Chapter 3

Quantum Base Size of $GL(2, q)$

Character Theory of GL(2,q)

We will take the following things for granted:

- For every $q = p^n$ there exists exactly one field up to isomorphism. We will call that field $\mathbb{F}_q$
- For every $s \in \mathbb{F}_q$, the sum of s with itself p times is 0. i.e. $ps = 0$. This is usually stated as $\mathbb{F}_q$ has characteristic p.
- The group $(\mathbb{F}_q^*, x)$ is cyclic.

A Useful Proposition

Let $F = \mathbb{F}_{q^2}$ and $S = \{s \in F | s^q = s\}$
Then

1. S is a subfield of F of order q (hence $\mathbb{F}_q \cong S$)
2. If $r \in F$ then $r + r^q, r^{1+q} \in S$

We will use this from here on out to identify the subfield, S, as $\mathbb{F}_q$.

Proof of our useful propsition

1. Suppose that $s, t, \in S$. Then $(s+t)^q = s^q + t^q = s + t$ by (Frobonius Homomorphism / Freshman's Dream.)
   Thus $s + t \in S$.
   This gives us that $(S, +)$ is an abelian group (since $1 \in S$) and since $(st)^q = s^q t^q = st$ we get (S^*, x) is also an abelian group.
2. Since $(\mathbb{F}_{q^a}^*)$ is a group of order $q^2 - 1$, it must that $r^{q^2} = r$ for all $r \in \mathbb{F}_{q^2}$ by Larange (?)
   This implies that $(r + r^q)^q = r^q + r^{q^2} = r + r^q$ so $r + r^q$ and $r^{1+q} \in S$.

Some Notation

We introduce some useful notation:

Let ϵ be a generator of the cyclic group $\mathbb{F}^*_{q^2}$ and let $\omega = e^{\frac{2\pi i}{q^2-1}}$.

Furthermore, suppose $r \in \mathbb{F}_{q^2}$.

We may write $r = \epsilon^m$ for some m and let $\bar{r} = \omega^m$.

Then the map $r \mapsto \bar{r}$ is an irreducible character of $\mathbb{F}^*_{q^2}$. Moreover, every irreducible character has the form $r \mapsto \bar{r}^j$ for some integer j.

Breaking this down further, let x_j be defined by $x(r) = \bar{r}^j$.

Then of course this is a character since it is a homomorphism from an abeliean group into $\mathbb{C}^*$.

The Size of GL(2,q)

Remark that we can trivially represent GL(2,q) as the set of matrices of the form

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

with determinate $\neq 0$.

Thus a matrix

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

belongs to GL(2,q) if and only if its rows are linearly independent. Therefore (a, b) can be anything as long as they are not both zero ($q^2 - 1$ choices) and then (c, d) can be anything that is not a scaler multiple of (a, b) giving us $q^2 - q$) choices. Therefore GL(2,q) has $(q^2 - q)(q^2 - q)$ elements.
This argument nice generlizes to GL(n,q).

Conjugacy Classes of GL(2,q)

There are 4 families of conjugacy classes of G. 3 of these are easy, one is hard.

1. $\begin{vmatrix} a & b \\ 0 & d \end{vmatrix}$ is conjuagte to $\begin{vmatrix} a' & b' \\ 0 & d' \end{vmatrix}$ only if $\{a, c\} = \{a', c'\}$ since conjuagate matrices have the same eigenvalues.

2. The matrices
$$sI = \begin{vmatrix} a & b \\ 0 & d \end{vmatrix}$$
belongs to the center of G. They give us $q - 1$ (the number of choices for s) conjugacy classes of size one.

3. Let
$$g = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \in G \text{ and } u_s = \begin{vmatrix} s & 1 \\ 0 & s \end{vmatrix}$$
Then
$$gu_s = \begin{vmatrix} as & a+bs \\ cs & c+ds \end{vmatrix}$$
and
$$u_s g = \begin{vmatrix} as & d+bs \\ cs & ds \end{vmatrix}$$
so g belongs to the centralizer of u_s if and only if $c = 0$ and $a = d$.
Thus the matrices u_s ($s \in \mathbb{F}_2$) give us $q-1$ conjugacy classes. The order of the centralizer is $(q-1)q$, so by the Orbit-Stabilizer Theorem, each conjugacy class contains $q^2 - 1$ elements.

4. Now let $d_{s,t} = \begin{vmatrix} s & 0 \\ 0 & t \end{vmatrix}$

   Note that
$$\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}^{-1} \begin{vmatrix} s & 0 \\ 0 & t \end{vmatrix} \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = \begin{vmatrix} t & 0 \\ 0 & s \end{vmatrix}$$
   On the other hand, if $\neq t$, then we have $gd_{s,t} = d_{s,t}g$ if and only if $b = c = 0$. Thus, the matrices $d_{s,t}$ $(s,t, \in \mathbb{F}_q^*, s \neq t)$ give us $/frac(q-1)(q-2)2$ conjuagacy classes. The centralizer order is $(q-1)^2$, so again by the orbit-stabalizer theorem each conjugacy class contains $q(q+1)$ elements.

5. Finally, consider
$$v_r = \begin{bmatrix} 0 & 1 \\ -r^{1+q} & r+r^2 \end{bmatrix} (r \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q)$$
   By our initial proposition $v_r \in G$
   The characteristic polynomial of v_r is
$$det(xI - v_r) = x(x - (r + r^2)) + r^{1+q} = (x - r)(x - r^2)$$
   so v_r has eigenvalues of r and r^2.
   Since $r \notin \mathbb{F}_2$ we see that v_r lies in none of the conjegacy classes we have constructed so far. Now
$$gv_r = \begin{bmatrix} -br^{1+q} & a + b(r + r^2) \\ -dr^{1+q} & c + d(r + r^q) \end{bmatrix}$$
   and
$$v_r g = \begin{bmatrix} c & d \\ -ar^{1+q} + c(r + r^q) & -br^{1+q} + d(r + r^q) \end{bmatrix}$$

Hence $gv_r = v_r g$ only if $c = -br^{1+q}$ and $d = a + b(r + r^2)$ If these conditions hold, then $ad - bc = a^2 + ab(r + r^2) + b^2 r^{1+q} = (a + br)(a + br^2)$
Since $(a, b) \neq (0, 0)$ and $r, r^q \notin \mathbb{F}_q$ we see that $a + br$ and $a + br^q$ are non zero.
Therefore $g \in C_G(v_r) \iff g = \begin{bmatrix} a & b \\ -br^{1+q} & a + b(r + r^2) \end{bmatrix}$
Thus $|C_G(v_r)| = q^2 - 1$ and the conjegacy class containing v_r has size $q^2 - 1$.

The matrix v_t has eigenvalues t and t^q so it is not conjugate to v_r unless $t = r$ or $t = r^q$. Therefore we can partitian $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ into subsets of $\{r, r^q\}$. Each subset gives us a conjugacy class represenative v_r and different subsets give us representatives of different conjugacy classes of G, in fact all of the classes of G.

Conjugacy Classes

Propostion: There are $q^2 - 1$ conjugacy classes of GL(2,q) and they are described as follows:

class rep	sI	u_s	$d_{s,t}$	v_r
$\lvert C_G(g)\rvert$	$(q^2-1)(q^2-q)$	$(q-1)q$	$(q-1)^2$	q^2-1
number of classes	$q-1$	$q-1$	$\frac{(q-1)(q-2)}{2}$	$\frac{q^2-q}{2}$

This can be verified by adding to see they sum to the order of the group.