteurs de C. Elle contient soit exactement une paire $\{\pm x\}$ avec $x.x = 4$ ou $x.x = 6$, soit exactement vingt-quatre paires $\{\pm x_i\}_{1 \le i \le 24}$, avec $x_i.x_i = 8$ et $x_i.x_j = 0$ si $i \neq j$.*

(*b*) *L'action du groupe des isométries de Λ définit sur $\Lambda/2\Lambda$ quatre orbites: $\{\bar{0}\}$ et $\{\bar{v} \mid v.v = k\}$, où $k = 4, 6, 8$.*

Démonstration. Le point (a) est démontré dans [Conway et Sloane 1988, chap. 12, théorème 2]. Le point (b) se déduit de (a) et du fait que le groupe des isométries du réseau de Leech est transitif sur ses vecteurs de norme 4, ainsi que sur ceux de norme 6 et sur ceux de norme 8 [Conway et Sloane 1988, chap. 10, théorème 27]. □

Théorème 3.2. *Il y a exactement trois classes d'isométrie de sous-réseaux d'indice* 2 *de Λ. Ce sont les ensembles $\{\Lambda_v \mid v.v = k\}$, pour $k = 4, 6, 8$.*

Démonstration. Soient Λ_4, Λ_6 et Λ_8 des représentants de ces classes. En vue de la proposition 3.1(b), il suffit de montrer que ces trois réseaux ne sont pas isométriques, ce qui n'est pas évident *a priori*. On montre d'abord que deux réseaux Λ_v et Λ_w ne peuvent être isométriques si les normes de v et w ne sont pas congrues modulo 4. Nous aurons besoin des définitions suivantes :

Soit R un réseau entier pour la forme bilinéaire symétrique $b(x, y)$. Le quotient R^*/R est muni de la forme $\mathbf{Z}$-bilinéaire symétrique $\bar{b} : R^*/R \times R^*/R \to \mathbf{Q}/\mathbf{Z}$ définie par

$$\bar{b}(\bar{x}, \bar{y}) = b(x, y) \pmod{\mathbf{Z}}.$$

Elle est non-dégénérée, c'est-à-dire qu'elle induit un isomorphisme entre R^*/R et le groupe

$$\mathrm{Hom}_{\mathbf{Z}}(R^*/R, \mathbf{Q}/\mathbf{Z}).$$

La classe d'équivalence du couple $(R^*/R, \bar{b})$ (modulo les isomorphismes de groupe conservant les formes associées) est un invariant de la classe d'isométrie du réseau R. La proposition suivante calcule cet invariant dans le cas où R est un sous-réseau d'indice 2 d'un réseau unimodulaire.

Proposition 3.3. *Soit R un réseau unimodulaire, et soient v et w deux vecteurs de R n'appartenant pas à $2R$. Alors $(R_v^*/R_v, \bar{b}) \sim (R_w^*/R_w, \bar{b})$ si et seulement si $b(v, v) \equiv b(w, w) \pmod 4$.*

Démonstration. Le dual du réseau R_v est $R_v^* = R + \mathbf{Z}\frac{1}{2}v$. Le quotient R_v^*/R_v est un groupe d'ordre 4, cyclique si $v.v \equiv 1 \pmod 2$, et bicyclique si $v.v \equiv 0 \pmod 2$.

Supposons que $v.v \equiv 1 \pmod 2$. Alors la forme induite est déterminée par la valeur de $\bar{b}(x, x)$ sur un générateur x du quotient, et elle est indépendante du choix de ce générateur. En prenant $x = \frac{1}{2}\bar{v}$, on a $\bar{b}(\frac{1}{2}\bar{v}, \frac{1}{2}\bar{v}) = \frac{1}{4}b(v, v) \pmod{\mathbf{Z}}$. Le couple $(R_v^*/R_v, \bar{b})$ ne dépend donc, à équivalence près, que de la valeur de $v.v \pmod 4$.

