Constructing Small Generating Sets for the Multiplicative Groups of Algebras over Finite Fields

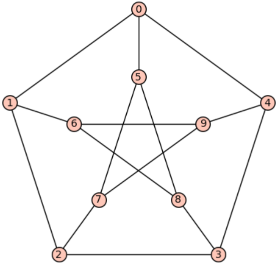
Ming-Deh Huang, Lian Liu

University of Southern California

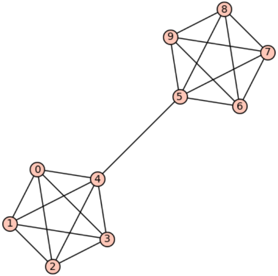
ISSAC'16, July 19-22

Motivation

Expander graphs are sparse graphs that are well connected. Intuitively, every small subset of vertices have a relatively large neighborhood.



(a) Petersen graph



(b) Barbell graph

Motivation

Properties of expander graphs:

- Large edge/vertex expansion;
- Small diameter;
- Fast mixing;
- Non-blocking;
- ...

Applications of expander graphs:

- Pseudorandom generators & extractors;
- Derandomization;
- Error-correcting codes;
- Communication networks;
- ...

How do we measure the "expansion" of a graph?

Let M be the adjacency matrix of an d-regular graph Γ (either directed or undirected), the spectrum of Γ is the sorted sequence of the eigenvalues of M:

$$d = |\lambda_1| \geq |\lambda_2| \geq \ldots \geq |\lambda_n|.$$

Definition (expander)

The eigenvalue of Γ is defined as $\lambda(\Gamma) := |\lambda_2|$. We call a d-regular graph Γ an (n, d, λ)-expander, or simply a λ-expander, if it has n vertices and $\lambda(\Gamma) \leq \lambda$.

Intuitively, for regular graphs with n and d fixed, smaller eigenvalue implies larger expansion.

How to construct expander graphs?

Two major types of approaches:

- Probabilistic constructions;
- Explicit constructions.

Most known explicit constructions are based on Cayley graphs.

Definition (Cayley graph)

Let G be a finite abelian group and $S \subseteq G$ be a subset of elements, the *Cayley graph* $\Gamma(G, S)$ is a directed graph where

- $g \in V(\Gamma)$ iff $g \in G$;
- $(g, h) \in E(\Gamma)$ iff $sg = h$ for some $s \in S$.

For simplicity, we say $\Gamma(G, S)$ is a *Cayley graph over* G.

Related work

Theorem (Chung)

Given $\mathbb{F}_q \simeq \mathbb{F}_p[x]/f$ a finite field of $q = p^d$ elements. Let $S = x + \mathbb{F}_p := \{x + a | a \in \mathbb{F}_p\}$. If $\sqrt{p} > n - 1$, then $\Gamma(\mathbb{F}_q^\times, S)$ is an $(n-1)\sqrt{p}$-expander.

Corollary

$x + \mathbb{F}_p$ is a generating set for $\mathbb{F}_q^\times$.

Our results

Part I: Expander construction

We present algorithms for constructing expander graphs over $B^{\times}$, where B is a finite algebra of the form $B := \mathbb{F}_p[x]/F$, and $F \in \mathbb{F}_p[x]$ is not necessarily irreducible. These expander constructions naturally gives different types of generating sets for $B^{\times}$.

Part II: Basis construction & decomposition

We study the structure of $B^{\times}$ and present algorithms for constructing a basis for $B^{\times}$ and decomposing elements w.r.t. the basis.

Expander graphs over finite commutative algebras

Notation

For simplicity of the presentation, we will focus on algebras of the form

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

where $f \in \mathbb{F}_p[x]$ is an irreducible polynomial and $e > 1$ is an integer. It's not hard to generalize all results to the general case via the Chinese Remainder isomorphism:

$$\psi : \bigoplus_{i=1}^{m} (\mathbb{F}_p[x]/f_i^{e_i})^\times \xrightarrow{\sim} (\mathbb{F}_p[x]/F)^\times,$$

where $F = \prod_i f_i^{e_i}$.

Eigenvalues of Cayley graphs

Eigenvalues of Cayley graphs are character sums:

Lemma

Let M be the adjacency matrix of $\Gamma(G, S)$, then the eigenvalues of M are of the form $\sum_{s \in S} \chi(s)$, where $\chi : G \xrightarrow{\sim} \mathbb{C}^*$ is a character of G.

Upper bounds for character sums

Theorem (Katz, Lenstra, Weil)

Let B be an arbitrary finite n-dimensional commutative $\mathbb{F}_q$-algebra and x be an element of B. If χ is a character of the multiplicative group $B^\times$ (extended by zero to all of B) which is non-trivial on $\mathbb{F}_q[x]$, then

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

The first small generating set

Since $A = \mathbb{F}_p[x]/f$ can be naturally regarded as an $\mathbb{F}_p$-algebra of dimension de, the following theorem is a quick consequence:

Theorem

If $\sqrt{p} > de - 1$, then $\Gamma(A^\times, \mathbb{F}_p - x)$ is an $(ne-1)p^{1/2}$-expander.

Corollary

If $\sqrt{p} > de - 1$, then $\mathbb{F}_p - x$ is a generating set of $A^\times$.

