# Codes et formes paramodulaires

**Manabu OURA** (*) (**)

INRIA - U.R. Sophia Antipolis, 06902 Sophia Antipolis Cedex, France
Courriel : moura@sophia.inria.fr
et
Département de mathématique, l'université Kyushu, Fukuoka, 812-8581, Japon
Courriel : ohura@math.kyushu-u.ac.jp

**Résumé.** On donne une construction des formes paramodulaires en utilisant la théorie des codes.

## *Codes and paramodular forms*

**Abstract.** We give a construction of paramodular forms using coding theory.

1. *Introduction.* — Dans les articles [2], [4], [7], [1] etc., on a vu la relation entre codes et formes modulaires. Ces formes modulaires, autrement dit, correspondent à des formes paramodulaires de polarisation principale. Il est naturel de demander à généraliser ces correspondances. Dans cette note, on annonce que l'on peut procéder d'une manière analogue pour obtenir une forme paramodulaire associée à la polarisation $\begin{pmatrix} k_1 & & & \\ & k_2 & & \\ & & \ddots & \\ & & & k_g \end{pmatrix}$, où tout $k_i$ est un entier positif tel que $k_1 = 1$, $k_i | k_{i+1}$ pour $i = 1, 2, \ldots, g-1$ et $g$ un entier $\geq 2$. Les arguments et calculs utilisés dans cette note sont standards et nous omettrons les démonstrations.

On fixe les notations. On note $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ l'ensemble des nombres entiers, rationnels, réels, complexes. On pose $\mathbf{Z}_l = \mathbf{Z}/l\mathbf{Z}$, $\mathbf{Z}_l^n = \underbrace{\mathbf{Z}_l \times \cdots \times \mathbf{Z}_l}_{n}$ et $\mathbf{e}(\cdot) = \exp(2\pi\sqrt{-1}\,\cdot)$. $\delta_{*,*}$ désigne le delta de Kronecker. Par $\mathrm{diag}(\alpha, \beta, \ldots, \gamma)$, nous désignons la matrice diagonale $\begin{pmatrix} \alpha & & & \\ & \beta & & \\ & & \ddots & \\ & & & \gamma \end{pmatrix}$.

Dans toute cette note, on suppose $g \geq 2$.

2. *$(l_1, l_2, \ldots, l_g)$-codes et polynômes des poids symétrisés.* — Dans cette section, nous rappelons les codes sur le groupe abélien fini $\mathbf{Z}_{2l}$ (*cf.* [1]) et étudions les $(l_1, l_2, \ldots, l_g)$-codes et les polynômes des poids symétrisés.

Nous dirons qu'un sous-ensemble de $\mathbf{Z}_{2l}^n$ est un code linéaire $\mathcal{C}$ de longueur $n$, ou un $\mathbf{Z}_{2l}$-code de longueur $n$, s'il forme un sous-groupe additif de $\mathbf{Z}_{2l}^n$. On muni $\mathbf{Z}_{2l}^n$ de la forme bilinéaire standard définie comme suit: $\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n \,(\mathrm{mod}\ 2l)$, où $x = (x_1, \cdots, x_n)$ et $y = (y_1, \cdots, y_n) \in \mathbf{Z}_{2l}^n$. L'ensemble $\mathcal{C}^\perp$ est constitué des éléments $x \in \mathbf{Z}_{2l}^n$ tels que $\langle x, y\rangle \equiv 0 \,(\mathrm{mod}\ 2l)$ pour tout élément $y \in \mathcal{C}$ et $\mathcal{C}^\perp$ est dit le code dual de $\mathcal{C}$. Nous dirons qu'un $\mathbf{Z}_{2l}$-code est de Type II si l'on a $\langle x, x\rangle \equiv 0 \,(\mathrm{mod}\ 4l)$ pour tout élément $x$ de $\mathcal{C}$ avec $\mathcal{C} = \mathcal{C}^\perp$. Nous savons que, pour qu'il

existe un code de Type II de longueur $n$ sur $\mathbf{Z}_{2l}$, il faut et il suffit que $n$ soit un multiple de huit (Proposition 3.4 dans [1]).

