Derandomizing Polynomial Identity Testing for Multilinear Constant-Read Formulae

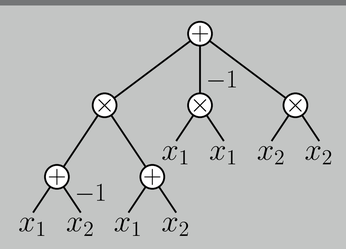
Matthew Anderson, UW-Madison
Dieter van Melkebeek, UW-Madison
Ilya Volkovich, Technion

Polynomial Identity Testing

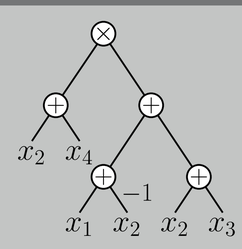
Input: $F \in \mathbb{F}[x_1, ..., x_n]$, given as an arithmetic formula.

Question: Is $F \equiv 0$?

Examples:



$(x_1 - x_2)(x_1 + x_2) - x_1^2 + x_2^2 \equiv 0$



$(x_2 + x_4)(x_1 + x_3) \not\equiv 0$

Deterministic Polynomial-Time Algorithms

Bounded-depth setting
- Depth-2 [several]
- Constant-Top-Fanin Depth-3 [DS06,KS07,KS08,KS09,SS11]
- Constant-Top-Fanin Multilinear Depth-4 [KMSV10,SV11]

"Multilinear" means each subformula is of degree at most 1 in each variable.

Bounded-read setting
- Sums of a Constant Number of Read-Once [SV08,SV09]
- Multilinear Constant-Read [we]

"Read-k" means the formula contains at most k occurrences of each variable.

Results

Main Result:

There is a deterministic algorithm for identity testing n-variable size-s multilinear read-k formulae that runs in time $s^{O(1)} \cdot n^{k^{O(k)}}$.

This poster shows the weaker bound of $s^{O(1)} \cdot n^{k^{O(k)} + O(k \log n)}$.

Extensions:
1. Blackbox: quasi-poly-time in general, and poly-time for constant depth.
2. Structurally-Multilinear Sparse-Substituted Formulae: quasi-poly-time.
   - Encompasses depth-four multilinear formulae [KMSV10], and pre-processed $\sum^k$-read-once formulae [SV09].

Proof Outline

Combine and iterate the following two steps.

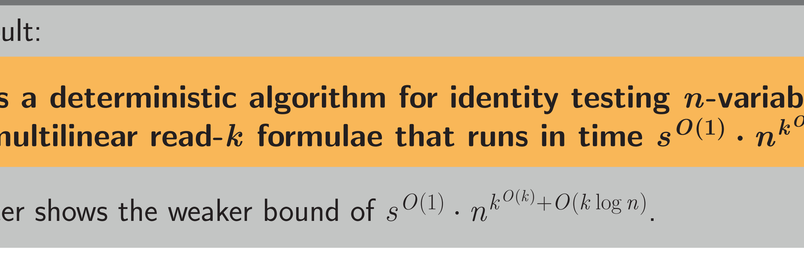
Step 1 – Reduce testing multilinear read-$(k+1)$ to testing multilinear $\sum^2$-read-k.

Step 2 – Reduce testing multilinear $\sum^2$-read-k to testing multilinear read-k.

Step 1

Fragmentation Lemma

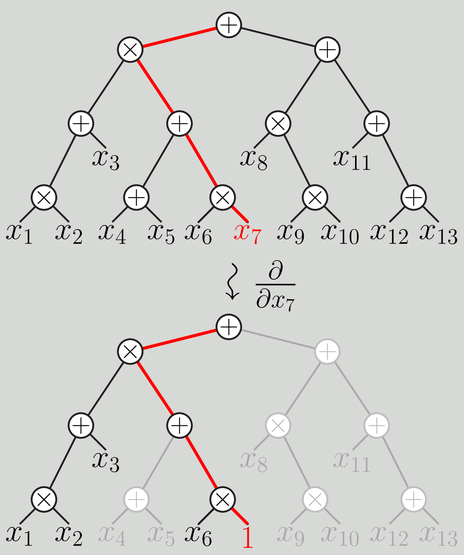
Let F be a nonzero multilinear read-$(k+1)$ formula. There exists a variable x such that $\frac{\partial F}{\partial x}$ is nonzero and well-structured, that is:



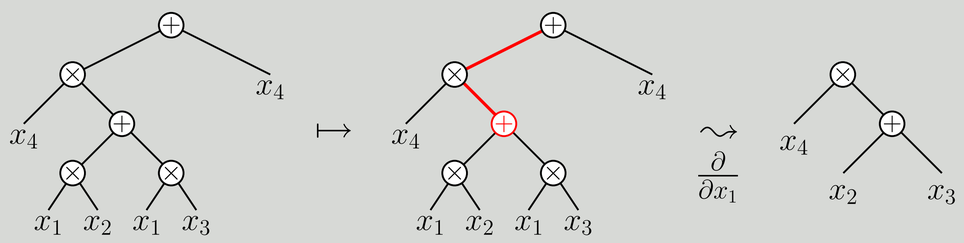
- Let F be a nonzero multilinear read-$(k+1)$ formula.
- By the **Fragmentation Lemma**, there is a variable x s.t. $\frac{\partial F}{\partial x}$ is nonzero and well-structured.
- $\frac{\partial F}{\partial x}$ can be hit by a tester for formulae that are on $\frac{n}{2}$ variables or are $\sum^2$-read-k.
- Iterating reduces to testing $\sum^2$-read-k formulae.
- This step contributes a factor of $n^{O(k \log n)}$ to the running time.

