Harmonic Analysis and a Bentness-like Notion in Certain Finite Abelian Groups Over Some Finite Fields

Laurent Poinsot

LIPN
University Paris XIII, France

Joint-work with N. El Mrabet from University Paris VIII, France
June, 24th 2014

Table of contents

1. Introduction
2. Character theory: the classical approach
3. Hermitian structure over finite field
4. Characters over a finite field
5. The Fourier transform
6. Conclusion

Motivations

The character theory, through the Fourier transform, is an important cryptographic tool for the study of cryptographic non-linearity of Boolean functions since it is related to bent functions and to perfect non linear functions.

It is essentially based on the Hermitian structure of the field extension $\mathbb{C}/\mathbb{R}$.

For a prime number p, the quadratic extension $GF(p^{2n})/GF(p^n)$ shares some similarities with $\mathbb{C}/\mathbb{R}$: it is possible to define an operation of conjugation, hence a kind of Hermitian structure, and a unit circle group namely the (cyclic) subgroup of order $p^n + 1$ of $GF(p^{2n}) \setminus \{ 0 \}$.

In this talk I introduce a character theory associated to this "Hermitian" structure, and develop some of its properties (and that of the associated Fourier transform). This permits to introduce a convenient notion of bent functions in this modulo p setting. Nevertheless due to time constraint I will only talk about the purely mathematical side of this work insisting on the formal analogy with the classical approach.

Table of contents

1. Introduction
2. Character theory: the classical approach
3. Hermitian structure over finite field
4. Characters over a finite field
5. The Fourier transform
6. Conclusion

Notations

In this talk,

G denotes a finite Abelian group (in additive notation)

0_G will be its identity element

$G^* := G \setminus \{ 0_G \}$.

Characters and dual group

The characters of G are the members of $\mathbf{Ab}(G, \mathcal{S}(\mathbb{C}))$, the group homomorphisms from G to the unit circle $\mathcal{S}(\mathbb{C}) := \{ z \in \mathbb{C} \colon |z| = 1 \}$ of the complex field.

$\hat{G} := \mathbf{Ab}(G, \mathcal{S}(\mathbb{C}))$ is called the dual group of G (it is a group with point-wise multiplication).

Essentially because $\mathcal{S}(\mathbb{C})$ contains a copy of each finite cyclic group, $\hat{G}$ is actually isomorphic to G (the isomorphism is not natural since it depends on a decomposition of G into a direct product of cyclic groups).

One fixes once for all such an isomorphism, and one denotes by $\chi_\alpha \in \hat{G}$ the image of $\alpha \in G$ under this isomorphism.

The characters as an orthogonal basis

The complex vector space $\mathbb{C}^G$ of complex-valued functions defined on G admits an inner product given for $f, g \in \mathbb{C}^G$ by

$$\langle f, g \rangle := \sum_{x \in G} f(x)\overline{g(x)} \ .$$

$\hat{G}$ forms an orthogonal basis, i.e., $\langle \chi_\alpha, \chi_\alpha \rangle = |G|$ and $\langle \chi_\alpha, \chi_\beta \rangle = 0$ for each $\alpha \neq \beta$.

The Fourier transform

The expression of a vector of $\mathbb{C}^G$ in the basis of characters gives rise to the so-called Fourier transform.

More precisely, let $f\colon G \to \mathbb{C}$, then its Fourier transform is $\hat{f}\colon G \to \mathbb{C}$ given for $\alpha \in G$ by

$$\hat{f}(\alpha) = \sum_{x \in G} f(x)\chi_\alpha(x) \ .$$

Because the "Dirac (characteristic) functions" δ_α, $\alpha \in G$, also form a basis for $\mathbb{C}^G$, one obtains an inverse for the Fourier transform

$$f(x) = \frac{1}{|G|} \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\chi_\alpha(x)} \ .$$

An algebra isomorphism

More than being just a linear isomorphism, the Fourier transform is actually an algebra isomorphism from $\mathbb{C}^G$ equipped with the convolution product into $\mathbb{C}^G$ with the point-wise multiplication.

Given $f, g \in \mathbb{C}^G$, their convolution product is the map from G to $\mathbb{C}$ given by

$$f * g \colon \alpha \mapsto \sum_{x \in G} f(x) g(\alpha - x) \ .$$

One has $\widehat{(f * g)}(\alpha) = \hat{f}(\alpha)\hat{g}(\alpha)$ for all $\alpha \in G$, which explains why it is more convenient and easier to make computations of signals in the frequency domain (via the Fourier transform) than in the time domain.

Other well-known properties

For every $f, g \in \mathbb{C}^G$, the following hold:

- Plancherel formula: $\sum_{x \in G} f(x)\overline{g(x)} = \frac{1}{|G|} \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\hat{g}(\alpha)}$.
- Parseval equation : $\sum_{x \in G} |f(x)|^2 = \frac{1}{|G|} \sum_{\alpha \in G} |\hat{f}(\alpha)|^2$.

