Discrete Fourier Analysis report

Lorenzo Baldi, Salvatore Schiavulli

May 24, 2018

Contents

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

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

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.

We give now some important definition about representations. In the following G indicates a finite group.

Definition 2.4. To representations α and β of G into $\mathrm{GL}(n,\mathbb{C})$ are said to be *equivalent* if there exists a matrix $T \in \mathrm{GL}(n,\mathbb{C})$ such that

$$T\alpha(g)T^{-1} = \beta(g), \quad \forall g \in G.$$

This is equivalent to say that we can obtain one representation from the other by a uniform change of basis.

Definition 2.5. A *unitary* representation is a representation π which maps G into the unitary group $\mathrm{U}(n)$, where

$$\mathrm{U}(n) = \{A \in \mathrm{GL}(n,\mathbb{C})\colon {}^t\bar{A}A = I\}.$$

Remark. If $\langle u, v\rangle = {}^t\bar{u}v$ is the standard Hermitian inner product of vectors of $\mathbb{C}^n$, the unitary matrices are those which preserve this product, that is, $\langle Au, Av\rangle = \langle u, v\rangle \ \forall u, v \in \mathbb{C}^n$. Indeed, if $A \in \mathrm{U}(n)$, then by the definition of the inner product, we have $\langle Au, Av\rangle = {}^t\overline{(Au)}Av = {}^t\bar{u}{}^t\bar{A}Av = {}^t\bar{u}v = \langle u, v\rangle \ \forall u, v \in \mathbb{C}^n$ and vice versa if $\langle Au, Av\rangle = \langle u, v\rangle \ \forall u, v \in \mathbb{C}^n$ then, by taking $u_i = (0,\dots,0,1,0,\dots,0)$ where the 1 is in the i-th coordinate, we see that, indicating with a_i the i-th column of A, $\delta_{i,j} = \langle u_i, u_j\rangle = \langle Au_i, Au_j\rangle = {}^t\bar{a}_i a_j$, that is ${}^t\bar{A}A = I$.

Definition 2.6. A *subrepresentation* ρ of a representation $\pi\colon G \to \mathrm{GL}(V)$ means that $\rho\colon G \to \mathrm{GL}(W)$, where W is a subspace of V such that $\pi(g)W \subset W$ for all $g \in G$ and $\rho(g)$ is the restriction of $\pi(g)$ to W, *i.e.*

$$\pi(g)_{|_W} = \rho(g) \ \forall g \in G$$

Using matrix language, this means that there is a basis of V such that $\pi(g)$ has the block form:

$$\begin{pmatrix} \rho(g) & * \\ 0 & * \end{pmatrix}$$

Definition 2.7. A representation π is *irreducible* if its only subrepresentations are π itself and 0.

When we deal with representations of a finite group G, we can just consider the unitary ones, due to the following result:

Proposition 2.8. *If G is a finite group, every representation is equivalent to a unitary representation.*

Proof sketch. To prove this preposition we'll use the fact (which we aren't going to prove) that if a matrix M leaves invariant some positive definite, Hermitian inner product $c(u,v)$ for $u,v \in \mathbb{C}^n$, then M is conjugate to a unitary matrix. So it suffices to find an inner product which is invariant under $\pi(g)$ for all $g \in G$. Such a inner product is given by

$$c(u,v) = \sum_{g\in G} \langle \pi(g)u, \pi(g)v \rangle, \text{ for } u,v \in \mathbb{C}^n.$$

Indeed, for $h \in G$, $u,v \in \mathbb{C}^n$, we have

$$\begin{aligned} c(\pi(h)u, \pi(h)v) &= \sum_{g\in G} \langle \pi(g)\pi(h)u, \pi(g)\pi(h)v \rangle \\ &= \sum_{g\in G} \langle \pi(gh)u, \pi(gh)v \rangle \\ &= \sum_{k\in G} \langle \pi(k)u, \pi(k)v \rangle = c(u,v). \end{aligned}$$

