SUMMER WORK

A Report On

Polynomial Identity Testing Using ROABP and Diagonal Circuits

by

Saswata Mukherjee (BSc CMI)
Somnath Bhattacharjee (BSc CMI)

under supervision of

Prof. Nitin Saxena
(Coumputer Science, IIT Kanpur)

August 12, 2021

Contents

PIT and Progress

Polynomial identity testing problem is basically checking a polynomial $p(x) \in R[x]$ is identically 0 or not in polynomial time. We can generalise it by checking whether a circuit family is 0 or not.

Blackbox PIT is solving the PIT problem using the circuit as an oracle.

Using schwartz zippel lemma we can write a co-RP algorithm for Blackbox PIT. Hence PIT $\in$ co-RP

1.1 Progress on PIT

For a general PIT we just have that co-RP algorithm. But if with some constrains we can have better result. Through out our report we will assume the given circuit we are working with has size s, number of variables n and degree d unless it is mentioned in other way. Further more $n = O(\log s)$. And our working Ring will be UFD.

1.1.1 Less-sparse Polynomials

Let $p(x)$ be a polynomial of sparsity (i.e., number of monomials) m then we can have a blackbox PIT for $p(x)$ which runs in pol(s, m, d) time. Now if m is small (i.e., polynomial of n) then we can have a polytime algorithm. Here is the idea how to design the algorithm. The detailed version is in the PIT surveys by Saxena ([Sax06; Sax12])

Theorem 1.1.1. Let $p(x_1, \ldots, x_n)$ be such polynomial which is non-zero, then there exists $1 \le r \le (mn \log d)^2$ s.t. $q(y) = p(y, y^d, y^{d^2}, \ldots, y^{d^{n-1}}) \neq 0 \ (mod\, y^r - 1)$

proof idea: Now we will say r is bad if $y^r - 1 \big| q(y)$. Now let y^a is a monomial of $q(y)$ with non-zero coefficient anf r is bad, then there must be some monomial y^b with non-zero coeff in q s.t. $y^r - 1 \big| y^b - y^a \iff r \big| (b - a)$
Now for safety we will take r which does not divides all possible $(b - a)$. Hence r will be good if

$$r \nmid \prod_{y^b \in q(y), b \neq a} (b - a) := R$$

Clearly $R \le (d^n)^m$
and the $(\log R + 1)$th prime can definitley be treated as a 'good' r
These together will imply there exists some $1 \le r \le (\log R + 1)^2 = (mn \log d)^2$

Note because of this theorem, for a good r the map $\varphi : x_i \to y^{d^{i-1} \bmod r}$ is injective hence preserves the nonzeroness. Now we can easily generate a small hitting set for $\varphi(p(x))$ as its degree is bounded by some polynomial of n, d and it is univariate. Also note if p is 0 then there will be no good r.

Hence for a given polynomial p we can guess all such r and check whether it is good or not. if there is no good r then we can simply conclude p is identity otherwise not. There will be polynomially many such r and each checking will be in poly time. So overall complexity will be in polynomial.

Using this idea we can create a black box PIT algorithm for depth-2 circuits as any $\Sigma\Pi$ circuit has sparsity $O(s)$

Now not every time we will be lucky enough to get a less-sparse polynomial. A polynomial can have 2^n many monomials which is clearly not small :)

1.1.2 Constant fan-in Depth-3 Circuits (Whitebox)

A const fan-in depth-3 circuit will look like $\sum_{i=1}^{k} T_i$ where k is a constant and T_i will be in the form of $T_i = \prod_{j=1}^{d} l_{ij}$ where each l_{ij} is linear polynomial of x_is.

Now assume $k = 2$,i.e., $p(x) = T_1 + T_2$

Now $p = 0 \iff T_1 = -T_2$ where each T_i is factorized into irreducible elements. And since $R[x]$ is UFD we can easily check whether the factorizations are same or not.

So the problem arises if $k > 2$. According to Kayal and Saxena [KS07] it is possible. First Assume $k = 3$.

Suppose we have $d+1$ many co primes $q_1, \ldots, q_{d+1}$ in the set $\{l_{ij}\}$. Then

$$p = 0 \iff \forall i \text{ we have } q_i \mid p$$

Now note q_i must divide one of T_1, T_2, T_3 (say T_3 WLOG) so checking for $p \ (mod \ q_i) = 0$ is enough to check for $(T_1 + T_2)(mod \ q_i) = 0$ or not.

Now consider the map $\tau : x_j \to$ some linear combinations of xs s.t. $q_i \to x_1$ and it preserves the non-zeroness.

Now it is enough to check for $p(\tau(x_1), \ldots, \tau(x_n)) \ mod \ x_1 = 0$. Now setting $x_i = 0$ gives us the $k = 2$ case. Now only thing is to find such q_is. If they exist then surely it can be done in poly time.

What if they don't exist. For example $P(x) = x_1^9 + x_2^5 x_3^4 + (x_1 + x_2 + x_3)^9$.

Let $q_1, \ldots, q_l$ be all possible co-primes. then it can be easily checked that there exist $e_1, \ldots, e_l$ s.t.

1. $q_i^{e_i} \mid p$
2. $\sum e_i > d$

Again

$$p = 0 \iff \forall i \text{ we have } p \bmod q_i^{e_i} = 0$$

So again we will take the injective map τ which sends $q_i \to x_1$ and will check for $\tau(p)\Big|_{x_1=0} = 0$ which boils down to the $k = 2$ case.

tab So basically for any $k > 2$ case we can reduce to $k-1$ case in polytime by recursion and we know how to solve the base case (i.e., $k = 2$ case).