Table of contents

1. Introduction
2. Character theory: the classical approach
3. Hermitian structure over finite field
4. Characters over a finite field
5. The Fourier transform
6. Conclusion

The Frobenius automorphism and the conjugation

One fixes once for all a prime number p, a positive integer n, and $q := p^{2n}$.

Let $\mathcal{F}\colon GF(q) \to GF(q)$ be the Frobenius automorphism $x \mapsto x^p$ that fixes the elements of the prime field $GF(p)$ (it is the generator of the Galois group of $GF(q)/GF(p)$).

Let $\mathcal{F}_k\colon GF(q) \to GF(q)$ given by $\mathcal{F}_k(x) := x^{p^k}$.

Let $x \in GF(q)$. The conjugate of x is $\bar{x} := \mathcal{F}_n(x) = x^{\sqrt{q}}$.

Properties of the conjugation

Given $x, y \in GF(q)$, one has

- $\overline{x+y} = \bar{x} + \bar{y}$.
- $\overline{-x} = -\bar{x}$.
- $\overline{xy} = \bar{x}\ \bar{y}$.
- $\bar{\bar{x}} = x$.

Proof: The three first equalities come from the fact that $\mathcal{F}_n$ is a field homomorphism. The last point holds since for each $x \in GF(q)$, $x^q = x$. $\square$

Norm and unit circle

The (relative) norm with respect to $GF(q)/GF(\sqrt{q})$ is defined by

$$norm(x) := x\bar{x} = x^{\sqrt{q}+1}$$

for each $x \in GF(q)$.

Let me make an observation: $norm(x) \in GF(\sqrt{q})$ because
$norm(x)^{\sqrt{q}} = (x\bar{x})^{\sqrt{q}} = x^{\sqrt{q}}x^{q} = x^{\sqrt{q}}x = x^{\sqrt{q}+1} = norm(x)$.

The unit circle is defined as
$\mathcal{S}(GF(q)) := \{\, x \in GF(q) \colon norm(x) = 1 \,\} \subseteq GF(\sqrt{q})$.

It is a cyclic group of order $\sqrt{q} + 1$ (subgroup of the group of invertible elements of $GF(\sqrt{q})$).

Table of contents

1. Introduction
2. Character theory: the classical approach
3. Hermitian structure over finite field
4. Characters over a finite field
5. The Fourier transform
6. Conclusion

Limitations

Because $\mathcal{S}(GF(q))$ is a cyclic group of order $\sqrt{q}+1$, any of its subgroups is cyclic of order a divisor of $\sqrt{q}+1$, and for each divisor d of $\sqrt{q}+1$, $\mathcal{S}(GF(q))$ contains a unique subgroup $\mathcal{S}_d(GF(q))$ of order d.

Hence, contrary to $\mathcal{S}(\mathbb{C})$, $\mathcal{S}(GF(q))$ may be used to define a character theory but is limited to finite groups that admit a decomposition into a direct product of cyclic groups of order dividing $\sqrt{q}+1$.

Convention

From now on, d denotes an integer that divides $\sqrt{q}+1$.

If u is a generator of $\mathcal{S}(GF(q))$, then $u^{\frac{\sqrt{q}+1}{d}}$ is a generator of the subgroup $\mathcal{S}_d(GF(q))$.

Characters

A character of G is a homomorphism of groups from G to $\mathcal{S}(GF(q))$.

For a character χ, one has $\chi(-x) = \chi(x)^{-1} = \overline{\chi(x)}$ and $norm(\chi(x)) = 1$.

By analogy with the usual complex-valued characters one denotes by $\hat{G}$ the (group) of all characters of G.

Theorem

The groups $\mathbb{Z}/d\mathbb{Z}$ and $\widehat{\mathbb{Z}/d\mathbb{Z}}$ are isomorphic.

Proof: The characters of $\mathbb{Z}/d\mathbb{Z}$ are $\mathcal{S}_d(GF(q))$-valued since $1 = \chi(0) = \chi(dx) = (\chi(x))^d$, so that $\chi(x)$ is a d-th root of unity. Let χ be a character. Then, $\chi(1) = u_d^j$ for some $0 \leq j \leq d-1$. One has $\chi(k) = \chi(1)^k = u_d^{kj}$. For $0 \leq j \leq d-1$, let $\chi_j \colon k \mapsto u_d^{jk}$. Hence χ_j is a character and all characters have this form. Let us define $\Psi \colon \mathbb{Z}/d\mathbb{Z} \to \widehat{\mathbb{Z}/d\mathbb{Z}}$ by $\Psi(j) = \chi_j$. Then, it is a group homomorphism and it is onto. It is also one-to-one since $\Psi(j) = 1$ implies that $u_d^j = \chi_j(1) = 1$ hence $j = 0$. $\square$

Property

Theorem

Let us assume that $G \cong \prod_{i=1}^{N} (\mathbb{Z}/d_i\mathbb{Z})^{m_i}$ where each d_i divides $\sqrt{q}+1$. Then, $\hat{G} \cong G$.

