Extension Property of the Lee metric

Yet Another Conference in Crypography,
Porquerolles,
june 10 2016.

Philippe Langevin

IMATH, université de Toulon

last revision June 13, 2016.

Deux analogues au déterminant de Maillet, S. Dyshko, P. Langevin, J. A. Wood, C. R. Acad. Sci. Paris, Ser. I (2016).

Linear Isometry

Let K be a finite field, n a positive interger

Hamming isometry

A *linear* map $f\colon C \to K^n$ that preserves the Hamming weight over a subspace C of K^n.

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

where $\mathrm{w_H}(x) = \sum_{i=1}^{n} \mathrm{H}(x_i)$ is the Hamming weight of x.

$$\mathrm{H}\colon K \to \mathbb{N}, \quad x \mapsto \mathrm{H}(x) = \begin{cases} 1, & x \neq 0; \\ 0, & x = 0. \end{cases}$$

Monomial transformation

Let $(e_i)_{1\leq i\leq n}$ be the canonical basis of K^n. An isometry over the full space K^n maps the unit sphere on itself

$$\forall i, \quad e_i \mapsto \lambda_i e_{\pi(i)}.$$

that is a monomial transformation of K^n whose λ_i's are the scalars.

Hamming isometry over K^n

An isometry f over the full space K^n

$$f(x_1, x_2, \ldots, x_n) = (\lambda_1 x_{\pi(1)}, \lambda_1 x_{\pi(2)}, \ldots, \lambda_n x_{\pi(n)})$$

U-monomial

An U-monomial transformation has scalars in $U \leqslant K^\times$.

MacWilliams Extension Theorem

isometry over a subspace

If f is an isometry over a subspace C of K^n then

$$f(x_1, x_2, \dots, x_n) = (\lambda_1 x_{\pi(1)}, \lambda_1 x_{\pi(2)}, \dots, \lambda_n x_{\pi(n)})$$

In other words,

Theorem (MacWilliams, 1964)

An isometry over $C \subseteq K^n$ extends to an isometry over K^n.

Generalizations,

- The theorem is valid over the Hamming spaces R^n where A is a finite Frobenius ring commutative or not.
- In this talk, we are interested by the extension property in the case of *Lee metric*.

Composition of a vector

Let U be a subgroup of $K^\times$.

$$G := K^\times / U$$

One defines the composition of $x \in K^n$ relatively to U

$$C_U(x) \colon G \to \mathbb{N}$$

that send $r \in G$ on

$$c_r(x) = \sharp\{i \mid x_i \in rU\}.$$

U-preserving map

A linear map $f \colon C \to K^n$ such that

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

Goldberg Extension Theorem

preserving map over K^n

The U-preserving maps over K^n are precisely the U-monomial transformations.

Theorem (Goldberg, 1980)

A linear U-preserving map extends to U-monomial transformation.

In particular

Goldberg $\Longrightarrow$ MacWilliams

Weight and isometry in general

We replace H by P !

- $\mathrm{P} \colon K \to \mathbb{C}$, such that $\mathrm{P}(0) = 0$.
- $\mathrm{w}_{\mathrm{P}}(x) = \sum_{i=1}^{n} \mathrm{P}(x_i)$.

Of course, $(x, y) \mapsto \mathrm{w}_{\mathrm{P}}(y - x)$ is not a distance in general but

P-isometry

A linear map $f \colon C \to K^n$ such that

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

Extensibility Property

The symmetry group of P.

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

Extension Property

We say the extension property holds for the weight P when each P-isometry of K^n is the restriction of a $U(\mathrm{P})$-monomial map.

A determinantal criterion

Recall that $G := K^\times/U$ where $U = U(\mathrm{P})$.
If

$$\Delta_{\mathrm{P}} = \begin{vmatrix} & \vdots & \\ \dots & \mathrm{P}(rs^{-1}) & \dots \\ & \vdots & \end{vmatrix}_{r,s\in G} \neq 0$$

then the extension property holds for the metric P.

A determinantal criterion

Recall that $G := K^\times / U$ where $U = U(\mathrm{P})$.
If

$$\Delta_{\mathrm{P}} = \begin{vmatrix} & \vdots & \\ \dots & \mathrm{P}(rs^{-1}) & \dots \\ & \vdots & \end{vmatrix}_{r,s\in G} \neq 0$$

then the extension property holds for the metric P.

$$\Delta_{\mathrm{P}} = \prod_{\chi \in \widehat{G}} \widehat{\mathrm{P}}(\chi)$$

A determinantal criterion

Recall that $G := K^\times / U$ where $U = U(\mathrm{P})$.
If

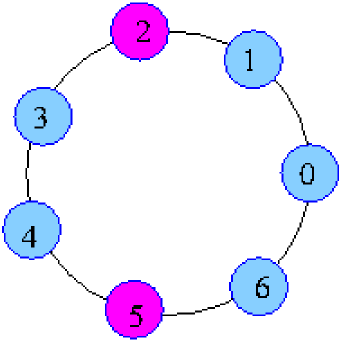
$$\Delta_{\mathrm{P}} = \begin{vmatrix} & \vdots & \\ \dots & \mathrm{P}(rs^{-1}) & \dots \\ & \vdots & \end{vmatrix}_{r,s\in G} \neq 0$$

then the extension property holds for the metric P.

$$\Delta_{\mathrm{P}} = \prod_{\chi\in\widehat{G}} \widehat{\mathrm{P}}(\chi)$$

where $\widehat{\mathrm{P}}(\chi) = \sum_{s\in G} \mathrm{P}(s)\chi(s)$ is the Fourier coefficient of P at χ.