Where we have made the substitution $gh = k$, so that if h runs through all the elements in G, so does k. □

Let us now introduce the space of functions from G to $\mathbb{C}$

$$\mathrm{L}^2(G) = \{\, f : G \to \mathbb{C} \,\},$$

which is a vector space over $\mathbb{C}$ of dimension $|G|$ (it is isomorphic to $\mathbb{C}^n$, with $n = |G|$). We can make $\mathrm{L}^2(G)$ an algebra by defining the *convolution* $a * b$, for $a, b \in \mathrm{L}^2(G)$, $x \in G$:

$$(a*b)(x) = \sum_{t\in G} a(xt^{-1})b(t) = \sum_{y\in G} a(y)b(y^{-1}x)$$

Remark (non necessario). This definition of convolution coincides with that given for the commutative group $\mathbb{Z}/n\mathbb{Z}$ ($(a*b)(x) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} a(y)b(x-y)$). Moreover we have that, given $f \in \mathrm{L}^2(G)$,

$$f * h = h * f \quad \forall h \in \mathrm{L}^2(G) \tag{1}$$

if and only if f is constant on conjugacy classes

$$\{\, g \,\} = \left\{ xgx^{-1} : x \in G \right\}.$$

Indeed if f is constant on conjugacy classes, then for all $x \in G$

$$(f * h)(x) = \sum_{t \in G} f(xt^{-1})h(t) = \sum_{xt \in G} f(x(xt)^{-1})h(xt)$$
$$= \sum_{xt \in G} f(xt^{-1}x^{-1})h(xt) = \sum_{xt \in G} f(t^{-1})h(xt) = \sum_{y \in G} f(y^{-1}x)h(y) = (h * f)(x),$$

and, conversely, if 1 holds, then, taking $h = \delta_k$, for $k \in G$, we have that $(f * h)(ky) = f(kyk^{-1})$ and $(h * f)(ky) = f(y)$ for all $y \in G$, so that f is constant on conjugacy classes. Since if G is commutative the conjugacy class $\{g\}$ contains only g, it follows that the convolution is commutative for abelian groups, as we already know.

Exercise. *We define the* Left Regular Representation L *of G by*

$$\mathrm{L}\colon G \to \mathrm{GL}(\mathrm{L}^2(G))$$
$$g \mapsto \mathrm{L}(g)$$

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

$$H_q = \left\{ z = x + y\sqrt{\delta}\colon\ x \in \mathbb{F}_q,\, y \in \mathbb{F}_q^* \right\} \tag{2}$$

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:

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

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

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

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*:

$$\forall g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_q), \forall z \in H_q, \quad g \cdot z = \frac{az + b}{cz + d}. \tag{3}$$

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. $\mathfrak{Im}(g \cdot z) = \frac{\mathfrak{Im} z \det g}{\Omega(cz+d)}$ *and* $\mathfrak{Re}(g \cdot z) = \frac{ac\Omega z + bd + (ad+bc)\mathfrak{Re} z}{\Omega(cz+d)}$;
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:* $\exists\, \bar{z} \in H_q \colon \left(\forall z \in H_q \, \exists g \in \mathrm{Aff}(q) \text{ such that } z = g \cdot \bar{z} \right)$.

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

$$cz + d = 0 \iff (cx + d) + (cy)\sqrt{\delta} = 0 \iff cy = 0 \wedge cx + d = 0 \iff c = d = 0, \tag{4}$$

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 4. We have now to show that $g \cdot z \in H_q$, that is $\operatorname{Im}(g \cdot z) \neq 0$. But this follows from point 1: $\operatorname{Im}(g \cdot z) = \frac{\operatorname{Im} z \det g}{\Omega(cz+d)}$, where $\operatorname{Im} z \neq 0$ 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 $\mathrm{Aff}(q)$). □

Remark. $\mathrm{Aff}\, q$ is a subgroup of $\mathrm{GL}(2, \mathbb{F}_q)$, so the action of $\mathrm{GL}(2, \mathbb{F}_q)$ is transitive too.

