La classification des réseaux entiers unimodulaires en dimension 28

B. Allombert
avec Gaetan Chenevier, Orsay

IMB
Université de Bordeaux/CNRS

26/11/2022

Espaces euclidiens

Espace euclidien : $E : (\mathbb{R}^n, b)$
b est une forme bilinéaire symmétrique tel que la forme quadratique $Q(x) = b(x, x)$ est définie positive.
Matrice de Gram : $M = (b(e_i, e_j))_{i,j}$.
Isométrie entre $(\mathbb{R}^n, b)$ et $(\mathbb{R}^n, b')$: $P \in GL_n(\mathbb{R})$ tel que $b(x, y) = b'(P(x), P(y))$ pour tout $(x, y) \in \mathbb{R}^n$.
Groupe d'Isométrie :
$O(b)(\mathbb{R}) = \{P \in GL_n(\mathbb{R}) | b(x, y) = b(P(x), P(y))\}$.
Classification (Gauss) : Il y a une seule classe d'isométrie pour chaque dimension.

Réseaux euclidiens

Réseaux Euclidien : $L : (\mathbb{Z}^n, b)$
b est une forme bilinéaire symmétrique tel que la forme quadratique $Q(x) = b(x, x)$ est définie positive.
Matrice de Gram : $M = (b(e_i, e_j))_{i,j}$.
Isométrie entre $(\mathbb{Z}^n, b)$ et $(\mathbb{Z}^n, b')$: $P \in GL_n(\mathbb{Z})$ tel que $b(x, y) = b'(P(x), P(y))$ pour tout $(x, y) \in \mathbb{Z}^n$.
Groupe d'Isométrie :
$O(b)(\mathbb{Z}) = \{P \in GL_n(\mathbb{Z}) | b(x, y) = b(P(x), P(y))\}$.
Il y a une infinité de classe d'isométrie pour chaque dimension (car l'isométrie préserve le determinant de M).

Réseaux entiers unimodulaires

Le minimum du réseau $(\mathbb{Z}^n, b)$ est

$$m = \inf_{v \in \mathbb{Z}^n - \{0\}} b(v, v)$$

.

- Si M est à coefficients entiers, le réseau est dit entier.
- Si M est de déterminant 1, le réseau est dit unimodulaire.
- Si Q prend uniquement des valeurs paires, le réseau est dit pair, sinon impair.
- Si le minimum est ≥ 3, le réseau est dit sans racine.

Exemple : Soit $n \geq 1$ un entier soit $b(x, y) = \sum_{i=1}^{n} x_i y_i$ le produit scalaire usuel, alors M est la matrice identité et donc $(\mathbb{Z}^n, b)$ est un réseau unimodulaire entier, de minimum 1. Il possède $2n$ vecteurs minimaux. Il est impair.
Exemple de réseaux unimodulaires pairs sans racines : le réseau E_8 et le réseau de Leech (de dimension 24).

Lien avec les formes modulaires

Pour tout k, l'ensemble $\{v \in \mathbb{Z}^n | b(v,v) = k\}$ est fini. Nous posons

$$a_k = |\{v \in \mathbb{Z}^n | b(v,v) = k\}|$$

Soit $q(z) = exp(i\pi z)$ le nôme.
La forme modulaire associée au réseau est définie par

$$f(z) = \sum_{v \in \mathbb{Z}^n} q(z)^{b(v,v)}$$

nous avons

$$f(z) = \sum_{k \geq 0} a_k q(z)^k$$

Si le réseau est unimodulaire, f une forme modulaire de poids $n/2$, et de niveau 1 si n est pair et 4 sinon.
Les nombres a_k sont invariants par isométries.

Classification : Que dit Wikipedia ?

Not logged in Talk Contributions Create account Log in

Article Talk | Read Edit View history | Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Current events
Random article
About Wikipedia
Contact us
Donate

Contribute
Help
Learn to edit
Community portal
Recent changes
Upload file

Tools
What links here
Related changes

Unimodular lattice

From Wikipedia, the free encyclopedia

Not to be confused with modular lattice.

In geometry and mathematical group theory, a **unimodular lattice** is an integral lattice of determinant 1 or −1. For a lattice in n-dimensional Euclidean space, this is equivalent to requiring that the volume of any fundamental domain for the lattice be 1.

The E_8 lattice and the Leech lattice are two famous examples.

