

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

MICHEL BROUÉ

Codes et formes quadratiques

Séminaire Dubreil. Algèbre et théorie des nombres, tome 28, n° 1 (1974-1975), exp. n° 23, p. 1-3

http://www.numdam.org/item?id=SD_1974-1975__28_1_A17_0

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1974-1975, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

CODES ET FORMES QUADRATIQUES

par Michel BROUÉ

On met en évidence des analogies remarquables entre la théorie des codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments, et certains aspects de la théorie des formes quadratiques entières définies positives à discriminant $+1$.

On se contente de présenter ici un tableau mettant en parallèle les deux théories. Un exposé complet, sur le même sujet, a été publié dans les Comptes Rendus des Journées mathématiques de la Société mathématique de France [1974. Montpellier] (*). On pourra s'y reporter pour les définitions, les développements, et l'exposé des "ponts" actuellement connus entre les deux théories.

On désigne par Ω un ensemble fini de cardinal ω pair.

Si E est un ensemble fini, on désigne par $|E|$ son cardinal.

<u>Réseaux dans $\mathbb{R}^\omega$</u>	<u>Codes dans $\mathcal{P}(\Omega)$</u>
Volume 1 - Réseaux autoduals, de type II.	Dimension $(\omega/2)$ - Codes auto-orthogonaux, de type II.
Carré minimum :	Poids minimum :
$ms(L) = \inf\{x \cdot x\}_{(x \neq 0)(x \in L)} ;$	$mw(C) = \inf\{ x \}_{(x \neq 0)(x \in C)} ;$
$ms(\omega) = \sup ms(L)$ pour L de volume 1 .	$mw(\omega) = \sup mw(C)$ pour C de dimension $(\omega/2)$.
Borne de Rogers :	Borne d'Elias :
$ms(\omega) \leq \lambda_\omega \sim (1/\pi e) \cdot \omega \simeq 0,116 \omega .$	$mw(\omega) \leq \gamma_\omega \sim 0,196 \omega .$
Fonction thêta :	Polynôme des poids :
$\Theta_L(z) = \sum_{x \in L} e^{\pi i(x \cdot x)z} .$	$P_C(X,Y) = \sum_{x \in C} X^{ x } \cdot Y^{\omega - x } .$

(*) BROUÉ (M.). - Codes correcteurs d'erreurs auto-orthogonaux sur le corps à 2 éléments et formes quadratiques entières définies positives à discriminant $+1$, "Comptes rendus des journées mathématiques S. M. F.", p. 71-108. - Montpellier, Université du Languedoc, UER de Mathématiques, 1974 (Cahiers mathématiques, Montpellier, n° 3).

Les algèbres associées

Formule de Poisson : Si L^0 est le dual du réseau L , on a

$$\Theta_{L^0}(z) = (z/i)^{(\omega/2)} \cdot \text{Vol}(L) \cdot \Theta_L(-1/z) .$$

Les fonctions thêta des réseaux autoduals appartiennent à l'algèbre $\mathcal{H}_{\mathbb{Z}} = \mathbb{Z}[\Theta_{\mathbb{Z}}^2, \Delta_4]$, où $\Theta_{\mathbb{Z}}^2$ et Δ_4 sont des fonctions de "degrés" respectifs 2 et 4 .

Les fonctions thêta des réseaux de type II appartiennent à l'algèbre $\mathcal{H}_{\mathbb{Z}} = \mathbb{Z}[E_4, \Delta_{12}]$, où E_4 et Δ_{12} sont des fonctions de "degrés" respectifs 8 et 24, et où

$$\Delta_{12}(z) = e^{2\pi iz} \cdot \prod_{m \geq 1} (1 - e^{2\pi imz})^{24} .$$

Les fonctions extrêmes

Pour ω multiple de 24, soit U_{ω} l'élément de $\mathcal{H}_{\mathbb{Z}}$ tel que, si

$$U_{\omega}(z) = u_0 + u_1 e^{\pi iz} + u_2 e^{2\pi iz} + \dots ,$$

on ait :

$$u_0 = 1, \quad u_1 = u_2 = \dots = u_{2m_{\omega}-1}$$

(avec $m_{\omega} = [\omega/24] + 1$). Alors $u_{2m_{\omega}} > 0$, et pour $\omega = 24$ et 48, il existe des réseaux de fonction thêta U_{ω} . Cependant, pour ω assez grand, U_{ω} a des coefficients négatifs.

Les algèbres associées

Formules de Mac-Williams : Si C^0 est l'orthogonal du code C , on a

$$P_{C^0}(X, Y) = 2^{((\omega/2) - \dim C)} \cdot P_C\left(\frac{Y-X}{\sqrt{2}}, \frac{X+Y}{\sqrt{2}}\right) .$$

Les polynômes des poids des codes auto-orthogonaux appartiennent à l'algèbre $\mathcal{W}_{\mathbb{Z}} = \mathbb{Z}[A_2, C]$, où A_2 et C sont deux polynômes de degrés respectifs 2 et 4 .

Les polynômes des poids des codes de type II appartiennent à l'algèbre $\mathcal{W}_{\mathbb{Z}} = \mathbb{Z}[B_8, D]$, où B_8 et D sont deux polynômes de degrés respectifs 8 et 24, et où

$$D(X, Y) = X^4 Y^4 (X^4 - Y^4)^4 .$$

Les polynômes extrêmes

Pour ω multiple de 24, soit Q_{ω} l'élément de $\mathcal{W}_{\mathbb{Z}}$ tel que, si

$$Q_{\omega}(X, Y) = q_0 X^{\omega} + q_1 X^{\omega-1} Y + \dots ,$$

on ait :

$$q_0 = 1, \quad q_1 = q_2 = \dots = q_{4m_{\omega}-1} = 0$$

(avec $m_{\omega} = [\omega/24] + 1$). Alors $q_{4m_{\omega}} > 0$, et pour $\omega = 24$ et 48, il existe des codes de polynôme des poids Q_{ω} . Cependant, pour ω assez grand, Q_{ω} a des coefficients négatifs.

Les moyennes pondérées

$\Theta_{\omega}^{II} = \sum (1/|G(L)|) \cdot \Theta_L$ (somme étendue à l'ensemble des classes d'isomorphismes de réseaux de type II de $\underline{R}^{\omega}$).

Du calcul de Θ_{ω}^{II} , on déduit l'existence d'une famille $(L_{\omega})_{\omega}$ où L_{ω} est un réseau de type II de $\underline{R}^{\omega}$, telle que $ms(L_{\omega})/\omega$ est équivalent à 0,116/2 lorsque ω tend vers l'infini.

On ne connaît pas explicitement une telle famille.

Les moyennes pondérées

$Pm_{\omega}^{II} = \sum (1/|G(C)|) \cdot P_C$ (somme sur l'ensemble des classes d'isomorphismes des codes de type II de $\mathcal{P}(\Omega)$).

Du calcul de Pm_{ω}^{II} , on déduit l'existence d'une famille $(C_{\omega})_{\omega}$ où C_{ω} est un code de type II de $\mathcal{P}(\Omega)$, telle que $mw(C_{\omega})/\omega$ est équivalent à 0,110 lorsque ω tend vers l'infini.

On ne connaît pas explicitement une telle famille.

(Texte reçu le 21 juillet 1975)

Michel BROUÉ
18 rue du Général Pajol
77130 MONTEREAU
