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

Ming-Deh Huang
Department of Computer Science
University of Southern California
Los Angeles, CA 90089
mdhuang@usc.edu

Lian Liu
Department of Computer Science
University of Southern California
Los Angeles, CA 90089
lianliu@usc.edu

ABSTRACT

We consider computational problems concerning algebras over finite fields. In particular, we propose an algorithm for finding a small generating set for the multiplicative group of $\mathbb{F}_p[x]/F$, where p is a prime number and $F \in \mathbb{F}_p[x]$ is an arbitrary polynomial. Based on this result, a new set of expander graphs can be explicitly constructed. In addition, we present algorithms for basis construction and decomposition of a given element with respect to the basis.

CCS Concepts

•Theory of computation → Expander graphs and randomness extractors; •Computing methodologies → Algebraic algorithms; •Mathematics of computing → Spectra of graphs;

Keywords

computational algebra; generating sets; character sums; expander graphs

1. INTRODUCTION

In computational algebra, it is often desired to find small generating sets for given groups. This problem has many applications. For example, in the index calculus method for solving the discrete logarithm problem over the multiplicative groups of finite fields, one is interested in finding a reasonably small generating set over which enough relations can be found [2, 11]. Generating sets are also involved in explicit construction of expander graphs [4, 13]. Informally, expander graphs are graphs with strong expansion properties. They have been applied in many areas including computational complexity theory, coding theory and communication networks [6, 9].

In this paper we are interested in finding small generating sets for the multiplicative groups of algebras of the form $B := \mathbb{F}_p[x]/F$, where p is a prime number and $F \in \mathbb{F}_p[x]$ is an arbitrary polynomial.

ISSAC '16, July 19 - 22, 2016, Waterloo, ON, Canada

ISBN 978-1-4503-4380-0/16/07…$15.00

DOI: http://dx.doi.org/10.1145/2930889.2930921

When F is irreducible of degree d, a fundamental result of Chung [4] states that if $\sqrt{p} > d-1$, then the set $x+\mathbb{F}_p := \{x+t : t \in \mathbb{F}_p\}$ forms a generating set for $\mathbb{F}_q^\times \simeq (\mathbb{F}_p[x]/F)^\times$, where $q := p^d$. In addition, the *Cayley graphs* built on $\mathbb{F}_q^\times$ with the generating set $x+\mathbb{F}_p$, with $q = p^d$ and $\sqrt{p} > d-1$, form a set of expander graphs.

A goal of this paper is to generalize Chung's results [4] to the general case of $B := \mathbb{F}_p[x]/F$ where F is not necessarily irreducible. In Section 3.1, we present algorithms for finding different types of generating sets for $B^\times$. We also show that they offer more flexibility for expander graph construction.

Another issue discussed in this paper is the construction of a basis for $B^\times$ and the decomposition of elements in $B^\times$ with respect to the basis. In the special case where F is irreducible, the problem of finding a basis for $B^\times := (\mathbb{F}_p[x]/F)^\times$ is also called finding a *primitive element* for the finite field $\mathbb{F}_p[x]/F$, which is known to be hard in general [10]. In fact, it is an important open problem which has not yet been fully settled. However, there are existing algorithms for solving its relaxations or special cases under certain assumptions. For example, in [18] and its extensions [15], the author showed that for certain (p, d) pairs, elements of high order can be constructed using Gauss periods. And in [3, 10, 16], the authors addressed the special case of finding primitive elements in finite fields of small characteristics. The decomposition problem in this special case is better known as the *discrete logarithm* problem, which is a classic hard problem that has been extensively studied. Recent breakthroughs include Gologlu et. al. [8] and Joux [11], both of which compute discrete logarithms in finite fields of small characteristics faster than previously known under certain heuristics.

In Section 3.2, we analyze the structure of $B^\times$. We propose algorithms for finding a basis for $B^\times$ as well as decomposing elements with respect to this basis when p is relatively large. Both algorithms require an existing primitive element or discrete logarithm algorithm as their subroutine.

One of the goals of designing these algorithms is to validate the generating sets we proposed in Section 3.1. Since these algorithms enable us to test whether a given set of elements generates $B^\times$, we would be able to see whether or not our theoretically proven generating sets are actually larger than necessary. Our experimental results in Section 4 suggest that a square-root number of elements in our generating sets might already be sufficient to generate the entire group. However further investigation is required to determine whether this is indeed the case.

2. PRELIMINARIES

2.1 Character Sums

A *character* of a group G is a group homomorphism $\chi : G \to \mathbb{C}^*$. Clearly, sending all elements to 1 yields a character, which is called a *trivial character*, while all other characters are said to be *nontrivial*. We use $X(G)$ to denote the set of all distinct characters of G, and let $\tilde{X}(G)$ denote the set of all nontrivial characters of G. When G is a finite abelian group, we have $|X(G)| = |G|$, and the following fundamental property is known (see [9], Proposition 8.5):

PROPOSITION 1. *Assume a fixed order $g_1, \ldots, g_{|G|} \in G$ on the elements of G, then $\{(\chi(g_1), \ldots, \chi(g_{|G|}))|\chi \in X\}$ form a orthogonal basis for $\mathbb{C}^n$, where $n = |G|$.*

Character sums have been extensively studied in the past decades [5, 12, 14]. In particular, Weil's estimate [20] and its generalizations are important to our approach.

PROPOSITION 2. *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*

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

Proposition 2 was initially conjectured by Katz in [12]. Subsequently, Lenstra observed in his unpublished notes ("Multiplicative groups generated by linear expression") that the proposition actually follows as a consequence of Weil's character sum estimate [20]. We refer readers to [19] (Corollary 2.2) for details of this proposition.

2.2 Expanders and Cayley Graphs

Informally speaking, *expander graphs* (abbr. *expanders*) are sparse graphs which are well-connected. Intuitively, every small subset of vertices has a relatively large neighborhood. The expansion of a k-regular graph (or k-regular directed graph) Γ can be measured by its *spectral gap*, which is defined as $k - \lambda$, where λ is the second largest eigenvalue (in absolute value) of the adjacency matrix of Γ [9]. We say Γ is an (n, k, γ)-*expander* if it is a k-regular graph (or k-regular directed graph) with n vertices and its spectral gap is at least γ. In this paper, we would simply call Γ an *expander* if the parameters n, k, γ are clear from the context.

