Bounds on polynomial approximations of the discrete logarithm function

Swastik Kopparty* Rishabh Kothary† Ashutosh Shankar‡

October 26, 2026

Abstract

We revisit a classical result of Coppersmith and Shparlinski [CS00] showing bounds on how well polynomials can approximate the discrete log function. They showed that for any univariate polynomial $f(X) \in \mathbb{F}_p[X]$ with $\deg(f) \leq D$, we have:

$$|\{x \in \mathbb{F}_p^\times \mid f(x) = \mathsf{dlog}(x)\}| \leq \sqrt{2Dp}.$$

We show two improvements:

- For all D, we improve the upper bound above to $(1 + o(1)) \cdot \sqrt{Dp}$. In particular, we give nontrivial upper bounds on the approximation even for $D > p/2$. This new upper bound is the *Johnson bound* from the theory of list-decoding of error-correcting codes, and in fact our proof uses a connection to that problem, as well as other combinatorial ideas.
- For $D = 1$, where both the above bounds are $\mathcal{O}(\sqrt{p})$, we give an asymptotically improved upper bound of $\mathcal{O}(p^{2/5})$. This is based on the sum-product phenomenon of additive combinatorics.

We also improve the [CS00] bounds on the number of points of the form $(x, \mathsf{dlog}(x)) \in \mathbb{F}_p^2$ that any bivariate polynomial $Q(X, Y) \in \mathbb{F}_p[X, Y]$ with $\deg(Q) \leq D$ can vanish on, with our new bounds approaching the analogue of the Johnson bound for this problem.

1 Introduction

The discrete logarithm function has been a central object in cryptography since the work of Diffie and Hellman [DH76]. It plays a prominent role in innumerable cryptographic constructions. It is

*Department of Mathematics and Department of Computer Science, University of Toronto, Canada. Email: swastik.kopparty@utoronto.ca. Research partially supported by an NSERC Discovery Grant.

†Department of Computer Science, University of Toronto, Canada. Email: rishabh.kothary@mail.utoronto.ca. Research partially supported by an NSERC Discovery Grant

‡Tata Institute of Fundamental Research, Mumbai, India. Email:ashutosh.shankar@tifr.res.in Research conducted while the author was visiting the University of Toronto.

therefore of great importance to understand its algebraic and combinatorial characteristics, with the goal of identifying any computational weakness.

This paper is concerned with the best *low-degree approximation* to the discrete log function in the finite field $\mathbb{F}_p$, with prime p. Concretely, for a given degree bound d, we are interested in determining an upper bound A such that for every polynomial $f(X) \in \mathbb{F}_p[X]$ of degree at most D, we have:

$$|\{x \in \mathbb{F}_p \mid f(x) = \mathsf{dlog}(x)\}| \leq A.$$

(Thus we are talking about approximation in terms of the number of points with exact equality, not any numerical approximation notion.)

This question was first studied by Coppersmith and Shparlinski [CS00], who showed that for any $f(X) \in \mathbb{F}_p[X]$ of degree at most D,

$$|\{x \in \mathbb{F}_p \mid f(x) = \mathsf{dlog}(x)\}| \leq \sqrt{2Dp}.$$

Subsequent work of Winterhof [Win02] extended this to non-prime finite fields $\mathbb{F}_q$. Even further extensions, to fractional linear maps and beyond were given by Kiltz and Winterhof [KW06], Isik and Winterhof [IW18], and Bienvenu and Winterhof [BW26]. A different extension, of Niederreiter and Winterhof [NW02], gave bounds on the largest interval of agreement. However there has been no improvement of the Coppersmith-Shparlinski bound over prime fields for any D.

Our first main result gives an improved bound. We show that for any $f(X) \in \mathbb{F}_p[X]$ of degree at most D,

$$|\{x \in \mathbb{F}_p \mid f(x) = \mathsf{dlog}(x)\}| \leq (1 + o(1)) \cdot \sqrt{Dp}.$$

In particular, this gives nontrivial bounds even in the setting of $D > \frac{p}{2}$.

The quantity $\sqrt{Dp}$ in the upper bound is of special significance; it is the *Johnson agreement* parameter in the list-decoding of Reed-Solomon codes. The Johnson bound for Reed-Solomon codes states that if $g : \mathbb{F}_p \to \mathbb{F}_p$ is a function, and there exist distinct polynomials $f_1(X), \ldots, f_L(X)$ of degree at most D such that $|\{x \mid f_i(x) = g(x)\}| \geq (1 + \varepsilon)\sqrt{Dp}$, then $L \leq \mathcal{O}_\varepsilon(\sqrt{p/D})$. There are two steps to our proof: (1) we show that if some polynomial $f(X)$ approximates dlog well, then there are many polynomials $f_1(X), f_2(X), \ldots, f_L(X)$ of the same degree that also approximate dlog quite well, and (2) using the list-decodability of Reed-Solomon codes to get a contradiction.

The first step uses the almost-homomorphism property of dlog: $\mathsf{dlog}(x) + \mathsf{dlog}(y) \in \mathsf{dlog}(xy) + \{0, -1\}$, where the last term is because of the mismatch between the sizes of $\mathbb{F}_p$ and $\mathbb{F}_p^\times$. The extra complexity introduced by the "almost" aspect is handled by some shifting arguments, along with Szemeredi's theorem from additive combinatorics.

One consequence of our approach is that improved bounds on the list-decoding of Reed-Solomon codes, with sublinear list size L, will give improved bounds for our problem. We think this is strong

evidence in favour of the existence of better upper bounds[1]. In fact, we believe that the true upper bound is much smaller:

Conjecture 1.1. *For any $f(X) \in \mathbb{F}_p[X]$ of degree at most D,*

$$|\{x \in \mathbb{F}_p \mid f(x) = \mathsf{dlog}(x)\}| \leq (1 + o(1)) \cdot D \cdot \frac{\log p}{\log(D+1)},$$

as $p \to \infty$.

The quantitative form is motivated by the best known impossibility results for list-decodability of Reed-Solomon codes over prime fields.

Our second main result makes some further progress towards this conjecture for the case of $D = 1$, i.e, linear polynomials. We show that for any $f(X) \in \mathbb{F}_p[X]$ of degree at most 1:

$$|\{x \in \mathbb{F}_p \mid f(x) = \mathsf{dlog}(x)\}| \leq \mathcal{O}(p^{2/5}).$$

This improves on the $\Theta(\sqrt{p})$ bound of Coppersmith-Shparlinski by a polynomial factor.