1.1.3 Depth-3 Blackbox

We will introduce some terminologies here.

Definition 1.1.1. **Minimal circuit:** A circuit $C = \sum T_i$ is said to be minimal if no proper subset of $\{T_i\}$ sums to zero.

Definition 1.1.2. **Simple circuit:** A circuit $C = \sum T_i$ is said to be minimal if GCD of $\{T_i\}$ is 1

Definition 1.1.3. **Rank of a circuit:** Rank of a circuit $C = \sum \prod l_{ij}$ is the dimension of the space $\langle l_{ij} \rangle$

We will discuss about about the rank bounds in the next section but for now assume the rank bound for a depth-3 minimal simple circuit is $R(k,d)$ (k is the top fan-in). Then we will have a black-box PIT of time complexity $poly(n, d^{R(k,d)})$. We will include the algorithm in the section under rank bound.

Now according to Seshadhri and Saxena [SS09] we have $k^3 \log d$ rank bound. Hence we have quasi polynomial black-box algorithm for depth-3 circuit. Although if the ring is $\mathbb{R}$ then the rankbound is constant hence the algorithm is polynomial time. I is still open for other rings. We will discuss this in the next section.

1.1.4 Depth-4 Circuits

With some constrains there are some progression in Depth-4 circuits.

Non-commuting Idea: This works when the multiplication gates have *unmixed variables*, i.e., $p(\overline{x}) = \sum^{k} M_i$ and each $M_i = \prod^{n} f_{ij}(x_j)$ where each f_{ij} is an univariate polynomial. Raz and Shpilka [RS04] gave a controled way to solve this case.

Idea is to compute the polynomail $f_{i1}(x_1) f_{i2}(x_2)$ for each $i = 1(1)k$. Then we will replace them by a new variable $z_{1,i}$. Now it will be a new polynomial $p_1(z_{11}, \ldots, z_{1l}, x_3, \ldots, x_n)$ (clearly $l \le k$) which will preserve the non-zeroness. It reduces two factors from each M_i and the increase in the number of variables is $O(k)$ which is under control since there will be $O(n)$ reductions if we continue this reduction. Hence everything is in polynomial.

Powering Idea: If the circuit is in the form $\sum M_i$ where each $M_i = \prod \alpha_i (f_{i1}(x_1) + \cdots + f_{in}(x_n))^{e_i}$. We will reduce this case to the previous one. For this we need to use the following theorem.

Theorem 1.1.2. [Sax08] let $\mathbb{F}$ be a field of characteristic zero, $a_0,\ldots,a_n \in \mathbb{F}$ then, we can compute polynomials $f_{ij} \in \mathbb{F}[x_j]$ in $poly(nd)$ field operations so that,

$$(a_0 + a_1x_1 + \cdots + a_nx_n)^d = \sum_{i=1}^{d(n+1)+1} f_{i,1}(x_1)\ldots f_{i,n}(x_n)$$

proof idea: $exp(x) = e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots.$
and define $E_d(x) = \sum_{i=0}^{d} \frac{x^k}{k!}$.
Now,

$$\begin{aligned}(d!)^{-1}(a_0 + a_1x_1 + \cdots + a_nx_n)^d &= coeff[z^d](exp((a_0 + a_1x_1 + \cdots + a_nx_n)z).\\ &= coeff[z^d](exp(a_0z)exp(a_1x_1z)\ldots exp(a_nx_nz))\\ &= coeff[z^d](E_d(a_0z)\ldots E_d(a_nx_nz))\end{aligned}$$

$E_d(a_0z)\ldots E_d(a_nx_nz)$ is a polynomial over z of degree $(n+1)d$
Hence, taking $\alpha_0,\ldots,\alpha_{nd+d+1} \in \mathbb{F}$ distinct elements, by interpolation we compute $\beta_0,\ldots,\beta_{nd+d+1}$ so that,

$$coeff[z^d](E_d(a_0z)\ldots E_d(a_nx_nz)) = \sum_{i=1}^{d(n+1)+1} \beta_i E_d(a_0\alpha_i)\ldots E_d(a_n\alpha_i x_n)$$

and polynomials $E_d(.)$ can be computed in $poly(nd)$ field operations.

Applying this theorem to all multiple gate M_is we can convert our circuit to another circuit which is sum of product of univariates preserving the non-zeroness.

Bounded Fan-in: Pranjal Dutta, Prateek Dwivedi and Nitin Saxena [DDS21] gave three results for this case:

1. (**Whitebox** $\Sigma\Pi\Sigma\wedge$ **PIT**). There is a deterministic, whitebox $O(s^{k7^k})$ PIT algorithm for $\Sigma^k\Pi\Sigma\wedge$ size s circuit over $\mathbb{F}[x]$.
2. (**Blackbox** $\Sigma\Pi\Sigma\wedge$ **PIT**). There is a deterministic, Blackbox $O(s^{k\log\log s})$ PIT algorithm for $\Sigma^k\Pi\Sigma\wedge$ size s circuit over $\mathbb{F}[x]$.
3. (**Blackbox** $\Sigma\Pi\Sigma\Pi$ **PIT**). There is a deterministic, Blackbox $O(s^{\delta^2 k\log s})$ PIT algorithm for $\Sigma^k\Pi\Sigma\Pi^\delta$ size s circuit over $\mathbb{F}[x]$.