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:

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

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

$$\mathfrak{N}(az) = az\overline{az} = az\bar{a}\bar{z} = azaz\bar{z} = a^2 z\bar{z} = a^2\,\mathfrak{N}\,z. \tag{5}$$

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

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

□

3.3 Graphs and their properties

Now we can finally introduce the graphs we are interested in.

Definition 3.10. Fix $0 \neq a \in \mathbb{F}_q$. The graph $X_q(\delta, a)$ is defined with vertexes the elements of H_q, and with edges the pairs of vertexes $z, w \in H_q$ such that $\mathfrak{d}(z,w) = a$.

Remark. We notice that the graph is undirected because $\mathfrak{d}(z,w) = \mathfrak{d}(w,z)$.

(qui ci vanno gli esempi, sia ripresi dal libro che no) (ci sono altre osservazioni carine sulle similutini col caso continuo, ma dovrei studiarci bene e non so se c'è spazio)

We can now state and prove one of the main theorems of the report.

Theorem 3.11. *Let $q = p^r$, where p is an odd prime. Let $0 \neq a \in \mathbb{F}_q$, and let $\delta \in \mathbb{F}_q$ be a non square element. Then the following holds:*

1. *if $a \neq 4\delta$ then the graph is $(q+1)-regular$;*
2. *if $0 \neq c \in \mathbb{F}_q$ then the graphs $X_q(\delta, a)$ and $X_q(\delta c^2, ac^2)$ are isomorphic;*
3. *$\forall 0 \leq s < r, s \in \mathbb{N}$ the graphs $X_q(\delta, a)$ and $X_q(\delta^{p^s}, a^{p^s})$ are isomorphic;*
4. *if $a \neq 4\delta$ then $X_q(\delta, a)$ is the Cayley graph for the group $\mathrm{Aff}\,q$ with generators:*
$$S_q(\delta, a) = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}\,q \colon x^2 = ay + (y-1)^2\delta \right\}; \tag{6}$$
5. *if $a \neq 4\delta$ then $X_q(\delta, a)$ is connected.*

(ci sarebbe un altro punto, non mi sembra né utile né interessante, lo ometto per adesso)

Proof. 1. WLOG I can assume $z = \sqrt{\delta}$, because of the transitivity of the action and the invariance of the distance. In fact, if $g \cdot \sqrt{\delta} = z$, then

$$|\{\bar{w} \colon \mathfrak{d}(\sqrt{\delta}, \bar{w}) = a\}| = |\{w \colon \mathfrak{d}(z, w) = a\}|.$$

So we are interested in the solutions of the equation $\mathfrak{d}(\sqrt{\delta}, z) = a$.

Suppose $z = x + y\sqrt{\delta}$. Then

$$\begin{aligned} \mathfrak{d}(\sqrt{\delta}, z) = a &\iff \mathfrak{N}(\sqrt{\delta} - z) = ay \\ &\iff (\sqrt{\delta} - z)\overline{(\sqrt{\delta} - z)} = ay \\ &\iff (-x + (1-y)\sqrt{\delta})(-x - (1-y)\sqrt{\delta}) = ay \\ &\iff x^2 = ay + (y-1)^2\delta. \end{aligned} \tag{7}$$

We must be careful: if z is a solution of the previous equation, we must check that $z \in H_q$, that is $y \neq 0$. But this is always true: if $y = 0$ from the previous equation we obtain $\delta = (x(y-1)^{-1})^2$, but this is impossible, since δ is a non square element. So we can simply find solutions of $\mathfrak{N}(\sqrt{\delta} - z) = ay$ in $\mathbb{F}_{q^2}$, and they will belong to H_q as well.