Contents [hide]

1 Definitions
2 Examples
3 Properties
4 Classification
5 Applications
6 References
7 External links

Dimension	Odd lattices	Odd lattices no roots	Even lattices	Even lattices no roots
0	0	0	1	1
1	1	0		
2	1	0		
3	1	0		
4	1	0		
5	1	0		
6	1	0		
7	1	0		
8	1	0	1 (E_8 lattice)	0
9	2	0		
10	2	0		
11	2	0		
12	3	0		
13	3	0		
14	4	0		
15	5	0		

16	6	0	2 (E_8^2, D_{16}^+)	0
17	9	0		
18	13	0		
19	16	0		
20	28	0		
21	40	0		
22	68	0		
23	117	1 (shorter Leech lattice)		
24	273	1 (odd Leech lattice)	24 (Niemeier lattices)	1 (Leech lattice)
25	665	0		
26	≥ 2307	1		
27	≥ 14179	3		
28	≥ 327972	38		
29	≥ 37938009	≥ 8900		
30	≥ 20169641025	≥ 82000000		
31	≥ 5000000000000	≥ 800000000000		
32	≥ 80000000000000000	≥ 10000000000000000	≥ 1160000000	≥ 10900000

Zoom

26	≥ 2307	1
27	≥ 14179	3
28	≥ 327972	38
29	≥ 37938009	≥ 8900

Nos résultats

Gràce à ce travail, nous pouvons mettre à jour Wikipedia ainsi

26	2566	1
27	17059	3
28	374062	38
29	$\geq$ 37938009	10092

Formules de masse

Si $(\mathbb{Z}^n, b)$ est un réseau alors $\mathrm{Aut}(b) = \mathcal{O}(b)(\mathbb{Z})$ est un groupe fini, ($O(b)(\mathbb{R})$ est infini dès que $n \geq 2$).
Soit $\mathcal{F}$ une famille de réseaux. La formule de masse pour $\mathcal{F}$ est la somme

$$S = \sum_{b \in \mathcal{F}} 1/|\mathrm{Aut}(b)| \ .$$

Cette quantité est connue pour certaines familles de réseaux. Minkowski et Siegel donnent une formule de masse pour les réseaux unimodulaires entiers pairs. Ils sont de dimension divisible par 8.

Formules de King

Oliver King (2003) généralise les formules de masses aux réseaux unimodulaire entiers sans racines.

23	$\frac{1}{84610842624000}$	$\sim 1.18 \times 10^{-14}$
24	$\frac{1}{1002795171840}$	$\sim 9.97 \times 10^{-13}$
25	0	0
26	$\frac{1}{18720000}$	$\sim 5.34 \times 10^{-8}$
27	$\frac{206867}{1585059840}$	$\sim 1.31 \times 10^{-4}$
28	$\frac{17924389897}{26202009600}$	$\sim 6.84 \times 10^{-1}$
29	$\frac{49612728929}{11136000}$	$\sim 4.46 \times 10^{3}$
30	$\frac{71800695768345628 39}{175111372800}$	$\sim 4.10 \times 10^{7}$

Applications des formules de masses

Les nombres $1/|\mathrm{Aut}(b)|$ étant positifs, si $\mathcal{F}'$ est un sous-ensemble de $\mathcal{F}$, alors $\mathcal{F}' = \mathcal{F}$ si et seulement si

$$\sum_{b \in \mathcal{F}'} 1/|\mathrm{Aut}(b)| = S$$

De plus comme $1/|\mathrm{Aut}(b)| \leq 1/2$ alors $F \geq 2|S|$. C'est comme cela que sont obtenu les minorations. En particulier pour 29, on trouve au moins $2 \times 4.46 \times 10^3 = 8920$ réseaux.

Voisins de Kneser

Deux réseaux unimodulaires sont dit k-voisins au sens de Kneser si leur intersection est un sous-groupe d'indice k dans chacun d'entre eux. Deux réseaux unimodulaires sont toujours k-voisins pour au moins un k. Kneser donne un algorithme pour énumérer les k-voisins d'un réseau, qui utilise de l'algèbre linéaire sur $\mathbb{Z}$ (HNF).
Chaque classes de réseaux apparait avec probabilité heuristique $1/\mathrm{Aut}(b)$. Avec la formule de masse, cela donne un algorithme théorique pour classifier les réseaux.

Problèmes pratiques

- L'algorithme de Kneser trouve très souvent des réseaux isomorphes, tester les isométries entre eux deux par deux devient trop lent.
- Les normes des éléments de la base des réseaux obtenus sont trop grandes pour pouvoir calculer $\mathrm{Aut}(b)$

Invariant de Bacher-Venkov

Un invariant est une fonction d'un réseau qui ne dépend que de sa classe d'isométrie. Les invariants permettent de vérifier que les classes d'isométries de réseaux sont distinctes.
L'invariant de Bacher-Venkov est obtenu à partir des vecteurs de normes 3.
Soit $V = \{v \in \mathbb{Z}^n, b(v,v) = 3\}$ que l'on numérote $V = \{v_1, \ldots, v_N\}$. Une isométrie permute les éléments de V.
Soit G le graphe de sommets V tel que deux vecteurs sont reliés si et seulement si leur produit scalaire est pair. Deux réseaux isomorphes conduisent à des graphes isomorphes. Les invariants du graphe G sont donc aussi des invariants du réseau.