   Hence we have polynomial whitebox and quasi polynomial blackbox.

1.1.5 Diagonal Circuits

For this part we need to introduce ROABP. We will discuss about this section in the next chapter in details. For diagonal depth 3 we have polytime black box, for $\Sigma\wedge\Sigma\wedge$ we have quasi polynomial time PIT Blackbox.

Also there is a **subexponential PIT algorithm for constant depth circuits** given by Srikanth, Nutan and Tavenas [LST21].

Open Problems: Upto depth 3 circuits we have efficient algorithms. But for depth 4 circuits our research is still incomplete except for some specific cases. So this field is still open.

For fan-in 2 depth 4 circuits, find a faithful map φ that preserves the algebraic independence of two products-of-sparse polynomials $\prod_i f_i$ and $\prod_j g_j$. If we look at the relevant 2×2 Jacobian determinant, say wrt variable $X := \{x_1, x_2\}$ then the question boils down to finding a hitting-set for the special rational function $\sum_{ij} = \frac{det\mathscr{J}_x(f_i,g_j)}{f_i g_j}$. Can this version of rational sparse PIT be done in sub-exponential time? ([Sax12])

For multilinear depth-3 circuits, achieve $o(n)$-concentration in multilinear depth-3 circuits, in $n^{o(n)}$ time.

For diagonal circuits we have open problems using ROABP and weight assignment which will be discussed in the next chapter.

1.2 Rankbounds

We have already introduce the notion of rank of a circuit. It is clear that we need to found some better upper bounds since in the complexity it arises in the exponent.

1.2.1 Algorithm using rank bounds

Karnin and Shpilka [KS08] showed this idea. The idea is mainly finding a set of linear transformations $\{\tau\}$ which preserves the non-zeroness and maps a n variate depth-3 circuit to a $R(k,d)$ variate circuit but the degree doesn't increase. Now we can apply the brute force version of scwartz-zipple test.

Lemma 1. [GR08] Let $W_1, \ldots, W_s$ be the subspaces of $\mathbb{F}^n$ with $\dim(W_i) \leq t$. Consider the linear maps

$$\varphi_{\alpha,t,n}(\overline{x}) = \left(\alpha^{i(j-1)}\right)_{i=1(1)t, j=1(1)n} (\overline{x})$$

Then there is atmost snt^2 many $\alpha \in \mathbb{F}$ s.t. for some W_i $\varphi_{\alpha,t,n}\Big|_{W_i}$ map is NOT injective, i.e., the dimension of W_i drops.

proof idea: We will mainly capture all such bad αs in a univariate polynomial and bound them using the degree of it.

Suppose for some α degree of W_i decreases then the first $\dim(W_i) \times \dim(W_i)$ submatrix of $\varphi_{\alpha,t,n}$ will be singular, hence the determinate will give us univariate polynomial of α with degree atmost nt^2. Hence it gives us the bound snt^2

Using this lemma they gave us the following theorem

Theorem 1.2.1. [KS08] Let C be a depth-3 circuit and $S \subseteq F$ of size $n2^k d^2 R(k,d)^2$. If C is non-ero then there is some $\alpha \in S$ s.t. $\varphi_{\alpha,n,R(k,d)}(C)$ is also non zero

Now the algorithm is mainly try out $n2^k d^2 R(k,d)^2$ many αs and create the new

circuit C'. Evaluate C' on $(d+1)^{R(k,d)}$ many points on $\mathbb{F}^{R(k,d)}$. Schwartz- zipple lemma ensures the correctness. And the complexity will be indeed $poly(n, 2^k, d^{R(k,d)})$.

1.2.2 An almost optimal rankbound

The best known lowerbound is $k^3 \log d$ as we discussed already. But this is close to optimal as there are identities of rank $\Omega(k \log d)$ ([KS07; SS09]).

Here is such example. Define on $\mathbb{F}_2$

$$C(x_1,\ldots,x_n) := \prod_{b_1+\cdots+b_{n-1}=1} (b_1x_1+\cdots+b_{n-1}x_{n-1}) + \prod_{b_1+\cdots+b_{n-1}=0} (b_1x_1+\cdots+b_{n-1}x_{n-1}+x_n) \prod_{b_1+\cdots+b_{n-1}=1} (b_1x_1+\cdots+b_{n-1}x_{n-1}+x_n)$$

Although if we restrict our working ring then we have results which will not be disappointing :)

1.2.3 Rank bounds over real numbers

Dvir and Sphilka [DS06] gave a conjecture that fields with infinite characteristics should have rankbound $O(k)$. Kayal and Saraf proved a weaker version which is $O(k^k)$ [KS09] which is efficient when k is constant. But when $k=3$ then we have the bound exact 4.

Assume the circuit $C = T_1+T_2+T_3$ and has rank $r+1$ with the basis $\{v_1,\ldots,v_{r+1}\}$. Idea is to work on *projected* space. Let $\{l_i\}$ be the set of the linear polynomials of the circuit. Consider the map which takes $l_i := a_1v_1+\cdots+a_{r+1}v_{r+1}$ to $(\frac{a_1}{a_{r+1}}, \frac{a_2}{a_{r+1}}, \ldots, \frac{a_{n-1}}{a_{r+1}}) \in \mathbb{R}^r$

Assume A_1, A_2, A_3 are the sets of the points corresponds to the linear factors of T_1, T_2, T_3 respectively.