Cayley graphs have been used as a general technique for expander graph construction [4, 6, 9, 19]. Let G be a finite abelian group and $S \subseteq G$ be a subset of elements, the *Cayley graph* induced by G and S, denoted by $\Gamma(G, S)$, is the directed graph with vertex set G and for all $g, h \in G$, there is an directed edge $g \to h$ if and only if $sg = h$ for some $s \in S$. For simplicity, we say $\Gamma(G, S)$ is a Cayley graph over G. By construction, Cayley graphs are $|S|$-*regular directed graphs*, meaning that all vertices have the same in-degree and out-degree, both equaling $|S|$. In addition, S is a generating set of G if and only if $\Gamma(G, S)$ is strongly connected, or in other words, $\Gamma(G, S)$ has a finite diameter. Chung [4] showed that the diameter of a directed graph is related to the eigenvalues of its adjacency matrix:

PROPOSITION 3. *If a directed regular graph Γ with n vertices has out-degree k and the eigenvectors of its adjacency matrix M form an orthogonal basis, then*

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

where λ is the second largest eigenvalue (in absolute value) of M.

It is worth mentioning that a recent work by Shparlinski [17] showed that in the special case where Γ is a Cayley graph over $\mathbb{F}_q^\times$ induced by certain types of generating sets, this diameter bound can be improved.

A natural question to ask is what are the eigenvalues of a Cayley graph. It is easy to verify that the eigenvalues can be expressed as character sums (see [4, 9]):

PROPOSITION 4. *Let M be the adjacency matrix of $\Gamma(G, S)$. Assume the rows and columns are both indexed by $g_1, \ldots, g_{|G|}$, then the eigenvectors of M are $\{(\chi(g_1), \ldots, \chi(g_{|G|}))|\chi \in X(G)\}$ corresponding to eigenvalues $\{\sum_{s\in S} \chi(s)|\chi \in X(G)\}$.*

Combining Propositions 1, 3 and 4, we can see that S generates G if $|\sum_{s\in S} \chi(S)| < |S|$ for all nontrivial characters in $X(G)$. In expander graph construction, on one hand, we want the resulting graph, $\Gamma(G, S)$ to be sparse, so a small cardinality of S is desired. On the other hand, the spectral gap $\gamma = |S| - \lambda = |S| - \max_{\chi\in\tilde{X}(G)} |\sum_{s\in S} \chi(s)|$ should be large in order to guarantee a "large" expansion. In this paper, our goal is to find such a small generating set S for $B^\times$ so that the resulting Cayley graph $\Gamma(B^\times, S)$ is provably an expander.

3. ALGORITHMS

3.1 Generating Sets and Expander Graphs

Given the standard factorization of $F = \prod_{i=1}^m f_i^{e_i}$ where for all $1 \leq i \leq m$, f_i is irreducible, by Chinese Remainder Theorem, we have the isomorphism

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

where ψ can be computed using standard Chinese Remainder Theorem algorithms. We may first consider a simplified problem of finding a small generating set for each component on the left-hand side before handling the general case. Let $v_{i,s}^m \in \bigoplus_{i=1}^m A_i^\times$ where $A_i := \mathbb{F}_p[x]/f_i^{e_i}$ denote an m-dimensional vector with s in the i-th entry and zeros elsewhere. That is,

$$v_{i,s}^m := \underbrace{0 \oplus \ldots \oplus 0}_{i-1} \oplus s \oplus \underbrace{0 \oplus \ldots \oplus 0}_{m-i}.$$

Suppose a generating set S_i for $A_i^\times$ is given for all $1 \leq i \leq m$, then clearly, $\{\psi(v_{i,s}^m)|1 \leq i \leq m, s \in S_i\}$ would be a generating set for $B^\times$. Therefore, in Sections 3.1.1, 3.1.2 and 3.1.3, we will focus our discussion on finding a small generating set for the multiplicative groups of algebras $A := \mathbb{F}_p[x]/f^e$, where $f \in \mathbb{F}_p[x]$ stands for an irreducible polynomial of degree $d \geq 1$, and $e \geq 1$ is an integer. Note that we will use A as the abbreviation for $\mathbb{F}_p[x]/f^e$. When $e = 1$, we are done, since $x + \mathbb{F}_p$ is a generating set for $A^\times$, which directly follows from Chung [4]. Therefore, in Sections 3.1.1, 3.1.2 and 3.1.3, we will assume $e > 1$.

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

Observe that A can be naturally regarded as an $\mathbb{F}_p$-algebra. Based on this observation, we obtain the first type of small generating sets for $A^\times$, as stated in Theorem 1.

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

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

PROOF. A is an $\mathbb{F}_p$-algebra having dimension de, by Proposition 2, for all nontrivial character χ of $A^\times$ (extended by zero to all of A),

$$\left| \sum_{t \in \mathbb{F}_p} \chi(t-x) \right| \le (de-1)\sqrt{p}. \tag{2}$$

The rest of the proof follows from Propositions 3 and 4. □

THEOREM 2. *If $\sqrt{p} > de - 1$, then $\Gamma(A^\times, S)$ is an expander, where $S = (\mathbb{F}_p - x) \cap A^\times$.*

PROOF. The spectral gap γ satisfies

$$\gamma = p - \max_{\chi \in \hat{X}(A^\times)} \left| \sum_{t \in \mathbb{F}_p} \chi(t-x) \right| \ge p - (de-1)\sqrt{p} > 0 \tag{3}$$

where the first inequality follows from Equation (2). □

3.1.2 Regarding A as an $\mathbb{F}_q$-algebra

Theorem 1 requires $\sqrt{p} > de-1$, which could be too strict a requirement on p. In situations where p is small, we would like to look for other types of generating sets. We define $q := p^d$ and $\mathbb{F}_q := \mathbb{F}_p[x]/f$. Notice that by enlarging the ground field from $\mathbb{F}_p$ to $\mathbb{F}_q$, A can actually be regarded as an $\mathbb{F}_q$-algebra. In order to see this, we will begin with a few lemmas.

LEMMA 1. *Let $a \in A$ be written in the form $a = \sum_{i=0}^{e-1} a_i f^i$ with each $a_i \in A$ having degree less than d. Then $a \in A^\times$ if and only if $a_0 \neq 0 \pmod f$.*

PROOF. For sufficiency, since $a \in A^\times$, there is an inverse element $b = \sum_{i=0}^{e-1} b_i f^i$ such that $ab = 1$. That is,

$$\begin{aligned} \left(\sum_{i=0}^{e-1} a_i f^i\right)\left(\sum_{i=0}^{e-1} b_i f^i\right) &= a_0 b_0 + (a_0 b_1 + a_1 b_0) f + \dots \\ &= 1 \pmod{f^e}, \end{aligned} \tag{4}$$

so $a_0 b_0 = 1 \pmod f \Rightarrow a_0 \neq 0 \pmod f$.