Supposons que $v.v \equiv 0 \pmod 2$. Alors le quotient R_v^*/R_v est un espace vectoriel de dimension 2 sur le corps $\mathbf{F}_2$. La forme $\bar{b}$ est à valeurs dans $\frac{1}{2}\mathbf{Z}/\mathbf{Z}$; on considère plutôt la forme $2\bar{b}$, à valeurs dans $\mathbf{Z}/2\mathbf{Z}$. Le couple $(R_v^*/R_v, 2\bar{b})$ est un plan vectoriel muni d'une $\mathbf{F}_2$-forme bilinéaire symétrique non dégénérée. Soit w un vecteur de R tel que $w.v \equiv 1 \pmod 2$; l'existence de w est assurée car on a supposé que v n'appartient pas à $2R$. Alors $(\frac{1}{2}\bar{v}, \bar{w})$ est une base de R_v^*/R_v sur $\mathbf{F}_2$. La matrice de $2\bar{b}$ dans cette base est

$$\begin{pmatrix} \frac{1}{2}v.v & 1 \\ 1 & 0 \end{pmatrix}.$$

Suivant la congruence de $v.v$ modulo 4, on trouve les deux possibilités $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, qui ne sont pas équivalentes sur $\mathbf{F}_2$. □

Revenons maintenant aux sous-réseaux du réseau de Leech. La proposition précédente montre que ni Λ_4 et Λ_6, ni Λ_6 et Λ_8 ne peuvent être isométriques. Le calcul montre que Λ_4 et Λ_8 n'ont pas le même nombre de vecteurs minimaux (de norme 4). En effet, on trouve que $s(\Lambda_4) = 51176$ et $s(\Lambda_8) = 49128$. Ils ne sont donc pas isométriques, ce que prouve le théorème. (En revanche, $s(\Lambda_6) = s(\Lambda_8)$.) □

Pour construire une matrice de Gram pour chacun de ces réseaux, nous avons procédé de la façon suivante : soit A une matrice de Gram du réseau de Leech (nous avons utilisé la matrice décrite au paragraphe 2), que nous supposons relative à une base $(e_i)_{1 \le i \le 24}$. Alors la matrice A^{-1} est la matrice de Gram de la base duale $(e_i^*)_{1 \le i \le 24}$, définie par les conditions $e_i.e_j^* = \delta_{i,j}$ pour tout i, j. Une base du réseau $\Lambda_{e_i^*}$ est formée des vecteurs e_j pour $j \ne i$, et de $2e_i$. Il suffit donc de doubler la i-ème ligne et la i-ème colonne de A pour obtenir une matrice de Gram de $\Lambda_{e_i^*}$. Nous avons pris e_2^* pour Λ_4 ($e_2^*.e_2^* = 4$), e_1^* pour Λ_6 ($e_1^*.e_1^* = 14 \equiv 6 \pmod 4$), et e_{12}^* pour Λ_8 ($e_{12}^*.e_{12}^* = 8$).

Pour $k = 4, 6, 8$, on note A_k la matrice de Gram du réseau Λ_k obtenue dans cette base.

Les réseaux Λ_4 et Λ_6 sont eutactiques, avec deux coefficients d'eutaxie :

$$A_4^{-1} = \frac{1}{9315} \sum_{\substack{x \in S(\Lambda_4) \\ x.v=0}} xx^t + \frac{1}{4600} \sum_{\substack{x \in S(\Lambda_4) \\ x.v=\pm 2}} xx^t,$$

$$A_6^{-1} = \frac{243}{2049300} \sum_{\substack{x \in S(\Lambda_6) \\ x.v=0}} xx^t + \frac{275}{2049300} \sum_{\substack{x \in S(\Lambda_6) \\ x.v=\pm 2}} xx^t.$$

Le réseau Λ_8 est eutactique, avec un seul coefficient d'eutaxie :

$$A_8^{-1} = \frac{1}{8188} \sum_{x \in S(\Lambda_8)} xx^t.$$

Le réseau de Leech court et le réseau de Leech impair

Le *réseau de Leech court* est l'unique réseau unimodulaire de dimension 23 et de minimum 3 ; il est noté O_{23} [Conway et Sloane 1988, chap. 6, app.]. Si Λ est le réseau de Leech et v un vecteur minimal de Λ, alors O_{23} est la projection orthogonale de Λ_v sur l'orthogonal de v. Le groupe des isométries du réseau de Leech étant transitif sur l'ensemble de ses vecteurs minimaux, le choix de v est indifférent.

Le réseau O_{23} est parfait et eutactique, avec un seul coefficient d'eutaxie, égal à $\frac{1}{300}$.

