

# On the power of algebraic branching programs of width two

Eric Allender\*  
 Department of Computer Science  
 Rutgers University  
 Piscataway, NJ 08855, USA  
 allender@cs.rutgers.edu

Fengming Wang†  
 Department of Computer Science  
 Rutgers University  
 Piscataway, NJ 08855, USA  
 fengming@cs.rutgers.edu

May 21, 2011

## Abstract

We show that there are families of polynomials having small depth-two arithmetic circuits that cannot be expressed by algebraic branching programs of width two. This clarifies the complexity of the problem of computing the product of a sequence of two-by-two matrices, which arises in several settings.

## 1 Introduction

The  $n^{\text{th}}$  Iterated Matrix Multiplication polynomial of degree  $d$ , denoted  $\text{IMM}_{d,n}$  is the multilinear polynomial with  $d^2n$  variables that is the result of multiplying  $n$   $d$ -by- $d$  matrices of indeterminates. This family plays a central role in the study of algebraic complexity. Ben-Or and Cleve showed that  $\text{IMM}_{3,n}$  is complete (under projections) for the class of polynomials that can be expressed by arithmetic formulae of polynomial size [5, 6]. This class is sometimes denoted  $\text{VNC}^1$  [13] (as the analog of the Boolean class  $\text{NC}^1$  in the setting of algebraic complexity initiated by Valiant [18]) and is also sometimes denoted  $\text{VP}_e$  (corresponding to the subclass of Valiant's class  $\text{VP}$  of polynomials of polynomial degree that have arithmetic circuits of polynomial size, where we restrict the circuits to be *expressions*).

It is natural to wonder if Ben-Or and Cleve's construction is optimal, in terms of dimension. That is: What can one say about  $\text{IMM}_{2,n}$ ?

There are some indications that  $\text{IMM}_{2,n}$  should be nearly as powerful as  $\text{IMM}_{3,n}$ . For instance, Ben-Or and Cleve's completeness argument proceeds by showing that arithmetic formulae can be efficiently evaluated by a restricted type of straight-line program with three registers (and this translates into an implementation with 3-by-3 matrices). In the original conference publication of their results [5], Ben-Or and Cleve credit Coppersmith with the observation that if the underlying ring is commutative and has an element  $\frac{1}{2}$  such that  $\frac{1}{2} + \frac{1}{2} = 1$ , then in fact *two* registers suffice to evaluate any arithmetic formula (albeit via straight-line programs that do not immediately lend themselves to implementation as  $\text{IMM}_{2,n}$  computations).

Perhaps the first study of the complexity of evaluating  $\text{IMM}_{2,n}$  arose in the work of Lipton and Zalcstein [11], who (in modern terminology) showed that the word problem over the free group with two generators (also known as the two-sided Dyck language) is  $\text{AC}^0$ -reducible to the problem of determining if a product of

---

\*Supported in part by NSF Grants CCF-0830133, and CCF-0832787.

†Supported in part by NSF Grants CCF-0830133 and CCF-0832787.

$n$  two-by-two integer matrices evaluates to the identity matrix. Since the two-sided Dyck language is hard for  $\text{NC}^1$  [15], this gives a lower bound on the complexity of evaluating  $\text{IMM}_{2,n}$  instances.

This lower bound is rather close to the best known upper bound. The problem of evaluating integer instances of  $\text{IMM}_{3,n}$  is complete for the Boolean complexity class  $\text{GapNC}^1$  [7] (consisting of functions that have *arithmetic* circuits of polynomial size and logarithmic depth), and every problem in this latter class has *Boolean* circuits of polynomial size, bounded-fan-in, and depth  $O(\log n \log^* n)$  [10]. The closeness of these bounds has led some researchers to wonder whether the classes of functions in  $\text{NC}^1$  and  $\text{GapNC}^1$  are in fact equal [2], in which case  $\text{IMM}_{2,n}$  and  $\text{IMM}_{3,n}$  would be interreducible under  $\text{AC}^0$  reductions.

The  $\text{NC}^1$ -hardness of  $\text{IMM}_{2,n}$  over the integers holds even for restricted cases of the problem. In [3], it is asserted that counting paths in planar width-two graphs (a restricted case of  $\text{IMM}_{2,n}$  over the integers) is hard for  $\text{NC}^1$  under  $\text{ACC}^0$  reductions. (Mahajan, Saurabh, and Sreenivasaiiah [12] have identified and corrected an error in the proof of this claim in [3].)

On the other hand, there have also been indications that  $\text{IMM}_{2,n}$  should be weaker than  $\text{IMM}_{3,n}$ . Ben-Or and Cleve point out that problems over  $\text{GF}(2)$  having what they called “LBS” straight-line programs (i.e., restricted straight-line programs which they used as a tool in presenting their completeness result) that use only two registers translate into permutation branching programs of width three [6], which Barrington showed require exponential size in order to compute the AND function [4]. However, this does not strictly rule out more general computations over  $\text{IMM}_{2,n}$ .

The  $\text{AC}^0$  reductions from problems in  $\text{NC}^1$  to  $\text{IMM}_{2,n}$  are not projections, which are the usual type of reductions that are used in studying algebraic complexity classes. To illustrate the difference, consider functions in the class  $\text{GapAC}^0$ ; this class consists of functions computed by polynomial-size constant-depth arithmetic circuits over the integers, where the input variables take only Boolean inputs.  $\text{GapAC}^0 \subseteq \text{TC}^0 \subseteq \text{NC}^1$  [1], and hence any bit of any function  $f \in \text{GapAC}^0$  can be computed by an  $\text{AC}^0$  reduction to the problem of multiplying a sequence of 2-by-2 integer matrices. However, any such function  $f$  can also be viewed as a polynomial  $f(x_1, \dots, x_n)$  in its input variables, and the  $\text{AC}^0$  reduction does not allow us to obtain  $f$  from  $\text{IMM}_{2,n^k}$  by substituting field elements and the variables  $x_1, \dots, x_n$  for the variables of  $\text{IMM}$ , even though this is possible for  $\text{IMM}_{3,n^k}$ . It follows from our main result that, even for fairly simple functions  $f \in \text{GapAC}^0$ , no such reduction is possible – even if we allow projections to arbitrarily large  $\text{IMM}$  instances, and even if we greatly enlarge the type of substitutions that are considered (beyond the projections that are usually considered in the framework of Valiant’s complexity classes).

## 1.1 Algebraic Branching Programs

If we expand the notion of projection, to allow not only variables and field elements to be plugged in for the variables of a polynomial, but also allow variables of  $\text{IMM}$  instances to be replaced by arbitrary linear expressions, then we obtain an alternative characterization of algebraic branching programs, which were introduced by Nisan in order to study the complexity of determinant and permanent computations in various settings [14].

**Definition 1** *An Algebraic Branching Program over some field  $\mathbb{F}$  and variables  $\{x_i \mid 1 \leq i \leq n\}$  is a layered directed acyclic graph with a single source vertex  $s$  and exactly one sink vertex  $t$ . The layers are numbered as  $0, 1, 2, \dots, d$ ; let  $V_i$  denote the set of vertices in the  $i$ th layer. The source (the sink, respectively) is the unique vertex in  $V_0$  ( $V_d$ , respectively). Edges exist only between vertices in adjacent layers (i.e., each edge  $(a, b)$  has  $a \in V_i$  and  $b \in V_{i+1}$  for some  $0 \leq i < d$ ). Each edge  $e$  is associated with a linear function  $l_e$  over  $\mathbb{F}$  in the variables  $\{x_i \mid 1 \leq i \leq n\}$ . Every directed path  $p = e_1 e_2 \dots e_k$  represents the product  $f_p = \prod_{j=1}^k l_{e_j}$ . For every vertex  $v$ , the polynomial represented by  $v$ , denoted by  $f_v$ , is  $\sum_{p \in P_{s,v}} f_p$ , where*

$P_{s,v}$  is the set of all paths from  $s$  to  $v$ . The output of the algebraic branching program is  $f_t$ . The width of the program is  $\max_i |V_i|$ .

It follows from [6] that polynomial-size algebraic branching programs of width three (or of any constant width  $w \geq 3$ ) characterize exactly the polynomials in  $VNC^1$ . Algebraic branching programs of constant width have been studied by several authors; we cite some recent examples [9, 8]. We show that width three is optimal; the expressive power of width two algebraic branching programs is severely limited.

**Theorem 2** *Let  $l(\bar{x})$  be an arbitrary linear function.  $\forall k \geq 8$ , the polynomial  $f(\bar{x}) = \sum_{i=1}^k x_{2i-1}x_{2i} + l(\bar{x})$  can not be computed by algebraic branching programs of width two over any field  $\mathbb{F}$ . This implies that  $IMM_{2,n}$  is not complete for  $VNC^1$  under regular projections (defined in Section 2).*

The limitations of width-two algebraic branching programs were also explored by Saha, Saptharishi and Saxena [17]. They considered “degree-restricted” algebraic branching programs (meaning that, if the output polynomial has degree  $n$ , then no intermediate polynomial in the branching program has degree greater than  $n$ ). Their Theorem 16 shows that degree-restricted width-two algebraic branching programs compute polynomials only if they belong to an ideal generated by at most five linear forms (and thus they cannot compute the polynomial  $f$  in our Theorem 2 [16]). We do not know whether width-two algebraic branching programs can be simulated by width-two degree-restricted branching programs. Thus our Theorem 2 is incomparable with [17, Theorem 16]; their result applies to a larger class of polynomials, but relies on the degree restriction.

## 1.2 Organization

The remaining part of the paper is organized as follows: Section 2 provides the formal definitions and terminology that we use. In Section 3, we study homogeneous projections (defined in Section 2) of  $IMM_{2,n}$  and prove a structural theorem for this type of computation as well as an impossibility result. Finally, we extend these results to more general settings in Section 4.