Afin de définir les $(l_1, l_2, \ldots, l_g)$-codes, nous avons besoin d'introduire les conventions. Soient $l, l^{'}$ les entiers positifs tels que $l^{'}|l$. Un élément de $\mathbf{Z}_l$ définit par congruence un élément de $\mathbf{Z}_{l'}$. Réciproquement, on obtient un élément $\frac{l}{l'}x$ de $\mathbf{Z}_l$ pour un élément $x$ de $\mathbf{Z}_{l'}$. On étend ces conventions à $\mathbf{Z}_l^n$ et $\mathbf{Z}_{l'}^n$.

Définition 1. – Soit $l_1, l_2, \ldots, l_g$ une suite ordonnée d'entiers positifs tels que $l_i|l_{i+1}$ pour $i = 1, 2, \ldots, g-1$ et soit $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g$ une suite ordonnée de $\mathbf{Z}_{l_i}$-codes de longueur $n$ pour $i = 1, 2, \ldots, g$. Nous dirons $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g)$ un $(l_1, l_2, \ldots, l_g)$-code de longueur $n$, si l'on a, pour tout $i, j$ $(1 \leq i < j \leq g)$,

(i) $x \in \mathcal{C}_i$ pour tout $x \in \mathcal{C}_j$,

et (ii) $\frac{l_j}{l_i}y \in \mathcal{C}_j$ pour tout $y \in \mathcal{C}_i$.

Nous dirons qu'un $(l_1, l_2, \ldots, l_g)$-code $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g$ est de Type II si chaque $\mathcal{C}_i$ est de Type II comme $\mathbf{Z}_{2l_i}$-codes.

*Exemple.* – Considérons un $\mathbf{Z}_2$-code $\mathcal{H}$ (code de Hamming étendu) et un $\mathbf{Z}_4$-code $\mathcal{O}$ (Octa code), qui sont donnés respectivement par les matrices génératrices $\begin{pmatrix} 1\,0\,1\,1\,0\,0\,0\,1 \\ 0\,1\,0\,1\,1\,0\,0\,1 \\ 0\,0\,1\,0\,1\,1\,0\,1 \\ 0\,0\,0\,1\,0\,1\,1\,1 \end{pmatrix}$ et $\begin{pmatrix} 1\,2\,1 & -1 & 0 & 0 & 0 & 1 \\ 0\,1\,2 & 1 & -1 & 0 & 0 & 1 \\ 0\,0\,1 & 2 & 1 & -1 & 0 & 1 \\ 0\,0\,0 & 1 & 2 & 1 & -1 & 1 \end{pmatrix}$ (*cf.* [3]). Alors on a un $(1, 2)$-code $(\mathcal{H}, \mathcal{O})$ de Type II de longueur 8.

Il y a différents types de polynômes des poids. Du point de vue de la prochaine section, les polynômes des poids symétrisés seront plus appropriés. Pour cela, on pose $R = \mathbf{Z}_{2l_1} \times \mathbf{Z}_{2l_2} \times \cdots \times \mathbf{Z}_{2l_g}$, et on définit sur $R$ la relation $\sim$ suivante: $a \sim b \Leftrightarrow a = b$ ou $a = -b$, où $a, b \in R$. Alors la relation $\sim$ est une relation d'équivalence. On pose $\overline{R} = R/\sim$.

Définition 2. – Soit $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g)$ un $(l_1, l_2, \ldots, l_g)$-code, où $l_1, l_2, \ldots, l_g$ est une suite ordonnée d'entiers positifs tels que $l_i|l_{i+1}$ pour $i = 1, 2, \ldots, g-1$. Le polynôme de poids symétrisés de $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g)$ est défini par

$$W_{(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g)}(x_{\overline{a}}) = W_{(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g)}(x_{\overline{a}} \text{ avec } \overline{a} \in \overline{R}) = \sum_{c_1 \in \mathcal{C}_1, c_2 \in \mathcal{C}_2, \ldots, c_g \in \mathcal{C}_g} \prod_{\overline{a} \in \overline{R}} x_{\overline{a}}^{n_{\overline{a}}(c_1, c_2, \ldots, c_g)},$$

où $n_{\overline{a}}(c_1, c_2, \ldots, c_g)$ désigne le nombre de $i$ tel que $\overline{a} = \overline{(c_{1i}, c_{2i}, \ldots, c_{gi})}$.