Now note for any $l_1 \in T_1, l_2 \in T_2$ $C \bmod (l_1, l_2) = 0 \iff \exists l_3 \in T_3$ s.t. $l_3 \in \langle l_1, l_2 \rangle$ This means any line passing through a point of A_1 and A_2 each must passes through a point of A_3. Such A_1, A_2, A_3 sets are special.

Now we will use the following theorem

Theorem 1.2.2. **(Sylvester-Gallai)** Given a finite set of non-colinear points S in $\mathbb{R}^2$, there is always a line which exactly passes through exactly two points of S

Generalised version: Let S be a finite set of points spanning an affine space $V \subseteq \mathbb{R}^n$ with $\dim(V) \geq 2t$. Then there exist $t+1$ many points in S that span a t dimensional space $H \subseteq V$ s.t. $|H \cap S| = t+1$
($t=1$ gives us the previous case)

Now applying the sylvester gallai theorem on A_1, A_2, A_3 Edelstein and Kelly showed that $r \leq 3$ [EK66].

Now for general case (i.e., $k > 3$) Kayal and Saraf used the generalised sylvaster-gallai and gave the bound k^k.

Open Problems: "Above result holds for any zero characteristic Ring" is still open.

Conjecture: Let S be a finite set of points spanning an affine space $V \subseteq \mathbb{C}^n$ s.t. $\dim(V) \geq 3t$, then there exist $(t+1)$ points in S that span a t dimensional affine space $H \leq V$ s.t. $|H \cap S| = t+1$
(We have proof for special case $t = 1$)

PIT using ROABP and Diagonal Circuits

Here we introduce the model ABP, defined by Nisan and then ROABP as a subclass of it.

Definition 2.0.1. An **Algebraic Branching Program or ABP** over a field $\mathbb{F}$ is a layered directed acyclic graph with vertex set V where $V_0 = \{s\}$, $V_2, \ldots, V_d = \{t\}$ are disjoint partition of V and edge set E where E_1, $E_2, \ldots, E_d$ are disjoint partition of E. s and t are source and sink respectively.
Here $E_i \subseteq V_{i-1} \times V_i \ \forall i \in [d]$ (each edge e in E_i goes from V_{i-1} to V_i)
And there is a labelling function $\mathscr{L} : E \to \mathbb{F}[\overline{x}]$ so that $\forall e \in E$, $\mathscr{L}(e)$ is a polynomial in $\mathbb{F}[\overline{x}]$ of degree ≤ 1.
An edge $e \in E$ is labelled as $\mathscr{L}$.
A polynomial $f \in \mathbb{F}[\overline{x}]$ computed by the ABP is

$$f = \sum_{\text{path } p:\, s \rightsquigarrow t} \prod_{e \in p} \mathscr{L}(e)$$

width of an ABP $w = \max_{i \in \{0,\ldots,d\}} |V_i|$
depth $d = \max_{\text{path } p:\, s \rightsquigarrow t} \text{length}(p)$

Definition 2.0.2. $\pi : [n] \to [n]$ be a permutation. An **Read-Once (Oblivious) Algebraic Branching Program or ROABP** with variable order π over a field $\mathbb{F}$ is depth n ABP over $\mathbb{F}$ where label function for ith layer is
$\mathscr{L}_i = \mathscr{L}|_{E_i} : E_i \to \{f \mid f \in \mathbb{F}[x_{\pi(i)}]\}$.
An ABP is **read-once** if along each path each variable occures in at most one layer.
and an ABP is **oblivious** if in each path variables occure in same order (in some permutation π).

Lemma 2. say, $\pi : [n] \to [n]$ is a permutation of $[n]$ and f is a $n-$variate polynomial over $\mathbb{F}$.
Then following two statements are equivalent.

1. f is computed by a width w ROABP with individual degree d and variable order π.
2. $\exists C, D \in \mathbb{F}^{w \times 1}$ and for $i \in [n]$, $A_i \in \mathbb{F}^{w \times w}[x_{\pi(i)}]$ so that $f = C^T \prod_{i=1}^{n} A_i D$

2.1 Relation between diagonal circuits and ROABP

In this section we mainly focus on diagonal depth-3 and diagonal depth-4 circuits. Diagonal depth-3 circuit ($\Sigma^k \bigwedge^d \Sigma$) over field $\mathbb{F}$ looks like

$$C(\overline{x}) = \sum_{i=1}^{k} a_i l_i^{d_i}$$

where each l_i is linear polynomial in $\mathbb{F}[x_1,\ldots,x_n]$, each $d_i \leq d$ and $a_i \in \mathbb{F}$.

Diagonal depth-4 circuits($\Sigma^k \bigwedge^d \Sigma \bigwedge$) looks like

$$C(\overline{x}) = \sum_{i=1}^{k} a_i (f_{i,1}(x_1) + \cdots + f_{i,n}(x_n))^{d_i}$$

where each $f_{i,j}(x_j) \in \mathbb{F}[x_j]$, $d_i \leq d$ and $a_i \in \mathbb{F}$.

