# Roots of Sparse Polynomials over a Finite Field

Zander Kelley

ANTS-XII

August 30, 2016

# Sparsity-Dependant Bounds

$$f(x) = c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_t x^{a_t} \in \mathbb{R}[x].$$

- $f$ is "sparse" if $t \ll \deg f$.
- Descartes' Rule of Signs: The number of positive, real roots of $f$ is bounded by the number of sign alternations in the sequence $(c_0, c_1, \ldots, c_t)$.
- Thus, $f$ has no more than $2t$ real roots.
- Question: Do similar sparsity-dependent bounds exists for other non-algebraically closed fields?

# Sparsity-Dependant Bound over $\mathbb{F}_q$

$$f(x) = c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_t x^{a_t} \in \mathbb{F}_q[x].$$

**Theorem (Canetti, Friedlander, Konyagin, Larsen, Lieman, Shparlinski - 2002)**

$$\#\text{roots}(f) \leq 2(q-1)^{1-1/t} D^{1/t} + O\left((q-1)^{1-2/t} D^{2/t}\right),$$

where

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

- For $\vartheta \in \mathbb{F}_p^*$, the associated Diffie-Hellman distribution is the set of triples $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ with $x, y \in \{1, 2, \ldots, p\}$.
- Application: Diffie-Hellman distributions are nearly uniform in $[0, p)^3$ when $p$ is large for $\vartheta$ of high order.

# Improved Bound

$$f(x) = c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_t x^{a_t} \in \mathbb{F}_q[x].$$

## Theorem (ZK - 2016)

$$\#\text{roots}(f) \leq 2(q-1)^{1-1/t} C^{1/t},$$

where

$$C = \max\{\#H \ : \ H \leq \mathbb{F}_q^* \text{ and } f|_{aH} \equiv 0 \text{ for some } a \in \mathbb{F}_q^*\}.$$

## Proposition

- $C(f) \in \{k \mid (q-1) \ : \ \forall a_i, \exists a_{j \neq i} \text{ with } a_i \equiv a_j \bmod k\}$
- $C(f) \leq D(f) = \min_i \max_{j \neq i} \gcd(a_i - a_j, q-1)$.
- $C(f) \mid Q(f) = \gcd_i \operatorname{lcm}_{j \neq i} \gcd(a_i - a_j, q-1)$.

# Sketch of Proof

$$f(x) = c_0 + c_1 x^{a_1} + c_2 x^{a_2} + \cdots + c_t x^{a_t} \in \mathbb{F}_q[x].$$

- Suppose $\gcd(e, q-1) = 1$: then, the map $x \mapsto x^e$ is a bijection which simply shuffles the elements of $\mathbb{F}_q^*$.
- Let $g(x) = f(x^e) = c_0 + c_1 x^{ea_1} + c_2 x^{ea_2} + \cdots + c_t x^{ea_t}$.
- Let $h(x) = c_0 + c_1 x^{ea_1 \bmod (q-1)} + \cdots + c_t x^{ea_t \bmod (q-1)}$.
- 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.

If $k = \gcd(e, q-1) > 1$, then we still have

$$\#\text{roots}(f) = \frac{1}{k} \sum_{i=0}^{k} \#\text{roots}(f(\sigma^i x^e)) \leq \text{degree}(h),$$

unless $f(\sigma^i x^e)$ is identically zero for some $i$. Thus we are safe to choose $e \in \{1, 2, \ldots, (q-1)/C(f) - 1\}$.