Le *réseau de Leech impair* est l'unique réseau unimodulaire de dimension 24 et de minimum 3 ; il est noté O_{24}. C'est un voisin du réseau de Leech au sens de Kneser [Conway et Sloane 1988, chap. 17], c'est-à-dire qu'il existe un vecteur v de Λ tel que $O_{24} = \Lambda_v + \mathbf{Z}\frac{1}{2}v$. On peut choisir pour v la somme de trois vecteurs minimaux orthogonaux de Λ, $v = v_1+v_2+v_3$, à condition qu'il n'existe pas $w \in S(\Lambda)$ tel que $v_i.w = -2$ pour tout $i = 1, 2, 3$. En effet, dans le cas contraire, le minimum de $\Lambda_v + \mathbf{Z}\frac{1}{2}v$ est 1 ; ce réseau est alors la somme orthogonale d'un vecteur de norme 1 et d'un réseau isométrique à O_{23}.

Pour construire O_{24}, le choix $v = e_1 + e_4 + e_2^*$ convient ; on peut également montrer que, avec les notations qui précèdent, le réseau $\Lambda_8+\mathbf{Z}(\frac{1}{2}e_{12}^*+e_{12})$ est isométrique à O_{24}.

Le réseau O_{24} n'est pas parfait, mais il est eutactique, avec un seul coefficient d'eutaxie, égal à $\frac{1}{256}$.

4. LES RESEAUX DE CRAIG

Craig définit des réseaux notés $A_n^{(k)}$ pour $k \geq 1$ et $n \geq 1$ [Conway et Sloane 1988, chap. 8, § 6], qui, lorsque $n = p-1$ avec p un nombre premier, ont l'interprétation cyclotomique suivante. Soit $\mathfrak{P}$ l'idéal de $\mathbf{Q}(\zeta_p)$ au-dessus de p. Alors

$$A_{p-1}^{(k)} = (\mathfrak{P}^k, \tfrac{1}{p} \operatorname{Trace}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(x\bar{x})).$$

La proposition suivante résume les propriétés des réseaux $A_{p-1}^{(k)}$:

Proposition 4.1. (a) *Pour $k \geq 1$, $A_{p-1}^{(k)}$ est un réseau entier, pair, de dimension $p-1$ et de discriminant p^{2k-1}.*

(b) *$A_{p-1}^{(1)}$ est isométrique au réseau de racines A_{p-1}.*

(c) *$A_{p-1}^{(2)}$ est isométrique au réseau P_{p-1} de Barnes* [Barnes 1959].

(d) *$A_{p-1}^{(k)}$ est semblable à $A_{p-1}^{(k+(p-1)/2)}$, pour tout $k \geq 1$.*

(e) *$(A_{p-1}^{(k)})^*$ est semblable à $A_{p-1}^{(-k+(p+1)/2)}$, pour tout $k \geq 1$.*

(f) *$\operatorname{Min}(A_{p-1}^{(k)}) \geq 2k$, avec égalité si k divise $p-1$, ou si $k \equiv 3 \pmod 4$ et $k = \frac{1}{4}(p+1)$.*

Démonstration. Soit $\mathfrak{D} = \mathfrak{P}^{p-2}$ la différente de l'extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$. Alors le réseau dual de $A_{p-1}^{(k)}$ est $p\mathfrak{P}^{-k}\mathfrak{D}^{-1} = \mathfrak{P}^{1-k}$, ce qui démontre (a). Soit π un élément de $\mathbf{Q}(\zeta_p)$ vérifiant $\pi^2 = \pm p$. Alors la multiplication par π est une similitude qui envoie $A_{p-1}^{(k)}$ sur $A_{p-1}^{(k+(p-1)/2)}$ et $(A_{p-1}^{(k)})^*$ sur $A_{p-1}^{(-k+(p+1)/2)}$.

La minoration du minimum du réseau $A_{p-1}^{(k)}$ par $2k$ est démontrée dans [Conway et Sloane 1988, chap. 8, § 6]. Cette valeur n'est pas toujours atteinte, comme le montre le tableau 2, en particulier lorsque k est assez proche de $\frac{1}{2}(p-1)$. Toutefois, si k divise $p-1$, on peut donner explicitement des vecteurs de $A_{p-1}^{(k)}$ dont la norme est $2k$: en effet, un élément de $A_{p-1}^{(k)}$ de norme $2k$ est de la forme