Our proof of the second result uses the sum-product phenomenon in finite fields [BKT04], and specifically its consequence for incidences between lines and points in $\mathbb{F}_p^2$ [BKT04, Lew26, MX26, Yu26]. The main technical construction comes from a 2-source extractor construction of Bourgain [Bou05] (see also Rao's exposition [Rao07]), who showed how to construct good two-source extractors from the discrete log function using the line-point incidence theorem in finite fields.

Finally, we also mention that Coppersmith and Shparlinski proved another bound on approximating the discrete log function with "algebraic functions". Specifically, they showed that for any bivariate polynomial $Q(X, Y) \in \mathbb{F}_p[X, Y]$ of degree at most D:

$$|\{(x, \mathsf{dlog}(x)) \in \mathbb{F}_p^2 \mid Q(x, y) = 0\}| \leq \sqrt{3} \cdot D\sqrt{p}.$$

We again improve this bound to the analogous Johnson bound[2] threshold, namely $(1 + o(1)) \cdot D\sqrt{p}$.

One final related work in the same spirit that we would like to mention is the paper of Kedlaya and Kopparty [KK23]. They gave limits on the approximation by polynomials of the (multi-valued) "square root" function in finite fields.

[1] We remark that the very recent breakthrough of Brakensiek, Chen, Putterman, Zhang and Zheng [BCP+26] on list-decoding Reed-Solomon codes over $\mathbb{F}_p$ (see also the paper of Harsha, Kumar and Saptharishi [HKS26]) does not yield anything yet because of the large polynomial list sizes in their result.

[2] Here the relevant Johnson bound is the following statement: if $S \subseteq \mathbb{F}_p^2$ is a set of size N, and $Q_1(X, Y), \ldots, Q_L(X, Y)$ are distinct irreducible polynomials of degree at most D, such that each Q_i vanishes at at least $(1 + \varepsilon) \cdot D\sqrt{N}$ points of S, then $L \leq O_\varepsilon(\sqrt{N}/D)$. This follows from Bézout's theorem and the classical Johnson bound on set systems with restricted intersections.

AI use: The results were obtained without any AI involvement. The writing was done without any AI involvement. We used AI for literature search and for feedback on our writeup.

Organization of this paper: In the next section we set up some notation and preliminaries about list decoding and additive combinatorics. In Section 3 we prove our main structural lemmas about conjugates, which yields many approximations from one approximation. Our results for univariate polynomial approximation appear in Section 4. Our results for bivariate polynomial approximation appear in Section 5. Our results for degree $D = 1$ appear in Section 6.

2 Notation and preliminaries

We work in a finite field $\mathbb{F}_p$ for some fixed prime p. We will often use N to denote $p-1$ for ease of notation. Fix a generator g of the field. The discrete logarithm is defined with respect to this generator.

Definition 2.1 (Discrete logarithm)**.** *For $x \in \mathbb{F}_p^*$, $\mathsf{dlog}(x)$ is defined to be the unique $j \in \{0, 1, \ldots, p-2\}$ with $g^j = x$ in $\mathbb{F}_p$.* ⌟

We will invoke the following well-known result from algebra.

Theorem 2.2 (Bézout's theorem [Ful89])**.** *Let $f, g \in \mathbb{F}[X, Y]$ such that $\deg(f) \le d$, $\deg(g) \le e$ and f, g are co-prime. Then, the number of common zeroes of f and g is at most $d \cdot e$.*

We will also talk about sumsets. For a subset V of an abelian group G, we let $m \cdot V$ denote the m-fold sumset $V + V + \ldots + V$.

2.1 Johnson bound

The Johnson bound is generally stated as a bound on the number of codewords within a certain radius of a received word, given that the code has some minimum distance. Simple forms of the Johnson bound are proved by counting methods. We use the following rearrangement of standard Johnson bound statements, for instance Theorem 4.2 of [GRS00], so it is phrased as a bound on the size of the agreement sets (i.e. a lower bound on the radius) given a list of codewords and the minimum distance of the code.

Lemma 2.3 (Johnson Bound)**.** *Let $T_1, ..., T_L \subset [n]$ be such that $|T_i| \ge A$ for all $i \in [L]$, and for any $i \ne j \in [L]$, $|T_i \cap T_j| \le r$, then*

$$A \le \frac{n}{2L} + \sqrt{\frac{n^2}{4L^2} + nr}.$$

2.2 Theorems from additive combinatorics

In the sections on low-degree univariate and bivariate polynomials (Sections 4 and 5), we will use results on arithmetic-progression-free sets. Szeméredi's Theorem states that a large enough set of natural numbers must contain a long arithmetic progression. Below we state a quantitative version due to Gowers.

Theorem 2.4 ([Gow01])**.** *For every $k \in \mathbb{N}$, there exists a constant n_k such that for any $n \geq n_k$ and $S \subset [n]$ where $|S| \geq n \cdot (\log \log n)^{-2^{-2^{k+9}}}$, then S contains a k term arithmetic progression.*

In the section on linear functions (Section 6), we will invoke the following bound on line-point incidences. Let $\mathcal{P} \subseteq \mathbb{F}_p^2$ be a set of points and $\mathcal{L}$ a set of lines in $\mathbb{F}_p^2$. An incidence is a pair (a, ℓ) of $a \in \mathcal{P}$ and $\ell \in \mathcal{L}$ with $a \in \ell$. The set of incidences is denoted $\mathcal{I}(\mathcal{P}, \mathcal{L})$. The first nontrivial upper bounds on the number of incidences over prime fields were obtained by Bourgain, Katz and Tao [BKT04]. The main challenge that [BKT04] had to overcome is that finite fields which contain subfields actually have point-line configurations with many incidences; a nontrivial upper bound needs to use the absence of subfields of $\mathbb{F}_p$. The very recent breakthrough works of Lewko [Lew26] and Miao and Xie [MX26] gave optimal quantitative estimates for the number of incidences (see also the elegant paper of Yu [Yu26]). We will use the following estimate by Lewko [Lew26]:

Theorem 2.5 ([Lew26])**.** *Let $\mathcal{P}$ be a set of m points in $\mathbb{F}_q^2$ and $\mathcal{L}$ be a set of n lines in $\mathbb{F}_q^2$. Let $p = \mathrm{char}(\mathbb{F}_q)$ and if $mn \leq p^3$, then*

$$|\mathcal{I}(\mathcal{P}, \mathcal{L})| \leq 3(mn)^{2/3} + m + n.$$

3 Agreement sets and conjugates

3.1 Distinctness of Conjugates

In this section, we define the conjugates of a bivariate polynomial $Q(X, Y) \in \mathbb{F}_p[X, Y]$ and prove some properties of the conjugates. At the high level, the conjugates $Q_{i,b}(X, Y)$ of $Q(X, Y)$ are bivariate polynomials such that if $Q(X, Y)$ vanishes at many points of the form (g^α, α), then so do (many of) the conjugates. They are based on the algebraic properties of the discrete log function.