# A Short Vector mod $q-1$ by Volume-Packing

**Lemma**

Let $a_1, a_2, \ldots, a_t, N \in \mathbb{N}$. If $1 < n \leq N$, there is an $e \in \{1, 2, \ldots, n-1\}$ and a $v \in N\mathbb{Z}^t$ so that

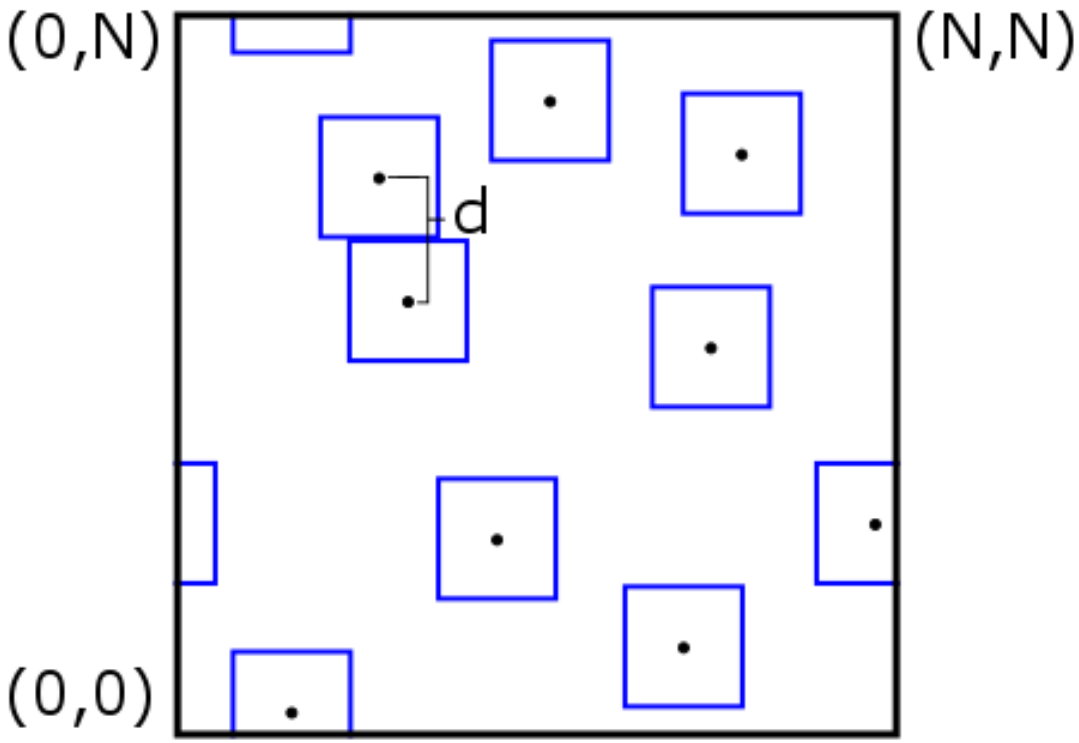
$$\max_{1 \leq i \leq t} |ea_i + v_i| \leq N/n^{1/t}.$$

*proof:*

- Consider the vectors $l_i = i(a_1, \ldots, a_t) = (ia_1, \ldots, ia_t) \in (\mathbb{R}/N\mathbb{Z})^t$ for each $i \in \{1, 2, \ldots n\}$.
- Define $\|l\|_N = \min_{v \in N\mathbb{Z}^t} \|l + v\|_\infty$.
- We need only to find two nearby vectors $l_i$ and $l_j$, since we can set $e = j - i$ and $l_e = l_{j-i} = l_j - l_i$.

# A Short Vector mod $q-1$ by Volume-Packing

- Let $d = \min_{1 \le i < j \le n} \|l_j - l_i\|_N$.
- Each of the vector $l_i$ sits in its own personal box $B_i = \{x \in (\mathbb{R}/N\mathbb{Z})^t \ : \ \|x - l_i\|_N < d/2\}$.
- By representing these sets in the fundamental domain $[0, N)^t$, we get the volume constraint $nd^t \le N^t \implies d \le N/n^{1/t}$.



# How good is the bound?

Let $f(x) = \sum_{i=1}^{t} c_i x^{a_i} \in \mathbb{F}_q[x]$.
Let $R(f) = \#\{x \in \mathbb{F}_q^* \ : \ f(x) = 0\}$.
Recall that $R(f) \leq 2(q-1)^{1-1/(t-1)} C(f)^{1/(t-1)}$.