From theorem 1.1.2 any diagonal depth-3 model can be represented as,

$$C(x_1,\ldots,x_n) = \sum_{i=1}^{k} a_i l_i^{d_i} = \sum_{i=1}^{k} \sum_{j=1}^{nd_i+d_i+1} g_{i,j,1}(x_1)\ldots g_{i,j,n}(x_n)$$

where each $g_{i,j,k}$ has degree $\leq d_i$.
And diagonal depth-4 circuit can be written as,

$$C(\overline{x}) = \sum_{i=1}^{k} a_i (f_{i,1}(x_1) + \cdots + f_{i,n}(x_n))^{d_i} = \sum_{i=1}^{k} \sum_{j=1}^{nd_i+d_i+1} g_{i,j,1}(f_{i,1}(x_1))\ldots g_{i,j,n}(f_{i,n}(x_n))$$

Hence, poly time PIT for ROABP implies poly time PIT for diagonal circuits.

2.2 Progress on ROABP

1. **Whitebox PIT:** Raz and Shpilka [RS04] gave $poly(s,n)$ time whitebox PIT for size s, n-variate ROABP.
2. **Blackbox PIT:** There are more than one result where we have quasipoly black box PIT. Gurjar, Korwar and Saxena [GKS16] gave a $(ndw)^{\log\log w}$ black box PIT for w width ROABP, where n = number of variables and d = individual degree.

   Their main Idea was to reduce the n-variate problem to $\frac{n}{2}$-variate case And they gave the following theorem.

   Theorem 2.2.1. [Gur+15] Suppose the circuit $C \in \mathbb{F}[\overline{x}]$ with $char(\mathbb{F}) = 0$ or $> d$ has a w width ROABP then the map $\phi : \mathbb{F}[\overline{x}] \to \mathbb{F}[t_1,\ldots,t_{\frac{n}{2}}]$ sending $\forall i = 1(1)\frac{n}{2}$ $x_{2i}, x_{2i-1} \to t_i^w$ is injective and $\phi(C)$ can be computed by w width ROABP as well

   proof idea: We have discussed about the proof idea in the next chapter (2.4.1)

2.3 Blackbox PIT for log-variate Circuits

Now it is enough to study log-variate circuits for blackbox PIT, because of the following theorem, given by Manindra Agrawal, Sumanta Ghosh, Nitin Saxena.

Theorem 2.3.1. [AGS18] If for some $c \in \mathbb{N}$ we have $poly(s)$ time blackbox PIT for size-s, degree-s, $\lceil \log^{\circ c} s \rceil$-variate circuits, then, we have $poly(sd)$ time blackbox PIT for size-s, degree-d circuits.
(where $\log^{\circ c} s = \underbrace{\log\log\ldots\log}_{c \text{ times}} s$)

2.3.1 Blackbox PIT for log-variate diagonal depth-3 circuits

Michael A. Forbes, Sumanta Ghosh, Nitin Saxena [FGS18] gave $poly(s)$-time blackbox PIT for $O(\log s)$-variate, size-s diagonal depth-3 circuits. Here we describe the idea in a few words.

Definition 2.3.1. If $\overline{x}^{\overline{e}} = x_1^{e_1}\ldots x_n^{e_n}$ be a monomial then, **cone of** $\overline{x}^{\overline{e}}$ is the set of all sub-monomials of it (monimials that divide $\overline{x}^{\overline{e}}$, including 1 and itself).
Cone-size of a monomial ($\text{cs}(\overline{x}^{\overline{e}})$) is cardinality of this set ($= \prod_{i=1}^{n}(e_i+1)$)
A set S of monomials is said to be **cone-closed** if for each monomials in S, all of its sub-monomials are also in S.

Definition 2.3.2. A **monomial ordering** over field $\mathbb{F}$ is a total order of monomials in $\mathbb{F}[\overline{x}]$ so that,
1. for all $\overline{a} \in \mathbb{N}^n \setminus \{\overline{0}\}$, $1 \prec \overline{x}^{\overline{a}}$.
2. if $\overline{x}^{\overline{a}} \prec \overline{x}^{\overline{b}}$ then, $\overline{x}^{\overline{a}+\overline{c}} \prec \overline{x}^{\overline{b}+\overline{c}}$ for all $\overline{c} \in \mathbb{N}^n$.

For any polynomial $f \in \mathbb{F}[\overline{x}]$, the **leading monomial of** f (with respect to monomial order $\prec$) is the largest monomial of f and it is denoted by $\text{LM}(f)$.

Lemma 3. [FGS18] Let C be a blackbox circuit, computes n-variate, degree-d polynomial over a field of characteristic $> d$. Then, for any monomial m, there is a $poly(|C|d, \text{cs}(m))$ time algorithm to compute the coefficient of m in C.

Lemma 4. [FGS18] Number of n-variate monomials, with cone-size r in a polynomial is at most $O(rk^2)$ where $r = (3n/\log k)^{\log k}$.

Theorem 2.3.2. [For14] Say, $f \in \mathbb{F}[\overline{x}]$ and $\mathbb{F}$ be a field of characteristic $> deg\ f$. Let, $\prec$ be any monomial ordering in $\mathbb{F}[\overline{x}]$ and $\text{LM}(f) = \overline{x}^{\overline{a}}$.
then $\dim \partial_{\overline{x}^{\leq\infty}}(f) \geq \text{cs}(\overline{x}^{\overline{a}})$.
where $\partial_{\overline{x}^{\leq\infty}}(f)$ is the partial derivative space of f.

Theorem 2.3.3. [FGS18] Say, $\mathbb{F}$ be a field of characteristic $> d$ and $\mathscr{P}$ be the family of n-variate polynomials P of degree d, and computed by a circuit of size s. For all $P \in \mathscr{P}$, $\dim \partial_{\overline{x}^{\leq\infty}}(P) \leq k$, then, blackbox PIT for $\mathscr{P}$ can be solved in time $(sdk)^{O(1)}(3n/\log k)^{O(\log k)}$.