Definition 3.1 (Conjugates)**.** *Let $Q(X, Y) \in \mathbb{F}_p[X, Y]$ be a non-zero polynomial, then for any $i \in \{0, ..., p-2\}$ and $b \in \{0, 1\}$, define*

$$Q_{i,b}(X, Y) = Q(g^i X, Y + i + b).$$

These are called the conjugates of $Q(X, Y)$. ⌟

These conjugates will serve as our "list elements". Our proof will proceed by showing that the agreement set cannot be too large if all of these are to be in the list.

We formally define this agreement set below, along with some conjugate agreement sets.

Definition 3.2 (Agreement set T)**.** *Let $Q(X,Y) \in \mathbb{F}_p[X,Y]$ be a non-zero polynomial, then define $T(Q) \subset \mathbb{F}_p$ as*

$$T(Q) = \{\alpha \in \{0,...,N-1\} \mid Q(g^\alpha, \alpha) = 0\}.$$

Further for any $i \in [N-1]$, define

$$T(Q)_{i,0} = \{\alpha \in \{0,...,N-i-1\} \mid \alpha + i \in T(Q)\}$$
$$T(Q)_{i,1} = \{\alpha \in \{N-i,..,N-1\} \mid \alpha + i - N \in T(Q)\}.$$

In particular note that $|T(Q)| = |T(Q)_{i,0}| + |T(Q)_{i,1}|$. ⌟

The latter set $T(Q)_{i,1}$ is meant to handle the case when $\alpha + i$ exceeds N. Notice that for $\alpha \in T(Q)_{i,1}$, we have $\alpha + i - N = \alpha + i - (p-1) = \alpha + i + 1$.

Now we will show that $T(Q)_{i,b}$ contain the projection of the roots of $Q_{i,b}$ onto the second coordinate.

Proposition 3.3. *For any $(i,b) \in [N-1] \times \{0,1\}$, let $\alpha \in T(Q)_{i,b}$. Then $Q_{i,b}(g^\alpha, \alpha) = 0$.*

Proof. Let $\alpha \in T(Q)_{i,b}$, then by definition $\alpha + i - b \cdot N \in T(Q)$. Evaluating $Q_{i,b}$ at (g^α, α), we get

$$\begin{aligned} Q_{i,b}(g^\alpha, \alpha) &= Q(g^i \cdot g^\alpha, \alpha + i + b) \\ &= Q(g^{\alpha+i-b\cdot N}, \alpha + i - b \cdot N) && \text{(Since } g^N = 1 \text{ and } N = -1 \bmod p\text{)} \\ &= 0 && \text{(Since } \alpha + i - b \cdot N \in T(Q)\text{)} \end{aligned}$$

which finishes the proof. □

Lemma 3.4 (Distinctness of conjugates)**.** *Let $Q(X,Y) \in \mathbb{F}_p[X,Y]$ be a non-zero polynomial of degree less than p such that Q depends on both X and Y. For any $(i,b),(i',b) \in \{0,..,N-1\} \times \{0,1\}$ where $i \neq i'$, we have $Q_{i,b}(X,Y) \neq \lambda Q_{i',b}(X,Y)$ for any $\lambda \in \mathbb{F}_p$.*

Proof. Let $Q(X,Y)$ be of the form

$$Q(X,Y) = \sum_{i=0}^{p-1} Q^{(i)}(Y) X^i$$

where $Q^{(i)} \in \mathbb{F}_p[Y]$. Since Q depends on both X and Y, there exists some $k < p$ such that $Q^{(k)}(Y) \notin \mathbb{F}_p$. For the sake of contradiction suppose there exists $\lambda \in \mathbb{F}_p$ such that $Q_{(i,b)}(X,Y) = \lambda \cdot Q_{(i',b)}(X,Y)$. Then it follows that

$$g^{ik} \cdot Q^{(k)}(Y + i + b) \cdot X^k = \lambda \cdot g^{i'k} \cdot Q^{(k)}(Y + i' + b) \cdot X^k$$

by comparing monomials in X of degree k. By comparing coefficients of the largest degree monomial in the above expression we get that $\lambda = g^{(i-i')k}$ and $Q^{(k)}(Y+i+b) = Q^{(k)}(Y+i'+b)$. However since $i \neq i'$, it follows that $Q^{(k)}(Y) = Q^{(k)}(Y+i'-i)$. Since $\deg(Q^{(k)}(Y)) < p$, this is only possible if $Q^{(k)}(Y) \in \mathbb{F}_p$. This contradicts our choice of k and thus we are done. □

3.2 Structure of agreement set $T(Q)$

Here we will state the main observation about the geometry of $T(Q)$ when Q is an irreducible polynomial. In particular we show that $T(Q)$ cannot contain long arithmetic progressions.

Lemma 3.5. *Let $Q(X,Y) \in \mathbb{F}_p[X,Y]$ be an irreducible non-zero polynomial of degree D. Then $T(Q)$ cannot contain an arithmetic progression (over $\mathbb{Z}$) of size D^2+2.*

Proof. For the sake of contradiction assume $T(Q)$ has an arithmetic progression of size D^2+2. Let α be the starting point of the arithmetic progression and $\beta \neq 0$ be the common difference. Then,

$$\{\alpha, \alpha+\beta, ..., \alpha+(D^2+1)\cdot\beta\} \subset T(Q).$$

Since $T(Q) \subset \{0, .., N-1\}$ and the arithmetic progression is over the integers,

$$\{\alpha, \alpha+\beta, ..., \alpha+D^2\cdot\beta\} \subset \{0, .., N-1-\beta\}.$$

By definition of $T(Q)_{\beta,0}$, it follows that

$$\{\alpha, \alpha+\beta, ..., \alpha+D^2\cdot\beta\} \subset T(Q)_{\beta,0}$$

and thus by Proposition 3.3, $\alpha + i\cdot\beta$ is a root of $Q_{\beta.0}(X,Y)$ for $0 \leq i \leq D^2$. Hence $Q(X,Y)$ and $Q_{\beta,0}(X,Y)$ have D^2+1 common roots.

