

Deux déterminants

Serhii Dyshko ^a, Philippe Langevin ^a Jay Wood ^b

^a*Université de Toulon*

^b*Western Michigan University*

Reçu le *****; accepté après révision le ++++++

Présenté par £££££

Résumé

Dans cette note, nous utilisons des résultats classiques sur les zéros des fonctions L de Dirichlet pour prouver la non nullité de deux déterminants. Nous en déduisons un théorème d'extension pour les isométries de Lee des codes linéaires analogue à celui obtenu par MacWilliams pour le poids de Hamming.

Abstract

Voici le titre en anglais. Votre abstract en anglais ici. *To cite this article: A. Nom1, A. Nom2, C. R. Acad. Sci. Paris, Ser. I 340 (2005).*

1 Théorème de MacWilliams

Soient K un corps fini, n un entier naturel non nul et $\mathbb{H}: K \rightarrow \mathbb{N}$ la fonction indicatrice des éléments non nuls de K , c'est-à-dire $\mathbb{H}(x) = 1$ si $x \neq 0$ et $\mathbb{H}(0) = 0$ sinon. L'espace vectoriel K^n est muni de la métrique discrète $(x, y) \mapsto w_{\mathbb{H}}(y - x)$, où $w_{\mathbb{H}}(x) = \sum_{i=1}^n \mathbb{H}(x_i)$ est le poids de Hamming de x . Dans ce contexte, une isométrie est par définition une application linéaire $f: C \rightarrow K^n$ qui préserve le poids de Hamming sur un sous-espace vectoriel C de K^n :

$$\forall x \in C, \quad w_{\mathbb{H}}(f(x)) = w_{\mathbb{H}}(x).$$

Email addresses: serhii.dyshko@univ-tln.fr (Serhii Dyshko),
langevin@univ-tln.fr (Philippe Langevin), jay.wood@wmich.edu (Jay Wood).

Considérons la base canonique $(e_i)_{1 \leq i \leq n}$ de K^n . Il est facile de vérifier que les isométries de domaine K^n sont précisément les applications monomiales de K^n . Une application monomiale étant un élément $(\pi, \lambda_1, \dots, \lambda_n)$ du produit semi-directe $\mathfrak{S}(n) \ltimes (K^\times)^n$ qui envoie $e_i \mapsto \lambda_i e_{\pi(i)}$. Une telle application est dite U -monomiale quand tous les scalaires λ_i sont dans un certain sous-groupe U de K^\times .

Théorème 1.1 (MacWilliams, [3]) *Toute isométrie de K^n est la restriction d'une application monomiale.*

Autrement dit, toute isométrie de K^n se prolonge en une isométrie de domaine K^n , raison pour laquelle le théorème ci-dessus est souvent appelé théorème d'extension de MacWilliams. On sait que le théorème de MacWilliams se généralise aux espaces de Hamming A^n où A est un anneau fini quasi-Fröbenius non nécessairement commutatif. Le lecteur intéressé par ces développements peut consulter de [5]. Revenant aux corps fini, il est naturel d'étudier l'existence d'un prolongement d'une isométrie pour des fonctions de poids plus générale que le poids de Hamming. Dans cette note, nous traitons le cas de la métrique de Lee sur un corps premier.

2 Critère d'extensibilité

Soit U un sous-groupe de K^\times . Notons G le groupe quotient K^\times/U . Pour tout vecteur $x \in K^n$, on définit la composition de x relativement à U comme étant une application $C_U(x): G \rightarrow \mathbb{N}$ qui envoie un élément $r \in G$ sur le nombre $c_r(x)$ de composantes de x qui sont dans la classe latérale rU . Une application linéaire $f: C \rightarrow K^n$ telle que

$$\forall x \in C, \quad C_U(x) = C_U(f(x)),$$

est dite U -stable. Ici encore, il est facile de vérifier que les applications U -stables définie sur K^n tout entier sont précisément les applications U -monomiales.

Théorème 2.1 (Goldberg, [2]) *Toute application U -stable est la restriction d'une application U -monomiale.*

Une fonction de poids sur K est une fonction numérique $P: K \rightarrow \mathbb{C}$ à valeurs dans le corps des nombres complexes qui s'annule en 0. On prolonge w_P à l'espace vectoriel K^n en posant $w_P(x) = \sum_{i=1}^n P(x_i)$. En particulier, $(x, y) \mapsto w_P(y-x)$ n'est pas nécessairement une distance sur K^n . Néanmoins, convenons d'appeler P -isométrie une application linéaire $f: C \rightarrow K^n$ vérifiant

$$\forall x \in C, \quad w_p(x) = w_p(f(x)).$$

Pour préciser la notion d'extensibilité dans ce contexte, on introduit le groupe des symétries de P . Il s'agit du sous-groupe de K^\times défini par

