Discrete Fourier Analysis report

Lorenzo Baldi, Salvatore Schiavulli

May 22, 2018

Contents

1 Inroduction **2**

2 Representation of finite groups **2**

3 Graphs in the finite upper half plane **3**

3.1 Poincaré upper half plane 3

3.2 The finite upper half plane 3

3.3 Graphs and their properties 6

1 Inroduction

2 Representation of finite groups

In this report $\mathbb{F}_q$ indicates the finite field with $q = p^r$ elements, where p is a prime and r is an integer greater then zero.

Here we are interested in doing Fourier analysis on some subgroups of the *General linear group*, which is defined below.

Definition 2.1. The *General Linear group* of dimension n over the field $\mathbb{F}_q$ is the group of $n \times n$ invertible matrices with entries in $\mathbb{F}_q$:

$$\mathrm{GL}(n, \mathbb{F}_q) = \left\{ A \in \mathbb{F}_q^{n\times n} : \ \det A = |A| \neq 0 \right\}.$$

In particular we will focus on $GL(2, \mathbb{F}_q)$ and on its subgroup $\mathrm{Aff}(q)$, *i.e.* the *Affine group*:

Definition 2.2. The *Affine group* of dimension two over the field $\mathbb{F}_q$ is:

$$\mathrm{Aff}(q) = \left\{ A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_q) \right\} = \left\{ A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : \ a, b \in \mathbb{F}_q, \, a \neq 0 \right\}.$$

Since we want to do Fourier analysis on these groups, first of all we must map them (homomorphically) into groups of complex matrices. To do that we need to introduce the concept of representation of finite group G.

Definition 2.3. A (finite dimensional) representation of a finite group G is a group homomorphism

$$\pi : G \to \mathrm{GL}(n, \mathbb{C}).$$

If, for $g \in G$, $\pi(g)$ is a matrix with i, j entry $\pi_{i,j}(g)$, we call the functions $\pi_{i,j} : G \to \mathbb{C}$ the *matrix entries* of π.

Remark. We can identify $\mathrm{GL}(n,\mathbb{C})$ and

$$\mathrm{GL}(V) = \{T : V \to V \mid T \text{ is linear and invertible}\},$$

where V is an n-dimensional vector space over $\mathbb{C}$. However notice that in this case the matrix entries $\pi_{i,j}$ change if change the basis of V and this can cause some issue. In any case, will use the two concepts interchangeably.

3 Graphs in the finite upper half plane

3.1 Poincaré upper half plane

3.2 The finite upper half plane

Definition 3.1. An element $\gamma \in \mathbb{F}_q$ is a *square* if $\exists\, x \in \mathbb{F}_q\colon \gamma = x^2$.

If δ is a non square element of $\mathbb{F}_q$, then the polynomial $x^2 - \delta$ has no solutions in $\mathbb{F}_q$. Its splitting field is $\mathbb{F}_{q^2}$ and one of its roots will be denoted by $\sqrt{\delta}$ (the other is $-\sqrt{\delta}$).

$\sqrt{\delta}$ will play the same role of the imaginary unit i. Given $z = x + y\sqrt{\delta} \in \mathbb{F}_{q^2}$ we define, using the notation from complex analysis, the *real part* of z as $\mathfrak{Re}\, z = x$; the *imaginary part* of z as $\mathfrak{Im}\, z = y$; the *conjugate* of z as $\bar{z} = x - y\sqrt{\delta}$; the *norm* of z as $\mathfrak{N}\, z = z\bar{z}$; the *trace* of z as $\mathfrak{T}\, z = z + \bar{z}$.

Remark. The norm and the trace above are the ones usually defined in theory of finite fields (in the special case of the field extension $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$), because $z^q = (x + y\sqrt{\delta})^q = x^q + y^q\sqrt{\delta}^q = x + y(-\sqrt{\delta}) = \bar{z}$. See for instance [LN94].

Definition 3.2. The *finite upper half plane* is

$$H_q = \left\{ z = x + y\sqrt{\delta}\colon x \in \mathbb{F}_q, y \in \mathbb{F}_q^* \right\} \tag{1}$$

We recall the definition of group action.