Recall that $Q(X,Y)$ is irreducible. By Lemma 3.4, we know that $Q(X,Y) \neq \lambda \cdot Q_{\beta,0}(X,Y)$ for any $\lambda \in \mathbb{F}_p$. Thus $\gcd(Q, Q_{\beta,0}) = 1$. By Bezout's theorem (Theorem 2.2), we get that Q and $Q_{\beta,0}$ can have at most D^2 common roots, which is a contradiction. □

Corollary 3.6. *Let $Q(X,Y) \in \mathbb{F}_p[X,Y]$ be an irreducible non-zero polynomial of degree at most D, then there exists a constant $c_D < N$ such that for any $c_D \leq i \leq N-1$, $|T(Q)_{i,0}| \geq |T(Q)| - i \cdot (\log\log i)^{-2^{-2^{D^2+11}}}$.*

Proof. Since $Q(X,Y)$ is an irreducible and non-zero polynomial of degree at most D, $Q_{i,1}(X,Y) = Q(g^iX, Y+i+1)$ is also an irreducible polynomial of degree at most D. Since $T(Q)_{i,1} \subset T(Q_{i,1})$ (Proposition 3.3), then by Lemma 3.5, $T(Q)_{i,1}$ does not contain any arithmetic progression of size D^2+2. Since $T(Q)_{i,1} \subset \{N-i, ..., .N-1\}$, by Theorem 2.4,

$$|T(Q)_{i,1}| < i \cdot (\log\log i)^{-2^{-2^{D^2+11}}}$$

Further note that $|T(Q)| = |T(Q)_{i,0}| + |T(Q)_{i,1}|$ which implies

$$|T(Q)_{i,0}| \geq |T(Q)| - i \cdot (\log\log i)^{-2^{-2^{D^2+11}}}.$$

which is the required relation. □

4 Approximation by univariate polynomials

In this section, we consider low-degree univariate polynomials $f(X) \in \mathbb{F}_p[X]$. We are interested in the number of points α for which we can have $f(g^\alpha) = \alpha$, that is, f agrees with dlog on g^α.

Theorem 4.1. *For any $\varepsilon > 0$, there exists n_ε such that for any $N \geq n_\varepsilon$, the following is true. Let $f \in \mathbb{F}_p[X]$ be a non-zero polynomial of degree D. Define $Q(X,Y) \in \mathbb{F}_p[X,Y]$ as $Q(X,Y) := Y - f(X)$. Then,*

$$|T(Q)| \leq \sqrt{DN}\left(1 + \varepsilon + \mathcal{O}(\log\log N)^{-C_\varepsilon/2}\right)$$

where $C_\varepsilon = 2^{-2^{\left(\frac{81}{4\varepsilon^4}+11\right)}}$.

Proof. Let $A = |T(Q)|$ for ease of notation. Let m be a parameter which we will set later and set $d_\varepsilon = \left\lceil \frac{9}{2\varepsilon^2} \right\rceil$. Define a list $\mathcal{L}_m \subset \mathbb{F}_p[X,Y]$ of polynomials as $\mathcal{L}_m = \{\hat{Q}_{i,0}(X,Y) \mid 1 \leq i \leq m\}$. For any $1 \leq i \leq m$, define $T_i = T(Q_{i,0})$.

Our goal is to invoke the Johnson bound (Lemma 2.3) on the sets $\{T_i\}$. We have to show the hypotheses for it are satisfied. The proof will proceed based on two cases.

- **Case $D \geq d_\varepsilon$:** Note that $|T_i| \geq |T(Q)_{i,0}| = |T(Q)| - |T(Q)_{i,1}|$. Since $T(Q)_{i,1} \subset \{N - i, ..., N-1\}$, this implies $|T(Q)_{i,1}| \leq i$ which in turn implies

  $$|T_i| \geq A - i.$$

  Hence for every $1 \leq i \leq m$, we have

  $$|T_i| \geq A - m.$$

  Next we will show that for all $i \neq j$, $|T_i \cap T_j| \leq D$. For $1 \leq i \leq m$, define $f_i(X) = f(g^i \cdot X) - i$. Then for any $1 \leq i \leq m$,

  $$Q_{i,0}(X,Y) = Y - f_i(X).$$

  By Lemma 3.4, for any $i \neq j$, $f_i(X) \neq f_j(X)$. If $\alpha \in T_i \cap T_j$, then $f_i(g^\alpha) = f_j(g^\alpha) = \alpha$ and hence g^α is a root of $f_i(X) - f_j(X)$. Since $f_i(X) - f_j(X)$ is a non-zero polynomial of degree at most D, $f_i(X) - f_j(X)$ can have at most D roots. Since for any $\alpha \neq \beta \in \{0, ..., N-1\}$, $g^\alpha \neq g^\beta$, we get $|T_i \cap T_j| \leq D$.

Now we can apply the Johnson bound (Lemma 2.3) on $T_1, ..., T_m$, and get that

$$A - m \leq \frac{N}{2m} + \sqrt{\frac{N^2}{4m^2} + ND}.$$

Setting $m = \sqrt{N/2}$, we get

$$\begin{aligned}
A &\leq \sqrt{2N} + \sqrt{\frac{N}{2} + DN} \\
&= \sqrt{DN} \cdot \left(\sqrt{1 + \frac{1}{2D}} + \sqrt{\frac{2}{D}} \right) \\
&\leq \sqrt{DN} \cdot \left(1 + \sqrt{\frac{1}{2D}} + \sqrt{\frac{2}{D}} \right) \qquad \left(\text{Since } \left(x^2 + y^2\right) \leq \left(|x| + |y|\right)^2 \right) \\
&= \sqrt{DN} \cdot \left(1 + \frac{3}{\sqrt{2D}} \right) \\
&\leq \sqrt{DN} \cdot (1 + \varepsilon) \qquad (\text{Since } D \geq d_\varepsilon).
\end{aligned}$$

Hence we have shown that

$$|T(Q)| \leq \sqrt{DN} \cdot \left(1 + \varepsilon + \mathcal{O}(\log\log N)^{-C_\varepsilon/2} \right)$$

which finishes this case.

- **Case $D < d_\varepsilon$:** We will use $D \leq d_\varepsilon$, to get a better bound on $|T_i|$ than the previous case. Just like the previous case we know that $|T_i| \geq |T(Q_{i,0})|$. By Corollary 3.6, it follows that

$$|T_i| \geq A - i \cdot (\log\log i)^{-2^{-2^{\left(\frac{81}{4\varepsilon^4} + 11\right)}}}.$$

Thus for all $1 \leq i \leq m$, it follows that

$$|T_i| \geq A - m \cdot (\log\log m)^{-C_\varepsilon}$$

where $C_\varepsilon = 2^{-2^{\left(\frac{81}{4\varepsilon^4} + 11\right)}}$.