Invariant de Bacher-Venkov (du graphe)

La matrice d'adjacence de G est $A = (b(v_i, v_j) \pmod 2)_{i,j}$. A^2 est le nombre de chemin de longueur 2 entre i et j dans G. L'invariant de Bacher-Venkov est le multiensemble des multiensembles associés au colonnes de A^2. Il est invariant par permutation des vecteurs de V.

Calcul des automorphismes

À partir d'une matrice obtenue par l'algorithme de Kneser, nous appliquons l'algorithme LLL pour la réduire. Si la norme des éléments de bases est trop grande, nous cherchons d'autre bases en prenant des vecteurs minimaux au hasard. Cela est nécéssaire pour appliquer l'algorithme de Plesken-Souvignier de calcul des automorphismes.

Algorithme de classification

Hypothèse : deux réseaux non isomorphes ont des invariants de Bacher-Venkov différents.

1. énumérer les voisins de Kneser du réseau $\mathbb{Z}^n$
2. pour chaque réseau obtenu, vérifier ses invariants.
3. pour chaque réseau ayant le bon minimum, calculer son invariant de Bacher-Venkov
4. si l'invariant est nouveau, le rajouter dans la liste et calculer le nombre d'isométries du réseau.
5. Quand la formule de masse est satisfaite, terminer.

L'algorithme termine si et seulement si l'hypothèse est satisfaite.
Pour les degrés 28 et 29, l'algorithme termine.

Problème des doublons

Il est fréquent que deux voisins de Kneser sont isomorphes.
Considérons le problème suivant :
Nous tirons avec remise des images dans un ensemble de N images. Pour avoir plus de 50% de chance de voir toutes les images, il faut tirer au moins $O(N\log(N))$ images, plus si les images ne sont pas équiprobables, ce qui est le cas ici.
Cependant, les éléments les plus rares sont connus par des considérations théoriques.
Dans tout les cas le nombre de voisins considéré par notre algorithme est très supérieur

Vecteurs de norme 1

Le procédé d'othogonalisation de Gram-Schmidt ne s'applique pas en général car il ne donne pas des vecteurs à coordonnées entière. Par contre il fonctionne pour les vecteurs de norme 1.
Soit u de norme 1 et v quelconque alors
$b(u, v - b(u, v)u) = b(u, v) - b(u, v)b(u, u) = 0$
Cela permet de décomposer les réseau en somme orthogonale de deux réseaux. Cela ramène la classification des réseaux de dimension n avec vecteurs de norme 1 avec celle des réseaux de dimension $\leq n$ sans vecteurs de norme 1.

Vecteurs de norme 2

Soit v, w deux vectors de carré scalaires 2. Alors l'inégalité de Cauchy-Schwarz donne $|b(v, w)| \geq 2$ avec égalité si v et w sont colinéaire. Comme $b(v, w)$ est entier, $|b(v, w)| = 0$, 1 ou 2
Les vecteurs de normes 2 forment un système de racine, qui ont été classifié. Soit G le graphe dont les sommet sont les vecteurs de norme 2 et tel que v et w sont relié si et seulement si $|b(v, w)| = 1$. Ce graphe est le diagramme de Dynkin du système de racine, les composantes connexes sont classées àisomorphisme près en A_n, D_n, E_6, E_7, E_8 (classification ADE).

Dimension 28

Pour la dimension 28 Chenevier a calculé les formules de masses pour les 4722 diagrammes de Dynkin possibles du système de racine, ce qui permet de couper le calcul en 4722 calculs indépendant qui peuvent être traité simultanément ou séparément, ce qui permet d'économiser la mémoire. Cela donne la classification pour les réseaux de dimension 28 sans vecteurs de normes 1. En ajoutant les réseaux de dimension ≤ 27 sans vecteurs de normes 1 qui était déjà connu, cela donne la classification complète.

Calculs

Les calculs ont été fait en parallèle sur deux supercalculateurs, celui d'Orsay et celui de l'INRIA Bordeaux. Ils ont pris l'équivalent de 72 ans CPU. La version parallèle de PARI/GP a été utilisée.
Nous trouvons 10092 réseaux unimodulaires entiers sans racines en dimension 29 et 374062 réseaux unimodulaires entiers en dimension 28

Statistique en dimension 29

Nombre de réseaux par nombre d'isométries.

2	4	6	8	12	16	20	24	32
8081	1465	6	293	28	91	1	21	32
36	40	48	60	64	72	80	96	120
1	3	15	1	12	1	1	11	1
128	144	160	192	232	256	288	320	384
2	1	2	2	1	2	1	1	1
768	864	960	1024	1536	2400	2592	3072	5184
2	1	1	2	2	1	1	1	1
6144	18432	24000						
1	1	1						