Pour voir la propriété d'invariance des polynômes de poids symétrisés, nous définissons les matrices suivantes. Soit $k$ un entier positif, soit $l_1, l_2, \ldots, l_g$ une suite ordonnée d'entiers positifs tels que $l_i|l_{i+1}$ pour $i = 1, 2, \ldots, g-1$ et posons $k = l_1$ et $k_i = l_i/k$ pour $i = 1, 2, \ldots, g$. On pose $P = \mathrm{diag}\,(k_1, k_2, \ldots, k_g)$. Désignons par $T(k, P)$ la matrice

$$T(k, P) = \mathbf{e}(1/8)^g (2^g k^g k_1 k_2 \ldots k_g)^{-1/2} \left(\mathbf{e}(\langle P^{-1}a, b\rangle/2k)\right)_{a,\, b \in R}.$$

$\Omega(P)$ est l'ensemble des éléments $U \in GL(g, \mathbf{Z})$ tels que $P^{-1}UP$ est entier. Evidemment, c'est un sous-groupe de $GL(g, \mathbf{Z})$ et nous avons

$$\Omega(P) = \{(a_{ij}) \in GL(g, \mathbf{Z}); a_{ij} \equiv 0 \,(\mathrm{mod}\ k_i/k_j) \text{ pour } 1 \leq j < i \leq g\}\,.$$

$\Lambda(P)$ est l'ensemble des éléments symétriques $S \in \mathrm{Mat}(g, \mathbf{Q})$ tels que $SP$ est entier. Nous avons

$$\Lambda(P) = \left\{(s_{ij}) \in \mathrm{Mat}(g, \mathbf{Q}); s_{ij} = s_{ji} \in \frac{1}{k_i}\mathbf{Z} \text{ pour } 1 \leq i \leq j \leq g\right\}.$$

On pose
$$P_U(k,\, P) = \left(\sqrt{\det(U)}\,\delta_{Ua,b}\right)_{a,\,b\in R} \text{ pour } U \in \Omega(P),$$
$$D_S(k,\, P) = \text{ diag } (\mathbf{e}(S[a]/4k) \text{ avec } a \in R) \text{ pour } S \in \Lambda(P).$$

A tout $g = (g_{ab})_{a,b\in R}$, nous associons $\phi(g) = \left(\sum_{d\in R \text{ avec } \overline{d}=\overline{b}} g_{ad}\right)_{\overline{a},\overline{b}\in\overline{R}}$. Alors les éléments $\phi(T(k,\, P))$, $\phi(P_U(k,\, P))$, $\phi(D_S(k,\, P))$, $\mathbf{e}(1/8)$ de $GL(2^{g-1}(k^g k_1 k_2 \cdots k_g + 1), \mathbf{C})$ opèrent naturellement sur $\mathbf{C}[x_{\overline{a}}] = \mathbf{C}[x_{\overline{a}} \text{ avec } \overline{a} \in \overline{R}]$, où $U$ et $S$ parcourent respectivement $\Omega(P)$ et $\Lambda(P)$. La propriété d'invariance des polynômes de poids symétrisés est donnée comme suit:

Proposition 3. – *Soit $k$ un entier positif, soit $k_1, k_2, \ldots, k_g$ une suite ordonnée d'entiers positifs tels que $k_1 = 1$, $k_i | k_{i+1}$ pour $i = 1, 2, \ldots, g-1$ et posons $P = \mathrm{diag}\,(k_1, k_2, \ldots, k_g)$. Si un $(kk_1, kk_2, \ldots, kk_g)$-code $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g)$ est de Type II, $W_{(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g)}(x_{\overline{a}})$ est fixé par l'opération des éléments $\phi(T(k,\, P))$, $\phi(P_U(k,\, P))$, $\phi(D_S(k,\, P))$, $\mathbf{e}(1/8)$, où $U$ et $S$ parcourent respectivement $\Omega(P)$ et $\Lambda(P)$.*

3. *Formes paramodulaires.* – Dans cette section, nous étudierons la relation entre codes et formes paramodulaires.

