1 Characters of finite fields

Definition 1.1 A character of a finite field $F$ is a function $\chi : F \to \mathbb{C}$, satisfying the following conditions:

1. $\chi(0) = 0$
2. $\chi(1) = 1$
3. $(\forall a, b \in F)(\chi(ab) = \chi(a)\chi(b))$.

Note that a character is a homomorphism from the multiplicative group $F^\times = F \setminus \{0\}$ to the multiplicative group $\mathbb{C}^\times$.

Example 1.2 For any field $F$, we define the principal character, $\chi_0$, by $\chi_0(0) = 0$ and $(\forall a \neq 0)(\chi_0(a) = 1)$.

Notation. For a prime power $q = p^k$, $F_q$ denotes the field of order $q$ (i.e., the field $\mathbb{F}_q$ has $q$ elements). For $k = 1$, the field $\mathbb{F}_p$ is the field of mod $p$ residue classes. Note that for $k \geq 2$, the mod $p^k$ residue classes do not form a field, so for $k \geq 2$, the field $F_q$ is not the same as the ring of residue classes mod $q$. It is known, however, that for every prime power $q$ there exists a field $F_q$ and this field is unique up to isomorphism. If you are not familiar with finite fields, you may still read this note, always replacing $q$ by $p$.

Example 1.3 When $F = \mathbb{F}_p$ for an odd prime $p$, we define the quadratic character $\chi(a) := \left(\frac{a}{p}\right)$, where $\left(\frac{a}{p}\right)$ is 0 when $a = 0$, 1 when $a$ is a quadratic residue, and $-1$ when $a$ is a quadratic nonresidue. $\left(\frac{a}{p}\right)$ is called the Legendre symbol.

Exercise 1.4 Show that, for all $a$, $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.
Next, we extend the concept of the **quadratic character** to all finite fields of odd order.

**Example 1.5** Let $\mathbb{F}_q$ be a finite field of odd order $q$. The **quadratic character** $\chi$ of $\mathbb{F}_q$ is defined as follows: for $a \in \mathbb{F}_q$,

$$
\chi(a) = \begin{cases} 
1 & \text{if } (\exists b \in \mathbb{F}_q)(a = b^2 \neq 0); \\
-1 & \text{if } (\forall b \in \mathbb{F}_q)(a \neq b^2); \\
0 & \text{if } a = 0.
\end{cases}
$$

**Exercise 1.6** Let $q$ be an odd prime power and $\chi$ the quadratic character of $\mathbb{F}_q$. Prove: if $q \equiv -1 \pmod{4}$ then $\chi(-1) = -1$; and if $q \equiv 1 \pmod{4}$ then $\chi(-1) = 1$.

**Exercise 1.7** For any prime power $q$, prove: $(\forall a \in \mathbb{F}_q)(a^{q-1} = 1)$.

(Note that for $q = p$ a prime, this is Fermat’s Little Theorem.) *Hint.* Use Lagrange’s theorem from group theory (the order of a subgroup divides the order of the group).

The order of a nonzero element $a \in \mathbb{F}_q$ is the smallest positive $k$ such that $a^k = 1$. It follows from the preceding exercise that $k | q - 1$ ("$k$ divides $q - 1").

**Corollary 1.8** $(\forall a \in \mathbb{F}_q)(\chi(a) \text{ is a complex root of unity})$.

Indeed, if $a^k = 1$ then $(\chi(a))^k = \chi(a^k) = \chi(1) = 1$.

**Definition 1.9** The **order** of a character is the least positive integer $s$ such that $\chi(a)^s = 1$ for all $a \in \mathbb{F}_q$, $a \neq 0$.

Note that, for any character of $\mathbb{F}_q$, the order $s$ must divide $q - 1$.

The following is a basic fact about the structure of finite fields.

**Theorem 1.10** For any prime power $q$, the multiplicative group $\mathbb{F}_q^\times$ is cyclic. Equivalently, there exists some $g \in \mathbb{F}_q^\times$ such that $\mathbb{F}_q^\times = \{g, g^2, \ldots, g^{q-1} = 1\}$.