For necessity, suppose $a_0 \neq 0 \pmod f$, then it suffices to show the existence of $b = a^{-1}$. Assume that $b = \sum_{i=0}^{e-1} b_i f^i$ ($\deg b_i < d$ for all i), taking the product

$$\begin{aligned} \left(\sum_{i=0}^{e-1} a_i f^i\right)\left(\sum_{i=0}^{e-1} b_i f^i\right) &= a_0 b_0 + (a_0 b_1 + a_1 b_0) f + \dots \\ &= c_0 + c_1 f + \dots . \end{aligned} \tag{5}$$

Since $a_0 \neq 0 \pmod f$, there is b_0 such that $a_0 b_0 = 1 \pmod f$ and $b_0 \neq 0 \pmod f$. Given b_0, b_1 is uniquely determined by the linear equation $a_0 b_1 + a_1 b_0 = 0 \pmod f$ over $\mathbb{F}_q$. In general, each b_i ($1 \le i \le e-1$) is uniquely determined by the linear equation $c_i = 0 \pmod f$ over $\mathbb{F}_q$ for $b_0, \dots, b_{i-1}$ values that have been determined in previous steps. Therefore, there is a unique b such that $ab = 1 \pmod f$, and thus $a \in A^\times$. □

LEMMA 2. *For each $a_0 \in \mathbb{F}_q^\times$, there exists a unique $a \in A^\times$ which can be written as $a = \sum_{i=0}^{e-1} a_i f^i$, where each $a_i \in A$ has degree less than d, and $a^{q-1} = 1 \pmod{f^e}$.*

PROOF. Since $a_0 \in \mathbb{F}_q^\times$, $a \in A^\times$ by Lemma 1. Write $a = \sum_{i=0}^{e-1} a_i f^i$, with each $a_i \in A$ has degree less than d. We want $a^{q-1} = 1 \pmod{f^e}$, so we need

$$\begin{aligned} a^{q-1} &= \left(\sum_{i=0}^{e-1} a_i f^i\right)^{q-1} \\ &= a_0^{q-1} + (q-1)\, a_0^{q-2} a_1 f + \dots \\ &= 1 \pmod{f^e}. \end{aligned} \tag{6}$$

From Equation (6), we get

$$a_0^{q-1} + (q-1)\, a_0^{q-2} a_1 f = 1 \pmod{f^2}. \tag{7}$$

Because $a_0^{q-1} = 1 \pmod f$, we know there is some $A_0 \in A$ with $\deg A_0 < d$ such that

$$a_0^{q-1} = 1 + A_0 f \pmod{f^2}. \tag{8}$$

Combining Equations (7) and (8), we see that a_1 is uniquely determined by the linear equation

$$A_0 + (q-1)\, a_0^{q-2} a_1 = 0 \pmod f \tag{9}$$

over $\mathbb{F}_q$. Inductively, assume a_0, a_1, …, a_{k-1} are uniquely determined. In order to guarantee $a^{q-1} = 1 \pmod{f^e}$, we need

$$\begin{aligned} &\left(\sum_{i=0}^{e-1} a_i f^i\right)^{q-1} \\ &= \left(\sum_{i=0}^{k-1} a_i f^i + a_k f^k + \sum_{i=k+1}^{e-1} a_i f^i\right)^{q-1} \pmod{f^{k+1}} \\ &= \left(\sum_{i=0}^{k-1} a_i f^i + a_k f^k\right)^{q-1} \pmod{f^{k+1}} \\ &= \left(\sum_{i=0}^{k-1} a_i f^i\right)^{q-1} + (q-1)\left(\sum_{i=0}^{k-1} a_i f^i\right)^{q-2} a_k f^k \pmod{f^{k+1}} \\ &= 1 \pmod{f^{k+1}}. \end{aligned} \tag{10}$$

By induction, the first term can be written as

$$\left(\sum_{i=0}^{k-1} a_i f^i\right)^{q-1} = 1 + A_{k-1} f^k \tag{11}$$

for some $A_{k-1} \in A$ where $\deg A_{k-1} < d$. Then a_k is uniquely determined by the linear equation

$$A_{k-1} + (q-1)\left(\sum_{i=0}^{k-1} a_i f^i\right)^{q-2} a_k = 0 \pmod f \tag{12}$$

over $\mathbb{F}_q$. That completes the proof. □

Lemma 2 yields a well-defined function $\pi : \mathbb{F}_q^\times \to A^\times$, which can be extended to all of $\mathbb{F}_q$ by forcing $\pi(0) = 0$. We proved that π is essentially an embedding of $\mathbb{F}_q$ into A.

LEMMA 3. *Let $\pi : \mathbb{F}_q^\times \to A$ be the function where for all $a_0 \in \mathbb{F}_q$,*

$$\pi(a_0) = \begin{cases} 0 & , \text{ if } a_0 = 0 \\ a = \sum_{i=0}^{e-1} a_i f^i \in A \text{ s.t. } a^{q-1} = 1 & , \text{ otherwise} \end{cases}$$

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

PROOF. First of all, we enforce $\pi(0) = 0$, and we also have $\pi(1) = 1$. Assume $a_0, b_0 \in \mathbb{F}_q$, and that they can be written as $\pi(a_0) = \sum_{i=0}^{e-1} a_i f^i$, $\pi(b_0) = \sum_{i=0}^{e-1} b_i f^i$. We start by showing $\pi(a_0 b_0) = \pi(a_0)\pi(b_0)$. When $a_0 = 0$ or $b_0 = 0$, this is obvious. Otherwise, notice that the first term of both sides are $a_0 b_0$, and we have

$$(\pi(a_0)\pi(b_0))^{q-1} = \pi(a_0)^{q-1}\pi(b_0)^{q-1} = 1. \tag{13}$$

By Lemma 2 , $\pi(a_0 b_0) = \pi(a_0)\pi(b_0)$. Next, we verify $\pi(a_0^{-1}) = \pi(a_0)^{-1}$ for all $a_0 \neq 0$. Since $a_0^{q-1} = 1$, $a_0^{-1} = a_0^{q-2}$. Therefore,

$$\pi(a_0^{-1}) = \pi(a_0^{q-2}) = \pi(a_0)^{q-2}. \tag{14}$$

Since $\pi(a_0)^{q-1} = 1$, $\pi(a_0)^{q-2} = \pi(a_0)^{-1}$. Now it remains to show $\pi(a_0 + b_0) = \pi(a_0) + \pi(b_0)$. If $a_0 = 0$ or $b_0 = 0$, this is obvious. Otherwise, since the first term of both sides is $a_0 + b_0$, by Lemma 2, it suffices to show $(\pi(a_0) + \pi(b_0))^{q-1} = 1$. Denote the set $T = \{a \in A : a^{q-1} = 1\}$ and the set $T' = \{a \in A : a^q = a\} = T \cup \{0\}$. Since A is a ring of characteristic p,

$$(\pi(a_0) + \pi(b_0))^q = \pi(a_0)^q + \pi(b_0)^q = \pi(a_0) + \pi(b_0). \tag{15}$$