Question

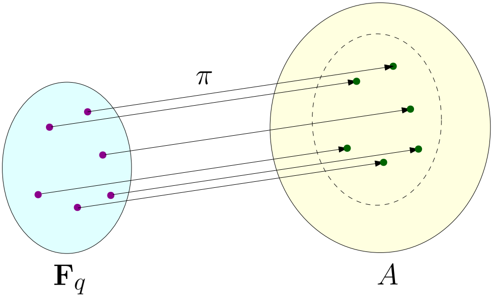
What if p is small but d, e are large?

Embed $\mathbb{F}_q$ into A

For the case $\sqrt{p} \leq de - 1$, we present an embedding

$$\pi : \mathbb{F}_q \simeq \mathbb{F}_p[x]/f \rightarrowtail A$$

such that $\pi(\mathbb{F}_q) \simeq \mathbb{F}_q$ as fields.



How to compute the embedding?

The embedding $\pi : \mathbb{F}_p[x]/f \to \mathbb{F}_p/f^e$ is computed based on

Lemma

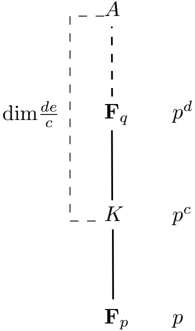
For each $a_0 \in \mathbb{F}_q^\times$, there exists a unique $a \in A^\times$ such that

$$\begin{cases} a = a_0 & \pmod{f}, \\ a^{q-1} = a_0 & \pmod{f^e}. \end{cases}$$

Given a_0, we assume $\pi(a_0) = a = \sum_{i=1}^{d-1} a_i f^i$, where $\deg a_i < d$ for all i. We show that each a_i is uniquely determined, and can be computed efficiently.

Expander graphs over $A^\times$ and generating sets

The embedding gives us a way to "enlarge" the ground field of A.



Theorem

If K is a subfield of $\mathbb{F}_q$ of size p^c where $c|d$ and $p^{c/2} > de/c - 1$, then $\Gamma(A^\times, \pi(K) - x)$ is an $(de/c - 1)p^{c/2}$-expander.

Corollary

If $p^{c/2} > de/c - 1$, then $\pi(K) - x$ is a generating set for $A^\times$.

Basis construction and decomposition

The structure of $A^\times$

Consider the map

$$\phi : A^\times \to \mathbb{F}_p[x]/f \text{ s.t. } \phi(a) = a \mod f.$$

It's easy to see that $\ker\phi = \{1 + af \,|\, \deg a < d(e-1)\}$. When $p \geq e$, it holds that $(1+af)^p = 1 + a^p f^p = 1 \pmod{p^e}$. Thereby, we have

Lemma

If $p \geq e$, then

$$A^\times = \pi(\mathbb{F}_q^\times) \times \ker\phi \simeq \mathbb{Z}/(p^d - 1)\mathbb{Z} \oplus \left(\bigoplus_{d(e-1)} \mathbb{Z}/p\mathbb{Z} \right).$$

Basis construction

$A^\times = \pi(\mathbb{F}_q^\times) \times \ker\phi$.

- For the first component, the problem reduces to finding a primitive element for $\mathbb{F}_q$;
- For the second component, we prove that

Lemma

The set $\{1 + x^k f^j | 0 \leq k \leq d-1, 1 \leq j \leq e-1\}$ *forms a basis for* $\ker\phi$*.*

Decomposition

Given an element $a = \sum_{i=0}^{d-1} a_i f^i \in A^\times$, we first write $a = \pi(a_0) \cdot k$, where $k \in \ker \phi$.

- Clearly, finding the coordinate of a in $\mathbb{Z}/(p^d - 1)\mathbb{Z}$ is equivalent to finding the discrete-log of a_0;
- The decomposition of k in $\bigoplus_{d(e-1)} \mathbb{Z}/p\mathbb{Z}$ can be computed efficiently via the filteration

$$K_1 \supsetneq K_2 \supsetneq \ldots \supsetneq K_e,$$

where each $K_j := \{1 + af^j \mod f^e\}$. We omit the details here.

Experiments and future work

Figure: $p = 5, e = 4$

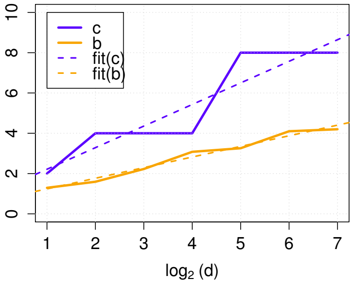
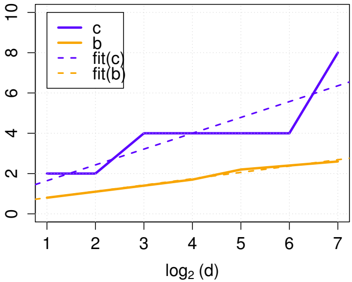


Figure: $p = 11, e = 4$



Experiments and future work

Figure: $p = 7, e = 3$

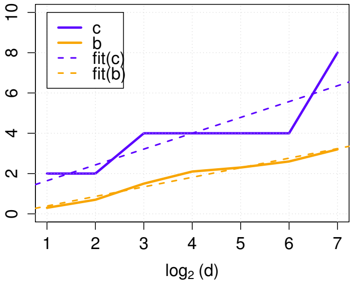
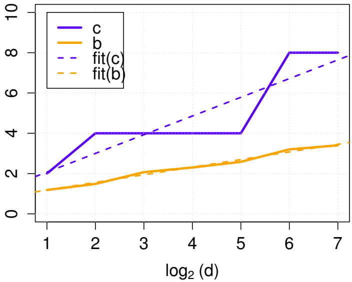


Figure: $p = 7, e = 5$



Thanks! Questions?