For any $i \neq j$, just like the previous case, it follows that $|T_i \cap T_j| \leq D$. Now we apply the Johnson Bound (Lemma 2.3) on $T_1, ..., T_m$ and get that

$$A - m \cdot (\log\log m)^{-C_\varepsilon} \leq \frac{N}{2m} + \sqrt{\frac{N^2}{4m^2} + DN}.$$

Rearranging the terms we get

$$A \le \sqrt{DN} \cdot \left(\sqrt{1 + \frac{N}{4m^2 D}} + \frac{\sqrt{N}}{2m\sqrt{D}} + \frac{m \cdot (\log\log m)^{-C_\varepsilon}}{\sqrt{DN}} \right)$$
$$\le \sqrt{DN} \cdot \left(1 + \frac{\sqrt{N}}{m\sqrt{D}} + \frac{m \cdot (\log\log m)^{-C_\varepsilon}}{\sqrt{DN}} \right) \qquad \left(\text{Since } \left(x^2 + y^2\right) \le \left(|x| + |y|\right)^2 \right).$$

Setting $m = \sqrt{N} \cdot (\log\log N)^{C_\varepsilon/2}$, we get

$$A \le \sqrt{DN} \cdot \left(1 + \frac{1}{\sqrt{D} \cdot (\log\log N)^{C_\varepsilon/2}} + \frac{(\log\log N)^{C_\varepsilon/2} \cdot \left(\log\log \left(\sqrt{N} \cdot (\log\log N)^{C_\varepsilon/2} \right) \right)^{-C_\varepsilon}}{\sqrt{D}} \right)$$
$$\le \sqrt{DN} \cdot \left(1 + \mathcal{O}(\log\log N)^{-C_\varepsilon/2} \right) \qquad (\text{Since } d \ge 1 \text{ and } N \text{ is large enough})$$

Hence we have shown that

$$|T(Q)| \le \sqrt{DN} \cdot \left(1 + \varepsilon + \mathcal{O}(\log\log N)^{-C_\varepsilon/2} \right)$$

which finishes this case.

□

Remark 4.2. *The lower-order term $\sqrt{DN} \cdot (\log\log N)^{-C_\varepsilon/2}$ may be improved using stronger quantitative estimates for Szeméredi's Theorem, for instance [GT17] and [LSS24]. For ease of presentation we do not invoke those in this paper.* ⌟

5 Approximation by bivariate polynomials

In this section, we will be interested in the number of locations where a bivariate polynomial $Q(X, Y)$ may satisfy $Q(g^\alpha, \alpha) = 0$. Recall from Definition 3.2 that this set is denoted $T(Q)$.

Theorem 5.1. *For any $\varepsilon > 0$, there exists n_ε such that for any $N \ge n_\varepsilon$, if $Q(X, Y) \in \mathbb{F}_p[X, Y]$ is a non zero polynomial of degree D then,*

$$|T(Q)| \le D\sqrt{N} \left(1 + \varepsilon + \mathcal{O}(\log\log N)^{-C_\varepsilon/2} \right).$$

where $C_\varepsilon = 2^{-2^{\left(\frac{9}{2\varepsilon^2} + 11\right)}}$.

Proof. Let $Q(X, Y) = Q^{(1)}(X, Y) \cdots Q^{(\ell)}(X, Y)$ be the irreducible factorization of $Q(X, Y)$ over $\mathbb{F}_p[X, Y]$. (The polynomials $\{Q^{(i)}\}$ need not be distinct.) By an averaging argument, there exists

$i_0 \in [\ell]$ such that

$$|T(Q^{(i_0)})| \geq |T(Q)| \frac{\deg(Q^{(i_0)})}{\deg(Q)}. \tag{5.2}$$

For ease of notation let $\hat{Q} = Q^{(i_0)}$, $A = |T(\hat{Q})|$ and $d = \deg(\hat{Q})$.

Let m be a parameter which we will set later and set $d_\varepsilon = \left\lceil \frac{3}{\sqrt{2}\varepsilon} \right\rceil$. Define $\mathcal{L}_m \subset \mathbb{F}_q[X,Y]$ where $\mathcal{L}_m = \{\hat{Q}_{i,0}(X,Y) \mid 1 \leq i \leq m\}$. For any $1 \leq i \leq m$, define $T_i = T(Q_{i,0})$. The proof will move ahead based on two cases, similar to the univariate case. Once again, our goal is to prove the hypotheses for the Johnson bound are satisfied, and then invoke it.

- **Case** $d \geq d_\varepsilon$ **:** Note that $|T_i| \geq |T(\hat{Q})_{i,0}| = |T(\hat{Q})| - |T(\hat{Q})_{i,1}|$. Since $T(\hat{Q})_{i,1} \subset \{N - i, ..., N-1\}$, this implies $|T(\hat{Q})_{i,1}| \leq i$ which in turn implies

$$|T_i| \geq A - i$$

Hence for all $1 \leq i \leq m$, we have

$$|T_i| \geq A - m.$$

Next we will show that for all $i \neq j$, $|T_i \cap T_j| \leq d^2$. We know that $\hat{Q}$ is an irreducible polynomial of degree d which implies that for any $1 \leq i \leq m$, $\hat{Q}_{i,0}$ is an irreducible polynomial of degree d. For any $i \neq j$, Lemma 3.4 shows that $\hat{Q}_{i,0} \neq \lambda \cdot \hat{Q}_{j,0}$ for any $\lambda \in \mathbb{F}_p$. This is equivalent to showing that $\gcd(\hat{Q}_{i,0}, \hat{Q}_{j,0}) = 1$. By definition of $T_i's$ it is clear that $T_i \cap T_j$ is the set of common zeros of $\hat{Q}_{i,0}$ and $\hat{Q}_{j,0}$. Thus by Theorem 2.2, it follows that $|T_i \cap T_j| \leq d^2$.

