Character Sums and Generating Sets

Ming-Deh A. Huang, Lian Liu

University of Southern California

July 14, 2015

Introduction

Let p be a prime number, $f \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree $d \geq 2$ and $q = p^d$ be a prime power.

Theorem (Chung)

Given $\mathbb{F}_q \cong \mathbb{F}_p[x]/f$, if $\sqrt{p} > d - 1$, then $\mathbb{F}_p + x$ is a generating set for $\mathbb{F}_q^{\times}$.

$\mathbb{F}_p + x := \{a + x | a \in \mathbb{F}_p\}$

Today's topic

Today, we will discuss more on the relationship between character sums and group generating sets. To illustrate, we will take a detailed look the multiplicative group of the algebra $A^{\times}$, where A is of the form:

$$A := \mathbb{F}_p[x] \big/ f^e$$

where $e \geq 1$ is an integer.

Outline

Question

- *Given $S \subseteq A^\times$ a subset of elements, what are the sufficient or necessary conditions for S to generate $A^\times$?*
- *How to construct a small generating set for $A^\times$?*
- *How strong are the above sufficient conditions for generating sets? Can they be substantially weakened in practice?*

Difference graphs

Given G, a nontrivial finite abelian group and $S \subseteq G$ a subset of elements, the difference graph $\mathcal{G}$ defined by the pair (G, S) is constructed as follows:

Algorithm

1. `For each element` $g \in G$, `create a vertex` g `in` $\mathcal{G}$;
2. `Create an arc` $g \to h$ `in` $\mathcal{G}$ `if and only if` $gs = h$ `for some` $s \in S$.

E.g., in Chung's situation, $G = \mathbb{F}_q^\times \cong (\mathbb{F}_p[x]/f)^\times$ and $S = x + \mathbb{F}_p$.

Lemma

If $\mathcal{G}$ has a finite diameter, then S is a generating set for G.

Diameters and eigenvalues

Theorem (Chung)

Suppose a k-regular directed graph G which has out-degree k for every vertex, and the eigenvectors of its adjacency matrix form an orthogonal basis. Then

$$\mathbf{diam}(G) \leq \left\lceil \frac{\log(n-1)}{log(\frac{k}{\lambda})} \right\rceil$$

where n is the number of vertices and λ is the second largest eigenvalue (in absolute value) of the adjacency matrix.

Adjacency matrices defined on general finite abelian groups

Assume that G is any nontrivial finite abelian group, and assume the adjacency matrix, M, of $\mathcal{G} := (G, S)$ has rows and columns indexed by $g_1, \ldots, g_n \in G$:

$$
\begin{array}{c c}
 & \begin{array}{ccccccc} g_1 & \cdots & & g_j & & \cdots & g_n \end{array} \\
\begin{array}{c} g_1 \\ \vdots \\ g_i \\ \vdots \\ g_n \end{array} &
\begin{pmatrix}
 & & & \vdots & & & \\
 & & & \vdots & & & \\
\cdots & \cdots & & \mathbb{I}[\exists s \in S : g_j = s g_i] & & \cdots & \cdots \\
 & & & \vdots & & & \\
 & & & \vdots & & &
\end{pmatrix}
\end{array}
$$

Dirichlet character sums

Let G be any nontrivial finite abelian group. Then

$$G \cong \mathbb{Z}_{d_1} \oplus \ldots \oplus \mathbb{Z}_{d_k}$$

for some integers $d_i > 1$.
Consider Dirichlet characters $\chi : G \to \mathbb{C}^\times$ of the following form:

$$g \cong (g_1, \ldots, g_k) \to \prod_i \omega_{d_i}^{g_i}$$

for every $g \in G$, where ω_{d_i} is a d_i^{th} root of unity.

A generalization of Chung's results

The adjacency matrix M has the following properties:

Lemma

The eigenvectors of M are $[\chi(g_1), \ldots, \chi(g_n)]^\top$, and the corresponding eigenvalutes are $\sum_{s \in S} \chi(s)$.

Lemma

The set of eigenvectors $[\chi(g_1), \ldots, \chi(g_n)]^\top$ form an orthogonal basis for $\mathbb{C}^n$.

A generalization of Chung's results

Following the diameter theorem for directed graphs, we may generalize Chung's results to obtain

Theorem (Main)

If

$$\left|\sum_{s\in S}\chi(s)\right| < |S|$$

for every nontrivial Dirichlet character χ of G, then S is a generating set for G.

The structure of $A^\times$

Now let us consider groups of the form $A := \mathbb{F}_p[x]/f^e$. Recall that $f \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree $d \geq 2$ and $e \geq 1$ is an integer.