That is, $\pi(a_0) + \pi(b_0) \in T'$, and hence either $\pi(a_0) + \pi(b_0) \in T$ or $\pi(a_0) + \pi(b_0) = 0$. In the first case, we are done; in the latter case, $a_0 = -b_0$, so we also have $\pi(a_0 + b_0) = \pi(0) = 0 = \pi(a_0) + \pi(b_0)$. □

The proofs for Lemmas 1, 2 and 3 actually describes an algorithm for computing the embedding of $\mathbb{F}_q$ into A, and the pseudo code is shown in Algorithm 1. Taking p, f, e and a polynomial $a_0 \in \mathbb{F}_p[x]$ with degree less than d as input, the algorithm computes $a \in \mathbb{F}_p[x]$ that corresponds to $\pi(a_0)$ in $\mathbb{F}_p[x]/f^e$. We comment that in Line 8, by inverse, we mean finding the inverse element in $\mathbb{F}_q$.

Algorithm 1 Embed(a_0, p, f, e)

```
1: if a_0 = 0 then
2:    return 0
3: else
4:    d := deg f, q := p^d
5:    a := a_0
6:    for k = 1, ..., e − 1 do
7:       A_{k−1} := ((a^{q−1} mod f^{k+1}) − 1)/f^k
8:       a_k := ((q − 1)(a^{q−2} mod f))^{−1}(−A_{k−1})
9:       a := a + a_k f^k
10:   end for
11:   return a
12: end if
```

LEMMA 4. *A is a $\mathbb{F}_q$-algebra of dimension e.*

PROOF. A is an $\mathbb{F}_q$-algebra through the embedding π, in the sense that the action of $b \in \mathbb{F}_q$ on A is such that for all $a \in A$, $b \cdot a := \pi(b)a$ where the product in the right hand side is the one in A. □

THEOREM 3. *If $\sqrt{q} \geq e-1$, then the set $(\pi(\mathbb{F}_q) - x) \cap A^\times$ is a generating set for $A^\times$. Furthermore, every element of $A^\times$ can be written as $\prod_{i=1}^t (\pi(a_i) - x)$ where $a_i \in \mathbb{F}_q$ and*

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

PROOF. By Lemma 4, A can be regarded as a $\mathbb{F}_q$-algebra of dimension e. By Proposition 2, for all nontrivial character χ of $A^\times$ (extended by zero to all of A),

$$\left|\sum_{t\in\mathbb{F}_q} \chi(\pi(t) - x)\right| \leq (e-1)\sqrt{q}. \tag{16}$$

The rest of the proof follows from Propositions 3 and 4. □

THEOREM 4. *If $\sqrt{q} > e-1$, then $\Gamma(A^\times, S)$ is an expander, where $S = (\pi(\mathbb{F}_q) - x) \cap A^\times$.*

PROOF. The spectral gap γ satisfies

$$\gamma = q - \max_{\chi\in\hat{X}(A^\times)} \left|\sum_{t\in\mathbb{F}_q} \chi(\pi(t) - x)\right| \geq q - (e-1)\sqrt{q} > 0 \tag{17}$$

where the first inequality follows from Equation (16). □

3.1.3 Finding small generating sets

Theorem 3 sets a relatively mild restriction on p, which only needs $\sqrt{q} > e - 1$, but this generating set is of size q, which might be more than necessary in many cases. Only a small fraction of this set might already be sufficient to generate the group. Besides, in terms of expander graphs construction, the resulting graphs might be dense. Thus, in this section, we go one step further to find generating sets of smaller sizes.

Let $K \subset \mathbb{F}_q$ be a subfield of size p^c, where $c|d$. We have

THEOREM 5. *If K is a subfield of $\mathbb{F}_q$ of size p^c and $p^{c/2} > (de/c) - 1$, then $(\pi(K) - x) \cap A^\times$ is a generating set for $A^\times$. Furthermore, every element of $A^\times$ can be written as $\prod_{i=1}^t (\pi(a_i) - x)$, where $a_i \in K$ and*

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

PROOF. By Lemma 4, A can be regarded as a K-algebra of dimension de/c. By Proposition 2, for all nontrivial character χ of $A^\times$ (extended by zero to all of A),

$$\left|\sum_{t\in K} \chi(\pi(t) - x)\right| \leq \left(\frac{de}{c} - 1\right) p^{c/2}. \tag{18}$$

The rest of the proof follows from Propositions 3 and 4. □

THEOREM 6. *Let $K \subset \mathbb{F}_{p^d}$ be a subfield of $\mathbb{F}_q$ of size p^c where $c|d$. If $p^{c/2} > (de/c) - 1$, then $\Gamma(A^\times, S)$ is an expander, where $S = (\pi(K) - x) \cap A^\times$.*

PROOF. The spectral gap γ satisfies

$$\begin{aligned} \gamma &= p^c - \max_{\chi\in\hat{X}(A^\times)} \left|\sum_{t\in K} \chi(\pi(t) - x)\right| \\ &\geq p^c - \left(\frac{de}{c} - 1\right) p^{c/2} > 0 \end{aligned} \tag{19}$$

where the first inequality follows from Equation (18). □

Algorithm 2 Genset(p, f, e)

1: Let $d := \deg f$, factorize d (if not provided)
2: Find c such that $c|d$ and $p^{c/2} > (de/c) - 1$
3: Let $\phi : \mathbb{F}_{p^c} \hookrightarrow \mathbb{F}_p[x]/f$ a finite field homomorphism
4: **return** $(\text{Embed}(\phi(\mathbb{F}_{p^c})) - x) \cap A^\times$

Based on the above discussion, we present the pseudo code of our algorithm for finding a small generating set for $A^\times$, as shown in Algorithm 2. It takes p, f and e as input, and the output will be the small subset $S \subset A$, and $\Gamma(A^\times, S)$ is provably an expander. Notice that Line 3 in this pseudo code is used to find a subfield of $\mathbb{F}_q$ of size p^c, which is available in some algebraic programming languages [1, 7], and thus we omit the details.