## 2 Preliminaries

Let the underlying field be  $\mathbb{F}$ . Let  $q(\bar{x}) \in \mathbb{F}[\bar{x}]$  be a multivariate polynomial over a set of variables  $\bar{x}$ . A projection  $p$  on  $q(\bar{x})$  is an operation to generate new polynomials; a projection is described by a set of assignments  $\{x_i \leftarrow v_i\}$ , where the values  $v_i$  come from a particular set (to be specified later), and each variable  $x_i \in \bar{x}$  appears at most once on the left-hand-side of a rule in  $p$ ; furthermore, variables on the left-hand-side never occur on the right-hand-side. We get the new instance  $q(\bar{x})|_p$  by replacing all occurrences of  $x_i$  in  $q(\bar{x})$  with its counterpart  $v_i$  and leaving untouched those variables that are not in  $p$ . We may simplify  $q(\bar{x})|_p$  according to the commutative polynomial ring algebra. In this way, we say that  $q(\bar{x})|_p$  is obtained from  $q(\bar{x})$  under the projection  $p$ .

Let  $\mathbb{H}$  be the set of homogeneous linear terms  $\{c \cdot x_i \mid c \in \mathbb{F}^*, i \in \mathbb{N}\}$  where  $\mathbb{F}^*$  is the set of units (i.e., non-zero elements). Let  $\mathbb{S}$  be the set of simple linear terms  $\{c \cdot x_i + w \mid c \in \mathbb{F}^*, i \in \mathbb{N}, w \in \mathbb{F}\}$  and  $\mathbb{L}$  be the set of general linear terms  $\{\sum_{i=1}^n c_i \cdot x_i + w \mid n \in \mathbb{N}, c_i, w \in \mathbb{F}\}$ . We define a projection  $p = \{x_i \leftarrow v_i\}$  to be a *homogeneous projection* if  $\forall i, v_i \in \mathbb{H} \cup \mathbb{F}$ . It is a *simple projection* if  $\forall i, v_i \in \mathbb{S} \cup \mathbb{F}$ . If  $\forall i, v_i \in \mathbb{L}$ , then  $p$  is a *regular projection*. We mention that the most restrictive of these three types of projections, homogeneous projections, are the usual types of projections studied in algebraic complexity [18, 6].

Consider  $n$  square matrices of dimension two  $m_1, m_2, \dots, m_n$ , the entries of which are distinct variables. The  $(1, 1)$ -entry of their product  $\prod_{i=1}^n m_i$  is a multi-linear polynomial, denoted as  $\text{IMM}_{2,n}$ , which is called the  $n$ th iterated matrix multiplication polynomial of dimension two. The matrix  $m_i|_p$  is obtained from  $m_i$  under the projection  $p$ , which means that the entries of  $m_i$  are substituted by the corresponding values in  $p$ . Given a polynomial  $f(\bar{x})$ , it is easy to see that  $f(\bar{x})$  is obtained from  $\text{IMM}_{2,n}$  under some projection  $p$  if and only if  $f(\bar{x})$  is the  $(1, 1)$ -entry of  $\prod_{i=1}^n m_i|_p$ , and moreover, the variables appearing in  $m_i|_p$  belong to the set  $\{x_j \mid x_j \text{ occurs in } f(\bar{x})\}$ . Note that  $f(\bar{x})$  is computable by some algebraic branching program of width two if and only if there exists  $n \in \mathbb{N}$  such that  $f(\bar{x})$  can be obtained from  $\text{IMM}_{2,n}$  under regular projections.

Let  $M$  be a set of square matrices of dimension two. We say a polynomial  $f(\bar{x})$  is *computable by  $M$*  if there is an integer  $n$  and a projection  $p$  such that  $f(\bar{x}) = \text{IMM}_{2,n}|_p$  and furthermore,  $\forall i \leq n, m_i|_p \in M$ . In other words,  $f(\bar{x})$  can be computed by the product of matrices in  $M$ .

Let  $\mathbb{H}_{2 \times 2}$  denote the set of square matrices of dimension two with entries from  $\mathbb{H} \cup \mathbb{F}$ . Similarly, let  $\mathbb{S}_{2 \times 2}$  ( $\mathbb{R}_{2 \times 2}$ , respectively) denote the set of square matrices of dimension two with entries from  $\mathbb{S} \cup \mathbb{F}$  ( $\mathbb{L}$ , respectively). Obviously,  $\mathbb{H}_{2 \times 2} \subseteq \mathbb{S}_{2 \times 2} \subseteq \mathbb{R}_{2 \times 2}$ .

We divide all square matrices of dimension two whose entries belong to  $\mathbb{L}$  into three groups, Indg, Idg and Pdg. The matrices in Indg are called *inherently non-degenerate matrices* and their determinants evaluate to a fixed element in  $\mathbb{F}^*$  while Idg consists of *inherently degenerate matrices* with zero determinants.  $\text{Pdg} = \mathbb{R}_{2 \times 2} \setminus (\text{Indg} \cup \text{Idg})$  is the set of *potentially degenerate matrices*. Obviously the determinants of matrices in Pdg are nonzero polynomials of degree at least one.

Our results deal with some simple degree-two polynomials; the following facts are easy to verify.

**Fact 3** *Over any field  $\mathbb{F}$ ,  $x_1x_2 + x_3x_4$  is an irreducible polynomial.*

**Fact 4** *Let  $\mathbb{F}$  be any field,  $k \geq 2$  and let  $l(\bar{x})$  be an arbitrary linear function. Then  $\sum_{i=1}^k x_{2i-1}x_{2i} + l(\bar{x})$  is an irreducible polynomial, and furthermore, its degree-two homogeneous part is irreducible as well.*

We group the variables  $x_{2i-1}$  and  $x_{2i}$  together, and call each the other's *partner variable*.

**Definition 5** *In a regular projection  $p$  given by  $\{x_j \leftarrow v_j\}$ , the partner variables  $x_{2i-1}, x_{2i}$  are called matched if*

- *Both of  $x_{2i-1}$  and  $x_{2i}$  appear on the left-hand-side.*
- $\{v_{2i-1}, v_{2i}\} \cap \mathbb{F} \neq \emptyset$ .

It is convenient to consider a restricted class of projections:

**Definition 6** *A regular projection  $p$  given by  $\{x_i \leftarrow v_i\}$  is well-formed if every left-hand-side variable  $x_i$  is matched.*

We will make use of the fact that any projection can be “extended” to obtain a well-formed projection. However, we must first be precise about what it means for one projection to be an “extension” of another. (To see what the issue is, consider the projection  $\{x_1 \leftarrow x_3, x_2 \leftarrow x_4\}$ . The partner variables  $x_1$  and  $x_2$  are not matched, since neither of them is assigned a field element. Thus we need to consider how to “extend” projections, by not only adding new rules, but also by changing existing rules appropriately.

**Definition 7** A regular projection  $p$  is an extension of a projection  $p'$  if there is a projection  $p''$  such that  $p = p' \circ p''$ .

Thus to continue the example above, the projection  $p' = \{x_1 \leftarrow x_3, x_2 \leftarrow x_4\}$  can be extended by  $p'' = \{x_4 \leftarrow 0\}$  to obtain the projection  $p = \{x_1 \leftarrow x_3, x_2 \leftarrow 0, x_4 \leftarrow 0\}$  (which is still not well-formed).

**Proposition 8** Any regular projection of size  $k$  with  $l$  unmatched left-hand-side variables can be extended to a well-formed regular projection of size at most  $k + l$ . Thus any regular projection of size  $k$  can be extended to a well-formed regular projection of size at most  $2k$ .

**Proof:** The proof proceeds by induction on  $l$ . The basis, when  $l = 0$ , is trivial.

Now consider a regular projection  $p$  with  $l$  unmatched left-hand-side variables, where we inductively assume that any regular projection of size  $k'$  with  $l' < l$  unmatched variables can be extended to a well-formed regular projection of size at most  $k' + l'$ . There are two cases:

**Case 1:** If there is an unmatched variable  $x$  whose partner variable  $y$  does not appear on the left-hand-side of any rule, then then we simply add the rule  $y \leftarrow 0$ . (If  $y$  appeared on the *right*-hand-side of any rule, then any such rule must also be simplified by setting  $y$  to zero. Such changes do not increase the size of the projection.) This yields a projection  $p'$  with at most  $l - 1$  unmatched variables, where we have added one rule. (It is possible that there will be *fewer* than  $l - 1$  unmatched variables, if there were some unmatched variable  $z$  such that  $z \leftarrow c \cdot y$  was a rule.) Now the claim follows by induction.

**Case 2:** If Case 1 does not hold, then there must be a pair of unmatched variables that are partners (without loss of generality call them  $x_1$  and  $x_2$ ) such that the projection has rules  $x_1 \rightarrow v_1$  and  $x_2 \rightarrow v_2$ , where  $\{v_1, v_2\} \cap \mathbb{F} = \emptyset$ . Since  $p$  is a regular projection,  $v_1$  is of the form  $c_0 + \sum_{k=1}^n c_k y_k$ , where none of the variables  $y_i$  appear on the left-hand-side of any rule in  $p$ . Note that the rule  $y_1 \leftarrow (-1/c_1) \cdot (c_0 + \sum_{k=1}^n c_k y_k)$  has the effect of setting  $x_1$  to 0. Let  $z$  be the partner variable of  $y_1$ ; note that  $z$  does not appear on the left-hand side of any rule (because otherwise Case 1 would have applied). Thus removing the rule  $x_1 \rightarrow v_1$  and adding the rules  $x_1 \leftarrow 0, y_1 \leftarrow -1/c_1 \cdot (c_0 + \sum_{k=1}^n c_k y_k), z \leftarrow 0$  has at most  $l - 2$  unmatched variables (since  $x_1$  and  $x_2$  are now both matched, as are  $y_1$  and  $z$ ), and it has two more rules than  $p$ . As above, it is now necessary to simplify any rule in which  $y_1$  or  $z$  appeared on the right-hand-side, but this does not increase the size of the projection. Now the claim follows by induction.  $\square$

The definition of “well-formed projection” is designed to make the following proposition obvious:

**Proposition 9** Let  $k, n \in \mathbb{N}$ , with  $n - k \geq 2$ . Consider the polynomial  $\sum_{i=1}^n x_{2i-1} x_{2i}$ . Then under any well-formed regular projection  $p$  of size  $2k$ ,  $f(\bar{x})|_p = \sum_{i=1}^{n-k} x_{2i-1} x_{2i} + l(\bar{x})$  (up to re-numbering the variables) is also an irreducible polynomial, where  $l(\bar{x})$  is a linear function. Furthermore, its degree-two homogeneous part is also irreducible.

