Roots of Sparse Polynomials over Finite Fields

Zander Kelley

Texas A&M University

UNDERGRADUATE
RESEARCH
SCHOLAR

Motivation: Finite Fields and Cryptography

- For a prime p, the associated prime field $\mathbb{F}_p$ is the set $\{0, 1, 2, \ldots, p-1\}$ equipped with *modular* addition and multiplication (i.e the results of computations "wrap around").
- Example: $\mathbb{F}_{11} = \{0, 1, 2, \ldots, 10\}$
  - $7 + 8 \quad = 15 \pmod{11} = 4$
  - $7 - 8 \quad = -1 \pmod{11} = 10$
  - $6 * 8 \quad = 48 \pmod{11} = 4$
  - $6/4 \quad = 8$
  - $2^4 \quad = 16 \pmod{11} = 5$
  - $\log_2 5 \quad = 4$
- There is no known fast algorithm for taking logs in finite fields (modular exponentiation is a "one-way function").

The Diffie-Hellman Public Key Exchange

- To send and receive encrypted messages, two parties must agree on a secret key k, a large integer which can be used to scramble and unscramble messages.
- Establishing a shared key over the Internet is a challenge: it is very easy to intercept or eavesdrop on messages.
- The Diffie-Hellman key exchange creates privacy in a public world (by using exponentiation in $\mathbb{F}_p$).

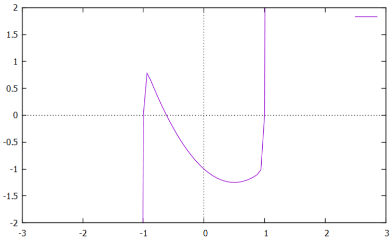
Alice	(public)	Bob
Pick a large prime p	$\longrightarrow p \longrightarrow$	
Pick a number $g \in \mathbb{F}_p$	$\longrightarrow g \longrightarrow$	
Pick a random $x \in \mathbb{F}_p$		Pick a random $y \in \mathbb{F}_p$
Compute & Send $g^x = a$	$\longrightarrow a \longrightarrow$	
	$\longleftarrow b \longleftarrow$	$b = g^y$
Set $k = b^x = (g^y)^x = g^{xy}$		$k = a^y = (g^x)^y = g^{xy}$

Canneti et al. - Statistical Properties of D-H Triples

- It is important that the result of D-H, $k = g^{xy}$, is not predictable.
- In 2002, Canetti et al. prove that the triples (g^x, g^y, g^{xy}) become uniformly disturbed as $p \to \infty$.
- The heart of their proof relies on an upper bound on the number of roots of tetranomials over $\mathbb{F}_p$ - polynomials of the form $f(x) = x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4}$.
- Since then, this bound has proved to be widely useful and has been applied to many other number-theoretic problems.

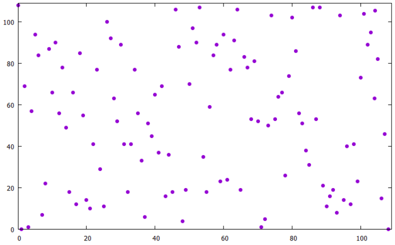
$\mathbb{R}$ vs $\mathbb{F}_p$

$x^{51} + x^2 - x - 1$ over $\mathbb{R}$



- #roots ≤ 51
  (degree bound)
- #roots $\leq 2(\#\text{terms}) = 8$
  (Descartes' rule)

$x^{51} + x^2 - x - 1$ over $\mathbb{F}_{109}$



- #roots ≤ 109
  (trivial bound)
- #roots ≤ 51
  (degree bound)

Refined Version of Sparsity-Dependent Bound

Let $f(x) = c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_t x^{a_t} \in \mathbb{F}_p[x]$.

Theorem (Canetti et al., 2002)

$$\#\text{roots}(f) \le 2(p-1)^{1-\frac{1}{t-1}} D^{\frac{1}{t-1}} + O\left((p-1)^{1-\frac{2}{t-1}} D^{\frac{2}{t-1}}\right),$$

where $D = \min_i \max_{j \neq i} \gcd(a_i - a_j, p-1)$.

Theorem (ZK, 2016)

$$\#\text{roots}(f) \le 2(p-1)^{1-\frac{1}{t-1}} C^{\frac{1}{t-1}},$$

where $C = \max\{|H| \ : \ H \le \mathbb{F}_p^* \text{ and } f|_{aH} \equiv 0 \text{ for some } a \in \mathbb{F}_p^*\}$. Furthermore,

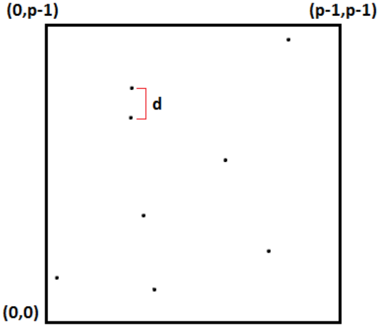
$$C \le \max\{k \mid (p-1) \ : \ \forall a_i, \exists a_{j \neq i} \text{ with } a_i \equiv a_j \bmod k\} \le D.$$

Outline of Proof

- Let $f(x) = c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_t x^{a_t} \in \mathbb{F}_p[x]$.
- The map $x \mapsto x^e$ is a bijection (unless $\gcd(e, p-1) > 1$), so it simply shuffles the elements of $\mathbb{F}_p$.
- Let $g(x) = f(x^e) = c_1 x^{ea_1} + c_2 x^{ea_2} + \cdots + c_t x^{ea_t}$.
- For all $x \in \mathbb{F}_p$, $x^{p-1} = 1$.
- Let $h(x) = c_1 x^{ea_1 \bmod (p-1)} + \cdots + c_t x^{ea_t \bmod (p-1)}$.
- We have $\#\text{roots}(f) = \#\text{roots}(g) = \#\text{roots}(h) \leq \text{degree}(h)$.
- Idea: find e so that all of the exponents of h are small.

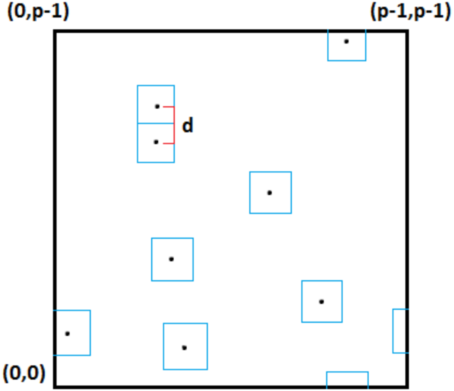
Reduction to Geometric Problem

- For $e = 1, 2, \ldots, p-1$, let
  $l_e = (ea_1 \bmod (p-1), \ldots, ea_t \bmod (p-1))$;
  look for l_e with small norm $\|l_e\| = \max_i |ea_i \bmod (p-1)|$.
- $l_i - l_j = l_{(i-j)}$, so we can equivalently look for two nearby vectors and take their difference.
- Let $d = \min_{i<j} \|l_i - l_j\|$.



Two-Dimensional Example

- $d = \min_{i<j} \|l_i - l_j\|$.
- $n \cdot \text{volume}(B) \leq \text{volume}(\Omega)$.
- $(p-1) \cdot d^2 \leq (p-1)^2 \implies d \leq \sqrt{p-1}$.
- By backtracking, we prove that $\#\text{roots}(f) \leq \sqrt{p-1}$.



Roots of Sparse Polynomials over Finite Fields

Zander Kelley

Texas A&M University

UNDERGRADUATE
RESEARCH
SCHOLAR