DEUX ANALOGUES AU DÉTERMINANT DE MAILLET

SERHII DYSHKO, PHILIPPE LANGEVIN, AND JAY A. WOOD

RÉSUMÉ. Nous utilisons des résultats classiques sur les zéros des fonctions L de Dirichlet pour prouver la non nullité de deux déterminants analogues au déterminant de Maillet. Nous en déduisons un théorème d'extension pour les isométries de Lee et euclidienne des codes linéaires sur un corps premier.

Two analogues of Maillet's determinant.

ABSTRACT. We use classical results on the zeroes of Dirichlet L-functions to prove the nonvanishing of two determinants analogous to Maillet's determinant. We deduce an extension theorem for Lee and Euclidean isometries of linear codes over a prime field.

1. Théorème de MacWilliams

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

$$\forall x \in C, \quad \mathrm{w_H}\big(f(x)\big) = \mathrm{w_H}(x).$$

Considérons la base canonique $(e_i)_{1\leq i\leq n}$ de K^n. On rappelle qu'une application monomiale est un élément $(\pi, \lambda_1, \ldots, \lambda_n)$ du produit semi-direct $\mathfrak{S}(n) \ltimes (K^\times)^n$ 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 $K^\times$. Il est facile de vérifier que les isométries de domaine K^n sont précisément les applications monomiales de K^n.

Théorème 1.1 (MacWilliams, [3, 4])**.** *Toute isométrie de K^n est la restriction d'une application monomiale.*

Date: May 19, 2016. To appear in Comptes Rendus Acad. Sci. Paris.

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 Frobenius non nécessairement commutatif. Le lecteur intéressé par ces développements peut consulter [8]. Revenant au cas des corps finis, il est naturel d'étudier l'existence d'un prolongement d'une isométrie pour des fonctions de poids plus généraux que le poids de Hamming. Un critère d'extensibilité conduit à l'étude de certains déterminants. 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 $K^\times/U$. L'ensemble sous-jacent de G est identifié à un système de représentants de $K^\times$ modulo U. Pour tout vecteur $x \in K^n$, on définit la composition de x relativement à U comme étant une application $C_U(x)\colon G \to \mathbb{N}$ 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 $f\colon C \to K^n$ 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 définies 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 $\mathrm{P}\colon K \to \mathbb{C}$ à valeurs dans le corps des nombres complexes qui s'annule en 0. On prolonge P à l'espace vectoriel K^n en posant $\mathrm{w}_\mathrm{P}(x) = \sum_{i=1}^n \mathrm{P}(x_i)$. En particulier, $(x, y) \mapsto \mathrm{w}_\mathrm{P}(y - x)$ n'est pas nécessairement une distance sur K^n. Néanmoins, convenons d'appeler P-isométrie une application linéaire $f\colon C \to K^n$ vérifiant

$$\forall x \in C, \quad \mathrm{w}_\mathrm{P}(x) = \mathrm{w}_\mathrm{P}\big(f(x)\big).$$

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

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

On dit que P satisfait la propriété d'extension si toute P-isométrie de K^n est la restriction d'une application $U(\mathrm{P})$-monomiale de K^n. Comme

plus haut, notons G le groupe quotient $K^\times/U$, avec $U = U(\mathrm{P})$. On rappelle que le produit de convolution $f * g$ entre deux applications complexes f et g de domaine G est défini par

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

Pour toute application $g\colon G \to \mathbb{C}$, 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 $h_x\colon G \to \mathbb{C}$ qui envoie r sur $c_{r^{-1}}(x)$, de sorte que :

$$h_x(r) = |\{i \mid x_i r = 1 \mod U\}| \quad \text{et} \quad \mathrm{w}_\mathrm{P}(x) = \sum_{r\in G} h_x(r)\mathrm{P}(r^{-1}).$$

Pour un scalaire $\lambda \in K^\times$,

$$h_{\lambda x}(r) = |\{i \mid \lambda x_i r = 1 \mod U\}| = h_x(\lambda r \mod U),$$

en particulier, le poids de λx est donné par le produit de convolution de h_x par P :

$$\mathrm{w}_\mathrm{P}(\lambda x) = \sum_{r\in G} h_{\lambda x}(r)\mathrm{P}(r^{-1}) = \sum_{r\in G} h_x(\lambda r)\mathrm{P}(r^{-1}) = h_x * \mathrm{P}(\lambda) \tag{1}$$

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 de f, la conservation des poids se traduit par $h_x * \mathrm{P} = h_{f(x)} * \mathrm{P}$. 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 [7, Lemma 5.26],

$$\Delta_\mathrm{P} = \left| \begin{matrix} & \vdots & \\ \dots & \mathrm{P}(rs^{-1}) & \dots \\ & \vdots & \end{matrix} \right|_{r,s\in G} = \prod_{\chi\in\widehat{G}} \widehat{\mathrm{P}}(\chi) \tag{2}$$

où $\widehat{\mathrm{P}}(\chi) = \sum_{s\in G} \mathrm{P}(s)\chi(s)$ est le coefficient de Fourier de P en χ. Pour appliquer le Corollaire (2.2) à P, il suffit de montrer que les coefficients de Fourier sont tous non nuls.