Definition 3.3. A *group action* of the group G on the set X is a map

$$\begin{aligned} \phi\colon H \times X &\longrightarrow X \\ (g,x) &\longmapsto \phi(g,x) = g \cdot x \end{aligned}$$

such that:

- $\forall\, x \in X$, $\iota \cdot x = x$, where ι denotes the identity of the group;
- $\forall\, h, g \in G, \forall\, x \in X$ we have $(gh) \cdot x = g \cdot (h \cdot x)$.

In our case will have $X = H_q$, while G will be the general linear group $\mathrm{GL}(2,\mathbb{F}_q)$ or its subgroup of affine transformations $\mathrm{Aff}(q)$, defined below.

Definition 3.4. The *General Linear group* of dimension two over the field $\mathbb{F}_q$ is:

$$\mathrm{GL}(2,\mathbb{F}_q) = \left\{ g = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} : a_{i,j} \in \mathbb{F}_q, \det g \neq 0 \right\}$$

Definition 3.5. The *Affine group* of dimension two over the field $\mathbb{F}_q$ is:

$$\mathrm{Aff}(q) = \left\{ g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{F}_q) \right\} = \left\{ g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{F}_q, a \neq 0 \right\}$$

Now we can define define the action we are interested in, and investigate some of its properties.

Definition 3.6. The group $\mathrm{GL}(2,\mathbb{F}_q)$ acts on H_q by *fractional linear transformation*:

$$\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{F}_q), \forall z \in H_q, \quad g \cdot z = \frac{az+b}{cz+d}. \tag{2}$$

We check the well definition of the action and find some properties in the following proposition.

Proposition 3.7. *Given $\cdot$ the action by fractional linear transformation, the following holds (with the same notations of 3.6):*

1. $\mathfrak{Im}(g \cdot z) = \frac{\mathfrak{Im} z \det g}{\mathfrak{N}(cz+d)}$ *and* $\mathfrak{Re}(g \cdot z) = \frac{ac\mathfrak{N} z + bd + (ad+bc)\mathfrak{Re} z}{\mathfrak{N}(cz+d)}$*;*
2. *the action is well defined;*
3. *the restriction of of the action to the subgroup* $\mathrm{Aff}(q)$ *is a transitive action, that is:* $\exists\, \bar{z} \in H_q : \big(\forall z \in H_q \exists g \in \mathrm{Aff}(q)$ *such that* $z = g \cdot \bar{z}\big)$.

Proof. To prove 1. we have to show first that $\mathfrak{N}(cz+d) \neq 0$. By definition of norm it suffices to prove that $cz+d \neq 0$ Let $z = x + y\sqrt{\delta}$. Then

$$cz + d = 0 \iff (cx+d) + (cy)\sqrt{\delta} = 0 \iff cy = 0 \wedge cx + d = 0 \iff c = d = 0, \tag{3}$$

but this cannot happen, because $\det g = ad - bc \neq 0$. Then is enough to perform some calculations.

Now we prove the second part. We already proved that $cz + d \neq 0$ in 3. We have now to show that $g \cdot z \in H_q$, that is $\mathfrak{Im}(g \cdot z) \neq 0$. But this follows from point 1: $\mathfrak{Im}(g \cdot z) = \frac{\mathfrak{Im} z \det g}{\mathfrak{N}(cz+d)}$, where $\mathfrak{Im} z \neq 0$ because $z \in H_q$, $\det g \neq 0$ because $g \in \mathrm{GL}(2,\mathbb{F}_q)$. (mancante: funziona bene col prodotto di matrici)

For the last part, take $\bar{z} = \sqrt{\delta} \in H_q$. Then for any $z = x + y\sqrt{\delta} \in H_q$ we have that $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \cdot \bar{z} = z$ (note that $y \neq 0$ because $z \in H_q$, so the matrix defined belongs to $\mathrm{Aff}(q)$). ◻

Now we can introduce a *distance* which is analogous to the arch length in the Poicaré upper half plane.