Now we apply the Johnson Bound (Lemma 2.3) on $T_1, ..., T_m$ and get that

$$A - m \leq \frac{N}{2m} + \sqrt{\frac{N^2}{4m^2} + Nd^2}.$$

Now we set $m = \sqrt{n/2}$ and get

$$\begin{aligned}
A &\leq \sqrt{2N} + \sqrt{\frac{N}{2} + Nd^2} \\
&= d\sqrt{N} \cdot \left(\sqrt{1 + \frac{1}{2d^2}} + \sqrt{\frac{2}{d^2}} \right) \\
&\leq d\sqrt{N} \cdot \left(1 + \frac{1}{d\sqrt{2}} + \frac{\sqrt{2}}{d} \right) \qquad \left(\text{Since } \left(x^2 + y^2\right) \leq \left(|x| + |y|\right)^2 \right) \\
&= d\sqrt{N} \cdot \left(1 + \frac{3}{\sqrt{2}d} \right) \\
&\leq d\sqrt{N} \cdot (1 + \varepsilon) \qquad (\text{Since } d \geq d_\varepsilon).
\end{aligned}$$

Eq. (5.2) would then imply

$$|T(Q)| \leq D\sqrt{N} \cdot (1+\varepsilon).$$

Thus we are done with this case.

- **Case $d < d_\varepsilon$:** We will use $d \leq d_\varepsilon$ to get a better bound on $|T_i|$ than the previous case. Just like the previous case we know that $|T_i| \geq |T(\hat{Q})_{i,0}|$. By Corollary 3.6, it follows that

$$|T_i| \geq A - i \cdot (\log\log i)^{-2^{-2^{\left(\frac{9}{2\varepsilon^2}+11\right)}}}$$

Thus for all $1 \leq i \leq m$, it follows that

$$|T_i| \geq A - m \cdot (\log\log m)^{-C_\varepsilon}$$

where $C_\varepsilon = 2^{-2^{\left(\frac{9}{2\varepsilon^2}+11\right)}}$.

For any $i \neq j$, $|T_i \cap T_j| \leq d^2$. The argument is identical to the one in the previous case. Now we apply the Johnson Bound (Lemma 2.3) on $T_1, ..., T_m$ and get that

$$A - m \cdot (\log\log m)^{-C_\varepsilon} \leq \frac{N}{2m} + \sqrt{\frac{N^2}{4m^2} + Nd^2}.$$

Rearranging the terms we get

$$\begin{aligned} A &\leq d\sqrt{N} \cdot \left(\sqrt{1 + \frac{N}{4m^2d^2}} + \frac{\sqrt{N}}{2md} + \frac{m \cdot (\log\log m)^{-C_\varepsilon}}{d\sqrt{N}} \right) \\ &\leq d\sqrt{N} \cdot \left(1 + \frac{\sqrt{N}}{md} + \frac{m \cdot (\log\log m)^{-C_\varepsilon}}{d\sqrt{N}} \right) \qquad \left(\text{Since } \left(x^2+y^2\right) \leq \left(|x|+|y|\right)^2\right) \end{aligned}$$

Setting $m = \sqrt{N} \cdot \log\log(N)^{C_\varepsilon/2}$ we get

$$\begin{aligned} A &\leq d\sqrt{N} \cdot \left(1 + \frac{1}{d \cdot (\log\log N)^{C_\varepsilon/2}} + \frac{(\log\log N)^{C_\varepsilon/2} \cdot \left(\log\log(N^{1/2} \cdot (\log\log N))^{C_\varepsilon/2}\right)^{-C_\varepsilon}}{d} \right) \\ &\leq d\sqrt{N} \cdot \left(1 + \mathcal{O}(\log\log N)^{-C_\varepsilon/2}\right) \qquad \text{(Since } d \geq 1 \text{ and } N \text{ is large enough)} \end{aligned}$$

Eq. (5.2) would then imply

$$|T(Q)| \leq D\sqrt{N} \cdot \left(1 + \mathcal{O}(\log\log N)^{-C_\varepsilon/2}\right).$$

Hence, we are done with this case as well.

□

Remark 5.3. *Similar to the univariate case, stronger estimates for Szemeredi's theorem improve the lower-order term* $D\sqrt{N} \cdot (\log\log N)^{-C_\varepsilon/2}$. ⌟

6 Approximation by linear functions

In this section we prove bounds on approximating the discrete log by polynomials of degree 1, namely linear functions.

Theorem 6.1. *Let* $f(X) \in \mathbb{F}_p[X]$ *have degree* ≤ 1. *Then:*

$$|\{x \in \mathbb{F}_p^* \mid f(x) = \mathsf{dlog}(x)| \leq O(p^{2/5}).$$

The strategy, of proving properties of the discrete log function via the line-point incidence theorem over finite fields, comes from the analysis of Bourgain's two-source extractor [Bou05] (made especially clear in Rao's exposition [Rao07]).

6.1 Proof Overview

We first give an overview of the argument.

Let $S \subseteq \mathbb{F}_p^2$ denote the intersection of the graphs of $f(X)$ and dlog, that is:

$$S = \{(x, y) \in \mathbb{F}_p^2 \ : x \neq 0, y = \mathsf{dlog}(x), y = f(x)\}.$$

Thus S is contained in a line in $\mathbb{F}_p^2$. Let $T \subseteq \mathbb{F}_p$ be the projection of S to the first coordinate:

$$T = \{x \in \mathbb{F}_p^* \mid \mathsf{dlog}(x) = f(x)\}.$$

Now consider the iterated sumset $S + S + S$.

On the one hand, $S + S + S$ is contained in a line in $\mathbb{F}_p^2$: indeed, if $f(X) = aX + b$, then every element (x, y) of $S + S + S$ satisfies $y = ax + 3b$. This means that $|S + S + S| \leq p$.

On the other hand

$$S + S + S = \{(x_1 + x_2 + x_3, \mathsf{dlog}(x_1) + \mathsf{dlog}(x_2) + \mathsf{dlog}(x_3)) \mid x_1, x_2, x_3 \in T\}.$$

Let us pretend for the moment that dlog satisfies the exact homomorphism identity $\mathsf{dlog}(u) + \mathsf{dlog}(v) = \mathsf{dlog}(uv)$. Then $S + S + S = \{x_1 + x_2 + x_3, \mathsf{dlog}(x_1x_2x_3) \mid x_1, x_2, x_3 \in T\}$, and thus $S + S + S$ has the same size as the set $\mathcal{P}$ given by:

$$\mathcal{P} = \{(x_1 + x_2 + x_3, x_1x_2x_3) \mid x_1, x_2, x_3 \in T\}.$$

We now define a set $\mathcal{L}$ of lines in $\mathbb{F}_p^2$. For each $\{x_1, x_2\} \subseteq T$, define the line $L_{x_1,x_2} = \{x_1 + x_2 +$

$z, x_1x_2z) \mid z \in \mathbb{F}_p\}$. There are $\binom{|T|}{2}$ such lines, and each is incident to $|T|$ points of $\mathcal{P}$. Putting this incidence data about $\mathcal{L}$ and $\mathcal{P}$ into the line-point incidence theorem, along with our upper bound $|\mathcal{P}| \leq p$, gives the desired upper bound on $|T|$.