Lemma (Decomposition)

If $p \geq e$, then

$$A^\times \cong \mathbb{Z}_{p^d-1} \oplus \left(\bigoplus_{d(e-1)} \mathbb{Z}_p \right)$$

Theorem

If $p \geq e$, then any generating set of $A^\times$ contains at least $d(e-1)+1$ elements.

The structure of $A^\times$

This isomorphism allows us to define a Dirichlet character from $A^\times$ to the unit circle. For every $\alpha \in A^\times$,

$$\chi : \alpha \to \omega \prod_{i=1}^{d(e-1)} \theta_i$$

where ω is a $(p^d - 1)^{\text{th}}$ root of unity and each θ_i is a p^{th} root of unity. χ is trivial if ω and every θ_i equals 1.

A as an $\mathbb{F}_p$-algebra

Let us first consider if the set of linear elements $S = \mathbb{F}_p - x$ generates $A^\times$.

Theorem (Katz, Lenstra)

Given $\mathbb{F}_q$ a finite filed and B an arbitrary finite n-dimensional commutative $\mathbb{F}_q$-algebra. For any nontrivial complex-valued multiplicative character χ on $B^\times$, extended by zero all of B,

$$\left| \sum_{a \in \mathbb{F}_q} \chi(a - x) \right| \leq (n-1)\sqrt{q}$$

A as an $\mathbb{F}_p$-algebra

Since A can be naturally regarded as an $\mathbb{F}_p$-algebra of dimension de, by the Main theorem we get

Theorem

If $\sqrt{p} > de - 1$, then $\mathbb{F}_p - x$ is a generating set for $A^\times$. Furthermore, every element $\alpha \in A^\times$ can be written as $\prod_{i=1}^{m}(a_i - x)$ where $a_i \in \mathbb{F}_q$ and

$$m < 2de + 1 + \frac{4de\log(de-1)}{\log p - 2\log(de-1)}$$

More on the structure of $A^\times$

The constraint $\sqrt{p} > de - 1$ might be critical on the size of the base field $\mathbb{F}_p$, and hence we wonder whether we can use other base fields of A to build generating sets in a similar way.
One candidate base field is $\mathbb{F}_q := \mathbb{F}_p[x]/f$, and we proved that A is indeed an $\mathbb{F}_q$-algebra:

Lemma

A is an $\mathbb{F}_q$-algebra of dimension e, and there exists a embedding $\pi : \mathbb{F}_q \to A$ such that $\mathbb{F}_q \cong \pi(\mathbb{F}_q)$ as rings.

The embedding

Given an element $a \in \mathbb{F}_q^\times$, the image $\pi(a)$ is uniquely determined by the following constraints:

- $\pi(a) \equiv a \pmod{f}$;
- $(\pi(a))^{q-1} \equiv 1 \pmod{f^e}$.

We extend the embedding to all of $\mathbb{F}_q$ by enforcing $\pi(0) = 0$.
Each image can be computed with $O(de \log p)$ group operations in $(\mathbb{F}_p[x]/f^i)^\times$ where $1 \le i \le e$.

Knowing that A as an $\mathbb{F}_q$-algebra of dimension e, we may similarly consider whether or not the set $\pi(\mathbb{F}_q) - x$ generates $A^\times$. Again, by Katz and Lenstra's character sum theorem, we have

Theorem

If $p \geq e$, then $\pi(\mathbb{F}_q) - x$ is a generating set for $A^\times$. Furthermore, every element $\alpha \in A^\times$ can be written as $\prod_{i=1}^{m} (\pi(a_i) - x)$ where $a_i \in \mathbb{F}_q$ and

$$m < 2e + 1 + \frac{4e\log(e-1)}{d\log p - 2\log(e-1)}$$

Constructing a small generating set

Based on previous discussions we observe that

- $\mathbb{F}_p - x$ generates $A^\times$ if $\sqrt{p} > de - 1$, but requires p to be large;
- $\pi(\mathbb{F}_q) - x$ generates $A^\times$ if $p \geq e$, but might be over-killing;
- Next step: take a *nice* subfield $K \subset \mathbb{F}_q$ and build a generating set from $\pi(K) - x$.

Constructing a small generating set

Let $K \subset \mathbb{F}_q$ be a subfield of size p^c where $c|d$. Then $\mathbb{F}_p[x]/f$ can be considered as an K-algebra of dimension de/c. Based on our previous discussion we can similarly show that

Theorem

If $p^{c/2} > de/c - 1$ and $p \geq e$, then $\pi(K) - x$ is a generating set for $A^\times$. Furthermore, every element $\alpha \in A^\times$ can be written as $\prod_{i=1}^{m} (\pi(a_i) - x)$ where $a_i \in K$ and

$$m < 2\frac{de}{c} + 1 + \frac{4\frac{de}{c}\log(\frac{de}{c} - 1)}{\frac{d}{c}\log p - 2\log(\frac{de}{c} - 1)}$$

Constructing a small generating set

Now we conclude the algorithm for constructing the smallest generating set for $A^\times$ in the situation that $p \geq e$:

Algorithm

1. `Find the smallest` c `such that` $c|d$ `which satisfies` $p^{c/2} > de/c - 1$`;`
2. `Take the subfield` $K \subset \mathbb{F}_q$ `of size` p^c `and return` $\pi(K) - x$ `as a generating set for` $A^\times$`.`

Theorem

Given fixed p and e with $p \geq e$, *if d is a perfect power, then there is (constructively) a generating set for* $A^\times$ *of size* $p^{O(\log d)}$.