Proof idea: say, $P \in \mathscr{P}$ and $\prec$ be lexicographic monomial ordering.
Then, from, 2.4.1, cone-size of leading monomial of $P \leq k$.
So, $P \neq 0 \iff \exists$ monomial m in P with non-zero coefficient so that, $\text{cs}(m) \leq k$
if, monomial m has cone-size $\leq k$ then, we can extract coefficient of m in time $poly(sdk)$.
And there are $O(rk^2)$ many such monomials.
Hence, total time needed is, $(sdk)^{O(1)}(3n/\log k)^{O(\log k)}$.

Here if we put $k = poly(sd)$ and $n = O(\log(sd))$ then, from the above theorem we have $poly(sd)$ time blackbox PIT for the log-variate circuits for which dimension of partial derivative space is polynomially bounded.

Lemma 5. [FGS18] say, P be a n-variate, degree-d polynomial, computed by size s diagonal depth-3 circuit. Then, there is a $poly(nds)$ time computable map Ψ so, that, $P \neq 0 \iff P \circ \Psi \neq 0$ and $P \circ \Psi$ is $\text{rank}(P)$-variate degree-d polynomial computed by $poly(s)$ size diagonal depth-3 circuit.

Now, for a n-variate diagonal depth-3 circuit C, $\text{rank}(C) \leq n$. And from [For14], dimension of the partial derivative space of a $n = O(\log sd)$-variate degree-d polynomial computed by size-s circuit is $poly(sd)$.

So, using 2.3.3 and 5 for any $n = O(\log sd)$-variate degree-d polynomial computed by size-s diagonal depth-3 circuit, we have $poly(sd)$ time blackbox PIT.

2.4 Polynomials over k-dimensional algebra $\mathbb{F}^k$

In this section, we will see some results on the polynomials over $\mathbb{F}^k$ for solving PIT on ROABP.
We consider $(\mathbb{F}^k, +, *)$ to be a ring with coordinate wise sum and multiplication. Also, it is a vector space (with coordinate wise sum) of dimension k over the field $\mathbb{F}$.
At first we introduce some terminologies.

Definition 2.4.1. say, $D(\overline{x}) \in \mathbb{F}^k[\overline{x}]$,
then, $\text{sp}(D)$ is the vector space spanned by the coefficients of D.
D has a **cone-closed basis** if there is a cone-closed set of monomials B so, that their coefficients in D form a basis for $\text{sp}(D)$.
D has l-**support concentration** if, there is a set of monomials B with support size $\leq l$ and, their coefficients form a basis for $\text{sp}(D)$.
D has l-**cone concentration** if if, there is a set of monomials B with cone size $\leq l$ and, their coefficients form a basis for $\text{sp}(D)$.

Lemma 6. [FGS18] if $D \in \mathbb{F}^k[\overline{x}]$ has a cone-closed basis then, it has $(k+1)$-cone concentration and $(\log 2k)$-support concentration.

2.4.1 Shift and Weight Assignment

For some polynomial $f(\overline{x})$, we shift its variables by $c_1, c_2, \ldots, c_n$, to get the new polynomial $f(x_1 + c_1, \ldots, x_n + c_n)$.
say, $f(\overline{x}) = x_1 x_2 \ldots x_n$, if we shift it by $\overline{1}$, then, $f(\overline{x} + \overline{1}) = \prod_i (x_i + 1)$ has many low support monomials. Hence this idea can be interesting in the study of PIT.

It was proved by [ASS13] that, **After applying a small shift, any $D \in \mathbb{F}^k[\overline{x}]$, becomes low-support concentrated, in quasi-polynomial time, although the initial polynomial $D(\overline{x})$ not necessarily satisfy that property.**
Using this idea, they gave quasi-polynomial time blackbox PIT for constant depth set-multilinear formulas.

Definition 2.4.2. **weight assignment** or **weight function** be a map $w : \{x_1, x_2 \ldots, x_n\} \to \mathbb{N}$ where x_i s are variables.And for any monomial $m = x_1^{e_1} \ldots x_n^{e_n}$, $w(m) = \sum_{i=1}^n e_i w(x_i)$.

Definition 2.4.3. A weight function $w : \{x_1, \ldots, x_n\} \to \mathbb{N}$ is called **Basis Isolating Weight Assignment** for a polynomial $D \in F^k[x_1, \ldots, x_n]$, if there is a set S of monomials, so that,the coefficients of the monomials in S, form a basis for $\text{sp}(D)$, and,

1. for any $m_1, m_2 \in S$, $w(m_1) \neq w(m_2)$.
2. for any $m \notin S$, $\text{coef}_D(m) \in \text{span}_{\mathbb{F}}\{\text{coef}_D(m') : m' \in S,\ w(m') < w(m)\}$.

[FGS18] has shown that, if $f(x_1, \ldots, x_n) \in \mathbb{F}^k[\overline{x}]$, ($\text{char}\mathbb{F}$ is large) and $w = (w_1, \ldots, w_n)$ be a basis isolating weight assignment for f. Then, $f(x_1 + t^{w_1}, \ldots, x_n + t^{w_n})$ has a cone-closed basis over $\mathbb{F}(t)$.