This concludes the proof overview. The only gap in this is the wished-for exact homomorphic property of dlog, which is not quite true because of wrap-around. To get around this, we will zoom in on subsets of S and T where some version of the homomorphic property holds.

6.2 Proof of Theorem 6.1

We start by partitioning S (and T) into m buckets, for a parameter m which we will fix later (to equal 2 or 3).
Define $S_{i,m}$ by:

$$S_{i,m} := \left\{(x, \mathsf{dlog}(x)) \in S \ : \ \frac{i-1}{m}(p-1) \leq \mathsf{dlog}(x) < \frac{i}{m}(p-1)\right\}$$

then note that $S_{i,m}$ for $i \in [m]$ partition S.

Further, let T and $T_{i,m}$ denote the respective projections of these sets to their first coordinate. That is, $T = \{x : (x, \mathsf{dlog}(x)) \in S\}$ and similarly for $T_{i,m}$.

We define a k-fold "sum and product" operation $U^{\star k}$ on subsets $U \subset \mathbb{F}_p$. This operation is motivated by the property of the (standard) logarithm: $\log(ab) = \log(a) + \log(b)$.

Definition 6.2. *For sets $U \subseteq \mathbb{F}_p$ and $k \in \mathbb{N}$, let*

$$U^{\star k} = \{(u_1 + u_2 + \cdots + u_k, u_1u_2...u_k) \in \mathbb{F}_p^2 : u_i \in U \ \forall \ i \in [k]\}.$$

⌟

We will now prove some properties of the sets $T_{i,m}$ under this operation.

Lemma 6.3. *For any i, m, $|T_{i,m}^{\star m}| = |m \cdot S_{i,m}|$.*

Recall that $m \cdot V$ denotes the m-fold sumset $V + V + \ldots + V$.

Proof. We prove this by defining a bijection

$$\begin{aligned} \phi : T_{i,m}^{\star m} &\to m \cdot S_{i,m} \\ (a, b) &\mapsto (a, \mathsf{dlog}(b) - (i-1)). \end{aligned}$$

We first have to show this map is well-defined, that is, the image of any element under the map lies in $m \cdot S_{i,m}$ as claimed. Take $(a, b) \in T_{i,m}^{\star m}$. Then, there exist $a_1, \ldots, a_m \in T_{i,m}$ such that $a = a_1 + \cdots + a_m$, $b = a_1a_2 \ldots a_m$. Let $b_j = \mathsf{dlog}(a_j)$ for each j; we are left to show

$\mathsf{dlog}(b) - (i-1) = b_1 + \cdots + b_m$. Since each $a_j \in T_{i,m}$, we have $\frac{i-1}{m}(p-1) \leq b_j < \frac{i}{m}(p-1)$. Then, $(i-1)(p-1) \leq \sum b_j < i(p-1)$.

$$\begin{aligned}\mathsf{dlog}(b) &= \mathsf{dlog}(a_1 a_2 \dots a_m) \\ &= \mathsf{dlog}(a_1) + \cdots \mathsf{dlog}(a_m) - (i-1)(p-1) \text{ since } (i-1)(p-1) \leq \sum \mathsf{dlog}(a_j) < i(p-1) \\ &\equiv b_1 + \cdots + b_m + (i-1) \mod p.\end{aligned}$$

This shows the map is well-defined. Now we are left to show injectivity and surjectivity.

For injectivity, suppose $\phi(a_1, b_1) = (a_2, b_2)$. Since ϕ fixes the first coordinate, we have $a_1 = a_2$. Further, we have $\mathsf{dlog}(b_1) = \mathsf{dlog}(b_2)$ which implies $b_1 = b_2$.

For surjectivity, let $(a', b') = (a_1 + \cdots + a_m, \mathsf{dlog}(a_1) + \cdots + \mathsf{dlog}(a_m)) \in m \cdot S_{i,m}$. By a similar argument to the well-definedness case, we can pick (a, b) with $a = a' = \sum a_j$ and $b = \prod_j a_j$, which would give $\phi(a, b) = (a', b')$ as required. □

Proposition 6.4. *Let $S \subseteq \mathbb{F}_p^2$ be the agreement set as above and T its projection onto the first coordinate. Then, $|2 \cdot S| \geq \frac{|T|^2}{8}$.*

Proof. Recall that T may be subdivided into $T_{1,2}$ and $T_{2,2}$. Without loss of generality we assume $|T_{1,2}| \geq |T|/2$, otherwise in the below argument replace $T_{1,2}$ with $T_{2,2}$.

Now since $S_{1,2} \subseteq S$,

$$|2 \cdot S| \geq |2 \cdot S_{1,2}| = |T_{1,2}^{\star 2}|$$

where the equality follows from Lemma 6.3.

We also have that $|T_{1,2}^{\star 2}|$ is at least the number of pairs (with repetition) up to ordering in $T_{1,2}$. This is because an element of $|T_{1,2}^{\star 2}|$ is a pair of the form $(a_1 + a_2, a_1 a_2)$, which determines a_1 and a_2 in $T_{1,2}$ up to labeling. Hence,

$$|T_{1,2}^{\star 2}| \geq \frac{|T_{1,2}|^2}{2}$$

Combining with the above, we have

$$|2 \cdot S| \geq \frac{|T_{1,2}|^2}{2} \geq \frac{|T|^2}{8}$$

which completes the proof. □

We are now ready to prove the main theorem of the section.

Proof of Theorem 6.1. Let c be a constant that we will fix later; we will eventually show $|S| < c(p^{1/2-\varepsilon})$ for some $\varepsilon > 0$.

Assume for contradiction that $|S| \geq c(p^{1/2-\varepsilon})$. Divide S into $S_{1,3}, S_{2,3}$ and $S_{3,3}$ as defined above (that is, $m = 3$). At least one of these has size at least $|S|/3$; replace S by that set $S_{i,3}$ and drop any extraneous elements so that $|S| = \frac{c}{3}(p^{1/2-\varepsilon})$ exactly.

Let T be the projection of S to the first coordinate, and thus $|T| = |S|$. Recall that $T^{\star 2}$ consists of pairs; take a pair $(a, b) \in T^{\star 2}$ and define the line $L_{a,b} = \{(a + z, bz) \ : \ z \in \mathbb{F}\}$. Let $\mathcal{L} = \{L_{a,b} : (a, b) \in T^{\star 2}\}$. This will be the set of lines that we invoke the line-point incidence result with. Observe that $|\mathcal{L}| = |T^{\star 2}|$.