Lee metric



Lee metric

We assume $K := \mathbb{F}_\ell$ where ℓ is an odd prime. We consider the Lee and Euclidean weights :

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

with the common symmetry

$$U := U(\mathrm{L}) = \{-1, +1\} = U(\mathrm{E}).$$

Theorem (main result)

If ℓ is an odd prime then $\Delta_{\mathrm{L}} \neq 0$ and $\Delta_{\mathrm{E}} \neq 0$.

Fourier coefficient of the Lee map

The quotient group

$$G := {\mathbb{F}_\ell}^\times/\{\pm 1\} = \{1, 2, \ldots, (\ell-1)/2\}$$

is cyclic of order $n := (\ell - 1)/2$.
we want to prove :

$$\forall \chi \in \widehat{G}, \quad 0 \neq \widehat{\mathrm{L}}(\chi) = \sum_{s \in G} \mathrm{L}(s)\chi(s).$$

- It is trivial when $\ell = 2p + 1$, p prime.
- Barra proved the case $\ell = 4p + 1$.

Fourier analysis

We identify $\widehat{G}$ with the group of even characters of $\mathbb{F}_\ell$:

$$\widehat{G} = \{\chi \in \widehat{\mathbb{F}_\ell^\times} \mid \chi(-1) = 1\}$$

The Fourier coefficients of L and E are given by

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

$$\widehat{\mathrm{E}}(\chi) = \sum_{x\in G} \mathrm{E}(x)\chi(x) = \sum_{k<\ell/2} \mathrm{E}(k)\chi(k) = \sum_{k<\ell/2} k^2\chi(k)$$

Links between the determinants

It is easy to verify the following quadratic relation holds

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

In other words

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

On spectra

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

Links between the determinants

It is easy to verify the following quadratic relation holds

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

In other words

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

On spectra

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

Scolie

Let r be the smallest positive integer such that $2^r \equiv \pm 1 \mod \ell$.

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

basic fact for non trivial even characters

Let $1 \neq \chi$ is even,

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

The first generalized Bernoulli's number vanishes too

$$B_1(\chi) = \frac{1}{\ell} \sum_{k=1}^{\ell} k\chi(k) = 0$$

basic fact for non trivial even characters

Let $1 \neq \chi$ is even,

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

The first generalized Bernoulli's number vanishes too

$$B_1(\chi) = \frac{1}{\ell} \sum_{k=1}^{\ell} k\chi(k) = 0$$

We want to prove that

$$0 \neq \frac{1}{\ell} \sum_{k<\ell/2} k\chi(k) = \widehat{\mathrm{L}}(\chi)$$

Consequence of $\widehat{\mathrm{L}}(\chi) = 0$ on the 2nd Bernoulli's number

Let us observe the consequence of

$$\widehat{\mathrm{L}}(\chi) = 0 = \widehat{\mathrm{E}}(\chi), \quad 1 \neq \chi, \quad \chi(-1) = 1,$$

on the second generalized Bernoulli's number

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

$$\begin{aligned} 2\ell B_2(\chi) &= 2\widehat{\mathrm{E}}(\chi) - 2\widehat{\mathrm{L}}(\chi)\ell + \widehat{1}(\chi)\ell^2 \\ &= \textit{zero}. \end{aligned}$$

Consequence of $\widehat{\mathrm{L}}(\chi) = 0$ on the 2nd Bernoulli's number

Let us observe the consequence of

$$\widehat{\mathrm{L}}(\chi) = 0 = \widehat{\mathrm{E}}(\chi), \quad 1 \neq \chi, \quad \chi(-1) = 1,$$

on the second generalized Bernoulli's number

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

$$2\ell B_2(\chi) = 2\widehat{\mathrm{E}}(\chi) - 2\widehat{\mathrm{L}}(\chi)\ell + \widehat{1}(\chi)\ell^2$$
$$= \textit{zero}.$$

Contradiction

From the theory of L-functions

- $-B_2(\chi)/2 = L(-1, \chi)$
- $L(-1, \chi) = 0$ if and only if χ is odd.

Contradiction

From the theory of L-functions

- $-B_2(\chi)/2 = L(-1,\chi)$
- $L(-1,\chi) = 0$ if and only if χ is odd.

whence the determinants Δ_{L} and Δ_{E} do not vanish.

Contradiction

From the theory of L-functions

- $-B_2(\chi)/2 = L(-1,\chi)$
- $L(-1,\chi) = 0$ if and only if χ is odd.

whence the determinants Δ_{L} and Δ_{E} do not vanish.

Corollary (extension property)

The Lee and Euclidean isometries are the restriction of $\{-1,+1\}$-monomial transformations.

Conclusion

The Extension Property holds for the Lee metric and the Euclidean weight with the alphabet

$$\mathbb{F}_\ell = \mathbb{Z}/(\ell)$$

Conclusion

The Extension Property holds for the Lee metric and the Euclidean weight with the alphabet

$$\mathbb{F}_\ell = \mathbb{Z}/(\ell)$$

We can prove it also holds in the case of the ring

$$\mathbb{Z}/(\ell^r)$$

Conclusion

The Extension Property holds for the Lee metric and the Euclidean weight with the alphabet

$$\mathbb{F}_\ell = \mathbb{Z}/(\ell)$$

We can prove it also holds in the case of the ring

$$\mathbb{Z}/(\ell^r)$$

and we conjecture it holds for any ring

$$\mathbb{Z}/(n)$$