JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

PIERRE LOYER
PATRICK SOLÉ

Les réseaux BW_{32} et U_{32} sont équivalents

Journal de Théorie des Nombres de Bordeaux, tome 6, n° 2 (1994), p. 359-362

<http://www.numdam.org/item?id=JTNB_1994__6_2_359_0>

Journal de Théorie des Nombres
de Bordeaux **6** *(1994), 359–362*

Les réseaux BW_{32} et U_{32} sont équivalents

par PIERRE LOYER ET PATRICK SOLÉ

RÉSUMÉ – On montre que le réseau de Barnes-Wall de rang 32 est équivalent au réseau à double congruence U_{32} de Martinet. La preuve utilise la notion de voisinage de Kneser et des résultats de Koch et Venkov sur le défaut du voisinage ("Nachbardefekt").

Tous les réseaux considérés dans cette note sont de rang 32. Ils sont unimodulaires, pour une normalisation convenable. Par conséquent, la notion d'équivalence, prise en général au sens de similitude, se restreint à la notion d'isométrie. Lorsque l'écriture utilisée pour désigner un réseau n'implique pas telle quelle qu'il est unimodulaire, nous sous-entendons qu'il faut le normaliser.

Nous recourons à un procédé de construction de réseaux à partir de codes, dit construction A. Les codes considérés sont des codes linéaires binaires de longueur 32. Un code C est équivalent à un code C' si et seulement si les mots de C sont obtenus par permutation sur les coordonnées des mots de C'. Soit C un tel code. La construction A telle que définie par Conway et Sloane (voir [3]) est

$$A[C] = C + 2\mathbb{Z}^{32}.$$

Plus généralement, pour tenir compte des isométries, on introduit une base orthonormale $e_1, \cdots, e_{32}$ et alors

$$A[C] = \left\{ \sum_{i=1}^{32} c_i e_i | (c_1, \cdots, c_{32}) \in C \right\} + 2(\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_{32}).$$

Pour normaliser cette écriture, il faut la multiplier par un facteur $1/\sqrt{2}$, de sorte que les codes autoduaux deviennent des réseaux unimodulaires (voir [9]).

Le but de cette note est de montrer que le réseau de Barnes-Wall de rang 32, BW_{32} et le réseau U_n de même rang, U_{32}, sont équivalents.

Manuscrit reçu le 27 Juin 1994, révisé le 20 Septembre 1994.

Pour la construction des réseaux U_n par Martinet à partir d'algèbres de quaternions, on se réfèrera à [4], [8], [7, ch. 8]. Pour la construction de BW_{32}, l'article fondamental est [1]. Cependant, nous conseillons plutôt des références qui font le lien avec les codes de Reed-Muller car elles sont plus en rapport avec notre note : ce sont [3, ch. 8], où les réseaux de Barnes-Wall sont analysées comme une construction D à partir des codes de Reed-Muller, et [5], [6]. Convenablement normalisé, BW_{32} est unimodulaire de norme 4, de même que U_{32}.

Nous noterons $RM(2)$ le code de Reed-Muller d'ordre 2.

Nous rappelons quelques notions tirées de [9].

On appelle *racines* d'un réseaux unimodulaires ses vecteurs de norme (longueur au carré) 2. Il est immédiat que ni BW_{32}, ni U_{32} n'ont de racines. De manière générale, on note G_ϕ l'ensemble des réseaux sans racines et G_{32A_1} l'ensemble des réseaux dont le système de racines consiste en 32 paires de vecteurs orthogonales entre elles.

On appelle *défaut* du réseau Λ le nombre $\delta(\Lambda) = 32 - m$, où m est le plus grand nombre possible de paires de racines orthogonales entre elles. C'est en quelque sorte une mesure de la distance du système de racines de Λ à $32A_1$. Les éléments de G_{32A_1} sont de défaut nul, ceux de G_ϕ sont de défaut 32.

On introduit encore la notion de voisinage : deux réseaux distincts Λ et Λ' entiers unimodulaires sont *voisins* s'il possèdent un sous-réseau d'indice 2 en commun. C'est alors nécessairement leur intersection. Soit $\overrightarrow{v} \in \Lambda' - \Lambda$. Alors

$$\Lambda \cap \Lambda' = \{\overrightarrow{x} \in \Lambda | 2\overrightarrow{x}.\overrightarrow{v} \in 2\mathbb{Z}\}$$

et Λ' est l'union de cet ensemble et du même translaté de $\overrightarrow{v}$. (Cet ensemble est bien d'indice deux dans Λ et Λ'. En effet, s'il était égal à Λ, par exemple, cela voudrait dire que pour tout $\overrightarrow{x} \in \Lambda$, le produit $\overrightarrow{x}.\overrightarrow{v}$ serait entier, donc $\overrightarrow{v}$ appartiendrait au dual de Λ c'est-à-dire Λ lui-même par unimodularité. Cela montre que l'hypothèse d'unimodularité est essentielle dans la définition du voisinage).