D'abord, on rappelle le groupe paramodulaire, les formes paramodulaires, et les fonctions thêta. Soit $k_1, k_2, \ldots, k_g$ une suite ordonnée d'entiers positifs tels que $k_1 = 1$, $k_i | k_{i+1}$ pour $i = 1, 2, \ldots, g-1$ et posons $P = \mathrm{diag}\,(k_1, k_2, \ldots, k_g)$. Nous appelerons par $\Gamma(P)$ le groupe paramodulaire, c'est à dire

$$\Gamma(P) = \left\{\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp(2g, \mathbf{R}); A,\, BP,\, P^{-1}C,\, P^{-1}DP \text{ entiers} \right\}.$$

Nous savons que le groupe paramodulaire $\Gamma(P)$ est engendré par $J_P = \begin{pmatrix} 0 & P^{-1} \\ -P & 0 \end{pmatrix}$ et deux sous-groupes $\left\{\begin{pmatrix} {}^tU^{-1} & 0 \\ 0 & U \end{pmatrix}; U \in \Omega(P)\right\}$ et $\left\{\begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix}; S \in \Lambda(P)\right\}$ (Theorem 2.1 dans [8]).

Le groupe symplectique $Sp(2g, \mathbf{R})$ opère sur l'espace de Siegel $\mathbf{H}_g = \{Z \in \mathrm{Mat}(g \times g, \mathbf{C})\,; {}^tZ = Z, \mathrm{Im}(Z) > 0\}$ de la manière suivante: $M\langle\tau\rangle = (A\tau + B)(C\tau + D)^{-1}$ pour $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp(2g, \mathbf{R})$ et $\tau \in \mathbf{H}_g$. Une fonction holomorphe $f$ sur $\mathbf{H}_g$ est une forme paramodulaire de poids $k$ pour $\Gamma(P)$ si l'on a $f(M\langle\tau\rangle) = \det(C\tau + D)^k f(\tau)$ pour tout élément $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma(P)$.

On définit des fonctions thêta partielles associées à la polarisation $P$ par

$$f_a^{(k,\,P)}(\tau) = \sum_{x \in \mathbf{Z}^g} \mathbf{e}\left(k\tau\left[Px + \frac{1}{2k}a\right]\right),$$

où $\tau[x] = {}^t x \tau x$ et ${}^t x$ désigne la transposé de $x$. Avec les notations de Petersson, nous avons

$$f_a^{(k,\,P)}\,|_{1/2} J_P \quad = \quad \sum_{b\in R} T(k,\, P)_{a,\,b} f_b^{(k,\,P)},$$

$$f_a^{(k,P)}\big|_{1/2}M = \sqrt{\det(U)}f_{Ua}^{(k,P)} \quad \text{pour } M=\begin{pmatrix} {}^tU & 0 \\ 0 & U^{-1}\end{pmatrix},\ U\in\Omega(P),$$

$$f_a^{(k,P)}\big|_{1/2}M = \mathbf{e}(S[a]/4k)f_a^{(k,P)} \quad \text{pour } M=\begin{pmatrix} 1 & S \\ 0 & 1\end{pmatrix},\ S\in\Lambda(P).$$

On peut poser $f_{\overline{a}}^{(k,P)} = f_a^{(k,P)}$. On déduit immédiatement grâce à la proposition 3,