A downside of this construction is that when d has few divisors, for example, d is a prime number, then $c = 1$ and $c = d$ are the only two options. On the other extreme, when d has abundant divisors, we may be able to construct better generating sets. For example, in expander graph construction, one may want to choose a perfect power as the value for d, say $d = b^n$ for some small number b. In this scenario, we have

COROLLARY 1. *If p and e are fixed and $d = b^n$ is a perfect power, where b fixed. Then Algorithm 2 returns a generating set of $A^\times$ of size $p^{O(\log d)}$.*

PROOF. Notice that $c \geq 2\log_p d + 2$ would be sufficient for the condition of Theorem 5, $p^{c/2} > (de/c) - 1$, to hold. Let $m_0 \in \mathbb{R}$ be such that $b^{m_0} = 2\log_p d + 2$. Write $c = b^m$, so we have $m = \lceil m_0 \rceil \leq m_0 + 1$. Thus, $c \leq 2b(\log_p d + 1) = O(\log d)$. □

3.1.4 Extending to the general case

In Sections 3.1.1, 3.1.2 and 3.1.3, we consider algebras of the form $A := \mathbb{F}_p[x]/f^e$. In this section, we are going to extend existing results to the more general case, where the algebra is of the form $B := \mathbb{F}_p[x]/F$, where $F \in \mathbb{F}_p[x]$ is an arbitrary polynomial. At the beginning of Section 3.1, we have seen the overall idea of our algorithm: with Algorithm 2, we generate a small generating set for each component; the union of these sets are then "pulled back" to $B^\times$ via the Chinese Remainder Theorem isomorphism ψ to get our final generating set for $B^\times$. It is straightforward to show that the resulting set obtained by this method forms a generating set for $B^\times$. In the rest of this paper, we will assume $F = \prod_{i=1}^m f_i^{e_i}$ where each $f_i \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree d_i. We will also use the abbreviation $A_i := \mathbb{F}_p[x]/f_i^{e_i}$ in our analysis.

THEOREM 7. *Let K_i be a subfield of $\mathbb{F}_p[x]/f_i$ of size p^{c_i}, and π_i be an embedding of K_i into A_i. If $p^{c_i/2} > (d_i e_i/c_i) - 1$ for all $1 \leq i \leq m$, then $\{\psi(v_{i,s}^m) | s \in (\pi_i(K_i) - x) \cap A_i^\times, 1 \leq i \leq m\}$ is a generating set for $B^\times$.*

PROOF. By Theorem 5, each $\pi_i(K_i) - x$ is a generating set for the component $A_i^\times$, so their union $\bigcup_{i=1}^m \pi_i(K_i) - x$ generates $\bigoplus_{i=1}^m A_i^\times$. Since ψ is an isomorphism, we can see the claim. □

The pseudo code is shown in Algorithm 3. Taking p and F as its input, Algorithm 3 finds a small generating set having the form described in Theorem 7 for $B^\times$.

Algorithm 3 FinalGenset(p, F)

1: Factorize F into $F = \prod_{i=1}^m f_i^{e_i}$ (if not provided), where each f_i is an irreducible polynomial of degree d_i
2: Let $\psi : \bigoplus_{i=1}^m (\mathbb{F}_p[x]/f_i^{e_i})^\times \xrightarrow{\sim} (\mathbb{F}_p[x]/F)^\times$ be the C.R.T isomorphism
3: $S := \emptyset$
4: **for** $i = 1, \ldots, m$ **do**
5: $\quad S_i := Genset(p, f_i, e_i)$
6: $\quad$ **for** each $s \in S_i$ **do**
7: $\quad\quad S := S \cup \{\psi(v_{i,s}^m)\}$
8: $\quad$ **end for**
9: **end for**
10: **return** S

COROLLARY 2. *If p is fixed and for all $1 \leq i \leq m$, e_i is fixed and $d_i = b_i^{n_i}$ is a perfect power, where b_i is fixed, then Algorithm 3 returns a generating set of $B^\times$ of size $\sum_{i=1}^m p^{O(\log d_i)}$.*

PROOF. This can be seen by applying Corollary 1 to each component $A_i^\times$. □

Now it only remains to show that graphs of the form $\Gamma(B^\times, S)$, where S is found by Algorithm 3, are a set of expanders.

THEOREM 8. *Let K_i is a subfield of $\mathbb{F}_p[x]/f_i$ of size p^{c_i}, and π_i be an embedding of K_i into A_i. If $p^{c_i/2} > (d_i e_i/c_i) - 1$ for all $1 \leq i \leq m$, then $\Gamma(B^\times, S)$ where $S := \{\psi(v_{i,s}^m) | i \in (\pi_i(K_i) - x) \cap A_i^\times, 1 \leq i \leq m\}$ is an expander.*

PROOF. Define $S_i := \pi_i(K_i) - x$, $1 \leq i \leq m$. Since $B^\times \simeq \bigoplus_{i=1}^m A_i^\times$, for all $\chi \in \tilde{X}(B^\times)$, there exists $\chi_i \in \tilde{X}(A_i^\times)$ $(1 \leq i \leq m)$ such that

$$\forall b \simeq \bigoplus_{i=1}^m b_i \in B^\times : \chi(b) = \prod_{i=1}^m \chi_i(b_i). \tag{20}$$

Consider an arbitrary character $\chi \in \tilde{X}(B^\times)$, and assume $\chi_1 \in \tilde{X}(A_1^\times), \ldots, \chi_m \in \tilde{X}(A_m^\times)$ are the characters that satisfy Equation (20). For all elements $b \in B^\times$ of the form $b \simeq v_{i,s}^m$, all but the i-th coordinate are zeros, so

$$\chi(\psi(v_{i,s}^m)) = \chi_i(s) \prod_{j \neq i} \chi_j(0) = \chi_i(s). \tag{21}$$

Combining Equation (21) with Proposition 2, we obtain

$$\begin{aligned} \left| \sum_{s \in S} \chi(s) \right| &= \left| \sum_{i=1}^m \sum_{s \in \{\psi(v_{i,s}^m) | s \in S_i\}} \chi(s) \right| \\ &= \left| \sum_{i=1}^m \sum_{s \in S_i} \chi_i(s) \right| \leq \sum_{i=1}^m \left| \sum_{s \in S_i} \chi_i(s) \right| \\ &\leq \sum_{i=1}^m \left(\frac{d_i e_i}{c_i} - 1 \right) p^{c_i/2}. \end{aligned} \tag{22}$$