Remarque 2.3. *Pour le poids de Hamming, $U(\mathrm{H}) = K^\times$ et G est trivial. Autrement dit, le théorème de MacWilliams est une conséquence du théorème de Goldberg.*

3. Métrique de Lee

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

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

Le groupe des symétries U du poids de Lee se réduit à $\{-1, +1\}$, nous notons $G = \{1, 2, \ldots, (\ell-1)/2\}$ 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, et ainsi, Δ_{L} est un analogue du déterminant de Maillet [5], [6, pp. 340-342]. Le carré de la fonction de Lee $\mathrm{E} = \mathrm{L}^2$ est souvent appelé poids euclidien ; ces deux poids partagent le même groupe de symétrie.

Théorème 3.1. *Si ℓ est un nombre premier impair alors $\Delta_{\mathrm{L}} \neq 0$.*

Le coefficient de Fourier au caractère principal vaut $\widehat{\mathrm{L}}(1) = \sum_{s\in G} \mathrm{L}(s) = \sum_{k=1}^{n} k = \frac{1}{2}(n+1)n$. Pour prouver le théorème (3.1), il reste à montrer que $\widehat{\mathrm{L}}(\chi) \neq 0$ 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 $\ell = 1 + 2p$ (premier de Sophie Germain), 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 $\mathbb{F}_\ell$ est dit pair lorsque $\chi(-1) = 1$. Les caractères pairs forment un sous-groupe d'ordre $(\ell - 1)/2$ qui par restriction s'identifie au groupe dual de $G = {\mathbb{F}_\ell}^\times/\{-1, +1\}$. Le coefficient de Fourier d'une fonction $f\colon G \to \mathbb{C}$ en χ correspond à une somme de caractères incomplète

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

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 $0\le x<\ell/2$ représentant un élément de G. Si $x<\ell/4$ alors $2x<\ell/2$ c'est-à-dire $\mathrm{L}(2x)=2\mathrm{L}(x)$. Si $\ell/4<x<\ell/2$ alors $\ell/2<2x<\ell$ et donc $\mathrm{L}(2x)=\ell-2\mathrm{L}(x)$. Il en résulte que le produit de $\big(\mathrm{L}(2x)-2\mathrm{L}(x)\big)$ par $\big(\mathrm{L}(2x)+2\mathrm{L}(x)-\ell\big)$ est nul sur G, d'où l'on tire la relation quadratique

$$\mathrm{L}(2x)^2-4\mathrm{L}(x)^2=\big(\mathrm{L}(2x)-2\mathrm{L}(x)\big)\ell.$$

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

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

Scholie 4.1. *Soit r le plus petit entier tel que $2^r\equiv\pm1 \mod\ell$. Le produit des égalités (3), conduit à l'élégante formule*

$$(2^r+1)^{\frac{\ell-1}{2r}}\ \Delta_{\mathrm{E}}=\ell^{\frac{\ell-1}{2}}\ \Delta_{\mathrm{L}}.$$

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

$$B_1(\chi)=\frac1\ell\sum_{k=1}^{\ell}k\chi(k),\quad B_2(\chi)=\frac1\ell\sum_{k=1}^{\ell}(k^2-lk)\chi(k).$$

Comme χ est pair et non trivial,

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

Et donc,

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

Sous la condition $\widehat{\mathrm{L}}(\chi)=0$, nous savons que $\widehat{\mathrm{E}}(\chi)=0$, et nous obtenons

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

L'obstruction vient du fait que $B_2(\chi)$ n'est lui jamais nul (pour χ pair). En effet, on sait [7, Theorem 4.2] que $-B_2(\chi)/2 = L(-1,\chi)$ où L est la fonction L correspondant à χ. On peut alors lire dans l'équation fonctionnelle [7, 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 4.2. *Une isométrie pour un poids de Lee ou euclidien 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*. Ph.D. thesis, Radcliffe College, Cambridge, Mass., 1962.

[4] F. J. MacWilliams. *Error-correcting codes for multiple-level transmission*. Bell System Technical Journal 40 (1961), 281-308.

[5] E. Maillet. Question 4269. *L'Intermédiaire des Mathématiciens* 20 : 218, 1913.

[6] T. Muir. *Contributions to the history of determinants, 1900–1920*. Blackie & Son Limited, London and Glasgow, 1930.

[7] L. C. Washington. *Introduction to Cyclotomic Fields*. Springer, 1997.

[8] J. A. Wood. Duality for modules over finite rings and applications to coding theory. *Amer. J. Math.*, 121 :555–575, 1999.

Laboratoire IMATH, Université de Toulon, 83957 La Garde Cedex, France

E-mail address: serhii.dyshko@univ-tln.fr, langevin@univ-tln.fr

Department of Mathematics, Western Michigan University, 1903 W. Michigan Ave., Kalamazoo, MI 49008–5248 USA http://homepages.wmich.edu/~jwood

E-mail address: jay.wood@wmich.edu