We recall (see [LN94]) that $\mathfrak{N} \colon \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ is an onto group omomorphism. We want to use this property to find the number of solutions of $\mathfrak{N}(\sqrt{\delta} - z) = ay$:

$$|\mathfrak{N}^{-1}(a)| = \frac{|\mathbb{F}_{q^2}^*|}{|\mathbb{F}_q^*|} = \frac{q^2+1}{q-1} = q + 1. \tag{8}$$

Fix $c = (\frac{a}{2\delta} - 1)\sqrt{\delta}$ and $d = (1 - \frac{a}{4\delta})a$. Then:

$$\begin{aligned} \mathfrak{N}(z + c) = d &\iff (z + c)(\bar{z} + \bar{c}) = d \\ &\iff ((z - \sqrt{\delta}) + \frac{a}{2\delta})((\bar{z} + \sqrt{\delta}) - \frac{a}{2\delta}) = (1 - \frac{a}{4\delta})a \\ &\iff (z - \sqrt{\delta})(\bar{z} + \sqrt{\delta}) + (\frac{a}{2\delta})(\bar{z} + \delta - z + \delta) + \frac{a^2}{4\delta} = a - \frac{a^2}{4\delta} \\ &\iff \mathfrak{N}(z - \sqrt{\delta}) + (\frac{a}{2\delta})(-2y\sqrt{\delta} + 2\sqrt{\delta}) = a \iff \mathfrak{N}(z - \sqrt{\delta}) = ay. \end{aligned}$$

So, if we set $w = z + c$, in the case $d \neq 0$, I can find $q + 1$ solutions in $\mathbb{F}_{q^2}^*$ of $\mathfrak{N}\, w = d$. But $d = 0 \iff a = 0, 4\delta$, cases that are excluded by hypothesis. (il libro fa altre considerazioni oer concludere che il numero di soluzioni è precisamente q+1, a me pare suff così per concludere).

Hence the equation $\mathfrak{d}(\sqrt{\delta}, z) = a$ has exactly $q + 1$ solutions, that is the graph is $(q+1) - regular$.

2. We first notice that that δc^2 is a non square element, so the definition of the graph $X_q(\delta c^2, ac^2)$ is well posed. Clearly multiplying by c^2 is a bijection of H_q to itself, so the vertexes of the two graphs are the same.

In the definition of $\mathfrak{N} z = z\bar{z}$ seems that the choice of $\sqrt{\delta}$ matters; but as we already noticed $\bar{z} = z^q$. This means that $\mathfrak{N} z = zz^q$ is independent from the choice of $\sqrt{\delta}$. The same does not hold for the imaginary part: if $z = x + y\sqrt{\delta}$, then $z = x + yc^{-1}c\sqrt{\delta}$. So, with an obvious notation,

$$\mathrm{Im}_{c\sqrt{\delta}}(z) = c^{-1}\,\mathrm{Im}_{\sqrt{\delta}}(z). \tag{9}$$

What we need to prove can be stated as follows:

$$\frac{\mathfrak{N}(z-w)}{\mathrm{Im}_{\sqrt{\delta}}(z)\mathrm{Im}_{\sqrt{\delta}}(w)} = \mathfrak{d}_{\sqrt{\delta}}(z,w) = a \iff \frac{\mathfrak{N}(z-w)}{\mathrm{Im}_{c\sqrt{\delta}}(z)\mathrm{Im}_{c\sqrt{\delta}}(w)} = \mathfrak{d}_{c\sqrt{\delta}}(z,w) = ac^2.$$

But this is easy thanks to 9:

$$\begin{aligned}\frac{\mathfrak{N}(z-w)}{\mathrm{Im}_{c\sqrt{\delta}}(z)\mathrm{Im}_{c\sqrt{\delta}}(w)} = ac^2 &\iff \frac{\mathfrak{N}(z-w)}{c^{-1}\,\mathrm{Im}_{\sqrt{\delta}}(z)c^{-1}\,\mathrm{Im}_{\sqrt{\delta}}(w)} = ac^2\\ &\iff \frac{\mathfrak{N}(z-w)}{\mathrm{Im}_{\sqrt{\delta}}(z)\mathrm{Im}_{\sqrt{\delta}}(w)} = a.\end{aligned}$$