THÉORÈME 4. – *Soit $k$ un entier positif, soit $k_1, k_2, \ldots, k_g$ une suite ordonnée d'entiers positifs tels que $k_1 = 1$, $k_i | k_{i+1}$ pour $i = 1, 2, \ldots, g-1$ et posons $P = \mathrm{diag}\,(k_1, k_2, \ldots, k_g)$. Si un $(kk_1, kk_2, \ldots, kk_g)$-code $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_g)$ est de Type II de longueur $n$, on obtient une forme paramodulaire $W_{(\mathcal{C}_1,\mathcal{C}_2,\ldots,\mathcal{C}_g)}(f_{\overline{a}}^{(k,P)}(\tau))$ de poids $n/2$ pour $\Gamma(P)$.*

*Remarques.* – (a) Dans [5], Freitag a étudié l'anneau des formes paramodulaires de poids pairs pour $\Gamma(P)$, où $P = \mathrm{diag}(1, 2)$.

(b) Par $\rho_l$ on désigne la projection naturelle de $\mathbf{Z}^n$ dans $\mathbf{Z}_{2l}^n$. Si l'on pose $\Lambda(\mathcal{C}_i) = \frac{1}{\sqrt{2k}}\rho_{kk_i}^{-1}(\mathcal{C}_i)$ pour $i = 1, 2, \ldots, g$, on a

$$\begin{aligned}\Theta_{\Lambda(\mathcal{C}_1),\Lambda(\mathcal{C}_2),\ldots,\Lambda(\mathcal{C}_g)}(\tau) &= \sum_{x_1\in\Lambda(\mathcal{C}_1),\,x_2\in\Lambda(\mathcal{C}_2),\,\ldots,\,x_g\in\Lambda(\mathcal{C}_g)} \mathbf{e}\left(\sum_{1\le m,\,n\le g}\frac{\tau_{mn}}{2}x_m\,{}^t x_n\right)\\ &= W_{(\mathcal{C}_1,\mathcal{C}_2,\ldots,\mathcal{C}_g)}(f_{\overline{a}}^{(k,P)}(\tau)).\end{aligned}$$

(*) Ce travail a été effectué dans le cadre de JSPS (the Japan Society for the Promotion of Science).

(**) Cette note était accomplie au INRIA - U.R. Sophia Antipolis, France. L'auteur désire remercier les Professeurs P. Solé et B. Mourrain, pour leur soutien durant son séjour en France et l'INRIA - U.R. Sophia Antipolis pour son hospitalité. Il désire aussi remercier le Professeur Runge pour d'intéressantes discussions.

## Références bibliographiques

[1] Bannai, E., Dougherty, S. T., Harada, M., Oura, M., "Type II Codes, Even Unimodular Lattices and Invariant Rings," *IEEE Trans. Inform. Theory*, à paraître.

[2] Broué, M., Enguehard, M., "Polynômes des poids de certains codes et fonctions thêta de certain réseaux," *Ann. Scient. Éc. Norm. Sup.* $4^e$ *série t.5* (1972) pp. 157–181.

[3] Calderbank, A. R., Sloane, N. J. A, "Modular and $p$-adic cyclic codes," *Designs, Codes and Cryptography* 6 (1995), pp. 21–35.

[4] Duke, W., "On codes and Siegel modular forms", *Inter. Math. Res. Notices*, pp. 125–136, 1993.

[5] Freitag, E., "Modulformen zweiten Grades zum rationalen und Gaußschen Zahlkörper," *Sitzungsber. Heidelb. Akad. Wiss.* (1967).

[6] Gleason, A. M., "Weight polynomials of self-dual codes and the MacWilliams identities," in *Actes Congrés Intern. des Mathématiciens* (Nice 1970), Tome 3 (Gauthier-Villars, Paris, 1971), 211–215.

[7] Runge, B., "Codes and Siegel modular forms," *Discrete Math.* **148** (1996) pp. 175–204.

[8] Runge, B., "On symmetric Hilbert modular forms," *Abh. Math. Sem. Univ. Hamburg*, **66** (1996) pp. 75–88.