ON THE POWER OF ALGEBRAIC BRANCHING PROGRAMS OF WIDTH TWO

ERIC ALLENDER AND FENGMING WANG

October 19, 2015

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.

Keywords. Iterated Matrix Multiplication, Arithmetic Circuits, Algebraic Branching Programs

Subject classification. 03D15, 68Q15, 68Q17

1. Introduction

The n^{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 Ben-Or & Cleve (1988, 1992). This class is sometimes denoted VNC^1 Mahajan & Rao (2013) (as the analog of the Boolean class NC^1 in the setting of algebraic complexity initiated by Valiant Valiant (1979)) and is also sometimes denoted VP_e (corresponding to the subclass of Valiant's class VP of polynomials of polynomial degree that have arithmetic circuits of polynomial size, where we restrict the circuits to be *expressions* – i.e., formulae).

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 $\mathrm{IMM}_{2,n}$?

Our main result answers this question, by showing that even the simple polynomial $x_1x_2 + x_3x_4 + \ldots + x_{15}x_{16}$ is not expressible as a projection of $\mathrm{IMM}_{2,n}$. (A somewhat more general statement of the result is presented later.)

In order to appreciate the significance of this theorem, it is useful to review the historical context.

1.1. Historical Context and Related Work. There were some indications that $\mathrm{IMM}_{2,n}$ should be nearly as powerful as $\mathrm{IMM}_{3,n}$. 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 Ben-Or & Cleve (1988), 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 $\mathrm{IMM}_{2,n}$ computations).

Perhaps the first study of the complexity of evaluating $\mathrm{IMM}_{2,n}$ arose in the work of Lipton and Zalcstein Lipton & Zalcstein (1977), 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 AC^0-reducible to the problem of determining if a product of n two-by-two integer matrices evaluates to the identity matrix. Since the two-sided Dyck language is hard for NC^1 Robinson (1993), this gives a lower bound, showing that evaluating $\mathrm{IMM}_{2,n}$ instances is also hard for NC^1.

This lower bound is rather close to the best known upper bound. The problem of evaluating integer instances of $\mathrm{IMM}_{3,n}$ is complete for the Boolean complexity class GapNC^1 Caussinus *et al.* (1998) (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 $O(\log n \log^* n)$ Jung (1985). The closeness of these bounds has led some researchers to wonder whether the classes of functions in NC^1 and GapNC^1 are in

fact equal Allender (2004), in which case $\mathrm{IMM}_{2,n}$ and $\mathrm{IMM}_{3,n}$ would be interreducible under AC^0 reductions.

The NC^1-hardness of $\mathrm{IMM}_{2,n}$ over the integers holds even for restricted cases of the problem. In Ambainis *et al.* (1999), it is asserted that counting paths in *planar* width-two graphs (a restricted case of $\mathrm{IMM}_{2,n}$ over the integers) is hard for NC^1 under ACC^0 reductions. (Mahajan, Saurabh, and Sreenivasaiah Mahajan *et al.* (2012) have identified and corrected an error in the proof of this claim in Ambainis *et al.* (1999).)

On the other hand, there have also been indications that $\mathrm{IMM}_{2,n}$ should be weaker than $\mathrm{IMM}_{3,n}$. Ben-Or and Cleve point out that problems over 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 Ben-Or & Cleve (1992), which Barrington showed require exponential size in order to compute the AND function Barrington (1985). However, this does not strictly rule out more general computations over $\mathrm{IMM}_{2,n}$.

It is important to note that the known AC^0 reductions from NC^1-complete problems to $\mathrm{IMM}_{2,n}$ Lipton & Zalcstein (1977); Robinson (1993) 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 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. $\mathrm{GapAC}^0 \subseteq \mathrm{TC}^0 \subseteq \mathrm{NC}^1$ Agrawal *et al.* (2000), and hence any bit of any function $f \in \mathrm{GapAC}^0$ can be computed by an 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 $f(x_1, \ldots, x_n)$ in its input variables, and the AC^0 reduction does not allow us to obtain f from IMM_{2,n^k} by substituting field elements and the variables $x_1, \ldots, x_n$ for the variables of IMM, even though this is possible for IMM_{3,n^k}. It follows from our main result that, even for some fairly simple functions $f \in \mathrm{GapAC}^0$, *no such reduction is possible* – even if we allow projections to *arbitrarily large* IMM instances, and even if we allow the projections to consist of a much more general class of substitutions (beyond the type of projections that is usually

considered in the framework of Valiant's algebraic complexity classes).