3. We can restrict the proof to the case $s = 1$, the general statement follows by induction. Raising to p is a field automorphisim, hence non square elements are mapped into non square elements and it is a bijection from H_q to itself. So the graph $X_q(\delta^p, a^p)$ is well defined and the vertexes of $X_q(\delta, a)$ and $X_q(\delta^p, a^p)$ are the same. We observe in particular that $(x + y\sqrt{\delta})^p = x^p + y^p\sqrt{\delta}^p$. Moreover, using a notation similar to the previous point,

$$\begin{aligned}\mathfrak{d}_{\sqrt{\delta}}(z,w) = a &\iff \frac{\mathfrak{N}(z-w)}{\mathrm{Im}_{\sqrt{\delta}}(z)\mathrm{Im}_{\sqrt{\delta}}(w)} = a\\ &\iff \Big(\frac{\mathfrak{N}(z-w)}{\mathrm{Im}_{\sqrt{\delta}}(z)\mathrm{Im}_{\sqrt{\delta}}(w)}\Big)^p = a^p\\ &\iff \frac{\mathfrak{N}((z-w)^p)}{\mathrm{Im}_{\sqrt{\delta}^p}(z^p)\mathrm{Im}_{\sqrt{\delta}^p}(w^p)} = a^p\\ &\iff \frac{\mathfrak{N}(z^p-w^p)}{\mathrm{Im}_{\sqrt{\delta}^p}(z^p)\mathrm{Im}_{\sqrt{\delta}^p}(w^p)} = a^p \iff \mathfrak{d}_{\sqrt{\delta}^p}(z^p,w^p) = a^p,\end{aligned}$$

and we conclude that the two graphs are isomorphic.

4. In the statement we identify H_q and $\mathrm{Aff}\,q$ by the bijection given by the action on the point $\sqrt{\delta}$: $x + y\sqrt{\delta} \leftrightarrow \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$. Suppose $S_q(\delta, a)$ as in 6. We

notice that the equation in the definition of $S_q(\delta, a)$ is the same as in 7. So we obtain $s \in S_q(\delta, a) \iff \mathfrak{d}(\sqrt{\delta}, s \cdot \sqrt{\delta}) = a$. Moreover

$$\begin{aligned} g, h \in \operatorname{Aff} q \quad \text{are adjacent} &\iff \mathfrak{d}(h \cdot \sqrt{\delta}, g \cdot \sqrt{\delta}) = a \iff \mathfrak{d}(\sqrt{\delta}, h^{-1} g \cdot \sqrt{\delta}) = a \\ &\iff h^{-1} g \in S_q(\delta, a) \iff \exists\, s \in S_q(\delta, a) \colon\ g = hs, \end{aligned}$$

so $S_q(\delta, a)$ is a set of generators for the graph. We only need to check that it is closed under inversion (our graph is undirected): but this follows from the fact that $\mathfrak{d}(\sqrt{\delta}, s \cdot \sqrt{\delta}) = \mathfrak{d}(s^{-1}\sqrt{\delta}, s^{-1} s \cdot \sqrt{\delta}) = \mathfrak{d}(\sqrt{\delta}, s^{-1} \cdot \sqrt{\delta})$. Hence $X_q(\delta, a)$ is a Cayley graph with generators $S_q(\delta, a)$.

5. I want to prove that $S_q(\delta, a)$ generates $\operatorname{Aff} q$, that is every $g \in \operatorname{Aff} q$ can be expressed by the product of a finite number of elements of $S_q(\delta, a)$. We first observe that

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix},$$

so it enough to show that $\forall b \in \mathbb{F}_q$ and $\forall a \in \mathbb{F}_q^*$ the matrices $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ belongs to the subgroup generated by $S_q(\delta, a)$.

Now, since $|S_q(\delta, a)| = q + 1$ (this is because its cardinality is exactly the number of points adjacent to $\sqrt{\delta}$, and in the case $a \neq 4\delta$ the graph is $q + 1$ regular), we have that □

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.