$$\sum_{1\leq i\leq k} \zeta_p^{a_i} - \sum_{1\leq i\leq k} \zeta_p^{b_i},$$

où ζ_p est une racine primitive p-ième de l'unité et les a_i et les b_i sont des valeurs deux à deux distinctes de $\{0, 1, \ldots, p-1\}$ vérifiant la relation

$$\sum_{1\leq i\leq k} a_i^j \equiv \sum_{1\leq i\leq k} b_i^j \pmod p$$

pour tout $1 \leq j \leq k-1$ (voir la démonstration du théorème 7 dans [Conway et Sloane 1988, chap. 8, § 6]). Or, si k divise $p-1$, il existe k valeurs distinctes a_i dans l'ensemble $\{1, \ldots, p-1\}$ vérifiant $a_i^k \equiv 1 \pmod p$. On peut prendre $b_i = xa_i$, où x n'appartient pas à l'ensemble des a_i. Alors les équations précédentes sont bien vérifiées, puisque toutes les sommes sont égales à $0 \pmod p$.

Si $p \equiv 3 \pmod 4$ et $k = \frac{1}{4}(p+1)$, alors N. Elkies a donné une interprétation de ce réseau comme réseau de Mordell–Weil, qui met en évidence des vecteurs de norme $\frac{1}{2}(p+1)$ [Gross 1990]. □

La proposition 4.1(d) montre que l'on peut se restreindre aux entiers k tels que $1 \leq k \leq \frac{1}{2}(p-1)$. Le tableau 2 résume les propriétés des réseaux $A_{p-1}^{(k)}$, obtenues grâce aux algorithmes de recherche des vecteurs minimaux et de perfection. Les lignes avec $k = 2$ ou $k = 3$ correspondent aux réseaux de racines A_{p-1} et aux réseaux P_{p-1} de Barnes, respectivement, dont la perfection est bien connue. L'eutaxie de ces réseaux est automatique, grâce au fait que le groupe de leurs isométries définit une représentation irréductible de l'espace vectoriel réel associé ; en effet, il contient le produit semi-direct d'un groupe d'ordre p, celui des racines p-ièmes

n	k	min	s	parfait?
5	1	2	10	oui
5	2	4	5	non
7	1	2	21	oui
7	2	4	21	oui
7	3	6	7	non
11	1	2	55	oui
11	2	4	110	oui
11	3	6	55	oui
11	4	10	66	oui
11	5	10	11	non
13	1	2	78	oui
13	2	4	195	oui
13	3	6	156	oui
13	4	8	39	non
13	5	12	13	non
13	6	12	13	non
17	1	2	136	oui
17	2	4	476	oui
17	3	6	544	oui
17	4	8	238	oui
17	5	12	408	non
17	6	16	153	non
17	7	16	17	non
17	8	16	17	non
19	1	2	171	oui
19	2	4	684	oui
19	3	6	969	oui
19	4	8	684	oui
19	5	10	171	oui
19	6	12	57	non
19	7	18	19	non
19	8	18	19	non
19	9	18	19	non
23	1	2	253	oui
23	2	4	1265	oui
23	3	6	2277	oui
23	4	8	2024	oui
23	5	10	506	oui
23	6	12	253	oui
23	7	18	506	oui
23	8	22	276	oui
23	9	22	23	non
23	10	22	23	non
23	11	22	23	non

TABLE 2. Propriétés des réseaux de Craig $A_{p-1}^{(k)}$. Tous les réseaux sont eutactiques (voir texte).

de l'unité, par un groupe cyclique d'ordre $p-1$, le groupe de Galois de l'extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$. (Ce résultat apparaît dans [Brauer et Coxeter 1940], avec l'hypothèse restrictive d'irréductibilité sur $\mathbf{C}$, et est démontré dans la proposition 3.7 de [Bergé et Martinet 1992].)

Conjecture 4.2. *Pour $k \leq \frac{1}{4}(p+1)$, le réseau $A_{p-1}^{(k)}$ est un réseau parfait de minimum $2k$.*

