Electronic Colloquium on Computational Complexity, Report No. 35 (2001)

Affine Projections of Symmetric Polynomials

Amir Shpilka
Institute of Computer Science
Hebrew University
Jerusalem, Israel
amirs@cs.huji.ac.il

Abstract

In this paper we introduce a new model for computing polynomials - a depth 2 circuit with a symmetric gate at the top and plus gates at the bottom, i.e the circuit computes a symmetric function in linear functions - $S^d_m(\ell_1,\ell_2,...,\ell_m)$ *(*S^d_m *is the* d*'th elementary symmetric polynomial in* m *variables, and the* ℓ_i*'s are linear functions). We refer to this model as the symmetric model. This new model is related to standard models of arithmetic circuits, especially to depth 3 circuits. In particular we show that in order to improve the results of [19], i.e to prove super-quadratic lower bounds for depth 3 circuits, one must first prove a super-linear lower bound for the symmetric model.*

We prove two nontrivial linear lower bounds for our model. The first lower bound is for computing the determinant, and the second is for computing the sum of two monomials. The main technical contribution relates the maximal dimension of linear subspaces on which S^d_m *vanishes, and lower bounds to the symmetric model. In particular we show that an answer of the following problem (which is very natural, and of independent interest) will imply lower bounds on symmetric circuits for many polynomials:*

"What is the maximal dimension of a linear subspace of $\mathcal{C}^m$*, on which* S^d_m *vanishes ?"*

We give two partial solutions to the problem above, each enables us to prove a different lower bound. Using our techniques we also prove quadratic lower bounds for depth 3 circuits computing the elementary symmetric polynomials of degree αn *(where* $0 < \alpha < 1$ *is a constant), thus extending the result of [19]. These are the best lower bounds known for depth 3 circuits over fields of characteristic zero.*

1. Introduction

1.1. Background

Arithmetic circuits and boolean circuits are very natural models for computing polynomials. Similar to most computational models almost no lower bounds are known for these models. The best lower bound is the classical $\Omega(n \log d)$ of [21, 2] for arithmetic circuits computing a polynomial of degree d in n variables over the complex field. No such lower bound is known for circuits over fields of bounded size. In addition there is no lower bound for depth.

Since it is difficult to prove lower bounds for the general model (independent of the characteristic of the field), research focused on restricted models such as monotone circuits, bounded depth circuits and more. Exponential lower bounds were proved for monotone circuits over any field. However, the results for bounded depth circuits depend on the field.

Exponential lower bounds are known for bounded depth Boolean circuits [1, 5, 25, 9]. [20, 16] showed that even if we allow the circuit to use $\bmod p$ gates (for some fixed prime p), then it is still exponentially hard to compute the majority function.

For general bounded depth arithmetic circuits (over characteristic $\neq$3D 2) there are no exponential lower bounds, in contrast to the boolean case. The best lower bound (beside the classical $\Omega(n \log d)$) is a slightly super-linear lower bound of [13, 15]

ISSN 1433-8092

for polynomials of bounded degree (over any field). Not only is it difficult to prove lower bounds for general bounded depth circuits, it seems that proving lower bounds for depth 3 circuits (the first non-trivial depth) is a difficult task in itself. Over fields of characteristic > 0, [6, 7] proved exponential lower bounds for depth 3 circuits computing a generalized majority function.

In spite of these results for depth 3 circuits over fields of characteristic > 0, it seems that the situation in characteristic 0 is completely different. [11, 12] proved exponential lower bounds for restricted $\Sigma\Pi\Sigma$ circuits, but for general $\Sigma\Pi\Sigma$ circuits, there are no such strong results. It seems that although these circuits look very restricted they are actually quite powerful. For example, [3] showed a quadratic depth 3 formula that computes the elementary symmetric polynomials. This construction shows that the efforts to generalize the result of [6, 7] to circuits over fields of characteristic 0, are in vain. The best lower bound is due to [19], who showed a quadratic lower bound for depth 3 circuits computing some of the elementary symmetric polynomials, thus showing that the construction of [3] is essentially optimal. This is the best lower bound for depth 3 circuits over characteristic 0 so far, no super-quadratic lower bounds are known for this model.

1.2. Results

From now on we will only consider computations over the complex field, $\mathcal{C}$.

In this paper we introduce a new model for computing polynomials. The new model is a depth two circuit with unbounded fan-in plus gates at the bottom and a gate computing an elementary symmetric polynomial of the gates of the first level, at the top. Clearly each plus gate computes some linear function ℓ_i, and the top gate computes

$$S^d_m(\ell_1, ..., \ell_m)$$

for some d (m is the number of gates in the first level). We call m the size of the circuit, and d its degree. We call such a circuit a symmetric circuit. We show the following:

- Universality of the model: We prove that every polynomial can be computed in this model. More specifically, we show that for every polynomial f we have
$$s_{\rm sym}(f) \leq 2^d \cdot d \cdot {\rm mon}(f) ,$$
where d =3D $\deg(f)$, $s_{\rm sym}(f)$ =3D the size of a smallest symmetric circuit for f, and ${\rm mon}(f)$ =3D the number of monomials of f.

- Relation to $\Sigma\Pi\Sigma$ circuits: We show that this model is weaker than $\Sigma\Pi\Sigma$ circuits (see definition 3.2). In particular we prove the following theorem
$$s_{\rm sym}(f) > \sqrt{s_3(f)} ,$$
where $s_3(f)$ is the size of a smallest $\Sigma\Pi\Sigma$ circuit computing f. As a corollary we get that super-quadratic lower bounds for depth 3 circuits imply super-linear lower bounds for the symmetric model. On the other hand if f has a $\Sigma\Pi\Sigma$ circuit with m multiplication gates, each of degree at most d then
$$s_{\rm sym}(f) \leq d \cdot 2^d \cdot m .$$

- Lower bounds for the symmetric model: We prove the following lower bounds
$$s_{\rm sym}(DET_{\sqrt{n}}) \geq 2n - 3\sqrt{n} ,$$
$$s_{\rm sym}(\prod_{i=3!1}^{\frac{n}{2}} x_i + \prod_{i=3\frac{n}{2}+1}^{n} x_i) \geq \frac{3}{2}n - 2 .$$
Using our techniques we are able to extend the results of [19] and prove the following lower bound
$$s_3(S^d_n) \text{ =3D } \Omega(d(n-d)) ,$$
for every $d > 1$. Thus for d =3D αn for some constant $0 < \alpha < 1$ we have
$$s_3(S^{\alpha n}_n) \text{ =3D } \Omega(n^2).$$