1.2. 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 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 Nisan (1991).

DEFINITION 1.1. *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* $0, 1, 2, \ldots, d$*; 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* $p = e_1 e_2 \ldots e_k$ *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 Ben-Or & Cleve (1992) 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 Agrawal *et al.* (2015); Jansen *et al.* (2013). We show that width three is optimal; the expressive power of width two algebraic branching programs is severely limited.

THEOREM 1.2. *Let* $l(\overline{x})$ *be an arbitrary linear function, and let* k *be any integer such that* $k \geq 8$*. Then the polynomial*

$$f(\overline{x}) = \sum_{i=1}^{k} x_{2i-1} x_{2i} + l(\overline{x})$$

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 Saha *et al.* (2009). 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 1.2 Saha (2011)). We do not know whether width-two algebraic branching programs can be simulated by width-two degree-restricted branching programs. Thus our Theorem 1.2 is incomparable with (Saha *et al.* 2009, Theorem 16); our impossibility result for the polynomials listed in Theorem 1.2 is stronger, since it is for the unrestricted model. However, their result applies to a larger class of polynomials, showing that they cannot be computed by the restricted model.

An obvious direction for future work is to provide a tighter characterization of the class of polynomials that can be computed by algebraic branching programs of width two. In particular, we mention the question of whether the constant 8 in Theorem 1.2 can be reduced to 3.

1.3. 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 $\mathrm{IMM}_{2,n}$ 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, to obtain our Theorem 1.2.

2. Preliminaries

Let the underlying field be $\mathbb{F}$. Let $q(\overline{x}) \in \mathbb{F}[\overline{x}]$ be a multivariate polynomial over a set of variables $\overline{x}$. The polynomial q can be used to express other polynomials, by means of *projections*. A projection is described by a set of assignments $p = \{x_i \leftarrow v_i\}$, where the values v_i come from

a particular set (to be specified later), and each variable $x_i \in \overline{x}$ 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. The *size* of a projection is the number of rules in the set; equivalently it is the number of variables that appear on the left-hand side of a rule. We get the new instance $q(\overline{x})|_p$ by replacing all occurrences of x_i in $q(\overline{x})$ with its counterpart v_i and leaving untouched those variables that are not in p. We may simplify $q(\overline{x})|_p$ according to the commutative polynomial ring algebra. In this way, we say that $q(\overline{x})|_p$ *is obtained from* $q(\overline{x})$ *under the projection* p.

We will be interested in three classes of projections. To define these classes, let us first consider three classes of terms:

- 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 affine forms $\{c \cdot x_i + w \mid c \in \mathbb{F}^*, i \in \mathbb{N}, w \in \mathbb{F}\}$.

- Let $\mathbb{L}$ be the set of general affine forms $\{\sum_{i=1}^{n} c_i \cdot x_i + w \mid n \in \mathbb{N}, c_i, w \in \mathbb{F}\}$.

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 Ben-Or & Cleve (1992); Valiant (1979).

Let $m_1, m_2, \ldots, m_n$ be square matrices of dimension two, 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 $\mathrm{IMM}_{2,n}$, which is called the *nth 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 $f(\overline{x})$, it follows immediately from the definitions that $f(\overline{x})$ is obtained from $\mathrm{IMM}_{2,n}$ under some projection p if and only if $f(\overline{x})$ is the $(1,1)$-entry of $\prod_{i=1}^{n} m_i|_p$. Note that $f(\overline{x})$ is computable by some algebraic branching program of width two if and

only if there exists $n \in \mathbb{N}$ such that $f(\overline{x})$ 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 $f(\overline{x})$ is *computable by* M if there is an integer n and a projection p such that $f(\overline{x}) = \text{IMM}_{2,n}|_p$ and furthermore, $\forall i \leq n,\ m_i|_p \in M$. In other words, $f(\overline{x})$ 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 partition all matrices in $\mathbb{R}_{2\times 2}$ into three blocks: 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 2.1. *Over any field* $\mathbb{F}$, $x_1x_2 + x_3x_4$ *is an irreducible polynomial.*

FACT 2.2. *Let* $\mathbb{F}$ *be any field,* $k \geq 2$ *and let* $l(\overline{x})$ *be an arbitrary linear function. Then* $\Sigma_{i=1}^{k} x_{2i-1}x_{2i} + l(\overline{x})$ *is an irreducible polynomial, and furthermore, its degree-two homogeneous part is irreducible as well.*

Many of our proofs involve applying projections to polynomials of the form $\Sigma_{i=1}^{k} x_{2i-1}x_{2i} + l(\overline{x})$. It is convenient to restrict attention to projections that carry out certain sorts of simplifications to these polynomials. To this end, we introduce several definitions:

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

DEFINITION 2.3. *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.*
- $\{v_{2i-1}, v_{2i}\} \cap \mathbb{F} \neq \emptyset$.

DEFINITION 2.4. *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 2.5. *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 2.6. *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 $x_1 \leftarrow v_1$ and $x_2 \leftarrow v_2$, 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 $x_1 \leftarrow v_1$ 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. □

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

PROPOSITION 2.7. *Let $k, n \in \mathbb{N}$, with $n - k \geq 2$. Consider the polynomial $f = \Sigma_{i=1}^{n} x_{2i-1} x_{2i}$. Then under any well-formed regular projection p of size $2k$, $f(\overline{x})|_p$ is an irreducible polynomial of the form $\Sigma_{i=1}^{n-k} x_{2i-1} x_{2i} + l(\overline{x})$ (that is, up to re-numbering the variables), where $l(\overline{x})$ 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 2.8. *Let $\mathbb{F}'$ be the algebraic closure of $\mathbb{F}$ and let M be a set of matrices. For any polynomial $f(\overline{x})$, if $f(\overline{x})$ is computable by M over $\mathbb{F}$, then it is computable by M over $\mathbb{F}'$ as well.*

3. $\mathbf{IMM}_{2,n}$ under homogeneous projections

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

In subsequent sections, we will see that the tools that we develop to deal with homogeneous projections also suffice when considering simple and regular projections. However, it is convenient to focus on the homogeneous case first.

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 μ 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 μ using 2 registers (μ-SLP) is a sequence of pairs of instructions from μ, 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 $p(\overline{x})$ 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 $p(\overline{x})$ 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 $\mathrm{IMM}_{2,n}$ under homogeneous projections compute the same set of polynomials. (Similar observations were made by Ben-Or and Cleve Ben-Or & Cleve (1992).) 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 $f(\overline{x})$ is computable by products of matrices in N if and only if there is a μ_N-SLP for it. Hence, given an arbitrary μ_N-SLP P, we may abuse the notations and identify the ith pair of instructions with its matrix representations m_P^i, which means that P can also be characterized by a sequence of matrices $\{m_P^i \mid 1 \leq i \leq |P|\}$. That is, the contents of the j-th register at time t is the j-th component of the column vector of

$$m_P^t \cdot m_P^{t-1} \cdots m_P^2 \cdot m_P^1 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

3.1. Classification of $\mathbb{H}_{2\times 2} \cap$ Indg. Now, we present a collection μ_N of rules (corresponding to a subset N of matrices in $\mathbb{H}_{2\times 2}$) that we

claim is sufficient 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.

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

2. Scalar rules.

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

3. Offsetting rules of degree one.

   (a)

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

   (b)

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

4. Offsetting rules of degree zero.

   (a)

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

   (b)

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

5. Other non-degenerate linear transformations.

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

   where $ab - cd \neq 0$.

OBSERVATION 3.1. *Any straight-line program using $\mu_{\mathbb{H}_{2\times 2}\cap \mathit{Indg}}$ can be simulated by a straight-line program using μ_N. This is because:*

- *The only rules that are missing from μ_N are the rules in the following list:*

$$\left[\begin{array}{cc} 0 & a \\ b & 0 \end{array}\right], \left[\begin{array}{cc} 0 & a \\ b & c \end{array}\right], \left[\begin{array}{cc} c & a \\ b & 0 \end{array}\right], \left[\begin{array}{cc} 0 & a \\ b & c\cdot x_i \end{array}\right], \left[\begin{array}{cc} c\cdot x_i & a \\ b & 0 \end{array}\right]$$

- *Each of these rules is a transposition of a rule in μ_N, hence can be replaced by a pair of rules from μ_N, via the following substitutions:*

$$\left[\begin{array}{cc} v & u \\ z & y \end{array}\right] = \left[\begin{array}{cc} u & v \\ y & z \end{array}\right]\left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right]$$

$$\left[\begin{array}{cc} y & z \\ u & v \end{array}\right] = \left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right]\left[\begin{array}{cc} u & v \\ y & z \end{array}\right]$$

- *Without loss of generality, one can assume that any straight-line program P has the property that if the transposition matrix ever appears in 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:*

$$\left[\begin{array}{cc} z & y \\ v & u \end{array}\right]\left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right] = \left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right]\left[\begin{array}{cc} u & v \\ y & z \end{array}\right]$$

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

DEFINITION 3.2. *Let $\mathit{deg}(f)$ denote the degree of the polynomial f. For any straight-line program P, let $\mathit{deg}(P,t) = \mathit{deg}(R_1^t) + \mathit{deg}(R_2^t)$ be* the degree of P at time t. *We call $\mathit{deg}(P,0), \mathit{deg}(P,1), \ldots, \mathit{deg}(P,|P|)$* 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 $t_1 < t' < t_2$, $\mathit{deg}(P,t') = d$;*

- $\deg(P, t_1) < d$;
- $\deg(P, t_2) < d$.

The number d is called the height *of this mesa. Note that P has no mesas if and only if the degree sequence of P is nondecreasing.*

FACT 3.3. *Recall that, by Observation 3.1, any straight-line program P over $\mu_{\mathbb{H}_{2\times 2}\cap \mathit{Indg}}$ can be converted into an equivalent straight-line program P' over μ_N. The conversion outlined in Observation 3.1 has the property that P has a mesa of height d iff P' does. Thus we may restrict attention to straight-line programs over μ_N.*

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

THEOREM 3.4. *If a polynomial f is computable by $\mathbb{H}_{2\times 2} \cap \mathit{Indg}$, then there is a $\mu_{\mathbb{H}_{2\times 2}\cap \mathit{Indg}}$-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 $\mu_{\mathbb{H}_{2\times 2}\cap \mathrm{Indg}}$-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 $\mu_{\mathbb{H}_{2\times 2}\cap \mathrm{Indg}}$-SLP while reducing the total height of all mesas by at least one. Ultimately we will obtain a $\mu_{\mathbb{H}_{2\times 2}\cap \mathrm{Indg}}$-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. Now we wish to show that Rule $3(b)$ is also impossible. Assume that the instruction at time t_1 is Rule $3(b)$. Thus $\deg(R_1^{t_1+1}) = \deg(R_1^{t_1})$. There are two subcases to consider:

- If $\deg(R_1^{t_1}) \geq \deg(R_2^{t_1})$, then $\deg(R_1^{t_1+1}) \leq \deg(R_2^{t_1+1})$. But we are assuming 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 runs counter to 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, $\deg(R_1^{t_1+1}) = \deg(R_2^{t_1+1})$, counter 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 $\deg(P', t_1) \geq \deg(P', t_1 + 1)$, which contradicts our assumption that (t_1, t_2) is a mesa.

For every time t' such that $t_1 < t' < t_2$, we have that $\deg(P', t') = d$. This, combined with the fact that $\deg(P', t_2) < d$ implies that rules $3(b)$, $4(b)$ and 5 are impossible at time t' (and at time t_2), since under our assumptions these rules would increase the degree of R_2 while maintaining the degree of R_1. Hence, for all t' such that $t_1 < t' \leq t_2$, 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 present here the argument that rule $3(a)$ does not hap-

pen at time $t_1 + 1$; the argument for $3(b)$ is symmetric. Assume that rule $3(a)$ happens at time $t_1 + 1$.

- 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, since for all t' such that $t_1 < t' < t_2$ we have that $\deg(P', t') = d$, this 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 3.1 and Fact 3.3.

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

COROLLARY 3.5. *If a polynomial $f(\overline{x})$ is computable by $\mathbb{H}_{2\times 2} \cap$ Indg, then there exists a $\mu_{\mathbb{H}_{2\times 2}\cap \text{Indg}}$-SLP for $f(\overline{x})$ with a nondecreasing degree sequence.*

Via a similar analysis, we can obtain the following lemma:

LEMMA 3.6. *For any $\mu_{\mathbb{H}_{2\times 2}\cap \text{Indg}}$-SLP P with a nondecreasing degree sequence, at all times t, $|\deg(R_1^t) - \deg(R_2^t)| \leq 1$. Furthermore, $\forall 0 < t \leq |P|$, 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 $\deg(R_1^t) = \deg(R_2^t)$.*

PROOF. We prove the lemma inductively, observing that at time $t = 0$, both registers have degree zero.