Such an element $g$ is called a **generator** of $\mathbb{F}_q^\times$, or a **primitive root** of the field $\mathbb{F}_q$.

**Exercise 1.11** Prove the Theorem. *Hint.* Use Sylow’s Theorem from group theory and the fact that a polynomial of degree $n$ has at most $n$ roots in a field.

**Corollary 1.12** If $\chi$ is a character of $\mathbb{F}_q$ of order $s$, and $g$ is a primitive root of $\mathbb{F}_q$, then $\chi(g)$ is a primitive $s^{th}$ root of unity. Conversely, for any $\omega \in \mathbb{C}$ such that $\omega^{q-1} = 1$, there exists a unique character $\chi$ of $\mathbb{F}_q$ with $\chi(g) = \omega$.

**Exercise 1.13** Prove the Corollary.

Note that if we take $\omega = 1$ we get the principal character, and, for $q$ odd, if we take $\omega = -1$, we get the quadratic character.
2 Character Sum: Weil’s Theorem

In this section we describe one of the most beautiful results of 20th century mathematics.

First we consider the sum of characters over all elements of a field.

**Exercise 2.1** If \( \chi \neq \chi_0 \), then \( \sum_{a \in \mathbb{F}_q} \chi(a) = 0 \).

Let now \( f \) be a polynomial of degree \( d \) over \( \mathbb{F}_q \). We wish to estimate the sum
\[
S(\chi,f) = \sum_{a \in \mathbb{F}_q} \chi(f(a))
\]

Clearly, since \( |\chi(f(a))| \) is 0 or 1 for all \( a \), we have \( |S(\chi,f)| \leq q \). This is the best possible upper bound; for example, if \( f \) is identically 1 then \( S(\chi,f) = q \); if \( \chi \) is the quadratic character and \( f(x) = x^2 \), then \( S(\chi,f) = q - 1 \).

Amazingly, once the trivial exceptions have been eliminated, a much stronger bound holds on the magnitude of \( S(\chi,f) \): the values of the character tend to cancel each other out roughly by the same amount as if they were chosen to be \( \pm 1 \) by coin flips.

**Theorem 2.2 (André Weil)** Let \( \mathbb{F}_q \) be a finite field, and let \( \chi \) be a character of \( \mathbb{F}_q \) of order \( s \). Let \( f(x) \) be a polynomial of degree \( d \) over \( \mathbb{F}_q \) such that \( f(x) \) cannot be written in the form \( c(h(x))^s \), where \( c \in \mathbb{F}_q \). Then
\[
\left| \sum_{a \in \mathbb{F}_q} \chi(f(a)) \right| \leq (d - 1)\sqrt{q}.
\]

Thus, in a sense, the values of a character over the range of a polynomial behave as “random” values, even though they are fully “deterministic.” This feature is the key to a large number of applications to combinatorics and the theory of computing where the goal is “derandomization”: the elimination of random choice from the proof of existence of a combinatorial object, i.e., replacing a probabilistic proof of existence by an explicit construction.

3 \( k \)-paradoxical tournaments: a proof by the Probabilistic Method

Let \( X = (V,E) \) be a digraph. Let \( x \in V \) and \( A \subseteq V \). We say that \( x \) dominates \( A \) if \( (\forall a \in A)(x,a) \in E \). We write \( x \rightarrow A \) to denote this statement.

**Definition 3.1** A digraph \( X = (V,E) \) is \( k \)-paradoxical if \( (\forall A \subseteq V)(|A| = k \Rightarrow \exists x \in V)(x \rightarrow A) \).
**Definition 3.2** A tournament is a digraph $T = (V,E)$ in which for every pair \{x, y\} of vertices, exactly one of the following holds: $x = y$ or $(x,y) \in E$ or $(y,x) \in E$.

Note that this concept corresponds to diagrams of round-robin tournaments without draws and without rematches. An edge (arrow) from $a$ to $b$ indicates that player $a$ beat player $b$.

In a 1-paradoxical tournament, every player is beaten by someone. In a 2-paradoxical tournament, every pair of players is beaten by someone. Even 2-paradoxical tournaments are not straightforward to construct.

