Department of Computer Science and Engg.
I.I.T Kanpur

# Equivalence of Polynomial Identity Testing and Polynomial Factorization

## Swastik Kopparty, Shubhangi Saraf, Amir Shpilka, 2014

Pranav Bisht

April 15, 2017

# Content

# Main Theorem



## Main Theorem

*Suppose white box (black box) PIT for size s, degree d, n-variate arithmetic circuits over $\mathbb{F}$ can be solved deterministically in time poly(n,s,d). Now, suppose we are given white-box(black box, resp.) access to a polynomial $f(\bar{x}) \in \mathbb{F}[x_1, \cdots, x_n]$ computed by an arithmetic circuit of size at most s and degree at most d. Let*

$$f = \prod_{i=1}^{k} {g_i}^{j_i \cdot p^{e_i}}$$

*be the factorization of f, where the $g_i$ are irreducibles and $p \nmid j_i$ for each i. Then, we can compute for each $i \in [k]$: (i) $e_i$, (ii) $j_i$, and (iii) an arithmetic circuit (black box, resp.) for the factor ${g_i}^{p^{e_i}}$ (the factor $g_i$ resp.) in deterministic time poly(n,s,d,t), where:*
*(i) $t = l.p$, if $\mathbb{F} = \mathbb{F}_{p^l}$*
*(ii) t = max bit-complexity of the constants used in the circuit, if $\mathbb{F} = \mathbb{Q}$*

# Recap - HIT



## Hilbert's Irreducibility Theorem

*Let $S \subseteq \mathbb{F}$ be a finite set of size $\geq 7d^7$, $f(x, \bar{y})$ be a polynomial in $\mathbb{F}[x, y_1, \cdots, y_n]$ of total degree d. If $\partial_x \neq 0$ and $\Pr_{\bar{a},\bar{b} \in S^n}[f(x, a_1 t + b_1, \cdots, a_n t + b_n)] \geq \frac{(7d^6+2d^2+d)}{|S|}$, then f is reducible.*

# Recap - Kaltofen Mutivariate Factoring



- Randomly reduce f to a three variate projection $f_{a,b}(x, t_1, t_2)$.
- Factor $f_{a,b}$ in randomized poly time
- Apply Hensel lifting and linear system solving to construct blackboxes for the absolute factors of $f$.

# Deterministic Whitebox Factoring algorithm


**Input:** An arithmetic circuit for the polynomial $f(x, \bar{y})$
**Ouput:** Irreducible factors of $f$.

1. If $ch(\mathbb{F}) = p$, then make $f$ not a $p^{th}$ power.
2. Make $f$ monic in $x$.
3. Reduce to the case where $f$ is square free.
4. Reduce to bivariate factoring over a large field.
   - 4.1 Define $\bar{f}(x, t, a_1, \cdots, a_n) = f(x, t.a_1, \cdots, t.a_n)$, where $\bar{a}$ are formal variables.
   - 4.2 Show correspondence between factors of $\bar{f}$ in $\mathbb{F}(\bar{a})[x, t]$ and factors of $f$ in $\mathbb{F}[x, \bar{a}]$.

# Deterministic Whitebox Factoring algorithm



5. Univariate factorization
   - 5.1 $\bar{f}(x, 0, \bar{a}) \in \mathbb{F}[x]$
   - 5.2 Find irreducible factor $g_0$ of $\bar{f}(x, 0, \bar{a})$, using univariate factorization.
   - 5.3 In $\mathbb{K}[x, t]$,

$$\bar{f}(x, t, \bar{a}) = g_0(x, t, \bar{a}) \cdot h_0(x, t, \bar{a}) \text{ (mod t)}$$

6. Hensel lift k times to get

$$\bar{f}(x, t, \bar{a}) = g_K(x, t, \bar{a}) \cdot h_K(x, t, \bar{a}) \text{ (mod } t^{2^k})$$

# Deterministic Whitebox Factoring algorithm


7. Solve linear system of $O(d.2^k)$ homogeneous linear equations in $O(d.2^k)$ unknowns.

$$\widetilde{g} = g_k \cdot l_k \pmod{t^{2^k}}$$

8. If no solution then $\bar{f}$ is irreducible, otherwise we get a non trivial factor $gcd(\bar{f}, \widetilde{g})$
9. Recursively repeat the algorithm to factor $f$ completely.