The proof depends on the following easy case.

One can prove that for each pair (d_1, d_1) of divisors of $\sqrt{q}+1$, then $\widehat{(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z})} \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z})$.

Double dual

Let us denote by $\mathbf{Ab}_{\sqrt{q}+1}$ the category of all finite Abelian groups $G \cong \prod_{i=1}^{N} (\mathbb{Z}/d_i\mathbb{Z})^{m_i}$, where each d_i divides $\sqrt{q}+1$.

Theorem

The correspondence $G \mapsto \widehat{\widehat{G}}$ from $\mathbf{Ab}_{\sqrt{q}+1}$ to itself is a functorial isomorphism. In particular, for each G in $\mathbf{Ab}_{\sqrt{q}+1}$, $G \cong \widehat{\widehat{G}}$.

The "inner" product

For every $f, g \colon G \to \overline{GF(q)}$, let us define
$\langle f, g \rangle := \sum_{x \in G} f(x)\overline{g(x)} \in GF(q)$.

Remark

Contrary to the complex case, this biadditive form is not "definite" in the sense that $\langle f, f \rangle = 0$ does not ensure that $f \equiv 0$.

One has a kind of an orthogonality relation: for each $\chi_1, \chi_2 \in \hat{G}$,
$\langle \chi_1, \chi_1 \rangle = |G| \mod p$ and $\langle \chi_1, \chi_2 \rangle = 0$ whenever $\chi_1 \neq \chi_2$.

Remark

Because $G \cong \prod_{i=1}^{N} (\mathbb{Z}/d_i\mathbb{Z})^{m_i}$ where each d_i divides $\sqrt{q} + 1 = p^n + 1$, then $d_i = 1 \mod p$, hence $|G| = \prod_{i=1}^{N} d_i^{m_i}$ is co-prime to p so that $|G|$ is invertible modulo p.

Table of contents

1 Introduction

2 Character theory: the classical approach

3 Hermitian structure over finite field

4 Characters over a finite field

5 The Fourier transform

6 Conclusion

Definition

For every $x, y \in (\mathbb{Z}/d\mathbb{Z})^m$, one defines $x \cdot y := \sum_{i=1}^{m} x_i y_i$.

Let $G = \prod_{i=1}^{N} (\mathbb{Z}/d_i\mathbb{Z})^{m_i}$ where each d_i divides $\sqrt{q} + 1$.

Then, for each $\alpha = (\alpha_1, \cdots, \alpha_N)$ (where $\alpha_i \in (\mathbb{Z}/d_i\mathbb{Z})^{m_i}$), let $\chi_\alpha \colon x = (x_1, \cdots, x_N) \in G \mapsto \prod_{i=1}^{m} u^{\frac{(\sqrt{q}+1)\alpha_i \cdot x_i}{d_i}} \in \mathcal{S}(GF(q))$. It defines an explicit isomorphism from G to $\widehat{G}$.

Let $f \colon G \to GF(q)$. Its Fourier transform is the map $\hat{f}$ from G to $GF(q)$ given for $\alpha \in G$ by

$$\hat{f}(\alpha) := \sum_{x \in G} f(x) \chi_\alpha(x) \ .$$

Its properties formally analog to that of the usual Fourier transform

- Fourier inversion formula: $f(x) = (|G| \mod p)^{-1} \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\chi_\alpha(x)}$.
- $\widehat{(f * g)}(\alpha) = \hat{f}(\alpha)\hat{g}(\alpha)$.
- Plancherel formula: $\sum_{x \in G} f(x)\overline{g(x)} = (|G| \mod p)^{-1} \sum_{\alpha \in G} \hat{f}(\alpha)\overline{\hat{g}(\alpha)}$.
- Parseval equation:

$\sum_{x \in G} norm(f(x)) = (|G| \mod p)^{-1} \sum_{\alpha \in G} norm(\hat{f}(\alpha))$.

Table of contents

1. Introduction
2. Character theory: the classical approach
3. Hermitian structure over finite field
4. Characters over a finite field
5. The Fourier transform
6. Conclusion

Afterword

All this modulo p setting makes it possible to introduce a convenient notion of bent functions.

Again these functions share many similarities with their usual complex-valued counterparts. In particular certain known constructions may be applied in the modular setting.

This work may be extended in two directions:

- first one needs to study the relations, if any, between usual bent functions and our own bent functions,

- secondly, the analogy between the two theories suggests that degree two field extensions should play a particular rôle in cryptography, and we have to understand it.

Terima kasih![1]

[1] Thank you!