On peut “tordre” les réseaux de Craig $A_{p-1}^{(k)} = (\mathfrak{P}^k, \frac{1}{p}\,\mathrm{Trace}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(x\bar{x}))$ de la façon suivante : soit $\mathfrak{A}$ un idéal fractionnaire de $\mathbf{Q}(\zeta_p)$ et α un élément de $\mathbf{Q}(\zeta_p) \cap \mathbf{R}$ totalement positif, tels que $\alpha\mathfrak{A}\bar{\mathfrak{A}} = \mathbf{Z}[\zeta_p]$. On peut considérer le réseau

$$(\mathfrak{P}^k\mathfrak{A}, \tfrac{1}{p}\,\mathrm{Trace}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\alpha x\bar{x})),$$

qui est encore de rang $p-1$, pair, de discriminant p^{2k-1}. D'après [Quebbemann 1981], il est isométrique à $A_{p-1}^{(k)}$ si et seulement si l'idéal $\mathfrak{A}$ est principal et engendré par un élément a de $\mathbf{Q}(\zeta_p)$ tel que $\alpha a\bar{a} = \varepsilon\bar{\varepsilon}$, où ε est une unité de $\mathbf{Q}(\zeta_p)$. Ces réseaux vérifient toujours les propriétés (d) et (e) de la proposition 4.1.

La plus petite valeur de p pour laquelle on obtient de nouveaux réseaux est $p = 23$. Dans $\mathbf{Q}(\zeta_{23})$, $2\mathbf{Z}[\zeta_{23}] = \mathfrak{q}\bar{\mathfrak{q}}$. L'idéal $\mathfrak{q}$ est non principal et engendré par 2 et $\frac{1}{2}(-1+\sqrt{-23})$. Pour obtenir une base de ce réseau, nous avons utilisé un algorithme de calcul de la forme normale d'Hermite des matrices. Le tableau 3 montre les résultats.

n	k	min	s	parfait?
23	1	4	17963	oui
23	2	4	759	oui
23	3	6	2024	oui
23	4	8	1771	oui
23	5	10	506	oui
23	6	12	506	oui
23	7	18	506	oui
23	8	24	506	oui
23	9	30	253	oui
23	10	36	253	oui
23	11	44	23	non

TABLE 3. Résumé des propriétés des réseaux de Craig tordus.

Ces réseaux apparaissent dans [Feit 1974, § 14]. Ce sont en fait des sous-réseaux du réseau de Leech, d'après [Conway et Sloane 1988, chap. 8, § 7.5].

REFERENCES

[Barnes 1959] E. S. Barnes, "The construction of perfect and extreme forms", *Acta Arith.* **5** (1959), 57–79 et 205–222.

[Bayer-Fluckiger 1984] Eva Bayer-Fluckiger, "Definite unimodular lattices having an automorphism of given characteristic polynomial", *Comment. Math. Helvetici* **59** (1984), 509–538.

[Bergé et Martinet 1989] A.-M. Bergé et J. Martinet, "Sur un problème de dualité lié aux sphères en géométrie des nombres", *J. Number Theory* **32** (1989), 14–42.

[Bergé et Martinet 1992] A.-M. Bergé et J. Martinet, "Réseaux extrêmes pour un groupe d'automorphismes", *Astérisque* **198–200** (1992), 41–66.

[Brauer et Coxeter 1940] R. Brauer et H. S. M. Coxeter, "A generalization of theorems of Schönhardt and Mehmke on polytopes", *Trans. Roy. Soc. Canada* (Sect. 3) **34** (1940), 29–34.

[Conway et Sloane 1988] J. H. Conway et N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, Heidelberg, 1988.

[Feit 1974] W. Feit, "On integral representation of finite groups", *Proc. London Math. Soc.* **29** (1974), 633–683.

[Gross 1990] B. H. Gross, "Group representations and lattices", *J. Amer. Math. Soc.* **3** (1990), 929–960.

[Lenstra et al. 1982] A. Lenstra, H. Lenstra and L. Lovász, "Factoring polynomials with rational coefficients", *Math. Ann.* **21** (1982), 515–534.

[Pohst et Zassenhaus 1989] M. Pohst et H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, Cambridge, 1989.

[Quebbemann 1981] H. G. Quebbemann, "Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung", *J. Reine Angew. Math.* **326** (1981), 158–170.

[Voronoï 1908] G. Voronoï, "Nouvelles applications des paramètres continus à la théorie des formes quadratiques, 1", *J. Reine Angew. Math.* **133** (1908).

Christine Bachoc, Laboratoire de Mathématiques de Bordeaux, 351, cours de la Libération, F-33405 Talence, France (bachoc@merak.greco-prog.fr)

Christian Batut, Laboratoire de Mathématiques de Bordeaux, 351, cours de la Libération, F-33405 Talence, France

Received March 23, 1992; revised June 15; accepted June 21