[Agr+15] has constructed a basis isolating weight assignment for a polynomial $D(\overline{x}) = P_1(\overline{x}_1) \ldots P_d(\overline{x}_d)$ (where $\overline{x}_1, \ldots, \overline{x}_d$ are disjoint partition of the variables and each $P_i \in \mathbb{F}^k[\overline{x}_i]$ is a polynomial of individual degree δ and sparsity s) in time $(poly(k, n, s, \delta))^{\log d}$.

And using this, they gave a hitting set for any polynomial D, computed by width-w and sparse factor-s ROABP in time $(poly(w, n, s, \delta))^{\log d}$.

Another result given by [Agr+15], on sparse-invertible ROABP :-

Say, $C = D_0 \prod_{i=1}^d D_{d+1} D_{n+1}$ be a polynomial computed by ROABP where $D_i(\overline{x}) \in \mathbb{F}^{w \times w}[\overline{x}_i]$ are polynomials of spasity s and individual degree δ. Moreover, each D_i is invertible matrix when represented as an element of $\mathbb{F}[\overline{x}_i]^{w \times w}$. ($\overline{x}_1, \ldots, \overline{x}_d$ are disjoint partition of the variable set $\{x_1, \ldots, x_n\}$).

Now, by efficiently shifting each variable of $D = \prod_{i=1}^d D_i \in \mathbb{F}^{w \times w}[\overline{x}]$, by some univariate polynomial on t, they have achieved $w^2(\log w^2 + 1)$-concentration. It implies $w^2(\log w^2 + 1)$-concentration on the polynomial $C(\overline{x} + \overline{t}) \in \mathbb{F}(t)[x]$. Again, degree of t is bounded by $poly(ns^w \log(w\delta))$.

Lemma 7. [ASS13] $C \in \mathbb{F}[\overline{x}]$ be a n-variate, l-concentrated polynomial with individual degree $\leq d$, then, there is $(nd)^{O(l)}$ time hitting set for C.

Using the lemma, they found a hitting set of size $(n\delta)^{O(w^2 \log w)}$ for the shifted polynomial and hence, from the degree bound of the shift, they have the blackbox PIT in time $poly\big((sn\delta)^{O(w^2 \log w)}\big)$.
And when each D_i is univariate, it will have $(n\delta)^{O(w^2)}$ time blackbox PIT.

Now, we move on to a result given by [Gur+15], on the sum of constantly many ROABPs (with not necessarily same variable order):-

Lemma 8. [Gur+15] say, $A(\overline{x}), B(\overline{x})$ be two n-variate, individual degree d polynomials, each computed by width-w ROABPs. say, $W_{w,2} = (d+1)(2w^2)$ and $l_{w,2} = \log(W_{w,2}^2+1)$. $\overline{f}_{w,2}(t) \in \mathbb{F}[t]^n$ be a shift that $l_{w,2}$-concentrates the polynomials, computed by ROABP of width $\leq W_{w,2}$. then $(A+B)(\overline{x}+\overline{f}_{w,2}(t))$ is $2l_{w,2}$-concentrated.

Hence, using this lemma, they have found $(nd)^{O(l_{w,2})} = (nd)^{O(\log dw)}$ size hitting set for the shifted polynomial.

Again, they have shown that, $\overline{f}_{w,2}(t) \in \mathbb{F}[t]^n$ (as mentioned in 8), has degree bound $(ndw)^{O(\log n)}$ and can be computed in time $(ndw)^{O(\log n)}$. In this way overall time complexity for the blackbox PIT will be $(ndw)^{O(\log ndw)}$.

In general, if $A = A_1 + A_2 + \cdots + A_c$ where each A_i be a n-variate polynomial of individual degree d computed by width w ROABP, then [Gur+15] have, $(ndw)^{O(c2^c \log ndw)}$ time (Quasi-polynomial time, when c is constant) blackbox PIT for A.

Next we will discuss about the results, given by [GKS16]. They have given two results for two special cases of ROABP. This is mainly proof idea of theorem 2.2.1

1. First we talk about the result given for known order ROABP.
   If f be a n-variate polynomial of individual degree d, computed by width-w ROABP, they have applied a map ϕ so that $\forall i \in [n/2]$,

   $$\phi(x_{2i-1}) = t_i^w$$
   $$\phi(x_{2i}) = t_i^w + t_i^{w-1}$$

   Here $f(x_1, \ldots, x_n) \neq 0 \iff f \circ \phi \neq 0$ and $f \circ \phi$ has individual degree $2dw$ and can be computed by ROABP of width w, variable order $(t_1, \ldots, t_{n/2})$. So, Inductively applying the same procedure for $\log n$ times, we get an univariate polynomial, preserving the nonzeroness of f where degree blows up to $ndw^{\log n}$. Hence we get blackbox PIT of time $ndw^{\log n}$.

2. This result is on the blackbox PIT for commutative ROABP.
   Say, $D(\overline{x}) = U^T \prod_{i=1}^n D_i(x_i) S$ be n-variate, width-w ROABP, with individual degree d. Here, they have modified the idea of lemma 8, in [Agr+15] to construct efficient shift $\overline{f}(t) \in \mathbb{F}[t]^n$ so that, $D(\overline{x}+\overline{f}(t))$ will be $\log(w^2+1) = O(\log w)$-concentrated.

The shift $\overline{f}(t)$, can be computed in time $(ndw)^{O(\log\log w)}$ and its degree will be $(ndw)^{O(\log\log w)}$. [FSS14] has given $(ndw)^{O(\log\log w)}$ time hitting set for n-variate , $O(\log w)$-concentrated polynomial (individual degree d), computed by width w commutative ROABP. Hence, the blackbox PIT will cost $(ndw)^{O(\log\log w)}$ time.

