On Blackbox Polynomial Identity Testing of sparse polynomials

Devansh Shringi

Advisor: Prof. Markus Bläser

June 28, 2022

1 New Hitting Set for Sparse Polynomials

We have as input $f \in \mathbb{F}_m[x_1, \ldots, x_n]$ such that f has m monomials and $\mathbb{F}$ is field like $\mathbb{R}$ or $\mathbb{Q}$ where Descartes' rule of signs follow.

Define the set

$$\mathcal{S}(n, m) := \{(c_1, \ldots, c_n) | c_i \in [m] \text{ and } \prod_{i=1}^{n} c_i \leq m\}$$

Lemma 1.1. *$\mathcal{S}(n, m)$ is a hitting set for $\mathbb{F}_m[x_1, \ldots, x_n]$.*

Proof. We will prove this by induction over n. For $n = 1$ and any $m \geq 1$, we have by Descartes' rule of signs that number of positive roots $\leq$number of sign changes, which is <m. So in the set $\{1, \ldots, m\}$, there must be a value for which the univariate is non-zero.

Now in the induction hypothesis we assume, for all m, $\mathcal{S}(n-1, m)$ is a hitting set for $\mathbb{F}_m[x_1, \ldots, x_{n-1}]$. Now consider for any m, $f \in \mathbb{F}_m[x_1, \ldots, x_n]$ as input. We consider it as a univariate in x_n as $f = \sum_{i=1}^{s_n} P_i(x_1, \ldots, x_{n-1}) x_n^{d_i}$ where s_n is the number of distinct degrees of x_n in f. There must exist an i such that the number of monomials in P_i is $\leq \left\lfloor \frac{m}{s_n} \right\rfloor$, as if all were larger, then the total number of monomials will be $> m$. If $f \neq 0$, then $P_i \neq 0$.

Using induction hypothesis, we get that $\mathcal{S}\left(n-1, \leq \left\lfloor \frac{m}{s_n} \right\rfloor\right)$ is a hitting set for P_i, i.e. $\exists (c_1, \ldots, c_{n-1}) \in \mathcal{S}(n, m)$ such that $P_i \neq 0$ and $\prod_{i=1}^{n-1} c_i \leq \left\lfloor \frac{m}{s_n} \right\rfloor$. Thus, fixing $x_i = c_i, \forall n \in [n-1]$, we have f as a univariate in x_n with s_n monomials. By Descartes' rule of signs, we have for some $c_n \in \{1, \ldots, s_n\}$ where $f(c_1, \ldots, c_n) \neq 0$. Also,

$$\prod_{i=1}^{n} = c_n \cdot \prod_{i=1}^{n-1} c_i \leq c_n \cdot \left\lfloor \frac{m}{s_n} \right\rfloor \leq s_n \cdot \left\lfloor \frac{m}{s_n} \right\rfloor \leq m$$

Thus, $\mathcal{S}(n, m)$ is a hitting set for $\mathbb{F}_m[x_1, \ldots, x_n]$. □

To estimate the size of the hitting set, we will need the following lemma by Kalmar

Lemma 1.2. *[Kal30] $g(n)$ is defined as the number of ordered factorizations of n into parts greater than 1. Then for ζ refers to the Riemann zeta function and $\rho \approx 1.73$ is the unique solution of $\zeta(\rho) = 2$ in $(1, \infty)$, we have*

$$\sum_{n \leq x} g(n) = -\frac{1}{\rho \zeta'(\rho)} x^\rho + o(x^\rho)$$

Now we estimate its size.

Lemma 1.3. *$|\mathcal{S}(n, m)|$ is $\mathcal{O}(2^n \cdot m^\rho)$, where $\rho \approx 1.73$.*

Proof. Let $A(x, t)$ be the number of ordered factorizations of x with t partitions. We can map these t values to t c_i's in $\binom{n}{t}$ ways, and since it's ordered factorizations we don't need to worry about permutations. Therefore, we have

$$\begin{aligned}
|\mathcal{S}(n, m)| &= \sum_{x=1}^{m} \sum_{t=1}^{n} \binom{n}{t} A(x, t) \\
&= \sum_{t=1}^{n} \sum_{x=1}^{m} \binom{n}{t} A(x, t) \\
&= \sum_{t=1}^{n} \binom{n}{t} \sum_{x=1}^{m} A(x, t)
\end{aligned}$$

By Theorem 1.2, we know that the number of ordered factorizations such that product is $\leq m$ is $\mathcal{O}(m^\rho)$. Therefore, $\sum_{x=1}^{m} A(x, t) < \mathcal{O}(m^\rho)$.

$$|\mathcal{S}(n, m)| \leq \sum_{t=1}^{n} \binom{n}{t} \mathcal{O}(m^\rho) = \mathcal{O}(2^n \cdot m^\rho)$$

□

We can use the reduction from [BE11] to get the number of variables to $\log(mn)$ to get $\text{poly}(m, n)$ bound on the size of hitting set.

References

[BE11] Markus Bläser and Christian Engels. Randomness efficient testing of sparse black box identities of unbounded degree over the reals. In *Symposium on Theoretical Aspects of Computer Science (STACS2011)*, volume 9, pages 555–566, 2011.

[Kal30] Laszlo Kalmár. Uber die mittlere anzahl der produktdarstellungen der zahlen, erste mitteilung. *Acta Litterarum ac Scientiarum, Szeged*, 5(95):107, 1930.