- When $t \mid q-1$, $f(x) = (x^{q-1}-1)/(x^{(q-1)/t}-1)$ is a $t$-nomial with $C(f) = (q-1)/t$ and $R(f) = (1-1/t)(q-1)$.
- When $q$ is an odd square, $f(x) = x^{q^{1/2}} + x - 2$ has $C(f) = 1$ and $R(f) = q^{1/2}$.
- Cheng, Gao, Rojas, and Wan provide a family of $t$-nomials with $C(f) \leq t/2$ and $R(f) \geq q^{1-2/t}$.

Observation: all known examples of sparse polynomials which attain a large number of roots do so by vanishing on entire cosets of subgroups or on entire translations of subspaces.

# Computer Data for Prime Fields

$\mathcal{F}(p) = \{f \in \mathbb{F}_p[x] \ : \ \deg f < p-1\}.$
$\mathcal{F}(p,t) = \{f \in \mathcal{F}(p) \ : \ f \text{ has } t \text{ terms}\}.$
$\mathcal{F}_1(p) = \{f \in \mathcal{F}(p) \ : \ C(f) = 1\}.$
$\mathcal{F}_1(p,t) = \{f \in \mathcal{F}(p,t) \ : \ C(f) = 1\}.$

$$\text{Let } R_{p,t} = \max\{R(f) \ : \ f \in \mathcal{F}_1(p,t)\}.$$

- $R_{p,3} < 1.8 \log p$ for $p \leq 139571$.
- $R_{p,4} < 2.5 \log p$ for $p \leq 907$.
- $R_{p,5} < 2.9 \log p$ for $p \leq 101$.
- (Compare to the current bound $R_{p,t} = O(p^{1-1/(t-1)})$).

# A Possible Explanation

$\mathcal{F}(p) = \{f \in \mathbb{F}_p[x] \ : \ \deg f < p-1\}$.
$\mathcal{F}(p,t) = \{f \in \mathcal{F}(p) \ : \ f \text{ has } t \text{ terms}\}$.
$\mathcal{F}_1(p) = \{f \in \mathcal{F}(p) \ : \ C(f) = 1\}$.
$\mathcal{F}_1(p,t) = \{f \in \mathcal{F}(p,t) \ : \ C(f) = 1\}$.

Fact: $\dfrac{\#\{f \in \mathcal{F}(p) \ : \ R(f) = r\}}{\#\mathcal{F}(p)} \leq \dfrac{1}{r!}$.

Heuristic: *$R(f)$ and $t(f)$ are statistically independent properties of a random $f \in \mathcal{F}_1(p)$.*

## Conjecture

There exists a constant $\gamma > 0$ such that

$$\frac{\#\{f \in \mathcal{F}_1(p,t) \ : \ R(f) = r\}}{\#\mathcal{F}_1(p,t)} \leq \left(\frac{1}{r!}\right)^{\gamma}$$

for all $p$ prime, $t \in \mathbb{N}$, and $r \in \mathbb{N}$.

# A Possible Explanation

**Conjecture**

There exists a constant $\gamma > 0$ such that

$$\frac{\#\{f \in \mathcal{F}_1(p,t) \ : \ R(f) = r\}}{\#\mathcal{F}_1(p,t)} \leq \left(\frac{1}{r!}\right)^{\gamma}$$

for all $p$ prime, $t \in \mathbb{N}$, and $r \in \mathbb{N}$.

- We have checked by computer that this inequality holds with $\gamma = 1/2$ in the following cases.
  - $t = 3$, $p \leq 30977$
  - $t = 4$, $p \leq 907$
  - $t = 5$, $p \leq 101$
- This inequality is true if we restrict to trinomials of low degree (by the function field Chebotarev density theorem).
- If this conjecture is true, we have $R_{p,t} = O(t \log p)$.

# Roots of Sparse Polynomials over a Finite Field

Zander Kelley

ANTS-XII

August 30, 2016