[FSS14] has given $d^{O(\log w)}(nw)^{O(\log\log w)}$ time blackbox PIT for n-variate polynomial, with individual degree d, computed by width w commutative ROABP.

There are so many approaches for blakbox PIT on ROABP. But all the results we know till now, is of time quasi-polynomial over (n,d,w), even for the log-variate case.

Bibliography

[EK66] M Edelstein and L N Kelly. “Bisecants of finite collection of sets in linear spaces”. In: *Canadian journal of Mathematics, 18* (1966), pp. 375–380.

[RS04] Ran Raz and Amir Shpilka. “Deterministic polynomial identity testing in non commutative models”. In: *Computational Complexity* 14 (2004), p. 2005.

[DS06] Z Dvir and A Shpilka. “Locally decodable codes with 2 queries and PIT for depth-3 circuits”. In: *SIAMJ on Computing* (2006), 36(5), 1404–1434.

[Sax06] Nitin Saxena. *Progress on Polynomial Identity Testing.* Bulletin of the EATCS. 2006. URL: https://www.cse.iitk.ac.in/users/nitin/papers/pit-survey09.pdf.

[KS07] N Kayal and N Saxena. “PIT for depth-3 circuits”. In: *Computational Complexity* (2007), 16(2):115–138.

[GR08] A. Gabizon and R. Raz. *Deterministic extract for affine source over large fields*. 2008.

[KS08] Z Karnin and A Shpilka. “Deterministic Blackbox Polynomial Identity Testing of Depth-3 Arithmetic Circuits with Bounded Top Fan-in”. In: *Computational Complexity Conference (CCC)* (2008).

[Sax08] Nitin Saxena. “Diagonal Circuit Identity Testing and Lower Bounds”. In: *35th International Colloquium on Automata, Languages and Programming (ICALP)* (2008). Ed. by Luca Aceto et al., pp. 60–71.

[KS09] N Kayal and S Saraf. “Blackbox PIT for depth-3 circuits”. In: *Proceeding of the 50th annual symposium on foundation of computer science(FOCS)* (2009).

[SS09] C S Seshadhri and N Saxena. “An optimal rankbound for depth-3 circuits”. In: *24th Computational Complexity Conference(CCC)* (2009).

[Sax12] Nitin Saxena. *Progress on Polynomial Identity Testing II.* Proceedings of the Workshop celebrating Somenath Biswas’ 60th Birthday. 2012. URL: https://www.cse.iitk.ac.in/users/nitin/papers/pit-survey13.pdf.

[ASS13] Manindra Agrawal, Chandan Saha, and Nitin Saxena. “Quasi-Polynomial Hitting-Set for Set-Depth-Δ Formulas”. In: *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*. STOC ’13. Palo Alto, California, USA: Association for Computing Machinery, 2013, pp. 321–330. ISBN: 9781450320290. DOI: 10.1145/2488608.2488649. URL: https://doi.org/10.1145/2488608.2488649.

[For14] Michael A. Forbes. “Polynomial identity testing of read-once oblivious algebraic branching programs”. PhD thesis. Massachusetts Institute of Technology, Cambridge, MA, USA, 2014. URL: http://hdl.handle.net/1721.1/89843.

[FSS14] Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. “Hitting Sets for Multilinear Read-Once Algebraic Branching Programs, in Any Order”. In: *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*. STOC ’14. New York, New York: Association for Computing Machinery, 2014, pp. 867–875. ISBN: 9781450327107. DOI: 10.1145/2591796.2591816. URL: https://doi.org/10.1145/2591796.2591816.

[Agr+15] Manindra Agrawal et al. “Hitting-Sets for ROABP and Sum of Set-Multilinear Circuits”. In: *SIAM Journal on Computing* 44.3 (2015), pp. 669–697. DOI: 10.1137/140975103. eprint: https://doi.org/10.1137/140975103. URL: https://doi.org/10.1137/140975103.

[Gur+15] Rohit Gurjar et al. “Deterministic Identity Testing for Sum of Read-Once Oblivious Arithmetic Branching Programs”. In: *Proceedings of the 30th Conference on Computational Complexity*. CCC ’15. Portland, Oregon: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015, pp. 323–346. ISBN: 9783939897811.

[GKS16] Rohit Gurjar, Arpita Korwar, and Nitin Saxena. “Identity testing for constant-width, and commutative, read-once oblivious ABPs”. In: *Computational Complexity Conference*. 2016, 29:1–29.16.

[AGS18] Manindra Agrawal, Sumanta Ghosh, and Nitin Saxena. “Bootstrapping variables in algebraic circuits”. In: *50th ACM Symposium on Theory of Computing (STOC)* (2018).

[FGS18] Michael A. Forbes, Sumanta Ghosh, and Nitin Saxena. “Towards black-box identity testing of log-variate circuits”. In: *45th International Colloquium on Automata, Languages, and Programming (ICALP)* (2018).

[DDS21] Pranjal Dutta, Prateek Dwivedi, and Nitin Saxena. “Deterministic Identity Testing Paradigms for Bounded Top Fan-in Depth-4 Circuits”. In: *Computational Complexity Conference (CCC)* (2021).

[LST21] Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. “Superpolynomial Lower Bounds Against Low-Depth Algebraic Circuits”. In: *ECCC* (2021).