Counting points on hypersurfaces: algorithms & complexity

(Affine)

1. The problem

$f(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$ $\quad q = p^h$ $\quad p = \mathrm{char}(\mathbb{F}_q)$

$$N(f) = \#\{(x_1, \dots, x_n) \in \mathbb{F}_q^n \mid f(x_1, \dots, x_n) = 0\}$$

By CRT, it is enough to study

$N_r(f) := N(f) \bmod r$, where $r = \begin{cases} \ell^b \\ p^b \end{cases}$, $\ell \neq p$ prime

Questions. 1) Decision version: when is $N(f) > 0$?
2) Counting version: evaluate $N(f)$
3) Modular counting: what is $N_r(f)$?

Input 1) Sparse input
2) Dense input
3) black-box input (g can only evaluate the polynomial) (not discussed here)

2. Sparse input

$$f = \sum_{j=1}^{m} a_j x_1^{v_{j1}} \cdots x_n^{v_{jn}}, \quad a_j \in \mathbb{F}_q^*, \quad 0 \le v_{ji} \le q-1$$

(can reduce, $x_i^q - x_i$)

Input size: $mn \log q$, $n \le m \le q^n$

Output size: $n \log q$

Trivial alg: $\tilde{O}(mnq^n) = \tilde{O}(mn\, 2^{n \log q})$, exp in n and $\log q$

2.1 Complexity

In general, all problems 1) – 3) are NP-hard.

eg. $f = a_1 x_1^{q-1} + \dots + a_n x_n^{q-1} - b$ $/\mathbb{F}_q = \mathbb{F}_{p^h}$

$N(f) > 0 \Leftrightarrow \exists \{a_{i_1}, \dots, a_{i_R}\}$ s.t. $a_{i_1} + \dots + a_{i_R} = b$

Theorem (Goplan-Guruswami-Lipton, 2006)

1) Deciding if $N(f) > 0$ is NP-hard if $ph \geq 2n$ (i.e. q large)

2) For any p fixed $r \neq p^b$, computing $N_r(f)$ is NP-hard under RP-reduction.

3) For $r = p^b$, computing $N_{p^b}(f)$ is NP-hardor under RP-reduction if $\begin{cases} \text{either } p \geq 2n & (\text{i.e. } q \text{ large}) \\ \text{or } h \geq 2n & \\ \text{or } b \geq nh & (p^b > q^n) \end{cases}$

"Cor" (under NP ≠ P)

1) Deciding if $N(f) > 0$ is fully exponential in p and h

2) Computing $N_{p^b}(f)$ is fully exponential in $\{p, b, h\}$

2.2 Algorithm

Thm:1 (Grigoriev-Karpinski, 1991)

Deciding if $N(f) > 0$ can be done in time $O(nm^q) = O(nm^{p^h})$

($\in P$ if q is fixed)

2) (GGL, 2006)

$N_{p^b}(f)$ can be computed in time $O(n m^{2qb}) = O(nm^{2p^{hb}})$

Thm (Wan, FOCM, 2008)

1) Deciding if $N(f)>0$ can be done in time $O(nm^{ph})$

2) $\in N_{pb}(f)$ can be computed in time $O(nm^{(h+b)p})$

Proof of 1): $N(f)=0 \iff f(x)^{q-1} \equiv 1 \pmod{x_1^q - x_1, \dots, x_n^q - x_n}$

$$f(x)^{(p-1)(1+p+\dots+p^{h-1})}$$

$$\prod_{i=}^{h-1} f^{\sigma^i}(x^{p^i})^{p-1}, \quad \sigma = Frob_p.$$

3. Dense input

$\deg(f) \le d$, $d \ge 2$.

$$f = \sum_{0 \le i_1+\dots+i_n \le d} a_{i_1,\dots i_n} x_1^{i_1} \dots x_n^{i_n}, \quad a_{i_1,\dots i_n} \in \mathbb{F}_q$$

Input size: $\tilde{O}(d^n \log q)$

Output size: $O(n \log q)$

Trivial alg: $O(d^n q^n) = O(d^n \cdot 2^{n \log q})$ ← aim to bring $\log q$ down as already exp. in n from input.

Problem: Is it possible to do the following in $\text{tm } O(d^n \log q)^{O(1)}$?

I. Decide if $N(f)>0$?

II. Evaluate $N(f)$.

3.1 Decision version

Thm: 1) (Huang-Wong, 1996) Deciding if $N(f)>0$ can be done in random time $O(d^{n^{O(n)}} \log q)^{O(1)}$

2) (Kayal, 2005) Deciding if $N(f)>0$ can be done in time $O(d^{2^{O(n)}} \log q)^{O(1)}$.

Proof: • If f has an absolutely irred. factor, use Lang-Weil for large q.

• If f is exceptional, $N(f) = N(V)$, $\dim V < n-1$ reduce to 0-dim

3.2 Counting version

If $n=1$, $N(f) = \gcd(f(x), x^q - x)$,

can be computed in time $O(d \log q)^{O(1)} \in P$

If $n=2$, $N(f)$ can be computed in time

$\begin{cases} O(d^{2^d} \log q)^{O(1)} & \text{(Schoof-Pila-Adleman-Huang)} \\ O(dp \log q)^{O(1)} & \text{(Kedlaya, ...)} \\ & \text{(Monsky trace formula)} \end{cases}$

For general n,

Thm: (Lauder-Wan, 01-08)

1) $N(f)$ can be computed in time $O(pdn \log q)^{O(n)}$ ($\in P$ if p is small)

2) $Z(f,T)$ can be computed in time $O(d^n p \log q)^{O(n)}$

Thm: (Lauder, 2004) If $f(x_1, \ldots, x_n)$ is sufficiently smooth of degree $d \nmid p$, then $Z(f,T)$ can be computed in time $O(d^n p \log q)^{O(1)}$ ($\in P$ if p is small)

Open problem: Can the smoothness condition be removed?

See: Kloosterman's talk, Lauder's talk

Question: For a fixed $\ell \neq p$, can $N_\ell(f)$ be computed in time $O(n \log q)^{O(n)}$?