Definition 3.8. The *distance* of two elements of H_q is defined by:

$$\begin{aligned}\mathfrak{d}\colon H_q \times H_q &\longrightarrow H_q \\ (z,w) &\longmapsto \mathfrak{d}(z,w) = \frac{\mathfrak{N}(z-w)}{\operatorname{Im} z \operatorname{Im} w} = \frac{(x-u)^2 - \delta(y-u)^2}{yu},\end{aligned}$$

where $z = x + y\sqrt{\delta}$ and $w = u + v\sqrt{\delta}$ (the definition is well posed because $z, w \in H_q \Rightarrow y, v \neq 0$).

Remark. The *distance* defined above is not a *metric*, that is its image is in $\mathbb{F}_q$ and not in $\mathbb{R}$. No triangle inequality is possible. The only properties of metric we have are:

1. $\mathfrak{d}(z,w) = \mathfrak{d}(w,z)$;
2. $\mathfrak{d}(z,w) = 0 \iff z = w$.

Proof. The first item is trivial by definition, while the second one requires more care.

If $z = w$ then $x = u \wedge y = v$, so $\mathfrak{d}(z,w) = 0$.

If $\mathfrak{d}(z,w) = 0$ then $(x-u)^2 - \delta(y-v)^2 = 0 \Rightarrow (x-u)^2 = \delta(y-v)^2$. If $y - v \neq 0$ then $\delta = ((x-u)(y-v)^{-1})^2$, but this is impossible because δ is a non square element. So $y = v$, which implies $x = u$ and $z = w$. □

We are interested in this distance because it is invariant under the action of the group $\mathrm{GL}(2, \mathbb{F}_q)$ on H_q.

Proposition 3.9. *Given $g \in \mathrm{GL}(2, \mathbb{F}_q)$ and $z, w \in H_q$, we have that $\mathfrak{d}(z,w) = \mathfrak{d}(g \cdot z, g \cdot w)$, where $\cdot$ is the action by fractal linear transformation.*

Proof. We first notice a property of the norm. Let $z \in H_q$, $a \in \mathbb{F}_q$. Then

$$\mathfrak{N}(az) = az\overline{az} = az\bar{a}\bar{z} = aza\bar{z} = a^2 z\bar{z} = a^2\, \mathfrak{N}\, z. \tag{4}$$

Moreover, we recall that if $z, w \in \mathbb{F}_{q^2}^*$, then $\mathfrak{N}(zw) = \mathfrak{N}\, z\, \mathfrak{N}\, w$. Now we can prove the proposition. With the usual notation

$$\begin{aligned}\mathfrak{d}(g \cdot z, g \cdot w) &= \frac{\mathfrak{N}(g \cdot z - g \cdot w)}{\operatorname{Im}(g \cdot z)\operatorname{Im}(g \cdot w)} = \frac{\mathfrak{N}\left(\frac{az+b}{cz+d} - \frac{aw+b}{cw+d}\right)}{\frac{\operatorname{Im} z \det g}{\mathfrak{N}(cz+d)} \frac{\operatorname{Im} w \det g}{\mathfrak{N}(cw+d)}} = \\ &= \frac{\frac{\mathfrak{N}\left((az+b)(cw+d) - (aw+b)(cz+d)\right)}{\mathfrak{N}(cz+d)\mathfrak{N}(cw+d)}}{\frac{\operatorname{Im} z \operatorname{Im} w (\det g)^2}{\mathfrak{N}(cz+d)\mathfrak{N}(cw+d)}} = \frac{\mathfrak{N}\left((z-w)(ad-bc)\right)}{\operatorname{Im} z \operatorname{Im} w (\det g)^2} = \\ &= \frac{(\det g)^2\, \mathfrak{N}(z-w)}{\operatorname{Im} z \operatorname{Im} w (\det g)^2} = \mathfrak{d}(z,w).\end{aligned}$$

□

3.3 Graphs and their properties

References

[LN94] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 1994. ISBN: 9780521460941. URL: https://books.google.it/books?id=AvY3PHlle3wC.