

Abstract

Consider the problem of Polynomial Identity Testing (PIT): we are given an arithmetic circuit computing a multivariate polynomial over some field and we have to determine whether that polynomial is identically zero or not. PIT is a fundamental problem and has applications in both algorithms and complexity theory. In this work, our aim is to study PIT for the model of multilinear depth three circuits for which no deterministic polynomial time identity test is known. An $n^{O(\log n)}$ time blackbox PIT for set-multilinear depth three circuits (a special kind of multilinear depth three circuits) is known due to [ASS12], [FS13]. To get a better understanding of the problem at hand, we move towards multilinear depth three circuits by considering intermediate circuit classes which encompass more polynomials than set-multilinear depth three circuits and are ‘natural’ subclasses of multilinear depth three circuits. One such model is ‘superposition of set-multilinear depth 3 circuits’. Our initial observations are:

- There is an $n^{O(\log n)}$ whitebox PIT for superposition of two set-multilinear depth 3 circuits.
- There is a sub-exponential time whitebox PIT for superposition of constantly many set-multilinear depth 3 circuits.

The second observation is subsumed by the recent independent and almost simultaneous work by [OSV15] that gives sub-exponential time hitting set for multilinear depth three circuits.

A recent line of research considers hitting set for Read Once Oblivious Algebraic Branching Programs (ROABP’s) which subsumes set-multilinear depth three circuits. An $n^{O(\log n)}$ black box PIT is given for ROABP’s of width polynomial in the number of variables in [AGKS14]. It is natural to ask whether this result on ROABP PIT can be used to give efficient (meaning polynomial or quasi-polynomial time) PIT for multilinear depth three circuits. For instance, the result by [OSV15] elegantly uses ROABP PIT as a ‘base case’ (in a certain sense) to give a sub-exponential time PIT algorithm for multilinear depth three circuits. At this point, we

wondered if multilinear depth three circuits of size s could also be computed by an ROABP of size polynomial in s . If true then this would immediately imply a quasi-polynomial time hitting set for multilinear depth three circuits, which is a long standing open problem in algebraic complexity theory. For instance, it can be shown that any multilinear depth three circuit with top fan-in two and just two variables per linear polynomial can be computed by an ROABP with constant width. But we show in our main result that this is not true for general multilinear depth three circuits that are superpositions of only two set-multilinear depth three circuits.

- There is a polynomial computed by a superposition of two set-multilinear depth 3 circuits with top fan-in just three and size polynomial in the number of variables n , such that any ROABP computing the polynomial has width $2^{\Omega(n)}$.
- There is a polynomial computed by a superposition of three set-multilinear depth 3 circuits with top fan-in just two and size polynomial in the number of variables n , such that any ROABP computing the polynomial has width $2^{\Omega(n)}$.

This means the approach of directly converting a multilinear depth 3 circuit (even a superposition of set-multilinear depth 3 circuits) to an ROABP and then applying the existing PIT for ROABP will not work. However the underlying techniques in [ASS12], [AGKS14] and [OSV15] might still be useful. The proofs of the above lower bounds are based on explicit construction of expander graphs that can be used to design multilinear depth three circuits (in particular superposition of set-multilinear depth 3 circuits) with high ‘*evaluation dimension*’ - a complexity measure that is well suited to capture a ‘weakness’ of ROABPs.