In this work, we will show that certain constant-size polynomials are not computable by various families of matrices over any algebraically closed field. By the following fact, we may as well assume that the underlying field  $\mathbb{F}$  is algebraically closed.

**Fact 10** Let  $\mathbb{F}'$  be the algebraic closure of  $\mathbb{F}$  and let  $M$  be a set of matrices. For any polynomial  $f(\bar{x})$ , if  $f(\bar{x})$  is computable by  $M$  over  $\mathbb{F}$ , then it is computable by  $M$  over  $\mathbb{F}'$  as well.

### 3 IMM<sub>2,n</sub> under homogeneous projections

In this section, we will show that the computational power of the family  $\{\text{IMM}_{2,n} \mid n \in \mathbb{N}\}$  under homogeneous projections is very limited.

Recall that  $\mathbb{H}_{2 \times 2}$  denotes the set of square matrices of dimension two with entries from  $\mathbb{H} \cup \mathbb{F}$ . We will show that it causes no loss of computational power, if we restrict the type of matrices that are used in  $\mathbb{H}_{2 \times 2}$  computations. First, however, it is very useful to observe that  $\mathbb{H}_{2 \times 2}$  computations correspond exactly to a type of straight-line programs.

Let  $\mu$  be a set of allowable straight-line program instructions (rules), and let  $R_i^t$  denote the contents of the register  $R_i$  at time  $t$ . A straight-line program  $P$  over the rule set  $\mu$  using 2 registers ( $\mu$ -SLP) is a sequence of pairs of instructions from  $\mu$ , denoted as  $\{(s_1^t, s_2^t) \mid 1 \leq t \leq |P|, (s_1^t, s_2^t) \in \mu\}$ , where  $|P|$  is the size of the program.  $P$  computes a function  $p(\bar{x})$  in the natural way: Initially,  $R_1^0 = 1$  and  $R_2^0 = 0$ . At the  $t$ -th step,  $R_i$  is updated according to the rule  $s_i^t$ . The final output  $p(\bar{x})$  is stored as  $R_1^{|P|}$ . In this section, we consider only instructions that come from the set  $\mu_{\mathbb{H}_{2 \times 2}} = \{(R_1^{t+1} \leftarrow a \cdot R_1^t + b \cdot R_2^t, R_2^{t+1} \leftarrow a' \cdot R_1^t + b' \cdot R_2^t) \mid a, b, a', b' \in \mathbb{H} \cup \mathbb{F}, t \in \mathbb{N}\}$ . Under these assumptions, each  $R_i^t$  is a polynomial over the variables  $\{x_j \mid j \in \mathbb{N}\}$ . It is not hard to see that  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLPs and  $\text{IMM}_{2,n}$  under homogeneous projections compute the same set of polynomials. (Similar observations were made by Ben-Or and Cleve [6].) Furthermore, for any subset  $N \subseteq \mathbb{H}_{2 \times 2}$ , there is a corresponding rule set  $\mu_N \subseteq \mu_{\mathbb{H}_{2 \times 2}}$  such that a polynomial  $f(\bar{x})$  is computable by  $N$  if and only if there is a  $\mu_N$ -SLP for it. Hence, given an arbitrary  $\mu_N$ -SLP  $P$ , we may abuse the notations and identify the  $i$ th pair of instructions with its matrix representations  $m_P^i$ , which means that  $P$  can also be characterized by a sequence of matrices  $\{m_P^i \mid 1 \leq i \leq |P|\}$ .

#### 3.1 Classification of $\mathbb{H}_{2 \times 2} \cap \text{Indg}$

Now, we present a collection  $\mu_N$  of rules (corresponding to a subset  $N$  of matrices in  $\mathbb{H}_{2 \times 2}$ ) which we claim suffice to simulate any straight-line program using the rules  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ . Let  $a, b, c, d \in \mathbb{F}^*$ .

1. Transposition rule.

$$\begin{array}{l} R_1^{t+1} \leftarrow R_2^t \\ R_2^{t+1} \leftarrow R_1^t \end{array} \text{ given by matrix } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

2. Scalar rules.

$$\begin{array}{l} R_1^{t+1} \leftarrow a \cdot R_1^t \\ R_2^{t+1} \leftarrow b \cdot R_2^t \end{array} \text{ given by matrix } \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

3. Offsetting rules of degree one.

(a)

$$\begin{array}{l} R_1^{t+1} \leftarrow a \cdot R_1^t + c \cdot x_i \cdot R_2^t \\ R_2^{t+1} \leftarrow b \cdot R_2^t \end{array} \text{ given by matrix } \begin{bmatrix} a & c \cdot x_i \\ 0 & b \end{bmatrix}$$

(b)

$$\begin{array}{l} R_1^{t+1} \leftarrow a \cdot R_1^t \\ R_2^{t+1} \leftarrow c \cdot x_i \cdot R_1^t + b \cdot R_2^t \end{array} \text{ given by matrix } \begin{bmatrix} a & 0 \\ c \cdot x_i & b \end{bmatrix}$$

4. Offsetting rules of degree zero.

(a)

$$\begin{aligned} R_1^{t+1} &\leftarrow a \cdot R_1^t + c \cdot R_2^t \\ R_2^{t+1} &\leftarrow b \cdot R_2^t \end{aligned} \quad \text{given by matrix } \begin{bmatrix} a & c \\ 0 & b \end{bmatrix}$$

(b)

$$\begin{aligned} R_1^{t+1} &\leftarrow a \cdot R_1^t \\ R_2^{t+1} &\leftarrow c \cdot R_1^t + b \cdot R_2^t \end{aligned} \quad \text{given by matrix } \begin{bmatrix} a & 0 \\ c & b \end{bmatrix}$$

5. Other non-degenerate linear transformations.

$$\begin{aligned} R_1^{t+1} &\leftarrow a \cdot R_1^t + c \cdot R_2^t \\ R_2^{t+1} &\leftarrow d \cdot R_1^t + b \cdot R_2^t \end{aligned} \quad \text{given by matrix } \begin{bmatrix} a & c \\ d & b \end{bmatrix}$$

where  $ab - cd \neq 0$ .

**Observation 11** Any straight-line program using  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$  can be simulated by a straight-line program using  $\mu_N$ . That is, without loss of generality, one can assume that any straight-line program  $P$  has the following properties.

- If the transposition matrix is ever adopted by  $P$ , it is applied only once as the final pair of instructions. (This is because we can cancel adjacent transpositions, and shift any single transposition toward the end of the program via the following transformation:

$$\begin{bmatrix} v & u \\ z & y \end{bmatrix} = \begin{bmatrix} u & v \\ y & z \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} y & z \\ u & v \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u & v \\ y & z \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u & v \\ y & z \end{bmatrix} = \begin{bmatrix} z & y \\ v & u \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- The following matrices need never appear, because they are transpositions of rules in  $\mu_N$  (and transpositions introduced in this way can be eliminated).

$$\begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix}, \begin{bmatrix} 0 & a \\ b & c \end{bmatrix}, \begin{bmatrix} c & a \\ b & 0 \end{bmatrix}, \begin{bmatrix} 0 & a \\ b & c \cdot x_i \end{bmatrix}, \begin{bmatrix} c \cdot x_i & a \\ b & 0 \end{bmatrix}$$

- This leaves only the rule set  $\mu_N$ .

### 3.2 Structure of $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLPs and its implications

**Definition 12** Let  $\deg(f)$  denote the degree of the polynomial  $f$ . For any straight-line program  $P$ , let  $\deg(P, t) = \deg(R_1^t) + \deg(R_2^t)$  be the degree of  $P$  at time  $t$ . We call  $\deg(P, 0), \deg(P, 1), \dots, \deg(P, |P|)$  the degree sequence of  $P$ .

An ordered pair of non-negative integers  $(t_1, t_2)$ , where  $t_1 + 1 < t_2$ , is called a mesa in the degree sequence of  $P$  if there exists  $d > 0$  such that

- For all  $t_1 < t' < t_2$ ,  $\deg(P, t') = d$ ;
- $\deg(P, t_1) < d$ ;
- $\deg(P, t_2) < d$ .

The number  $d$  is called the height of this mesa.

**Fact 13** The operations in Observation 11 that simplify the straight-line program  $P$  do not change the height of any mesa in which the operations are applied.

Now we are ready to show our structural theorem for  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLPs.

**Theorem 14** If a polynomial  $f$  is computable by  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ , then there is a  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP  $P$  for  $f$  with the property that there are no mesas in the degree sequence of  $P$ .

**Proof:** By our assumption, there is some  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP  $P'$  computing  $f$ . If  $P'$  does not contain any mesas in its degree sequence, then we are done. Otherwise, we will show how to obtain  $P$  from  $P'$  by a series of transformations. At every step, we turn the current  $P'$  into an equivalent  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP while reducing the total height of all mesas by at least one. Ultimately we will obtain a  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP  $P$  with the desired property. Hence, it suffices to verify the correctness of a single step.

Let  $(t_1, t_2)$  be the first mesa in the current  $P'$  and  $d$  be its height. There are three cases to consider.

1.  $\deg(R_1^{t_1+1}) > \deg(R_2^{t_1+1})$ .