**Exercise 3.3** Construct a 2-paradoxical tournament on 7 players. *Hint.* Make your diagram have a symmetry of order 7.

So it is quite surprising that $k$ paradoxical tournaments actually do exist for every $k$. Constructing such tournaments even for $k = 3$ is quite hard. However, Paul Erdős, in one of the gems of his Probabilistic Method, demonstrated the existence of such tournaments without telling us how to construct them.

**Theorem 3.4 (Erdős)** If $n > ck^{2}2^{k}$ then there exists a $k$-paradoxical tournament on $n$ vertices. (*c* is an absolute constant.)

What Erdős has shown is not just that such tournaments exist, but they abound: almost every tournament on a given set of $n$ vertices (players) is $k$-paradoxical. The model of “random tournaments” is very simple: flip a coin to decide the outcome of each match.

**Exercise 3.5** Let $A \subset V$ be a set of $k$ players (out of the set $V$ of $n$ players) and let $x$ be a player, not in $A$. Calculate the probability that $x \rightarrow A$.

**Exercise 3.6** Let $A$ be as before. Show that the probability that none of the remaining $n - k$ players dominates $A$ is exactly $(1 - 2^{-k})^{n-k}$.

**Exercise 3.7** Infer from the preceding exercise that the probability that our random tournament is not $k$-paradoxical is less than

$${n \choose k} (1 - 2^{-k})^{n-k}. \tag{1}$$

**Exercise 3.8** Conclude that if $n \choose k (1 - 2^{-k})^{n-k} \leq 1$ then there exists a $k$-paradoxical tournament on $n$ vertices.

**Exercise 3.9** Prove that if $k \geq 3$ and $n > 4k^{2}2^{k}$ then the inequality in the preceding exercise will hold. (A constant $c > 4$ works for $k = 2$; smaller constants work for larger values of $k$. As $k \to \infty$, the value of a suitable constant $\to 1$.) *Hint.* Use the following facts: $n \choose k < n^{k}/k!$; $1 - x < e^{-x}$; and the monotonicity of the function $x/\ln x$. 

4
This concludes the proof of Erdős’s Theorem.

**Exercise 3.10** Prove that if \( n > ck^22^k \) (for some absolute constant \( c \)) then almost all tournaments on a given set of \( n \) players are \( k \)-paradoxical.

Here “almost all” means that for every \( \epsilon > 0 \) there exists \( n_0 \) such that if \( n > n_0 \) and \( n > ck^22^k \) then the probability that the random tournament is \( k \)-paradoxical is greater than \( 1 - \epsilon \). *Hint.* Revisit the same calculations done for the previous exercises. Only minimal modifications are needed.

4 Paley tournaments: an explicit construction of \( k \)-paradoxical tournaments

We describe an explicit construction of \( k \)-paradoxical tournaments for arbitrarily large \( k \).

**Definition 4.1** Let \( q \equiv -1 \) be a prime power and let \( \chi \) denote the quadratic character of \( F_q \). The Paley tournament of order \( q \) is defined as a digraph \( P(q) = (V,E) \) where \( V = F_q \); we have a directed edge \( a \rightarrow b \) iff \( \chi(a-b) = 1 \).

Note that because \( q \equiv -1 \pmod{4} \), we have \( \chi(-1) = -1 \) (Exercise 1.6). Since the character is multiplicative, this ensures that \( \chi(a-b) = -\chi(b-a) \), so there is exactly one directed edge between any two distinct vertices. This shows that \( P(q) \) is a tournament. (We also need to note that \( \chi(0) = 0 \), so there are no loops in the digraph.)

**Theorem 4.2 (Graham-Spencer)** If \( q \equiv -1 \pmod{4} \) and \( q \geq k^24^k \), then \( P(q) \) is a \( k \)-paradoxical tournament.

**Proof:** Let \( A = \{a_1, \ldots, a_k\} \subset V \) be an arbitrary \( k \)-subset. Let \( N = \#\{x \in V : x \rightarrow A\} \) be the number of vertices which dominate the set \( A \). We seek to show that \( N > 0 \). In fact, we will show that \( N \approx \frac{q}{2^k} \).