Proof of the Fragmentation Lemma.

If F is read-once, pick the median variable:



If F is read-$(k+1)$, recurse to largest child containing $k+1$ occurrences of a variable; otherwise pick a variable that occurs $k+1$ times in the subformula:

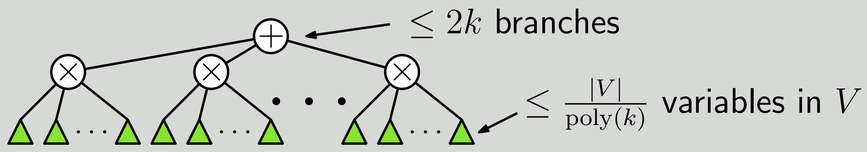


Pick x_1

Step 2

Shattering Lemma

For any nonzero multilinear $\sum^2$-read-k formula F on n variables, there exist disjoint sets of variables P and V, with $|P| = \text{poly}(k)$ and $|V| = \frac{n}{k^{O(k)}}$ such that $\frac{\partial F}{\partial P}$ is nonzero and can be written as

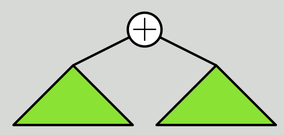


where each small subformula is the partial derivative of some subformula of F.

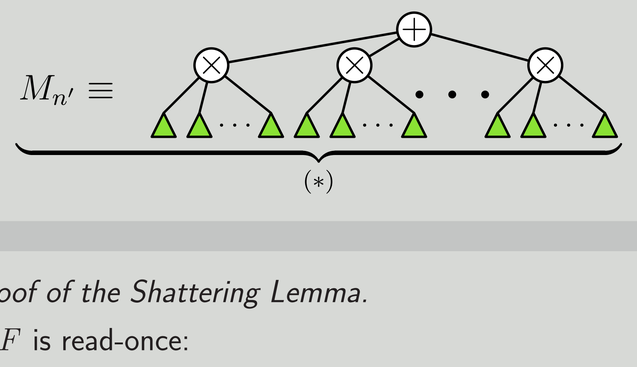
- Let $F = F_1 + F_2$ be a nonzero multilinear $\sum^2$-read-k formula.
- The set of binary strings H_w with Hamming weight at most w hits any class of multilinear polynomials that:
  1. is closed under zero-substitutions, and
  2. does not contain any monomial of degree $d \geq w$.
- Let $\mathcal{F}$ consist of $F(\bar{x} + \bar{\sigma})$ and all its zero-substitutions.
- **Claim**: It is easy to a compute a "good" $\bar{\sigma}$, i.e., such that $F(\bar{x} + \bar{\sigma})$ is not a monomial of degree $n \geq k^{O(k)}$.
- For such a $\bar{\sigma}$, $H_{k^{O(k)}} + \bar{\sigma}$ hits F.
- This step contributes a factor of $n^{k^{O(k)}}$ to the running time.

Proof of Claim.

Suppose $F(\bar{x} + \bar{\sigma})$ is a monomial, M_n,



By the **Shattering Lemma** there is some $n' \geq 1$ s.t.:



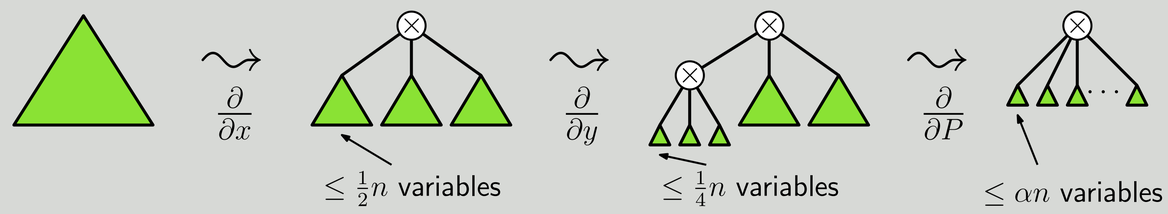
A structural witness theorem for identities of type $(*)$ shows that for some variable x_j, some branch has a root at $x_j = 0$.

Pick "good" to mean that $\bar{\sigma}$ is a common nonzero of the partial derivatives of all subformulae of F.

Then $x_j = 0$ cannot be a root of any branch.
Contradiction!
Since F is $\sum^2$-read-k, a good $\bar{\sigma}$ can be efficiently computed using a read-k identity test.

Proof of the Shattering Lemma.

If F is read-once:



If F is not read-once: