REU 2006 · Discrete Math · Lecture 9

Instructor: László Babai
Scribe: Travis Schedler
Editor: Sourav Chakraborty

July 14, 2006. Last updated July 15, 2006 at 4 p.m.
NOT PROOF-READ

9.1 Character of a group

Definition 9.1.1. A **character** of a group G is a homomorphism $\chi : G \to \mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ (homomorphism means $\chi(ab) = \chi(a)\chi(b)$).

Now, let $\mathbb{F}$ be a finite field. We can define two types of characters:

Definition 9.1.2. A **multiplicative character** of $\mathbb{F}$ is a character of the group $\mathbb{F}^\times = \mathbb{F}\setminus\{0\}$ under multiplication. That is, $\chi : \mathbb{F}^\times \to \mathbb{T}$. We formally set $\chi(0) = 0$ to extend to $F \to \mathbb{T} \cup \{0\}$.

Definition 9.1.3. An **additive character** of $\mathbb{F}$ is a character of the additive group $\mathbb{F}$, i.e. a map $\chi : (\mathbb{F}, +) \to \mathbb{T}$, with $\chi(a + b) = \chi(a)\chi(b)$.

Now, let $\mathbb{F}_q$ denote the field of order $q = p^k$. We can define it by $\mathbb{F}_q := \mathbb{F}_p[x]/(f)$, where f is any irreducible polynomial of degree k.

We know that $\mathbb{F}_q^\times$ is a cyclic group of order $q - 1$, and is generated by some $g \in \mathbb{F}_q^\times$ (in other word $\mathbb{F}_q^\times = \langle g\rangle$). That is, $g^{q-1} = 1$ and no smaller positive power of g is 1. We have $(\chi(g))^{q-1} = \chi(g^{q-1}) = 1$ for any multiplicative character g. So characters correspond to a choice of primitive $(q - 1)$-st root of unity ω, so that $\chi(g) = \omega$. Then, for any element $x = g^\ell \in \mathbb{F}_q^\times$, we have $\chi(x) = \chi(g^\ell) = \omega^\ell$.

In general, we have

Definition 9.1.4. The **order** of a multiplicative character χ is the smallest positive integer m such that $\chi^m(x) = 1$ for all $x \in \mathbb{F}_q^\times$. A **quadratic character** is a character of order 2.

Exercise 9.1.5. *If q is an odd prime number then $\mathbb{F}_q^\times$ has a unique quadratic character. (Hint: $\chi(g) = -1$ and $\chi(g^\ell) = (-1)^\ell$.)*

Let us return our attention to $\mathbb{F}_p^\times$ for the moment, where p is prime. We may define the **Legendre symbol** as follows: Let χ be the unique quadratic character. For $a \in \mathbb{F}_p^\times$, set $\left(\frac{a}{p}\right) = \chi(a)$.

We turn our attention back to a general field $\mathbb{F}_q$ with $q = p^k$. André Weil's character sum estimate is then given as follows:

Theorem 9.1.6. *(André Weil's character sum estimate) Let $\chi : \mathbb{F}_q^\times \to \mathbb{T}, \chi(0) = 0$, and let f be a polynomial. Then*

$$|\sum_{x \in \mathbb{F}_q} \chi(f(x))| < (d-1)\sqrt{q}, \tag{9.1.1}$$

where $d = \deg f, t =$ order of χ, unless $f = cg^t$.

9.2 Paley Tournament

Recall the **Paley tournament:** We have $p \equiv -1 \pmod 4$, i.e. $\left(\frac{-1}{p}\right) = -1$. We have $V = \{0, 1, \ldots, p-1\}$ and $i \to j$ if $\left(\frac{i-j}{p}\right) = 1$.

If there is a directed edge from vertex i to vertex j then we say i beats j. If i beats all the elements in a set A then we say $x \to A$.

Theorem 9.2.1. $(\forall k)(\exists p_0)$ *such that if $p > p_0$ then the Paley tournament is k-embarassing, that is, $\forall A \subset V, |A| = k$, there exists x such thar x beats all the vertices in A*

Proof. Let $A = \{a_1, \ldots, a_k\}$, and $\chi(a) = \left(\frac{a}{p}\right)$. Let $N = \#\{x \mid \chi(x - a_1) = \cdots = \chi(x - a_k) = 1\}$. We "expect" $N \approx \frac{p}{2^k}$. Now,

$$\frac{1}{2^k} \sum_{x \in \mathbb{F}_p} \prod_{i=1}^{k} (\chi(x - a_i) + 1) = N + \frac{\mu}{2}, \tag{9.2.1}$$

with $\mu = 0$ or 1. If $x \to A$, it contributes 1 to the sum. If x is beaten by anyone in A, it contributes 0. If $x \in A$ and beats $A \setminus \{x\}$, it's contribution is $2^{k-1}/2^k = \frac{1}{2}$.

Now, we have

$$2^k(N + \frac{\mu}{2}) = \sum_{x \in \mathbb{F}_p} \prod_{i=1}^{k} (\chi(x - a_i) + 1) = \sum_{x \in \mathbb{F}_p} \sum_{I \subset \{1, \ldots, k\}} \prod_{i \in I} \chi(x - a_i). \tag{9.2.2}$$

This is because

$$\prod_{i=1}^{k} (1 + z_i) = \sum_{I \subset \{1, \ldots, k\}} \prod_{i \in I} z_i, \tag{9.2.3}$$

To simplify (9.2.2), set $f_I(x) := \prod_{i \in I} \chi(x - a_i)$, with $f_\emptyset(x) := 1$. Then (9.2.2) becomes

$$\sum_{I \subset \{1, \ldots, k\}} \sum_{x \in \mathbb{F}_p} \chi(f_I(x)) = p + R, \tag{9.2.4}$$

where p comes from $I = \emptyset$, and R comes from $I \neq \emptyset$. We have

$$|R| = |\sum_{\emptyset \neq I \subset \{1, \ldots, k\}} \sum_{x \in \mathbb{F}_p} \chi(f_I(x))| \leq \sum_{\emptyset \neq I \subset \{1, \ldots, k\}} |\sum_{x \in \mathbb{F}_p} \chi(f_I(x))| < k 2^k \sqrt{p}. \tag{9.2.5}$$

The last inequality uses "Weil's Character Sum Estimate," because the inside sum is less than $(|I|-1)\sqrt{p} < k\sqrt{p}$. We used the triangle inequality, $|a+b| \leq |a|+|b|$ in the first inequality.

Now, $w^k(N+\frac{\mu}{2}) = p+R$, and $|2^k(N+\frac{\mu}{2})-p| < k2^k\sqrt{p}$. So

$$\begin{aligned} 2^k(N+\frac{\mu}{2}) &> p-k2^k\sqrt{p} \\ \Longrightarrow \qquad 2^kN &> p-2^k(k\sqrt{p}+\tfrac{1}{2}) \end{aligned}$$

Hence 2^kN will be >0 if $p > 2^k(k\sqrt{p}+\frac{1}{2})$. Hence the Paley tournament is k-embarassing is

$$p > k^2 2^{2k}. \tag{9.2.6}$$

□

9.3 Chromatic Number and Girth of a graph

Let us consider graphs that are not 3^k-colorable but does not contain any K_3 (a K_3 would immediately require all three have different colors).

Let's consider **Kneser's graph**: $K(r,s)$ for $r \geq 2s+1$, has $\binom{r}{s}$ vertices, labeled by s-subsets of $\{1,\ldots,r\}$. For any $A \subset \{1,\ldots,r\}$, $|A| = s$, call the associated vertex v_A. Then, we have $v_A \sim v_B$ if $A \cap B = \emptyset$. This is a generalization of Peterson's graph, which is the smallest case, $K(5,2)$.

Observation 9.3.1. $\chi(K(r,s)) \leq r-2s+2$.

Proof. Take all s-subsets that contain the number 1: a large independent set of vertices. The number of such subsets is $\binom{r-1}{s-1}$. Let's color all of this #1. For the remaining sets, color 2 those sets that contain the number 2. Is the number of colors needed r? Well, once we get down to only $2s-1$ numbers left, then all s-subsets in those are independent: so we can stop there. That is, we only need to use $r-2s+2$ colors: i.e. $\chi(K(r,s)) \leq r-2s+2$. □

In fact, Lovasz showed in 1980 that this is an equality: the chromatic number **equals** $r-2s+2$.

Now when does Kneser's graph not contain triangles? If $r < 3s$ the Kneser's graph has a triangle as then there are no 3 mutually disjoint subsets of size s).

So for a Kneser's graph to have no triangle $3s > r \geq 2s+1$: infact for such choices of r and s, the graph will not contain triangles.

On the other hand, Kneser's graph will contain large bipartite graphs (e.g. by partitioning $\{1,\ldots,r\}$ into two disjoint subsets.) So it turns out that it's much easier to avoid 3-cycles than to avoid large bipartite graphs. In fact, we can avoid 3-cycles, 5-cycles, and 7-cycles: still using Kneser's graph.

Exercise 9.3.2. Find parameters of Kneser's graph such that $\chi > 1000$ and the graph does not contain any **odd** cycles of length less than 100.

The question is, what do we do about even cycles? Can we avoid C_4, for example?

Theorem 9.3.3. *(Erdős) $\forall g, k$, $\exists$ a graph of girth $> g$ and $\chi \geq k$.*

(Recall that **girth** is one the length of the shortest cycle occurring in the graph. So girth $> g$ means that there are no cycles of length $\leq g$.)

Proof. (Sketch) Pick n vertices, and choose edges independently with probability $p = \frac{n^\varepsilon}{n} = n^{\varepsilon-1}$. That is, we pick the edges by "flipping a biased coin" so that it's not that likely we'll put an edge in each place, but it will happen sometimes with probability $n^{\varepsilon-1}$. So, $E(\text{degree of a given vertex}) \approx n^\epsilon$ (for large n). The goal is to show that there is no independent set of size $\geq \frac{n}{k}$, thus showing that $\chi \geq k$. Then, we want to show that there are no cycles of size $\leq g$.

Now, if $A \subset \{1, \ldots, n\}$, with $|A| = t$, then

$$P(A \text{ is independent}) = (1-p)^{\binom{t}{2}}$$

(remember independent means no edges are in A). So,

$$P(\exists \text{independent set of size } t) < \binom{n}{t}(1-p)^{\binom{t}{2}}$$

Therefore, we conclude, for example, that if $\binom{n}{t}(1-p)^{\binom{t}{2}} < \frac{1}{100}$, then

$$P(\exists \text{independent set of size } t) < \frac{1}{100}$$

We need $t = \frac{n}{2k}$.

Now, $P(\text{a given cycle of length } \ell \text{ is in } G) = p^\ell$. Then, the number of constructible cycles of length ℓ is $n(n-1)\cdots(n-\ell+1) < n^\ell$. So $E(\#\text{cycles of length } \ell) < (np)^\ell$. Also,

$$\sum_{\ell=1}^{g} (np)^\ell \approx (np)^g = n^{\varepsilon g}, \tag{9.3.1}$$

since $np = n^\varepsilon$. At the same time, we can make sure that the chromatic number $\chi > \frac{n/2}{n/2k} = k$. So this gives us what we want. $\square$

It was very difficult to actually give a construction of such a graph, which was finally done in 1980. It was done by taking the Cayley graph of the group $PSL(2,q)$ for appropriate choices of generators (this actually was done to find a graph with linear isoperimetric inequality, and in fact having a large eigenvalue gap in the eigenvalues of the adjacency matrix/Laplacian.)