$$U(P) = \{\lambda \in K^\times \mid \forall x \in K, P(\lambda x) = P(x)\}.$$

On dit que P satisfait la propriété d'extension si toute P -isométrie de K^n est la restriction d'une application U -monomiale de K^n . Comme plus haut, notons G le groupe quotient K^\times/U , avec $U = U(P)$. On rappelle que le produit de convolution $f * g$ entre deux applications complexes f et g de domaine G est défini par

$$t \mapsto f * g(t) = \sum_{xy=t} f(x)g(y) = \sum_{x \in G} f(x)g(tx^{-1}).$$

Pour toute application $g: G \rightarrow \mathbb{C}$, le produit de convolution par g définit un endomorphisme de \mathbb{C}^G , le \mathbb{C} -espace vectoriel des applications de G dans \mathbb{C} . A un vecteur $x \in K^n$, on associe l'application $h_x: G \rightarrow \mathbb{C}$ qui envoie r sur $c_r(x)$. Pour un scalaire $\lambda \in K^\times$, le poids de λx est donné par le produit de convolution de h_x par P :

$$w_p(\lambda x) = \sum_{r \in G} c_r(\lambda x)P(r) = \sum_{r \in G} c_{r/\lambda}(x)P(r) = h_x * P(\lambda) \quad (1)$$

Corollaire 2.2 *Soient P une fonction de poids sur K , U le groupe des symétries de P et G le groupe quotient K^\times/U . Si le produit de convolution par P définit un automorphisme de \mathbb{C}^G alors P satisfait la propriété d'extension.*

En effet, soit f une P -isométrie. Soit x dans le domaine f , la conservation des poids se traduit par $h_x * P = h_{f(x)} * P$. L'injectivité de la convolution par P implique que $h_x = h_{f(x)}$ et donc que $C_U(x) = C_U(f(x))$. Il ne reste plus qu'à appliquer le théorème (2.1) pour conclure.

Il est bien connu que le déterminant de l'endomorphisme de convolution par P est donné par la formule de Dedekind [4, Lemma 5.26],

$$\Delta_P = \left| \begin{array}{c} \vdots \\ \dots P(rs^{-1}) \dots \\ \vdots \end{array} \right|_{r,s \in G} = \prod_{\chi \in \widehat{G}} \widehat{P}(\chi) \quad (2)$$

où $\widehat{P}(\chi) = \sum_{s \in G} P(s)\chi(s)$ est le coefficient de Fourier de P en χ . Pour appliquer le Corollaire (2.2) à P , il suffit de montrer qu'aucun des coefficients de Fourier ne s'annulent.

3 Métrique de Lee

Dans la suite, on suppose que K est le corps premier \mathbb{F}_ℓ où ℓ est un nombre premier impair. Le poids de Lee L est la fonction numérique définie sur les résidus modulo ℓ , par :

$$L(t) = \begin{cases} t, & 0 \leq t \leq \ell/2; \\ \ell - t, & \ell/2 < t < \ell. \end{cases}$$

Le groupe des symétries U du poids de Lee se réduit à $\{-1, +1\}$, nous notons G le groupe quotient $\mathbb{F}_\ell^\times / \{\pm 1\}$, il est cyclique d'ordre $n := (\ell - 1)/2$. Notons bien que la fonction de Lee envoie $0 \neq t \in \mathbb{F}_\ell$ sur le représentant minimal de t modulo U . Le carré de la fonction de Lee $E = L^2$ est souvent appelé poids euclidien ; ces deux poids partagent le même groupe de symétrie. Pour illustrer, notre propos, les déterminants correspondant au cas $\ell = 7$, sont

Théorème 3.1 *Si ℓ est premier alors $\Delta_L \neq 0$.*

Le coefficient de Fourier en le caractère principal vaut $\widehat{L}(1) = \sum_{s \in G} L(s) = \sum_{k=1}^n k = \frac{1}{2}(n+1)n$. Pour prouver le théorème (3.1), il reste à montrer que $\widehat{L}(\chi) \neq 0$ pour les caractères χ non triviaux. Comme remarqué par Barra dans son mémoire de thèse [1], il s'agit d'une tâche facile quand ℓ est un premier de la forme $\ell = 1 + 2p$, ou encore $\ell = 1 + 4p$, avec p premier. On peut atteindre le résultat par des méthodes élémentaires lorsque $\ell = 1 + 6p$. Dans la suite, nous utilisons des propriétés des fonctions L de Dirichlet pour établir le théorème (3.1). En passant, nous montrerons que le déterminant euclidien Δ_E ne peut s'annuler non plus.

4 Analyse de Fourier

On rappelle qu'un caractère multiplicatif χ de \mathbb{F}_ℓ est dit pair lorsque $\chi(-1) = 1$. Les caractères pairs forment un sous-groupe d'ordre $\frac{\ell-1}{2}$ qui par restriction s'identifie au groupe dual de $G = \mathbb{F}_\ell^\times / \{-1, +1\}$. Le coefficient de Fourier d'une fonction $f: G \rightarrow \mathbb{C}$ en χ correspond à une somme de caractère incomplète

$$\widehat{f}(\chi) = \sum_{x \in G} f(x)\chi(x) = \sum_{k < \frac{\ell}{2}} f(k)\chi(k).$$

Rappelons que si τ_t désigne la multiplication par t dans G alors $\widehat{f \circ \tau}(\chi) = \bar{\chi}(t)\widehat{f}(\chi)$. Considérons un résidu $0 \leq x < \ell/2$ représentant un élément de G . Si $x < \ell/4$ alors $2x < \frac{\ell}{2}$ c'est-à-dire $L(2x) = 2L(x)$. Si $\ell/4 < x < \ell/2$ alors $\ell/2 < 2x < \ell$ et donc $L(2x) = \ell - 2L(x)$. Il suit que le produit de $(L(2x) - 2L(x))$ par $(L(2x) + 2L(x) - \ell)$ est nul sur G , d'où l'on tire la relation quadratique

$$L(2x)^2 - 4L(x)^2 = (L(2x) - 2L(x))\ell.$$

Le carré de L n'étant rien d'autre que E , nous obtenons la relation :

$$(\bar{\chi}(2) - 4)\widehat{E}(\chi) = (\bar{\chi}(2) - 2)\widehat{L}(\chi)\ell. \quad (3)$$

Scholie 4.1 *Soit r le plus petit entier tel que $2^r \equiv \pm 1 \pmod{\ell}$. Le produit des égalités (3), conduit à l'élégante formule*

$$(2^r + 1)^{\frac{\ell-1}{2^r}} \Delta_E = \ell^{\frac{\ell-1}{2}} \Delta_L$$

Faisons l'hypothèse $\widehat{L}(\chi) = 0$ pour un caractère pair non trivial. Observons les conséquences sur les deux nombres de Bernoulli généralisés $B_1(\chi)$ et $B_2(\chi)$ qui s'écrivent

$$B_1(\chi) = \frac{1}{\ell} \sum_{k=1}^{\ell} k\chi(k), \quad B_2(\chi) = \frac{1}{\ell} \sum_{k=1}^{\ell} (k^2 - lk)\chi(k).$$

Comme χ est pair et non trivial,

$$2\widehat{1}(\chi) = 2 \sum_{k < \frac{\ell}{2}} \chi(k) = \sum_{k=1}^{\ell} \chi(k) = 0.$$

Et donc

$$B_1(\chi) = \sum_{k < \frac{\ell}{2}} k\chi(k) + \sum_{k < \frac{\ell}{2}} (\ell - k)\chi(k) = \ell \sum_{k < \frac{\ell}{2}} \chi(k) = 2\widehat{1}(\chi) = 0$$

sous la condition $\widehat{L}(\chi) = 0$ et $\widehat{E}(\chi) = 0$, nous obtenons

$$\begin{aligned}
B_2(\chi)\ell &= \sum_{k=1}^{\ell} k^2\chi(k) = \sum_{k < \frac{\ell}{2}} k^2\chi(k) + \sum_{k < \frac{\ell}{2}} (\ell - k)^2\chi(k) \\
&= \widehat{E}(\chi) + \ell^2 \sum_{k < \ell} \chi(k) - 2\ell \sum_{k < \ell} k\chi(k) + \sum_{k < \ell} k^2\chi(k) \\
&= 2\widehat{E}(\chi) - 2\widehat{L}(\chi)\ell + \widehat{I}(\chi)\ell^2 = 0
\end{aligned}$$

L'obstruction vient du fait que $B_2(\chi)$ n'est lui jamais nul (pour χ pair). En effet, on sait [4, Theorem 4.2] que $-2B_2(\chi) = L(-1, \chi)$ où L est la fonction L correspondant à χ . On peut alors lire dans l'équation fonctionnelle [4, page 29] que les zéros dans le domaine $\Re(s) < 0$ d'une fonction L attachée à un caractère pair sont précisément les entiers pairs. Il suit de tout ce qui précède que les déterminants Δ_L et Δ_E sont simultanément non nuls.

Corollaire 4.1 *Une isométrie de Lee ou Euclidienne est la restriction d'une application $\{-1, +1\}$ -monomiale.*

Références

- [1] A. Barra. *Equivalence Theorems and the Local-Global Property*. ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)—University of Kentucky.
- [2] D. Y. Goldberg. A generalized weight for linear codes and a Witt-MacWilliams theorem. *J. Combin. Theory Ser. A*, 29(3) :363–367, 1980.
- [3] F. J. MacWilliams. *Combinatorial Problems of Elementary Abelian Groups*. 1962. Doctoral Thesis, University of Harvard.
- [4] L. C. Washington. *Introduction to Cyclotomic Fields*. Springer, 1997.
- [5] J. A. Wood. Weight functions and the extension theorem for linear codes over finite rings. In R. C. Mullin and G. L. Mullen, editors, *Finite fields : theory, applications, and algorithms (Waterloo, ON, 1997)*, volume 225 of *Contemp. Math.*, pages 231–243. Amer. Math. Soc., Providence, RI, 1999.