Given that $p^{c_i/2} > (d_i e_i/c_i) - 1$ for all $1 \leq i \leq m$, the

spectral gap γ of the Cayley graph satisfies

$$\begin{aligned}\gamma &\geq \sum_{i=1}^{m} |S_i| - \max_{\chi \in \hat{X}(B^\times)} \left| \sum_{s \in S} \chi(s) \right| \\ &\geq \sum_{i=1}^{m} p^{c_i} - \sum_{i=1}^{m} \left(\frac{d_i e_i}{c_i} - 1 \right) p^{c_i/2} \\ &> 0.\end{aligned} \tag{23}$$

□

3.2 Basis and Decomposition

3.2.1 Building a basis

In order to find a basis for $B^\times$, we first decide the structure of the group, so that the size of a basis can be determined. As we have already seen from Equation (1), $B^\times$ can first be decomposed into $\bigoplus_{i=1}^{m} A_i^\times$ (recall that $A_i := \mathbb{F}_p[x]/f_i^{e_i}$). Therefore, it only remains to find out the decomposition of the group $A^\times := \mathbb{F}_p[x]/f^e$, with f and e defined the same as in Section 3.1. We observe that if $p \geq e$, $A^\times$ can be decomposed as shown in Lemma 5 below.

LEMMA 5. *If $p \geq e$, then*

$$A^\times \simeq \mathbb{Z}/(p^d - 1)\mathbb{Z} \oplus \left(\bigoplus_{d(e-1)} \mathbb{Z}/p\mathbb{Z} \right).$$

PROOF. Consider the map $\varphi : A^\times \to (\mathbb{F}_p[x]/f)^\times$ where for each $a \in A^\times$, $\varphi(a) = a \pmod f$. Clearly, φ is an onto function. We can see that the kernel of the map is precisely

$$\ker \varphi = \{1 + bf : b \in A \text{ where } 0 \leq \deg b \leq d(e-1) - 1\}. \tag{24}$$

For every $1 + bf \in \ker \varphi$, since A as a ring has characteristic p, its p-th power is given by

$$(1 + bf)^p = 1 + b^p f^p \pmod{f^e}. \tag{25}$$

Given the condition that $p \geq e$, we have

$$1 + b^p f^p = 1 \pmod{f^e}. \tag{26}$$

So, by the structure theorem of finite abelian groups, we have

$$\ker \varphi \simeq \bigoplus_{d(e-1)} \mathbb{Z}/p\mathbb{Z}. \tag{27}$$

In addition, notice that $|\ker \varphi| = p^{d(e-1)}$, which is relatively prime to $|\mathrm{im}\varphi| = p^d - 1$. It follows that $A^\times$ is isomorphic to their direct product, as desired. □

THEOREM 9. *If $p \geq \max_{i=1}^{m} e_i$, then*

$$B^\times \simeq \bigoplus_{i=1}^{m} \left(\mathbb{Z}/(p^{d_i} - 1)\mathbb{Z} \oplus \bigoplus_{d_i(e_i - 1)} \mathbb{Z}/p\mathbb{Z} \right).$$

PROOF. It follows from Lemma 5 and Equation (1). □

Theorem 9 holds if and only if $p \geq \max_{i=1}^{m} e_i$, and thus our basis construction and decomposition algorithms will only deal with this situation. Assuming this condition, it suffices to find a basis for the group $A^\times$. From the proof for Lemma 5, we can see that

$$A^\times = \pi(\mathbb{F}_q^\times) \times \ker \varphi, \tag{28}$$

and as we have seen in Lemma 5, $\pi(\mathbb{F}_q^\times) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ and $\ker \varphi \simeq \bigoplus_{d(e-1)} \mathbb{Z}/p\mathbb{Z}$.

For the former component $\pi(\mathbb{F}_q^\times)$, we will simply use an existing algorithm such as [10] to find a generator.

We then consider the latter component $\ker \varphi$. Let K_j $(1 \leq j \leq e)$ denote the subset of $A^\times$ of the form $\{1 + hf^j \bmod f^e : h \in \mathbb{F}_p[x]\}$. By definition, $K_1 = \ker \varphi$ and $K_e = \{1\}$. One may verify that each K_j is actually a subgroup of $\ker \varphi$. Consider the following filtration of subgroups:

$$K_1 \supsetneq K_2 \supsetneq \ldots \supsetneq K_e.$$

We have

LEMMA 6. *For each $1 \leq j \leq e - 1$,*

$$K_j / K_{j+1} = \prod_{k=0}^{d-1} \langle 1 + x^k f^j \rangle \simeq \bigoplus_{k=0}^{d-1} \mathbb{Z}/p\mathbb{Z}$$

PROOF. Consider the map $K_j \to \mathbb{F}_p[x]/f$ sending $1 + hf^j$ to $h \bmod f$ for all $1 + hf^j \in K_j$ with $\deg h < d$. It is easy to verify that this is a group homomorphism with K_{j+1} as the kernel. Therefore, we have

$$K_j / K_{j+1} \simeq \mathbb{F}_p[x]/f \simeq \bigoplus_{k=0}^{d-1} \mathbb{Z}/p\mathbb{Z}, \tag{29}$$

whereby $1 + hf^j$ is mapped to $\bigoplus_{k=0}^{d-1} h_k$ if h is written in the form $h = \sum_{k=0}^{d-1} h_k x^k$. Under this isomorphism, the basis $\{x^k \bmod f | k = 0, ..., d-1\}$ for $\mathbb{F}_p[x]/f$ corresponds to the basis $\{1 + x^k f^j | k = 0, ..., d-1\}$ for K_j/K_{j+1}. □

LEMMA 7. *The set of polynomials $\{1 + x^k f^j | 0 \leq k \leq d-1, 1 \leq j \leq e-1\}$ forms a basis for $\ker \varphi$.*