# Arithmetic Tools


## Homogenization Lemma

*Given an arithmetic circuit of size s, that computes a polynomial $f \in \mathbb{F}[x, y_1, \cdots, y_n]$ of degree d, we can construct arithmetic circuits for the homogeneous components of f in time poly(n,d,s). Furthermore, the circuit for each $H^i(f)$ is of size $O(ds)$. Similarly, if we let $f(x, y_1, \cdots, y_n) = \sum_{i=0}^{d} f_i(y_1, \cdots, y_n) \cdot x^i$, then we can in time poly(n,d,s) compute arithmetic circuits of size $O(ds)$ for the polynomials $f_i$.*

# Arithmetic Tools


## Non-vanishing assignment Lemma

*Given an arithmetic circuit C of size s computing a non-zero n-variate polynomial $f(\bar{y})$ of degree d, and a white-box PIT algorithm that runs in time polynomial in s,n,d, then we can find a point $\bar{b} \in \mathbb{F}^n$ in time poly(s,n,d) such that $f(\bar{b}) \neq 0$*

# Algebraic Tools


## Discriminant Lemma

*Let $f(x, y_1, \cdots, y_n)$ be a degree d polynomial computed by an arithmetic circuit of size s. Given this arithmetic circuit, we can find in deterministic time poly(s,n,d) an arithmetic circuit of size poly(s,n,d) computing the discriminant $D_f(y_1, \cdots, y_n)$.*

# Linear Algebra using PIT



## Linear system solving Lemma

*Let $M = (m_{i,j})$ be a k X n matrix, with each entry being a degree $\leq \Delta$ polynomial in $\mathbb{F}[a_1, \cdots, a_n]$. Suppose we have an arithmetic circuit of size s computing M. Then, given access to a PIT oracle, we can deterministically in time poly$(k, n, s, \Delta)$, either:*
*(i) declare that there are no non-zero vectors $(\bar{v}) \in (\mathbb{F}[a_1, \cdots, a_n])^n$, such that $M\bar{v} = 0$, or*
*(ii) find arithmetic circuit of size at most poly$(k, n, s, \Delta)$ computing a non-zero vector $\bar{v}$, such that $M\bar{v} = 0$.*

# Division with remainder



## Division with remainder Lemma

*Let $f, g \in \mathbb{F}(a_1, \cdots, a_n)[x]$ be polynomials of degree atmost d, where g is monic in x. Assume there is a circuit of size s computing all the coefficients of f,g with respect to x. Then one can add to this circuit poly(d) many gates to obtain a circuit computing all the coefficients of polynomials h,r such that $f = hg + r$ with $deg(r) < deg(g)$. Moreover, this new circuit can be computed in a black box fashion.*

# Efficient GCD using PIT


## GCD Lemma

*Suppose we have access to a PIT oracle. Let f and g be univariate polynomials of degree at most $\Delta$ in $\mathbb{F}(t, \bar{y})[x]$. Assume there is a size s circuit computing all the coefficients of f and g. Then one can compute in time $s + poly(\Delta)$, a circuit that outputs the coefficients of f,g and the monic $GCD(f, g) \in \mathbb{F}(t, \bar{y})[x]$.*

# References


[1] Kopparty Swastik, Shubhangi Saraf, and Amir Shpilka. "Equivalence of polynomial identity testing and polynomial factorization." computational complexity 24.2 (2015): 295-331.

[2] Shpilka, Amir, and Ilya Volkovich. "On the relation between polynomial identity testing and finding variable disjoint factors." Automata, Languages and Programming (2010): 408-419.

[3] Nitin Saxena. Lecture Notes CS-748: Arithmetic Circuit Complexity. Sem II, 2015-16.

[4] Nitin Saxena. Lecture Notes CS-681: Computational Number Theory and Algebra. Sem II, 2016-17