We claim that the only instruction that can produce this outcome at time  $t_1 + 1$  is the degree-one offsetting rule 3(a). Rule 2 is impossible since it only scales the registers by a constant factor respectively. Rule 3(b) implies that  $\deg(R_1^{t_1+1}) = \deg(R_1^{t_1})$ ; there are two subcases to consider:

- If  $\deg(R_1^{t_1}) \geq \deg(R_2^{t_1})$ , then  $\deg(R_1^{t_1+1}) \leq \deg(R_2^{t_1+1})$ , a contradiction to our assumption that  $\deg(R_1^{t_1+1}) > \deg(R_2^{t_1+1})$ .
- If  $\deg(R_1^{t_1}) < \deg(R_2^{t_1})$ , then  $\deg(R_2^{t_1+1}) \leq \deg(R_2^{t_1})$ . This contradicts our assumption that  $\deg(P, t_1) < \deg(P, t_1 + 1)$ .

For similar reasons, one can show that rules 4(a) and 4(b) are not applicable either. There are two cases that arise, in dealing with rule 5:

- If  $\deg(R_1^{t_1}) \neq \deg(R_2^{t_1})$ , then under rule 5,  $\deg(R_1^{t_1+1}) = \deg(R_2^{t_1+1})$ , which contradicts our assumption that  $\deg(R_1^{t_1+1}) > \deg(R_2^{t_1+1})$ ;
- If  $\deg(R_1^{t_1}) = \deg(R_2^{t_1})$ , then  $\deg(P', t_1) \geq \deg(P', t_1 + 1)$ , which contradicts our assumption that  $(t_1, t_2)$  is a mesa.

$\forall t_1 < t' < t_2$ ,  $\deg(P', t') = d$  and  $\deg(P', t_2) < d$  implies that rules 3(b), 4(b) and 5 are impossible at time  $t'$  (and at time  $t_2$ ), since under our assumptions they would increase the degree of  $R_2$  while maintaining the degree of  $R_1$ . Hence, for all  $t_1 < t' \leq t_2$ , the product  $\prod_{i=t_1+1}^{t'} m_{P'}^i$  is an upper triangular matrix of the form  $\begin{bmatrix} a & g_{t'} + w \\ 0 & b \end{bmatrix}$ , where  $w \in \mathbb{F}$ ,  $a, b \in \mathbb{F}^*$  and  $g_{t'}$  is a linear homogeneous polynomial. In other words,  $R_1^{t'} = a \cdot R_1^{t_1} + (g_{t'} + w) \cdot R_2^{t_1}$  and  $R_2^{t'} = b \cdot R_2^{t_1}$ . Since  $\deg(P', t_2) < d = \deg(P', t_1 + 1)$ , it follows that  $\deg(R_1^{t_1}) < \deg(R_1^{t_1+1})$  and  $g_{t_2} = 0$ . Thus, we can replace the whole computation between  $t_1$  and  $t_2$  by a simple application of rule 2 or 4(a) while avoiding the mesa  $(t_1, t_2)$ .

2.  $\deg(R_1^{t_1+1}) < \deg(R_2^{t_1+1})$ .

This is completely analogous to case 1.

3.  $\deg(R_1^{t_1+1}) = \deg(R_2^{t_1+1})$ .

We argue that neither of rules 3(a) and 3(b) can happen at time  $t_1 + 1$ . We study the reasons for 3(a) and those for 3(b) are symmetric.

- If  $\deg(R_1^{t_1}) \leq \deg(R_2^{t_1})$ , then  $\deg(R_1^{t_1+1}) > \deg(R_2^{t_1+1})$ , a contradiction to our assumption  $\deg(R_1^{t_1+1}) = \deg(R_2^{t_1+1})$ .
- If  $\deg(R_1^{t_1}) > \deg(R_2^{t_1})$ , then  $\deg(P', t_1 + 1) < \deg(P', t_1)$  since  $\deg(R_2^{t_1}) = \deg(R_2^{t_1+1})$ . This contradicts our assumption that  $(t_1, t_2)$  is a mesa.

Furthermore,  $\forall t_1 < t' < t_2$ ,  $\deg(P', t') = d$  implies that rules 3(a) and 3(b) are impossible at time  $t'$  (and at time  $t_2$ ). Thus, we obtain that for all  $t_1 < t' \leq t_2$ , the product  $\prod_{i=t_1+1}^{t'} m_{P'}^i$  is a non-degenerate linear transformation, which can be captured by one of the other rules or their transposed counterparts. The analysis of this case can now be completed similarly to Case 1, by appealing to Observation 11 and Fact 13.

In all cases, we are able to reduce the total height of all mesas in  $P'$  by at least one, which concludes our proof.  $\square$

**Corollary 15** *If a polynomial  $f(\bar{x})$  is computable by  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ , then there exists a  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP for  $f(\bar{x})$  with a monotonically nondecreasing degree sequence.*

The analysis in the proof of Theorem 14 also allows one to draw the following conclusions:

**Fact 16** *For any  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP  $P$ ,  $\forall 0 < t \leq |P|$ , if  $\deg(P, t) > \deg(P, t - 1)$ , then only one of the following two scenarios can happen.*

- *If either 3(a) or 3(b) is applied at time  $t$ , then  $|\deg(R_1^t) - \deg(R_2^t)| = 1$ .*
- *If the other rules are used at time  $t$ , then  $\deg(R_1^t) = \deg(R_2^t)$ .*

**Lemma 17** *If  $P$  is a  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP with a monotonically nondecreasing degree sequence, then for all  $0 \leq t \leq |P|$ ,  $|\deg(R_1^t) - \deg(R_2^t)| \leq 1$ . Furthermore, we can assume that  $\deg(R_1^{|P|}) \geq \deg(R_2^{|P|})$ .*

**Proof:** The first part follows naturally from Fact 16. It suffices to justify the second claim. Suppose there is no presence of rule 1 in  $P$ . Let  $r = \deg(R_1^{|P|})$ . If  $\deg(R_2^{|P|}) = r + 1$ , then from the time  $t'$  when  $\deg(R_2^{|P|})$  is increased to  $r + 1$ , the polynomial in  $R_1$  will change only by multiplication by a nonzero field element. This is because of the monotonicity of the degree sequence. Hence, we can skip the steps following time  $t'$  and substitute them by an appropriate scalar matrix instead. Then the degree of  $R_2$  will remain no more than  $r$  in the new  $\mu_f$ -SLP. The argument in the case when rule 1 appears is completely symmetric.  $\square$

**Theorem 18** *Let  $f(\bar{x})$  be a polynomial of total degree at least two whose highest-degree homogeneous part is irreducible. Then  $f(\bar{x})$  is not computable by  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ .*

**Proof:** The proof is by contradiction. Suppose there exists a  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP  $P$  for  $f(\bar{x})$ . By Corollary 15 and Lemma 17,  $P$  has a monotonically nondecreasing degree sequence, and  $\deg(R_1^{|P|}) = \deg(f)$  while  $\deg(R_2^{|P|}) \leq \deg(f)$ . If  $\deg(R_2^{|P|}) < \deg(f)$ , the analysis of Theorem 14 and Fact 16 reveals that the highest-degree homogeneous part of  $f(\bar{x})$  contains a linear factor and hence, is reducible, which is a contradiction to our assumption. So assume  $\deg(R_2^{|P|}) = \deg(f)$  and without loss of generality, assume that  $R_2$ 's degree reaches  $\deg(f)$  first, at some time  $t_0$ , and that  $R_1$ 's degree is raised to  $\deg(f)$  at some time  $t > t_0$ . Thus all of the highest-degree monomials in  $R_2^{t_0}$  come from  $c \cdot x_i \cdot R_1^{t_0-1}$ . For any polynomial  $g$ , let  $H_d(g)$  denote the degree- $d$  homogeneous part of polynomial  $g$ . An easy induction shows that, for all  $t'$  such that  $t_0 \leq t' \leq t$ ,  $H_{\deg(f)-1}(R_1^{t_0-1})$  divides  $H_{\deg(f)}(R_2^{t'})$ . By Fact 16, rules 3(a) and 3(b) can not be applied at time  $t$ . Since the degree sequence is stable from then on, they will not happen afterwards either. Hence, by the linearity of the remaining rules, we claim that  $\forall t \leq t' \leq |P|$ ,  $\exists a, b \in \mathbb{F}^*$ ,  $H_{\deg(f)}(R_1^{t'}) = aH_{\deg(f)}(R_2^{t'}) = bH_{\deg(f)}(R_2^{t'-1})$ , which we argued above is divided by  $H_{\deg(f)-1}(R_1^{t_0-1})$ . This is a contradiction to our assumption that it is irreducible. This concludes our proof.  $\square$

**Remark 19** *The proof of Theorem 18 reveals that if  $f(\bar{x})$  is computable by  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ , then the highest-degree homogeneous part of  $f(\bar{x})$  can be completely factored into homogeneous linear polynomials.*

### 3.3 Limitation of $\mu_{\mathbb{H}_{2 \times 2}}$ -SLPs

First, by the following lemma, we can assume without loss of generality that for any  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLP  $P$  and any inherently degenerate matrix  $m$  in  $P$ , the entries of  $m$  all belong to  $\mathbb{F}$ .

**Proposition 20** *If a matrix  $m \in \mathbb{H}_{2 \times 2} \cap \text{Idg}$  contains at least one entry from  $\mathbb{H}$ , then  $m$  can be factored into a product of matrices, exactly one of which, denoted as  $m_1$ , belongs to  $\text{Idg}$  and furthermore, all  $m_1$ 's entries are from  $\mathbb{F}$ .*

**Proof:** If  $m$  has a zero column, then without loss of generality,  $m$  is either  $\begin{bmatrix} a \cdot x_i & 0 \\ w & 0 \end{bmatrix}$  or  $\begin{bmatrix} a \cdot x_i & 0 \\ b \cdot x_j & 0 \end{bmatrix}$  where  $a, b \in \mathbb{F}^*$  and  $w \in \mathbb{F}$ .  $\begin{bmatrix} a \cdot x_i & 0 \\ w & 0 \end{bmatrix} = \begin{bmatrix} x_i & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ w & 0 \end{bmatrix}$  while  $\begin{bmatrix} a \cdot x_i & 0 \\ b \cdot x_j & 0 \end{bmatrix} = \begin{bmatrix} x_i & 0 \\ 0 & x_j \end{bmatrix} \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ . In both cases, we obtain the desired factorization for  $m$ . The case where  $m$  has a zero row is symmetric.

For the other cases, it is not hard to see that under our assumption,  $m$  can be turned into a matrix with either a zero column or a zero row via multiplication by a non-degenerate linear transformation. Our proof is completed by referring to the previous case analysis.  $\square$

**Note 21** The statement of Proposition 20 can be generalized for matrices in  $\mathbb{S}_{2 \times 2} \cap \text{Idg}$  and  $\mathbb{R}_{2 \times 2} \cap \text{Idg}$  with almost the same proof. Hence, we can assume that for any  $\mu_{\mathbb{S}_{2 \times 2}}\text{-SLP}$  ( $\mu_{\mathbb{R}_{2 \times 2}}\text{-SLP}$ , respectively)  $P$  and any inherently degenerate matrix  $m$  in  $P$ , the entries of  $m$  all belong to  $\mathbb{F}$ .

**Lemma 22** If a nonzero polynomial  $f(\bar{x})$  is computable by a straight-line program  $P$ , then  $P$  does not contain any matrix of the form  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ .

**Proof:** Suppose  $P$  does have at least one such matrix, then the product of matrices in  $P$  evaluates to  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ , a contradiction to our assumption about  $f(\bar{x})$ .  $\square$

Given a projection  $p$  and a straight-line program  $P = \{m_P^i \mid 1 \leq i \leq |P|\}$  computing a polynomial  $f(\bar{x})$ , we obtain the straight-line program  $P|_p = \{m_P^i|_p \mid 1 \leq i \leq |P|\}$ , which is a new straight-line program (not incorporating any simplifications). Moreover,  $P|_p$  computes  $f(\bar{x})|_p$ . Note that this definition applies for any type of projections. In the remaining part, by Propositions 8 and 9, the polynomial  $f(\bar{x})$  considered will be nonzero under any regular projection of size at most four, which leads to the following lemma.

**Lemma 23** There does not exist a matrix in  $P$  such that all of its entries belong to  $\mathbb{H}$ . This implies all matrices in  $P$  must contain an entry from  $\mathbb{F}$ .

**Proof:** Suppose  $P$  does have one such matrix, and without loss of generality, assume that it has the form  $\begin{bmatrix} c_1x_1 & c_2x_2 \\ c_3x_3 & c_4x_4 \end{bmatrix}$ , where  $\forall 1 \leq i \leq 4, c_i \in \mathbb{F}^*$  and the  $x_i$ 's need not be distinct. Consider the projection  $p = \{x_i \leftarrow 0 \mid 1 \leq i \leq 4\}$ . Then  $f(\bar{x})|_p$  is nonzero while  $P|_p$  contains  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ , in contradiction to Lemma 22.  $\square$

**Lemma 24** For any matrix  $m \in P$  which belongs to  $\mathbb{H}_{2 \times 2} \cap \text{Pdg}$ , there exists a homogeneous projection  $p$  of size at most three such that  $m|_p$  is degenerate and all of the entries in  $m|_p$  belong to  $\mathbb{F}$ . Moreover, there is a well-formed homogeneous projection  $q$  of size at most six extending  $p$ .

**Proof:** The determinant of  $m$ , denoted as  $\det(m)$ , is a polynomial of degree at least one. Since  $\mathbb{F}$  is algebraically closed, the variety of  $\det(m)$  is always non-empty and furthermore, by Lemma 23,  $\det(m)$  contains at most three variables. This provides us the projection promised in the first claim. Proposition 8 implies the correctness of the second claim.  $\square$

**Definition 25** We call such a well-formed homogeneous projection  $q$  as in Lemma 24 a degenerating projection for the potentially degenerate matrix  $m$ .

**Lemma 26** Let  $f(\bar{x})$  be a polynomial and  $P$  be one of its  $\mu_{\mathbb{H}_{2 \times 2}}\text{-SLPs}$ . Suppose that there exists  $0 < t \leq |P|$  such that  $m_P^t$  is a potentially degenerate matrix. Let  $p$  be one of its degenerating projections. Let  $P' = P|_p$  and let  $R_i^t(P')$  be the contents of  $R_i$  at time  $t$  in  $P'$ . Then up to the permutation of the indices, only one of the three following cases will happen.

1.  $R_1^t(P') = R_2^t(P') = 0$  and  $f(\bar{x})|_p = 0$ . This is the uninteresting case and we ignore it in the remainder of the proof.

2.  $R_1^t(P') \in \mathbb{F}^*$  and  $R_2^t(P') = w \cdot R_1^t(P')$  for some  $w \in \mathbb{F}$ .
3.  $R_1^t(P')$  is a polynomial of degree at least one,  $R_2^t(P') = w \cdot R_1^t(P')$  for some  $w \in \mathbb{F}$ , and  $f(\bar{x})|_p$  is divisible by  $R_1^t(P')$ .

**Proof:** Our assumption is that  $m_P^t$  is a degenerate matrix; let us say that it is  $\begin{bmatrix} a & c \\ d & b \end{bmatrix}$ , where  $ab - cd = 0$ . Assume for now that  $c \neq 0$ . (The case where  $c = 0$  is easier.) Let  $f$  and  $g$  be the polynomials given by  $R_1^{t-1}(P')$  and  $R_2^{t-1}(P')$ , respectively. Thus  $R_1^t(P') = af + cg$  and  $R_2^t(P') = (b/c)(af + cg)$ . Thus  $R_2^t(P')$  is a multiple of  $R_1^t(P')$ , and an easy induction shows that  $R_1^t(P')$  will stay as a common factor of both registers from that point on (and thus  $R_1^t(P')$  also divides  $f(\bar{x})|_p$ ).  $\square$

**Corollary 27** *If  $f(\bar{x})|_p$  is a nonzero irreducible polynomial and the other hypotheses of Lemma 26 hold, then  $R_1^t(P') = c \cdot f(\bar{x})|_p$  for some  $c \in \mathbb{F}^*$ .*

**Definition 28** *Let  $f(\bar{x})$ ,  $P$ ,  $m_P^t$  and  $P'$  satisfy the conditions of Lemma 26. If under the degenerating projection  $p$ , case 2 of Lemma 26 happens, then we call  $p$  a cutting projection for  $m_P^t$  in  $P$ . If instead we have case 3, then we call  $p$  a finishing projection for  $m_P^t$  in  $P$ .*

**Observation 29** *Let  $f(\bar{x})$  be a polynomial such that under any well-formed homogeneous projection  $q$  of size at most six,  $f(\bar{x})|_q$  is always a nonzero irreducible polynomial. Let  $P$  be a  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLP for  $f(\bar{x})$ , and let  $m_P^t$ ,  $p$  and  $P'$  be the corresponding objects as in Lemma 26. We will show how to obtain a  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLP for  $f(\bar{x})|_p$  from  $P$  as follows:*

- *If the projection  $p$  is a cutting projection for  $m_P^t$  in  $P$ , then we can simply ignore the instructions in  $P'$  before time  $t$  (including the  $t$ -th instruction), and concatenate a single instruction, which is a linear transformation from the initial condition  $(R_1^0, R_2^0) = (1, 0)$  to the current status  $(R_1^t(P'), R_2^t(P'))$ , with the remaining segment of  $P'$ . This produces a  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLP of size at most  $|P| - t + 1$  for  $f(\bar{x})|_p$ .*
- *If  $p$  is a finishing projection for  $m_P^t$  in  $P$ , then by Corollary 27,  $R_1^t(P')$  is a nonzero multiple of  $f(\bar{x})|_p$  and moreover,  $R_1^t(P') = a \cdot R_1^{t-1}(P') + b \cdot R_2^{t-1}(P')$ , where  $a, b \in \mathbb{H} \cup \mathbb{F}$ , since by Lemma 24, all of entries in  $m_P^t|_p$  are field elements. We claim that one of  $a$  and  $b$  must be a unit. Otherwise,  $f(\bar{x})|_p \neq 0$  while  $R_1^t(P') = 0$ , a contradiction. Therefore, we can throw away the portion of  $P'$  after time  $t$  (including the  $t$ -th instruction) and generate  $R_1$ 's contents  $R_1^t(P')$  by an offsetting matrix  $m'$  at time  $t$ , as follows:*

*We have that  $R_1^t(P')$  is some non-zero multiple of  $f(\bar{x})|_p$ , say  $R_1^t(P') = s \cdot f(\bar{x})|_p$ . We also have that  $R_1^t(P') = a \cdot R_1^{t-1}(P') + b \cdot R_2^{t-1}(P')$ . If  $a$  is a unit, then the desired output  $f(\bar{x})|_p$  is produced by the assignment  $R_1^t(P') \leftarrow (a/s) \cdot R_1^{t-1}(P') + (b/s) \cdot R_2^{t-1}(P')$ , which can be accomplished by a rule of type 3(a) or 4(a) (since we do not care what value is placed in  $R_2$ ). If  $b$  is a unit, then the desired assignment instead is produced by a transposition of a rule of type 3(b) or 4(b). Thus, in either case, we obtain a  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLP of size at most  $t + 1$  for  $f(\bar{x})|_p$ .*

**Definition 30** *Let  $f(\bar{x})$  be a polynomial and  $P$  be one of its  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLPs. We classify the potentially degenerate matrices  $m_P^t$  in  $P$ , if they do exist, according to the following criterion: If  $m_P^t$  has at least one finishing projection, then  $m_P^t$  is good; Otherwise,  $m_P^t$  is bad.*

In the same spirit, we can classify inherently degenerate matrices in  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLPs. In this case, we can consider the degenerating projection to be the empty set. The following lemma is essentially a variant of Lemma 26. Hence, we omit its proof.

**Lemma 31** *Let  $f(\bar{x})$  be a nonzero polynomial under any well-formed regular projection of size at most four and  $P$  be one of its  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLPs. Suppose that there exists  $0 < t \leq |P|$  such that  $m_P^t$  is an inherently degenerate matrix. Let  $w \in \mathbb{F}$ . Then up to the permutation of the indices, only one of the two following cases will happen.*

1.  $R_1^t \in \mathbb{F}^*$  and  $R_2^t = w \cdot R_1^t$  for some  $w \in \mathbb{F}$ .
2.  $R_1^t$  has degree at least one,  $R_1^t = w \cdot R_2^t$  and  $f(\bar{x})$  is divisible by  $R_1^t$ , where  $w \in \mathbb{F}$ .

*Furthermore, If  $f(\bar{x})$  is a nonzero irreducible polynomial, then in the second case,  $R_1^t = c \cdot f(\bar{x})$  where  $c \in \mathbb{F}^*$ .*

**Definition 32** *Let  $f(\bar{x})$  be as in Lemma 31 and let  $P$  be one of its  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLPs. Let  $m_t$  be an inherently degenerate matrix in  $P$  if it exists. If the first case in Lemma 31 happens, then we say that  $m_t$  is bad, otherwise, it is good.*

Note that the notions of badness and goodness apply only to potentially and inherently degenerate matrices.

**Observation 33** *Let  $p$  be an arbitrary homogeneous projection and let  $P' = P|_p$ . If  $m_P^t$  is bad in  $P$ , then  $m_{P'}^t$  can not be good in  $P'$  (This is because, if  $m_P^t$  is bad, then under any extension of  $p$ , at time  $t$  both registers compute field elements which are constant polynomials with no variables). More precisely,  $m_{P'}^t$  either stays as a bad matrix or becomes an inherently non-degenerate matrix. Furthermore, inherently non-degenerate matrices will never be turned into some other type by any projection.*

Now we are ready to present our main impossibility theorem of this section.

**Theorem 34** *If  $k \geq 8$ , then  $f(\bar{x}) = \sum_{i=1}^k x_{2i-1}x_{2i}$  is not computable by  $\mathbb{H}_{2 \times 2}$ . That is, for every  $n$ ,  $f(\bar{x})$  can not be obtained from  $\text{IMM}_{2,n}$  under homogeneous projections.*

**Proof:** We prove the theorem by contradiction. Suppose  $P$  is a  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLP for  $f(\bar{x})$ . We define the set  $G$  of time steps as:

$$G = \{t \mid m_P^t \text{ is a good matrix}\}.$$

There are two cases to consider.

- The first case is that  $G = \emptyset$ . Define the set  $B$  similarly as:

$$B = \{t \mid m_P^t \text{ is a bad matrix}\}.$$

If  $B$  is empty as well, then  $P$  is indeed a  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP. By Fact 4, the highest-degree homogeneous part of  $f(\bar{x})$  is irreducible, and by Theorem 18, we have reached a contradiction. Otherwise, let  $t_B = \max(B)$ . Note that, by Proposition 9, the output at time  $|P|$  is a non-zero polynomial under any well-formed regular projection of size at most six, which means that  $m_P^{|P|}$  cannot be bad, and

hence  $t_B < |P|$ . Let  $p$  be one of the cutting projections of  $m_P^{t_B}$ . Consider  $P|_p$  and the polynomial  $f(\bar{x})|_p$  it computes. Since the size of  $p$  is bounded by six, by Proposition 9,  $f(\bar{x})|_p$  is again an irreducible polynomial and moreover, its degree-two homogeneous part is irreducible. For all  $t$  such that  $t_B \leq t \leq |P|$ ,  $m_P^t$  is an inherently non-degenerate matrix. By the first item of Observation 29, we now have a  $\mu_{\mathbb{H}_{2 \times 2} \cap \text{Indg}}$ -SLP for  $f(\bar{x})|_p$  which is a contradiction to Theorem 18. Notice that by Proposition 9, the above arguments apply to any polynomial of the form  $\sum_{i=1}^5 x_{2i-1}x_{2i} + l(\bar{x})$  where  $l(\bar{x})$  is an arbitrary linear function.

- We assume that  $G \neq \emptyset$ . Let  $t_G = \min G$ . Suppose first that  $m_P^{t_G}$  is an inherently degenerate matrix. Since  $m_P^{t_G}$  is good, we have by Lemma 31 that, at time  $t_G$ , register  $R_1$  computes a nonzero multiple of  $f$ . Hence by the second item of Observation 29 with  $p = \emptyset$ , we obtain a new  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLP for  $f(\bar{x})$ , consisting of only the matrices before  $t_G$  – none of which are good. This brings us back to the first case and a contradiction.

Otherwise, assume that  $m_P^{t_G}$  is a potentially degenerate matrix and let  $p$  be one of its finishing projections of size at most six. Consider  $P|_p$  and the polynomial  $f(\bar{x})|_p$  it computes. By the second item of Observation 29, we obtain a new  $\mu_{\mathbb{H}_{2 \times 2}}$ -SLP  $P'$  for  $f(\bar{x})|_p$  and furthermore, by Observation 33,  $P'$  does not contain any good matrices. Hence, this reduces us to the first case, since  $f(\bar{x})|_p$  is of the form  $\sum_{i=1}^5 x_{2i-1}x_{2i} + l(\bar{x})$  where  $l(\bar{x})$  is an arbitrary linear function. It is not hard to see that we will arrive at a contradiction for  $f(\bar{x})|_p$ , which completes our proof. □

The proof of Theorem 34 leads to the following corollary.

**Corollary 35** *If  $k \geq 8$ , then  $f(\bar{x}) = \sum_{i=1}^k x_{2i-1}x_{2i} + l(\bar{x})$  is not computable by  $\mathbb{H}_{2 \times 2}$ , where  $l(\bar{x})$  is an arbitrary linear function.*

## 4 Extensions to simple and regular projections

In this section, we show that in the seemingly more powerful models, it is still hard to compute simple polynomials. We start by extending the result of Section 3 to the case of simple projections. Then by similar techniques and some extra observations, we will prove that certain polynomials are not regular projections of  $\text{IMM}_{2,n}$ , and thus, they are not computable by algebraic branching programs of width two.

### 4.1 Impossibility result for simple projections

In order to show that an analogue of Theorem 18 holds in the setting of simple projections, we first show that, for nondegenerate matrices, the simple case reduces to the homogeneous case.

**Lemma 36** *Every matrix in  $\mathbb{S}_{2 \times 2} \cap \text{Indg}$  can be represented by a product of matrices in  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ .*

**Proof:** Let  $m$  be a matrix in  $\mathbb{S}_{2 \times 2}$  and

$$m = \begin{bmatrix} c_{1,1}y_{1,1} + w_{1,1} & c_{1,2}y_{1,2} + w_{1,2} \\ c_{2,1}y_{2,1} + w_{2,1} & c_{2,2}y_{2,2} + w_{2,2} \end{bmatrix},$$

where  $c_{i,j}, w_{i,j} \in \mathbb{F}$  and  $y_{i,j} \in \{x_k \mid k \in \mathbb{N}\}$ .

We say that the variable  $x_k = y_{i,j}$  occurs in  $m$  if  $c_{i,j} \neq 0$  and that  $y_{i,j}$  is an occurrence for  $x_k$ . Assume that  $m \in \mathbb{S}_{2 \times 2} \cap \text{Indg}$  and consider the following cases.

1. If there are no occurrences of any variables, then  $m$  is a linear transformation over  $\mathbb{F}$ . So  $m \in \mathbb{H}_{2 \times 2} \cap \text{Indg}$ .
2. If there are at least three distinct variables occurring in  $m$ , then  $\det(m)$  is a nonzero polynomial and  $m \in \text{Pdg}$ , a contradiction to our assumption.
3. If there is only a single variable  $x_k$  occurring in  $m$ , then obviously  $x_k$  has either two or four occurrences in  $m$  which can be divided into two subcases.

- If  $x_k$  has two occurrences in  $m$ , then these two occurrences can not be placed at the diagonal or anti-diagonal positions. Hence, without loss of generality, assume that  $m$  has the following form.

$$m = \begin{bmatrix} w_{1,1} & w_{1,2} \\ c_{2,1}x_k + w_{2,1} & c_{2,2}x_k + w_{2,2} \end{bmatrix},$$

where  $c_{2,1} \neq 0$  and  $c_{2,2} \neq 0$ .

The determinant of  $m$  is equal to  $(c_{2,2}w_{1,1} - c_{2,1}w_{1,2})x_k + (w_{1,1}w_{2,2} - w_{1,2}w_{2,1})$ , then by our assumption,  $c_{2,2}w_{1,1} - c_{2,1}w_{1,2} = 0$ . If  $w_{1,1} = w_{1,2} = 0$ , then  $m \in \text{Idg}$ , a contradiction to our assumption. If exactly one of them is equal to zero, then  $m \in \text{Pdg}$ , a contradiction as well. Hence, we can assume that  $\frac{c_{2,2}}{c_{2,1}} = \frac{w_{1,2}}{w_{1,1}} = d \neq 0$ . Then,

$$m = \begin{bmatrix} w_{1,1} & 0 \\ c_{2,1}x_k + w_{2,1} & w_{2,2} - dw_{2,1} \end{bmatrix} \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix}$$

$w_{2,2} - dw_{2,1} \neq 0$  since  $\det(m) \neq 0$ .

So

$$m = \begin{bmatrix} \frac{w_{1,1}}{c_{2,1}} & 0 \\ x_k & w_{2,2} - dw_{2,1} \end{bmatrix} \begin{bmatrix} c_{2,1} & 0 \\ \frac{w_{2,1}}{w_{2,2} - dw_{2,1}} & 1 \end{bmatrix} \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix}$$

This verifies that  $m$  is a product of matrices in  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ .

- If  $x_k$  has four occurrences in  $m$ , then assume  $m$  has the following form.

$$m = \begin{bmatrix} c_{1,1}x_k + w_{1,1} & c_{1,2}x_k + w_{1,2} \\ c_{2,1}x_k + w_{2,1} & c_{2,2}x_k + w_{2,2} \end{bmatrix},$$

where each  $c_{i,j} \neq 0$ .

The determinant of  $m$  is equal to  $(c_{1,1}x_k + w_{1,1})(c_{2,2}x_k + w_{2,2}) - (c_{1,2}x_k + w_{1,2})(c_{2,1}x_k + w_{2,1})$ . Because  $m \in \text{Indg}$ ,  $c_{1,1}c_{2,2} - c_{1,2}c_{2,1} = 0$ . Let  $d = \frac{c_{1,2}}{c_{1,1}} = \frac{c_{2,2}}{c_{2,1}} \neq 0$ . Then, there exists  $u, v \in \mathbb{F}$  such that

$$m = \begin{bmatrix} c_{1,1}x_k + w_{1,1} & u \\ c_{2,1}x_k + w_{2,1} & v \end{bmatrix} \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix}$$

Obviously the first matrix belongs to  $\text{Indg}$  because its determinant belongs to  $\mathbb{F}^*$ . Hence by the first subcase, it is a product of matrices in  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ , so is  $m$ .

4. If there are exactly two distinct variables  $x_k$  and  $x_l$  occurring in  $m$ , then they must have the same number of occurrences in  $m$ . Let  $c_{i,j} \in \mathbb{F}^*$ . It is clear that for all  $u, v \in \mathbb{F}$ , up to the permutation of rows and columns, the following matrices can not belong to  $\text{Indg}$ .

$$\begin{bmatrix} c_{1,1}x_k + w_{1,1} & u \\ c_{2,1}x_j + w_{2,1} & v \end{bmatrix}, \begin{bmatrix} c_{1,1}x_k + w_{1,1} & u \\ v & c_{2,1}x_j + w_{2,1} \end{bmatrix}$$

Hence, each of  $x_k$  and  $x_l$  has two occurrences. Without loss of generality,  $m$  has the following form.

$$m = \begin{bmatrix} c_{1,1}x_k + w_{1,1} & c_{1,2}x_k + w_{1,2} \\ c_{2,1}x_j + w_{2,1} & c_{2,2}x_j + w_{2,2} \end{bmatrix}.$$

Since  $\det(m) \in \mathbb{F}^*$ , we have  $c_{1,1}c_{2,2} - c_{1,2}c_{2,1} = 0$ . Let  $d = \frac{c_{1,2}}{c_{1,1}} = \frac{c_{2,2}}{c_{2,1}} \neq 0$ . Then, there exists  $u, v \in \mathbb{F}$  such that

$$m = \begin{bmatrix} c_{1,1}x_k + w_{1,1} & u \\ c_{2,1}x_j + w_{2,1} & v \end{bmatrix} \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix}$$

This implies that  $m$  can not be an inherently non-degenerate matrix, a contradiction.

In conclusion, we have proven our claim that every matrix in  $\mathbb{S}_{2 \times 2} \cap \text{Indg}$  is equal to a product of matrices in  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ .  $\square$

The preceding lemma, together with Theorem 18, immediately yield the following corollary:

**Corollary 37** *Let  $f(\bar{x})$  be a polynomial whose highest-degree homogeneous part is irreducible. Then  $f(\bar{x})$  is not computable by  $\mathbb{S}_{2 \times 2} \cap \text{Indg}$ .*

Next we show how to adapt the machinery in Section 3.3 and prove a similar impossibility theorem in terms of simple projections.

**Theorem 38** *Let  $l(\bar{x})$  be an arbitrary linear function. If  $k \geq 8$ , then  $f(\bar{x}) = \sum_{i=1}^k x_{2i-1}x_{2i} + l(\bar{x})$  is not computable by  $\mathbb{S}_{2 \times 2}$ , namely, for any  $n$ ,  $f(\bar{x})$  can not be obtained from  $\text{IMM}_{2,n}$  under simple projections.*

**Proof:** [Proof sketch] We prove the theorem via contradiction. Suppose there is a  $\mu_{\mathbb{S}_{2 \times 2}}$ -SLP  $P$  for  $f(\bar{x})$ .

Similar to Lemma 23, we prove the following lemma.

**Lemma 39** *There does not exist a matrix  $m$  in  $P$  such that each entry of  $m$  contains a distinct variable. This implies that all matrices in  $P$  must contain at most three variables.*

**Proof:** Suppose the statement is not true, and without loss of generality,  $m = \begin{bmatrix} c_1x_1 - w_1 & c_2x_2 - w_2 \\ c_3x_3 - w_3 & c_4x_4 - w_4 \end{bmatrix}$ , where  $\forall 1 \leq i \leq 4, c_i \in \mathbb{F}^*, w_i \in \mathbb{F}$  and the  $x_i$ s are all distinct. Consider the projection  $p = \{x_i \leftarrow \frac{w_i}{c_i} \mid 1 \leq i \leq 4\}$ . Then  $f(\bar{x})|_p$  is nonzero while  $P|_p$  contains  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ . By Propositions 8 and 9,  $f(\bar{x})$  is nonzero under any regular projection of size at most four. Thus by Lemma 22, we have reached a contradiction.  $\square$

A direct consequence of Lemma 39 is an analogue of Lemma 24. The proof of the following lemma proceeds in the same way as that of Lemma 24, so we omit it here.

**Lemma 40** *For any matrix  $m \in P$  which belongs to  $\mathbb{S}_{2 \times 2} \cap \text{Pdg}$ , there exists a homogeneous projection  $p$  of size at most three such that  $m|_p$  is degenerate and all of the entries in  $m|_p$  belong to  $\mathbb{F}$ . Moreover, there is a well-formed homogeneous projection  $q$  of size at most six extending  $p$ .*

The notions of degenerating projections, and of good and bad matrices, thus carry over also to the setting of simple projections, and the rest of the proof follows exactly as in Section 3.3.  $\square$

## 4.2 Impossibility result for regular projections

Let  $m \in \mathbb{R}_{2 \times 2}$  be of the following form:

$$m = \begin{bmatrix} l_{1,1} + w_{1,1} & l_{1,2} + w_{1,2} \\ l_{2,1} + w_{2,1} & l_{2,2} + w_{2,2} \end{bmatrix}.$$

where  $w_{i,j} \in \mathbb{F}$  and the  $l_{i,j}$ 's are homogeneous linear forms in  $\{\sum_{k=1}^n c_k x_k \mid n \in \mathbb{N}, c_k \in \mathbb{F}\}$ . We will pay attention to the rank of the subspace spanned by  $\{l_{i,j} \mid i, j \in \{1, 2\}\}$ , denoted as  $r(m)$ , which in some sense characterizes the number of ‘‘independent variables’’ among the  $l_{i,j}$ 's.

The following lemma illustrates the sense in which we can treat linearly-independent homogeneous linear forms as independent variables.

**Lemma 41** *Let  $l_1, l_2, \dots, l_k$  be linearly independent homogeneous linear forms, and let  $w_1, \dots, w_k$  be elements of  $\mathbb{F}$ . Then there is a regular projection  $p$  of size  $k$  such that, for all  $i$ ,  $l_i|_p = w_i$ . (Thus we can think of  $p$  as a ‘‘projection’’ of the form  $\{l_i \leftarrow w_i\}$ .)*

**Proof:** The homogeneous linear form  $l_1$  is of the form  $\sum_{j=1}^n c_j x_j$ , where each  $c_j \in \mathbb{F}^*$ . Start building the projection  $p$  with the rule  $x_1 \leftarrow (w_1 - \sum_{j=2}^n c_j x_j)/c_1$ . This clearly has the effect that  $l_1|_p = w_1$ . If  $k = 1$ , then the construction ends here.

Otherwise, let  $l_2 = \sum_{j=1}^{n'} d_j y_j$ , where each  $d_j \in \mathbb{F}^*$ . If the variable  $x_1$  appears as one of the variables  $y_j$ , then replace  $x_1$  with the expression  $(w_1 - \sum_{j=2}^n c_j x_j)/c_1$  and simplify. By linear independence, there must still be some variable remaining in the resulting expression. Without loss of generality, let the resulting expression be of the form  $\sum_{j=2}^{n''} a_j x_j$ . Then we add a new rule  $x_2 \leftarrow (w_2 - \sum_{j=3}^{n''} a_j x_j)/a_2$  (and if this variable  $x_2$  occurs in the right-hand-side of the rule for  $x_1$ , then substitute this expression in for  $x_2$  in that rule, and simplify). At this point, we have  $l_1|_p = w_1$  and  $l_2|_p = w_2$ .

We continue in this way for all of the remaining linear forms. The crucial observation is that there will always be a variable in each linear form  $l_j|_p$  when we first consider it, because of linear independence.  $\square$

Our next lemma is a generalization of Lemma 36.

**Lemma 42** *Every matrix  $m$  in  $\mathbb{R}_{2 \times 2} \cap \text{Indg}$  can be represented by a product of matrices in  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ .*

**Proof:** The correctness of the following claim is easy to verify.

If  $r(m) = 0, 3$  or  $4$ , then the proof is completely analogous to the corresponding cases in Lemma 36, where we do our case analysis based on  $r(m)$  instead of the number of variables that occur in  $m$ .