PROOF. Clearly, this set contains $d(e-1)$ elements, which is the right size. So it suffices to show it is a generating set for $\ker \varphi$. Given any element $k_j \in K_j$, we first write it into the form $k_j = 1 + \sum_{t=j}^{e-1} h_t f^t$, where each h_t has degree less than d. Under the isomorphism between K_j/K_{j+1} and $\mathbb{F}_p[x]/f$ in the proof of Lemma 6, we see that k_j, $1 + h_j f^j$, and $\prod_{k=0}^{d-1} \left(1 + x^k f^j\right)^{h_{j,k}}$ are all in the same class in K_j/K_{j+1} assuming h_j is written in the form $h_j = \sum_{k=0}^{d-1} h_{j,k} x^k$. By Lemma 6, the class of k_j modulo K_{j+1} is mapped to $\bigoplus_{k=0}^{d-1} h_{j,k}$. That is,

$$k_j = \left(\prod_{k=0}^{d-1} (1 + x^k f^j)^{h_{j,k}} \right) k_{j+1}, \tag{30}$$

where $k_{j+1} \in K_{j+1}$ is uniquely determined. Therefore, any element $k_1 = 1 + \sum_{t=1}^{e-1} h_t f^t \in K_1 = \ker \varphi$ can be decomposed recursively via Equation (30) for all $1 \leq i \leq e-1$, so k_1 can be written as a product of elements from the set. □

Therefore, if $p \geq e$, then we can use $Z := \{\pi(g)\} \cup \{1 + x^k f^j | 0 \leq k \leq d-1, 1 \leq j \leq e-1\}$ as a basis for $A^\times$, where g is a generator for $(\mathbb{F}_p[x]/f)^\times$. This observation can be quickly extended to the general case $B^\times$.

THEOREM 10. *Let g_i be a generator of $(\mathbb{F}_p[x]/f_i)^\times$ and π_i be the embedding map from $\mathbb{F}_p[x]/f_i$ into A_i. If $p \geq \max_{i=1}^{m} e_i$, then the set $Z := \bigcup_{i=1}^{m} \{\psi(v_{i,z}^m) | z \in Z_i\}$ forms a basis for $B^\times$, where for all $1 \leq i \leq m$, $Z_i := \pi_i(g_i) \cup \{1 + x^k f^j | 0 \leq k \leq d-1, 1 \leq j \leq e-1\}$.*

PROOF. By Lemma 5 and Lemma 7, each Z_i is a basis for $A_i^\times$. And $B^\times \simeq \bigoplus_{i=1}^m A_i^\times$. The union $\bigcup_{i=1}^m \{v_{i,z}^m | z \in Z_i\}$ forms a basis for the right-hand side. □

Based on Theorem 10, we developed Algorithm 4. Given the input p and F, if $p \geq \max_{i=1}^m e_i$, it outputs a basis for $B^\times$; otherwise, it reports failure in finding a basis.

Algorithm 4 Basis(p, F)

1: Factorize F into $F = \prod_{i=1}^m f_i^{e_i}$ (if not provided), where each f_i is an irreducible polynomial of degree d_i
2: **if** $p \geq \max_{i=1}^m e_i$ **then**
3: $Z := \emptyset$
4: **for** $i = 1, \ldots, m$ **do**
5: Find a generator g for $(\mathbb{F}_p[x]/f_i)^\times$ using existing algorithms such as [10]
6: $z := \text{Embed}(g, p, f_i, e_i)$
7: $Z := Z \cup \{\psi(v_{i,z}^m)\}$
8: **for** all $0 \leq j \leq d-1$ and all $1 \leq k \leq e$ **do**
9: $Z := Z \cup \{\psi(v_{i,1+x^j f^k}^m)\}$
10: **end for**
11: **end for**
12: **else**
13: **return** unknown
14: **end if**

3.2.2 *Decomposition*

In the proof for Theorem 7, we have seen an outline of our algorithm for decomposition. The pseudo code for this algorithm is shown in Algorithm 5. Given an element $b \in \mathbb{F}_p[x]$ corresponding to an element in $B^\times$, the algorithm either outputs its coordinates $\bigoplus_{i=1}^m (b_{i,0} \oplus \bigoplus_{j=1}^{d_i(e_i-1)} b_{i,j})$ with respect to Theorem 9 (if $p \geq \max_{i=1}^m e_i$), or claims a failure in decomposition. We comment that in Line 6 and 13, the inverse element is found in $A_i^\times$.

Algorithm 5 Decomposition(p, F, b)

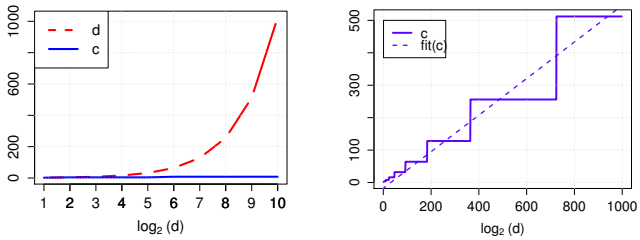
1: Factorize F into $F = \prod_{i=1}^m f_i^{e_i}$ (if not provided), where each f_i is an irreducible polynomial of degree d_i
2: **if** $p \geq \max_{i=1}^m e_i$ **then**
3: **for** i=1,..., m **do**
4: $a := b \mod f_i^{e_i}$
5: $\eta := \text{Embed}(a \mod f_i, p, f_i, e_i)$
6: $\kappa := \eta^{-1} a$
7: $b_{i,0} :=$ discrete-log of $a \mod f$ in $(\mathbb{F}_p[x]/f_i)^\times$
8: **for** $j = 1, \ldots, e-1$ **do**
9: $h_j := (\kappa \mod f^{j+1} - 1)/f^j$, and assume $h_j = \sum_{k=0}^{d-1} h_{j,k} x^k$
10: **for** $k = 0, \ldots, d-1$ **do**
11: $b_{i,j,k} := h_{j,k}$
12: **end for**
13: $\kappa := (\prod_{k=0}^{d-1} (1 + x^k f^j)^{h_{j,k}})^{-1} \kappa$
14: **end for**
15: **end for**
16: **return** $\bigoplus_{i=1}^m (b_{i,0} \oplus \bigoplus_{j=1}^{e-1} \bigoplus_{k=0}^{d-1} b_{i,j,k})$
17: **else**
18: **return** unknown
19: **end if**

4. EXPERIMENTS

An important question about the generating sets we presented in Section 3.1 is whether they are too large to be practical. That is, a small subset of our generating sets may be sufficient to generate the group. Therefore, we ran experiments to see whether the size of the generating sets we presented can be substantially reduced in practice, where a practically optimal generating set is constructed by drawing random subsets from our original construction. To some extent, we can infer from the results whether the restrictions in Theorems 1, 3 and 5 can be significantly weakened in practice.