Experiments

In the following experiments, we compare the size of the following three types of generating sets for $A^\times$:

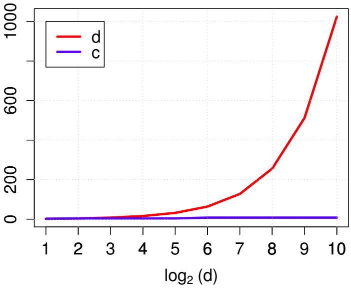
- $S := \pi(\mathbb{F}_q) - x$, the size is equal to p^d;
- $S^* := \pi(K) - x$, the size is equal to p^c;
- $\tilde{S}^*$, the set generated by adding elements in S^* one-by-one to $\emptyset$, until it generates the whole group. We denote its size as p^b for some real number b.

Obviously, we have $b \leq c \leq d$. Also note that $\tilde{S}^*$ might still be much bigger than the real smallest generating set.

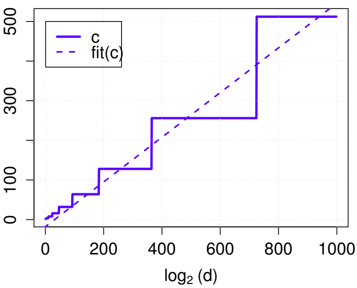
The relationship between c and d

Experiment setting:

- $p = 7, e = 5$;
- $d = 2^1, 2^2, 2^3, \ldots$.



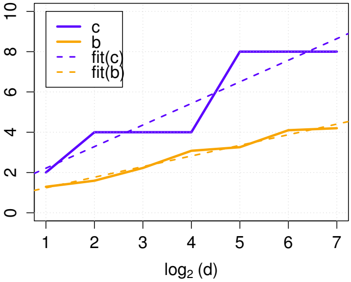
(a) Comparison between c and d



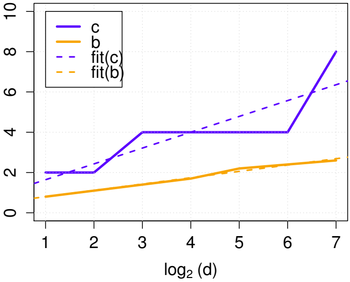
(b) The logarithmic growth of c

The relationship between c and b

- $d = 2^1, 2^2, 2^3, \ldots;$
- fix $e = 4$ and increase the value of p.



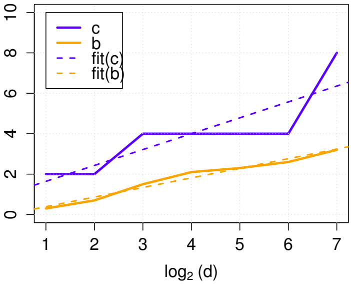
(c) $p = 5, e = 4$



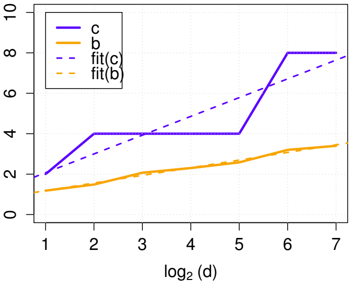
(d) $p = 11, e = 4$

The relationship between c and b

- $d = 2^1, 2^2, 2^3, \ldots;$
- fix $p = 7$ and increase the value of e.



(e) $p = 7, e = 3$



(f) $p = 7, e = 5$

Remarks and future work

We observe that both b and c grows linearly with $\log(d)$, and they may differ only by a constant ratio, i.e. $\tilde{S}^*$ is still of size $p^{O(\log d)}$ given d being a perfect power.

Problem

Given $p \geq e > 1$ and $f \in \mathbb{F}_p[x]$ an irreducible polynomial of degree d, a perfect power, how to construct a generating set of size $p^{o(\log d)}$ for the group $A^\times$?

Remarks and future work

A big assumption we made in our work is that $p \geq e$, which helps guarantee the decomposition of the group. It is therefore an important question to ask what if $p < e$?

Problem

If $p < e$, can we get similar results for the group $A^\times$?

Thanks! ☺Y