If  $r(m) = 1$ , then there exists a homogeneous linear form  $l$  such that all  $l_{i,j}$ s in  $m$  are multiples of  $l$ . By treating  $l$  as a single variable, the analysis of the third case in Lemma 36 reveals that  $m$  is a product of matrices from  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$  as well as matrices having the following form:

$$\begin{bmatrix} c & 0 \\ l & c' \end{bmatrix}, \begin{bmatrix} c & l \\ 0 & c' \end{bmatrix}.$$

Thus the case when  $r(m) = 1$  is completed by appealing to the following claim:

**Claim 43** *Any matrix having the following form can be expressed as the product of matrices in  $\mathbb{H}_{2 \times 2} \cap \text{Indg}$ .*

$$\begin{bmatrix} c & 0 \\ l & c' \end{bmatrix}, \begin{bmatrix} c & l \\ 0 & c' \end{bmatrix}$$

where  $c, c' \in \mathbb{F}^*$  and  $l \in \mathbb{L}$ .

**Proof:** We prove the claim by induction on the number of variables appearing in  $l$ . If  $l$  contains at most one variable, then the claim follows from Lemma 36.

Otherwise,  $l$  is of the form  $dx_1 + l'$ . Observe that

$$\begin{bmatrix} c & 0 \\ l & c' \end{bmatrix} = \begin{bmatrix} c/d & 0 \\ x_1 & 1 \end{bmatrix} \times \begin{bmatrix} d & 0 \\ l' & c' \end{bmatrix}.$$

(The other case is similar.) The claim now follows by induction.  $\square$

If  $r(m) = 2$ , then let  $l_1, l_2 \in \{l_{i,j} \mid i, j \in \{1, 2\}\}$  be a basis. If every  $l_{i,j}$  is a multiple of either  $l_1$  or  $l_2$ , then the proof of the fourth case of Lemma 36 provides us a contradiction. Thus, we only need to consider the case where there is at least one  $l' \in \{l_{i,j} \mid i, j \in \{1, 2\}\}$  and  $c, c' \in \mathbb{F}^*$  such that  $l' = cl_1 + c'l_2$ , which means that  $l'$  is a non-trivial linear combination of  $l_1$  and  $l_2$ . Therefore, without loss of generality, we assume that  $m$  has the following form.

$$m = \begin{bmatrix} l_1 + w_{1,1} & l_2 + w_{1,2} \\ cl_1 + c'l_2 + w_{2,1} & dl_1 + d'l_2 + w_{2,2} \end{bmatrix}.$$

where  $c, c' \in \mathbb{F}^*, d, d' \in \mathbb{F}$ .

But then the degree-two homogeneous part of  $\det(m)$  is equal to  $dl_1^2 + (d' - c)l_1l_2 - c'l_2^2$ , which is nonzero since  $c' \neq 0$ . This contradicts our assumption that  $m \in \text{Indg}$ .  $\square$

The preceding lemma, together with Theorem 18, immediately yield the following corollary:

**Corollary 44** *Let  $f(\bar{x})$  be a polynomial whose highest-degree homogeneous part is irreducible. Then  $f(\bar{x})$  is not computable by  $\mathbb{R}_{2 \times 2} \cap \text{Indg}$ .*

Now we are ready to prove our main theorem.

**Theorem 45 (Theorem 2 restated)** *If  $k \geq 8$ , then  $f(\bar{x}) = \sum_{i=1}^k x_{2i-1}x_{2i}$  is not computable by  $\mathbb{R}_{2 \times 2}$ , namely, for any  $n$ ,  $f(\bar{x})$  can not be obtained from  $\text{IMM}_{2,n}$  under regular projections.*

**Proof:** [Proof sketch] The proof is by contradiction. Suppose  $P$  is a  $\mu_{\mathbb{R}_{2 \times 2}}$ -SLP for  $f(\bar{x})$ .

By Propositions 8 and 9,  $f(\bar{x})$  is nonzero under any regular projection of size at most four, which leads to the following lemma.

**Lemma 46** *For any potentially degenerate matrix  $m_P^t$  in  $P$ ,  $r(m_P^t) \leq 3$ .*

**Proof:** Suppose  $r(m_P^t) = 4$ , then there exists a regular projection  $p$  of size four such that  $\forall 1 \leq i, j \leq 2$ ,  $l_{i,j} = -w_{i,j}$ . In other words,  $m_P^t|_p = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ . By Lemma 22, we have reached a contradiction to the aforementioned property of  $f(\bar{x})$ .  $\square$

**Lemma 47** *Any potentially degenerate matrix  $m_P^t$  in  $P$  has a regular projection  $p$  of size at most three such that  $m_P^t|_p$  is degenerate and all of the entries in  $m|_p$  belong to  $\mathbb{F}$ . Moreover, there is a well-formed regular projection  $q$  of size at most six extending  $p$ .*

**Proof:**  $\det(m_P^t)$  is a polynomial of degree at least one. by Lemma 46, after some suitable linear transformation,  $\det(m_P^t)$  can be viewed as a polynomial in at most three ‘‘new’’ variables that are linear forms in terms of the original set of variables. Since  $\mathbb{F}$  is algebraically closed, this provides us the desired projection  $p$ . The second part of the claim follows from Proposition 8.  $\square$

By Lemma 47, we can define degenerating projections in terms of well-formed regular projections. Note that the proofs of Lemma 26 and Corollary 27 hold, regardless of the type of projections. Thus we can also extend the definitions of cutting and finishing projections to well-formed regular projections. The following observation is a slight variant of Observation 29.

**Observation 48** *Let  $f(\bar{x})$  be a polynomial such that under any well-formed regular projection  $q$  of size at most six,  $f(\bar{x})|_q$  is always a nonzero irreducible polynomial. Let  $P$  be a  $\mu_{\mathbb{R}^{2 \times 2}}$ -SLP for  $f(\bar{x})$  and let  $m_P^t$  be a potentially degenerate matrix in  $P$ . Let  $p$  be one of degenerating regular projections of  $m_P^t$  and let  $P' = P|_p$ . Then, a  $\mu_{\mathbb{R}^{2 \times 2}}$ -SLP can be constructed for  $f(\bar{x})|_p$ .*

- *If  $p$  is a cutting projection for  $m_P^t$  in  $P$ , this case is identical to the first case in Observation 29.*
- *If  $p$  is a finishing projection for  $m_P^t$  in  $P$ , this case is identical to the second case in Observation 29.*

Now the remaining part of proof proceeds exactly as in Section 3.3, since it does not depend on the type of underlying projections at all, namely, regardless of whether they are homogeneous, simple or regular.  $\square$

## Acknowledgment

Discussions that the first author had with Meena Mahajan, Guillaume Malod, and Sylvain Perifel at the 2010 Dagstuhl Seminar 10481 on Computational Counting were very influential in helping us understand the limitations of width-two computations. We thank Luke Friedman, Chandan Saha, Ramprasad Satharishi and anonymous referees for many helpful comments. We are grateful to Luke Friedman and Ramprasad Satharishi for pointing out mistakes in earlier versions. Useful feedback was also provided by Maurice Jansen and Ran Raz.

## References

- [1] M. Agrawal, E. Allender, and S. Datta. On  $TC^0$ ,  $AC^0$ , and arithmetic circuits. *Journal of Computer and System Sciences*, 60:395–421, 2000.
- [2] Eric Allender. Arithmetic circuits and counting complexity classes. In J. Krajíček, editor, *Complexity of Computations and Proofs*, volume 13 of *Quaderni di Matematica*, pages 33–72. Seconda Università di Napoli, 2004.
- [3] A. Ambainis, E. Allender, D. A. M. Barrington, S. Datta, and H. LêThanh. Bounded depth arithmetic circuits: Counting and closure. In *Proc. ICALP*, number 1644 in Lecture Notes in Computer Science, pages 149–158. Springer, 1999.
- [4] David A. Barrington. Width-3 permutation branching programs. Technical Report Technical Memorandum MIT/LCS/TM-293, MIT, 1985.
- [5] Michael Ben-Or and Richard Cleve. Computing algebraic formulas using a constant number of registers. In *Proc. ACM Symp. on Theory of Computing (STOC)*, pages 254–257, 1988.
- [6] Michael Ben-Or and Richard Cleve. Computing algebraic formulas using a constant number of registers. *SIAM Journal on Computing*, 21(1):54–58, 1992.

- [7] H. Caussinus, P. McKenzie, D. Thérien, and H. Vollmer. Nondeterministic  $NC^1$  computation. *Journal of Computer and System Sciences*, 57:200–212, 1998.
- [8] Maurice J. Jansen. Lower bounds for syntactically multilinear algebraic branching programs. In *Proc. of Math. Foundations of Comp. Sci. (MFCS)*, number 5162 in Lecture Notes in Computer Science, pages 407–418. Springer, 2008.
- [9] Maurice J. Jansen and B. V. Raghavendra Rao. Simulation of arithmetical circuits by branching programs with preservation of constant width and syntactic multilinearity. In *CSR*, number 5675 in Lecture Notes in Computer Science, pages 179–190. Springer, 2009.
- [10] H. Jung. Depth efficient transformations of arithmetic into Boolean circuits. In *Proc. FCT*, number 199 in Lecture Notes in Computer Science, pages 167–173. Springer, 1985.
- [11] R. Lipton and Y. Zalcstein. Word problems solvable in logspace. *Journal of the ACM*, 24:522–526, 1977.
- [12] M. Mahajan, N. Saurabh, and K. Sreenivasaiiah. Counting paths in planar width 2 branching programs. Manuscript, 2011.
- [13] Meena Mahajan and B. V. Raghavendra Rao. Small-space analogues of valiant’s classes. In *FCT*, number 5699 in Lecture Notes in Computer Science, pages 250–261. Springer, 2009.
- [14] Noam Nisan. Lower bounds for non-commutative computation (extended abstract). In *Proc. ACM Symp. on Theory of Computing (STOC)*, pages 410–418, 1991.
- [15] D. Robinson. *Parallel algorithms for group word problems*. PhD thesis, Univ. of California, San Diego, 1993.
- [16] Chandan Saha. Private communication, 2011.
- [17] Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena. The power of depth 2 circuits over algebras. In *Proc. Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS)*, pages 371–382, 2009.
- [18] L. Valiant. Completeness classes in algebra. In *Proc. ACM Symp. on Theory of Computing (STOC)*, pages 249–261, 1979.