On peut alors parler du *défaut du voisinage* (Nachbardefekt) d'un réseau : c'est le minimum des défauts de ses voisins.

On est en mesure d'exprimer les résultats utiles à notre démonstration :

- il y a exactement (à équivalence près) cinq codes doublement pairs, de poids minimal 8, autoduaux (voir [2]);

- il y a exactement (à équivalence près) cinq réseaux unimodulaires pairs de systèmes de racines $32A_1$. Il s'obtiennent par construction A à partir des codes précédents (voir [9, §3 et p. 159]);

- Il y a exactement (à équivalence près) cinq réseaux unimodulaires sans racines de défaut nul dans le voisinage. Ce sont les voisins des précédents (voir [9, §10]).

Le code $RM(2)$, les réseaux $A[RM(2)]$ et U_{32} appartiennent respectivement à ces catégories. Coulangeon a démontré que $A[RM(2)]$ et U_{32} étaient voisins. Il suffit de démontrer la même chose pour $A[RM(2)]$ et BW_{32} pour que l'isométrie entre U_{32} et BW_{32} s'ensuive.

LEMME 1. *BW_{32} est le voisin de $A[RM(2)]$ construit à l'aide du vecteur "tout à un".*

Preuve : Construisons le voisin de $A[RM(2)]$ selon le schéma donné plus haut. Nous introduisons tout d'abord

$$\{\overrightarrow{x} \in A[RM(2)] | \overrightarrow{x}.1^{32} = \sum x_i \equiv 0 \bmod 4\}$$

(la congruence modulo 4 est due à des problèmes de normalisation), un réseau d'indice deux dans $A[RM(2)]$ qu'on peut aussi noter

$$RM(2) + 2P_{32} + 4\mathbb{Z}^{32}$$

(P^{32} est le code *à simple parité*, constitué des mots binaires de longueur 32 de poids pair ; c'est aussi le code de Reed-Muller d'ordre 4). Alors par définition du voisinage, le réseau recherché est semblable à

$$R_{32} + 2RM(2) + 4P_{32} + 8\mathbb{Z}^{32}$$

(R_{32} est le code *à répétition*, constitué du mot nul et du mot tout à un ; c'est aussi le code de Reed-Muller d'ordre 0). On reconnaît BW_{32} selon une formule de [6, p. 1169] où $BW_{32}, R_{32}, RM(2), P_{32}$ sont notés respectivement $R\Lambda_{32}, (32, 1, 32), (32, 16, 8)$ et $(32, 31, 2)$ (la première coordonnée désignant la longueur, la seconde, la dimension et la troisième, la distance minimale du code).

D'où le

THÉORÈME 1. *$A[RM(2)]$ et BW_{32} sont équivalents.*

Les deux auteurs remercient l'équipe A2X de Bordeaux pour de nombreux discussions et échanges. Le premier auteur la remercie plus particulièrement pour son accueil amical et, entre autres, Renaud Coulangeon pour l'avoir introduit à l'article de Koch et Venkov.

RÉFÉRENCES

[1] E.S. Barnes and G.E. Wall, *Some extreme forms defined in terms of abelian groups*, Journal of the Australian Mathematical Society, **1** (1959), 47–63.

[2] J.H. Conway and V. Pless, *On the enumeration of self-dual codes*, Journal of Combinatorial Theory Ser.A **28** (1980), 26–53.

[3] J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices and groups*, Springer-Verlag, 2nd édition, 1992.

[4] R. Coulangeon, *Réseaux quaternioniens et invariant de Venkov*, Manuscripta Mathematica **82** (1994), 41–50.

[5] G.D. Forney. Coset codes – part I, *Introduction and geometrical classification*, IEEE Trans. Inform. Theory, **34,5** (1988), 1123–1151.

[6] G.D. Forney. Coset codes – part II, *Binary lattices and related codes*, IEEE Trans. Inform. Theory, **34,5** (1988), 1152–1187.

[7] J. Martinet, *Les réseaux parfaits des espaces euclidiens*. En préparation.

[8] J. Martinet, *Structures algébriques sur les réseaux*, Séminaire de théorie des nombres de Paris (1993). Cambridge University Press. A paraître.

[9] H. Koch und B. Venkov, *Über ganzhalige unimodulare euklidische Gitter*, J. reine angew. Math. **398** (1989), 144–168.

P. Loyer et P. Solé
I3S
250 Avenue Albert Einstein
06560 Valbonne, France