Now, since every $(a, b) \in T^{\star 2}$ comes from two elements in T up to ordering, we have

$$\frac{|T|^2}{2} \leq |T^{\star 2}| \leq |T|^2$$

Substituting the bounds on T as per the contradiction assumption, and the observation about $\mathcal{L}$,

$$\frac{c^2 p^{1-2\varepsilon}}{18} \leq |\mathcal{L}| \leq \frac{c^2 p^{1-2\varepsilon}}{9}.$$

The set of points $\mathcal{P}$ we will use will be $T^{\star 3}$. By Lemma 6.3, $|T^{\star 3}| = |3 \cdot S|$. Recall that S was a subset of the original line that purported to approximate dlog. Hence, $3 \cdot S$ is also a subset of some line, and hence $|3 \cdot S| \leq p$. Then, we can conclude that $|T^{\star 3}| \leq p$.

We need to lower-bound the size of $\mathcal{P}$ as well. We have

$$|T^{\star 3}| = |3 \cdot S| \geq |2 \cdot S| \geq \frac{|T|^2}{8}.$$

where the last inequality is by Proposition 6.4. Then, combined with the contradiction assumption, this gives

$$\frac{c^2}{72} p^{1-2\varepsilon} \leq |\mathcal{P}| \leq p.$$

Now, $\mathcal{P}$ consists of points $(a_1 + a_2 + a_3, a_1 a_2 a_3)$ while $\mathcal{L}$ consists of lines of the form $\{(a_1 + a_2 + z, a_1 a_2 z) : z \in \mathbb{F}_p\}$. From this form, it is clear that any $z \in T$ and $L_{a,b} \in \mathcal{L}$ gives an incidence. Then,

$$\mathcal{I}(\mathcal{P}, \mathcal{L}) \geq |T||\mathcal{L}| \geq \frac{c^3 p^{3/2-3\varepsilon}}{54}$$

For a large enough prime p, we have $|\mathcal{P}| \cdot |\mathcal{L}| \leq \frac{c^2}{9} p^{2-2\varepsilon} \leq p^3$, which is the hypothesis of Theorem 2.5.

Then, we can invoke the bound to conclude

$$\begin{aligned}
|\mathcal{I}(\mathcal{P}, \mathcal{L})| &\leq 3(|\mathcal{L}| \cdot |\mathcal{P}|)^{2/3} + |\mathcal{L}| + |\mathcal{P}| \\
&\leq 3 \cdot \left(\frac{c^2}{9} p^{2-2\varepsilon}\right)^{2/3} + \left(\frac{c^2 p^{1-2\varepsilon}}{9}\right) + p \\
&\leq 3 \left(\frac{c^2}{9}\right)^{2/3} p^{\frac{4(1-\varepsilon)}{3}} + O(p)
\end{aligned}$$

which is a contradiction for $\varepsilon = 1/10$ and a large enough constant c.

□

References

[BCP+26] Joshua Brakensiek, Yeyuan Chen, Aaron Putterman, Zihan Zhang, and Kai Zhe Zheng. Algorithmic list decoding of Reed-Solomon codes up to capacity. *arXiv preprint arXiv:2609.08005*, 2026. 3

[BKT04] Jean Bourgain, Nets Katz, and Terence Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1):27–57, February 2004. 3, 5

[Bou05] J. Bourgain. More on the sum-product phenomenon in prime fields and its applications. *International Journal of Number Theory*, 01(01):1–32, 2005. 3, 13

[BW26] Pierre-Yves Bienvenu and Arne Winterhof. Additive index and Carlitz rank, 2026. 2

[CS00] Don Coppersmith and Igor Shparlinski. On polynomial approximation of the discrete logarithm and the Diffie–Hellman mapping. *Journal of Cryptology*, 13(3):339–360, 2000. 1, 2

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. 1

[Ful89] William Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. Advanced Book Classics. Addison-Wesley Publishing Company, 1989. 4

[Gow01] W. T. Gowers. A new proof of Szemerédi's theorem. *Geometric & Functional Analysis GAFA*, 11(3):465–588, 2001. 5

[GRS00] Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan. Learning polynomials with queries: The highly noisy case. *SIAM J. Discret. Math.*, 13(4):535–570, 2000. 4

[GT17] Ben Green and Terence Tao. New bounds for Szemerédi's theorem, iii: A polylogarithmic bound for. *Mathematika*, 63(3):944–1040, 2017. 10

[HKS26] Prahladh Harsha, Mrinal Kumar, and Ramprasad Saptharishi. Reed-Solomon codes at capacity: Algorithmic list-decoding and proximity gaps. *arXiv preprint arXiv:2610.08610*, 2026. 3

[IW18] Leyla Işık and Arne Winterhof. Carlitz rank and index of permutation polynomials. *Finite Fields and Their Applications*, 49:156–165, 2018. 2

[KK23] Kiran Kedlaya and Swastik Kopparty. On the degree of polynomials computing square roots mod p. *arXiv preprint arXiv:2311.10956*, 2023. 3

[KW06] Eike Kiltz and Arne Winterhof. Polynomial interpolation of cryptographic functions related to Diffie–Hellman and discrete logarithm problem. *Discrete Applied Mathematics*, 154(2):326–336, 2006. 2

[Lew26] Mark Lewko. A Szemerédi-Trotter theorem in arbitrary fields. *arXiv preprint arXiv:2609.27023*, 2026. 3, 5

[LSS24] James Leng, Ashwin Sah, and Mehtaab Sawhney. Improved bounds for Szemerédi's theorem. *arXiv preprint arXiv:2402.17995*, 2024. 10

[MX26] Changxing Miao and Rui Xie. The Szemerédi-Trotter estimate in finite field with its applications. *arXiv preprint arXiv:2609.35190*, 2026. 3, 5

[NW02] Harald Niederreiter and Arne Winterhof. Incomplete character sums and polynomial interpolation of the discrete logarithm. *Finite Fields and Their Applications*, 8(2):184–192, 2002. 2

[Rao07] Anup Rao. An exposition of Bourgain's 2-source extractor. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 14, 2007. 3, 13

[Win02] Arne Winterhof. Polynomial interpolation of the discrete logarithm. *Designs, Codes and Cryptography*, 25(1):63–72, 2002. 2

[Yu26] Hung-Hsun Hans Yu. Two proofs and a tight Szemerédi–Trotter theorem. *arXiv preprint arXiv:2610.10649*, 2026. 3, 5