Our programs are implemented in Sage [7]. For simplicity, we only run experiments on algebras of the form $A := \mathbb{F}_p[x]/f^e$, where $f \in \mathbb{F}_p[x]$ is irreducible of degree d. We compare the sizes of three types of generating sets for $A^\times$. The first type, having the form $\pi(\mathbb{F}_q) - x$, corresponds to Theorem 3. It's size equals $q := p^d$. The second type of generating sets are of the form $\pi(K) - x$ corresponding to Theorem 5, where $K \subset \mathbb{F}_q$ is a subfield of size p^c. The third type of generating sets are constructed by adding random elements of $\pi(K) - x$ to the empty set one by one, until it generates $A^\times$. We write its size as p^b where $b \in \mathbb{R}$. Clearly, we have the relationship $b \leq c \leq d$.

Our first experiment compares the growth of c and d. In this experiment, we set $p = 7$, $e = 5$ and $d = 2^1, 2^2, 2^3, \ldots$. The result is shown in Figure 1. From Figure 1 we see that when d is a perfect power, c grows linearly with $\log d$, as stated in Corollary 1.



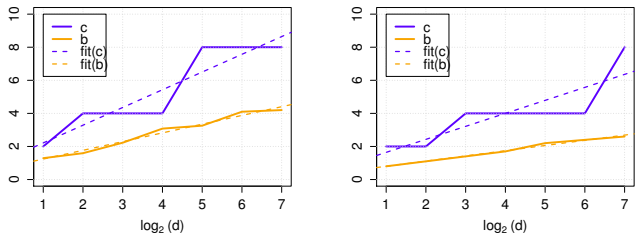
(a) Comparison of c and d (b) The growth of c with d

Figure 1: The growth of c and d

In the second set of experiments, we compare b and c with different choices of parameters. We first set $e = 4$ and $d = 2^1, 2^2, 2^3, \ldots$ and we increase p from 5 to 11. From Figure 2, we observe a logarithmic growth from both b and c against d, and $c \approx 2b$. Also, we can see that when p increases, the growth rate of b and c decreases.

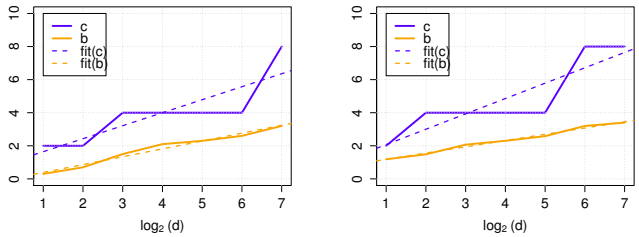
The third set of experiments studies the effect of e while fixing the value of $p = 7$, and the results are shown in Figure 3. From this experiment, we see that when e increases, the growth rate of both b and c increases.

From the experimental results shown in Figure 2 and 3, we observe that $c \approx 2b$, which implies that a square root number of random elements from $\pi(K) - x$ might already be sufficient as a generating set. This may imply that sparser expander graphs can possibly be constructed over the multiplicative groups of finite algebras. How to find such subsets that can be used for expander graph construction remains an open problem.



(a) $p = 5, e = 4$ (b) $p = 11, e = 4$

Figure 2: The effect of p



(a) $p = 7, e = 3$ (b) $p = 7, e = 5$

Figure 3: The effect of e

5. CONCLUSION

In this paper, we generalize Chung's [4] to the case of $\mathbb{F}_p[x]/F$ where $F \in \mathbb{F}_p[x]$ is not necessarily irreducible. We present algorithms for finding different types of small generating sets for $B^\times$ which can be applied to explicit construction of expander graphs. We also propose algorithms for finding a basis for $B^\times$ and decomposing elements with respect to this basis.

From our experiments, we observe that a square root number of elements in the generating set we found are usually sufficient to generate the whole group. How to find these elements and use them for expander graph construction remains an open problem. In addition, basis construction and decomposition for $B^\times$ when p is small will be another future work.

6. ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers for pointing out several errors and typos in the initial submission of this paper.

7. REFERENCES

[1] Finite field morphisms. http://doc.sagemath.org/html/en/reference/finite_rings/sage/rings/finite_rings/hom_finite_field.html.

[2] L. M. Adleman and M.-D. A. Huang. Function field sieve method for discrete logarithms over finite fields. *Information and Computation*, 151(1-2):5–16, 1999.

[3] A. Bhowmick and T. H. LÃł. On primitive elements in finite fields of low characteristic. *Finite Fields and Their Applications*, 35:64 – 77, 2015.

[4] F. R. K. Chung. Diameters and eigenvalues. *American Mathematical Society*, 2(2):187–196, 1989.

[5] F. R. K. Chung. Several generalizations of weil sums. *J. Number Theory*, 49:95–106, 1994.

[6] F. R. K. Chung. *Spectral Graph Theory*. American Mathematical Society, 1997.

[7] T. S. Developers. *Sage Mathematics Software (Version 7.1)*, 2016. `http://www.sagemath.org`.

[8] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel. *Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, pages 109–128. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[9] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *BULL. AMER. MATH. SOC.*, 43(4):439–561, 2006.

[10] M. Huang and A. K. Narayanan. Finding primitive elements in finite fields of small characteristic. *CoRR*, abs/1304.1206, 2013.

[11] A. Joux. A new index calculus algorithm with complexity $l(1/4 + o(1))$ in very small characteristic. Cryptology ePrint Archive, Report 2013/095, 2013.

[12] N. M. Katz. An estimate for character sums. *Journal of the American Mathematical Society*, 2(2):pp. 197–200, 1989.

[13] M. Lu, D. Wan, L.-P. Wang, and X.-D. Zhang. Algebraic cayley graphs over finite fields. *Finite Fields and Their Applications*, 28:43 – 56, 2014.

[14] G. L. Mullen and D. Panario. *Handbook of Finite Fields*. Chapman & Hall/CRC, 1st edition, 2013.

[15] R. Popovych. Elements of high order in finite fields of the form. *Finite Fields and Their Applications*, 19(1):86–92, 2013.

[16] V. Shoup. Searching for primitive roots in finite fields. *Mathematics of Computation*, 58(197):369–380, 1992.

[17] I. E. Shparlinski. Cayley graphs generated by small degree polynomials over finite fields. *SIAM Journal on Discrete Mathematics*, 29(1):376–381, 2015.

[18] J. von zur Gathen and I. Shparlinski. Orders of gauss periods in finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 9(1):15–24.

[19] D. Wan. Generators and irreducible polynomials over finite fields. *Mathematics of Computation*, 66:1195–1212, 1997.

[20] A. Weil. *Basic number theory*. Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1974.