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 P. DUBREIL
(Algèbre)
28e année, 1974/75, n° 23, 3 p.

5 mai 1975

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.

Réseaux dans R^{ω}

Volume 1 - Réseaux autoduaux, de type II.

Carré minimum :

$$ms(L) = \inf\{x.x\}_{(x\neq 0)(x\in L)} ;$$

$ms(\omega) = \sup ms(L)$ pour L de volume 1 .

Borne de Rogers :

$$ms(\omega) \leqslant \lambda_{\omega} \sim (1/\pi e).\omega \simeq 0{,}116\ \omega .$$

Fonction thêta :

$$\Theta_L(z) = \sum_{x\in L} e^{\pi i (x.x) z} .$$

Codes dans $\mathcal{P}(\Omega)$

Dimension $(\omega/2)$ - Codes auto-orthogonaux, de type II.

Poids minimum :

$$mw(C) = \inf\{|x|\}_{(x\neq 0)(x\in C)} ;$$

$mw(\omega) = \sup mw(C)$ pour C de dimension $(\omega/2)$.

Borne d'Elias :

$$mw(\omega) \leqslant \gamma_{\omega} \sim 0{,}196\ \omega .$$

Polynôme des poids :

$$P_C(X,Y) = \sum_{x\in C} X^{|x|}.Y^{\omega-|x|} .$$

(*) 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

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

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

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

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

Les algèbres associées

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

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

Les polynômes des poids des codes auto-orthogonaux appartiennent à l'algèbre $\mathcal{Y}_{\underset{\sim}{Z}} = \underset{\sim}{Z}[A_2 , C]$, 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 $\mathcal{W}_{\underset{\sim}{Z}} = \underset{\sim}{Z}[B_8,D]$, 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 fonctions extrêmes

Pour ω multiple de 24, soit U_ω l'élément de $\mathcal{M}_{\underset{\sim}{Z}}$ 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 $m_\omega = [m/24] + 1$). 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 polynômes extrêmes

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

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

on ait :

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

(avec $w_\omega = [\omega/24] + 1$). Alors $q_{4w_\omega} > 0$, 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

$\Theta m_\omega^{II} = \Sigma(1/|G(L)|).\Theta_L$ (somme étendue à l'ensemble des classes d'isomorphismes de réseaux de type II de $\underset{\sim}{R}^\omega$).

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

On ne connait pas explicitement une telle famille.

Les moyennes pondérées

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

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 $\mathbb{F}(\Omega)$, telle que $mw(C_\omega)/\omega$ est équivalent à $0{,}110$ lorsque ω tend vers l'infini.

On ne connait pas explicitement une telle famille.

(Texte reçu le 21 juillet 1975)

Michel BROUÉ
18 rue du Général Pajol
77130 MONTEREAU