Consider the following three cases:

- \( x \rightarrow A \Rightarrow (\forall i)(\chi(x-a_i) = 1) \).
- \( x \not\rightarrow A \) and \( x \notin A \Rightarrow (\forall i)(\chi(x-a_i) = \pm 1) \) and \( (\exists i)(\chi(x-a_i) = -1) \).
- \( x \in A \Rightarrow (\exists i)(\chi(x-a_i) = 0) \).

Now let \( \psi(x) := \prod_{i=1}^{k}(\chi(x-a_i) + 1) \). Considering the cases above, we have

\[
\psi(x) = \begin{cases} 
2^k, & x \rightarrow A \\
0, & x \not\rightarrow A, x \notin A \\
0 \text{ or } 2^{k-1}, & x \in A 
\end{cases}
\]

The case \( \psi(x) = 2^{k-1} \) occurs for at most one \( x \in A \); namely, if and only if \( x \) dominates the rest of \( A \).
Thus, we can compute the sum
\[ S := \sum_{x \in \mathbb{F}_q} \psi(x) = 2^k N + \epsilon 2^{k-1}, \]
where \( \epsilon \in \{0, 1\} \). We will have succeeded in showing that \( N > 0 \) if we can prove that \( S \) is large (\( S > 2^{k-1} \) will suffice).

Using the notation \( [k] := \{1, \ldots, k\} \), we obtain the expansion
\[
S = \sum_{x \in \mathbb{F}_q} \prod_{i=1}^k (\chi(x - a_i) + 1) = \sum_{x \in \mathbb{F}_q} \sum_{I \subseteq [k]} \prod_{i \in I} \chi(x - a_i).
\]

Letting \( f_I(x) := \prod_{i \in I} (x - a_i) \) and using the multiplicativity of \( \chi \) we see that
\[ S = \sum_{x \in \mathbb{F}_q} \sum_{I \subseteq [k]} \chi(f_I(x)) = \sum_{I \subseteq [k]} \sum_{x \in \mathbb{F}_q} \chi(f_I(x)) = \sum_{x \in \mathbb{F}_q} \chi(f_{\emptyset}(x)) + \sum_{I \neq \emptyset} \sum_{x \in \mathbb{F}_q} \chi(f_I(x)). \]

Let us denote by \( R \) the rest of the sum: \( R := \sum_{I \neq \emptyset} \sum_{x \in \mathbb{F}_q} \chi(f_I(x)) \). Since the empty product is 1 and \( \chi(1) = 1 \), we have \( S = (\sum_{I \subseteq [k]} 1) + R = q + R \). If we can show that \( q \) dominates \( R \) then we shall be done since then \( N \approx S/2^k \approx q/2^k \), as desired.

Now
\[
|R| = \left| \sum_{I \neq \emptyset} \sum_{x \in \mathbb{F}_q} \chi(f_I(x)) \right| \leq \sum_{I \neq \emptyset} \left| \sum_{x \in \mathbb{F}_q} \chi(f_I(x)) \right| \leq \sum_{I \neq \emptyset} (|I| - 1) \sqrt{q} \quad \text{(by Weil)}.
\]

Note we can apply Weil because \( f_I \), by definition, has no multiple roots, so in particular \( f_I(x) \neq c (h(x))^2 \). There are \( 2^k \) choices for \( I \subseteq [k] \) and, for each choice, \( |I| \leq k \). Thus, we have shown that \( |R| < 2^k \cdot (k - 1) \sqrt{q} \).

From above, \( S = 2^k N + \epsilon 2^{k-1} = q + R \), so
\[ N > \frac{q}{2^k} - (k - 1) \sqrt{q} - \frac{1}{2} > \frac{q}{2^k} - k \sqrt{q}. \]

So for \( N > 0 \) it suffices that \( \frac{q}{2^k} \geq k \sqrt{q} \), i.e., \( q \geq k^2 4^k \). \( \square \)