If we assume inductively that $|\deg(R_1^{t-1}) - \deg(R_2^{t-1})| \leq 1$, note first that if $\deg(P,t) = \deg(P,t-1)$, then either the degrees of each register are unchanged, or else they have swapped. Thus in either case the invariant holds. Thus we need only deal with the case where $\deg(P,t) > \deg(P,t-1)$. Note that the rule at time t cannot be of type 1 or 2, since these rules do not increase the degree.

Consider first the case where $\deg(R_1^{t-1}) = \deg(R_2^{t-1})$. In this case, rules 4 and 5 cannot occur at time t since they don't increase the degree, and thus the rule at time t is of type 3. The conclusion of the lemma holds in this case and the invariant is maintained.

If $\deg(R_1^{t-1}) - \deg(R_2^{t-1}) = 1$, then if rule 5 or $4(b)$ is used at time t then $\deg(R_1^t) = \deg(R_2^t)$. If rule $3(b)$ is used then $\deg(R_2^t) = \deg(R_1^t) + 1$. Rules $3(a)$ and $4(a)$ cannot be used in this case, since they do not increase the degree.

The case when $\deg(R_2^{t-1}) - \deg(R_1^{t-1}) = 1$ is symmetric. This completes the proof. □

Note that, for every time $t > 0$, $\deg(P,t) - \deg(P,t-1) \in \{0,1,2\}$. (Only one register's degree can increase at any step, but it might increase by 2.)

DEFINITION 3.7. *For any polynomial f, let $H(f)$ denote the polynomial consisting of all of the monomials of f having degree $\deg(f)$; that is, $H(f)$ is the highest-degree homogeneous part of f.*

LEMMA 3.8. *Let P be a $\mu_{\mathbb{H}_{2\times 2}\cap \mathit{Indg}}$-SLP with a nondecreasing degree sequence. Then at all times t, for all $i \in \{1,2\}$, if $\deg(R_i^t) > 0$, then $H(R_i^t)$ is a product of homogeneous linear forms. Furthermore, if $\deg(R_1^t) = \deg(R_2^t)$, then there exists some $a \in \mathbb{F}$ such that $H(R_1^t) = a \cdot H(R_2^t)$.*

PROOF. We prove the claim by induction on t. The claim clearly holds for all t such that $\deg(P,t) = 0$. Consider the first time t such that $\deg(P,t)) = 1$. At time t, either rule $3(a)$ or $3(b)$ is applied (by Lemma 3.6). Assume without loss of generality that it is rule $3(a)$. (The other case is symmetric.) Thus $H(R_1^t) = a \cdot x_j$ for some x_j and some a. This establishes the basis.

To establish the inductive step, we again employ an inductive argument. Assume that the claim holds at time $t-1$, and let t' be the largest number less than or equal to t such that $\deg(R_1^{t'}) = \deg(R_2^{t'})$. (Since this condition holds at time zero, t' must exist.) We show that the claim holds at time t, by induction on $e = t - t'$. In fact, we will prove the additional claim that, at time t, there are polynomials p_1 and p_2 that are either elements of $\mathbb{F}$ or are products of (zero or more) homogeneous linear forms, such that $\{H(R_1^t), H(R_2^t)\} = \{p_1 \cdot H(R_1^{t'}), p_2 \cdot p_1 \cdot H(R_1^{t'})\}$. (Of course, this additional claim is trivial when $e = 0$.)

To establish the basis, when $e = 0$, we deal first with the case when $\deg(R_1^{t-1}) \neq \deg(R_2^{t-1})$. In this case, we assume without loss of generality that $\deg(R_1^{t-1}) > \deg(R_2^{t-1})$. (The other case is symmetric.) Thus, by Lemma 3.6 the rule applied at time t is of type $4(b)$ or 5. In both cases, there exist a and d in $\mathbb{F}$ such that $H(R_1^t) = a \cdot H(R_1^{t-1})$ and $H(R_2^t) = d \cdot H(R_1^{t-1})$. This establishes the basis for this case.

If $\deg(R_1^{t-1}) = \deg(R_2^{t-1})$, then by our (outer) inductive hypothesis $H(R_1^{t-1})$ and $H(R_2^{t-1})$ are multiples of each other. Since, in this case $\deg(P, t-1) = \deg(P, t)$, the rule applied at time t must be of type 1, 2, 4, or 5. These rules result in no significant change to the highest-degree homogeneous part of the registers in this case, and this completes the proof of the basis case $e = 0$.

The case when $e = 1$ is different than the case when $e > 1$, and thus we separate that case out as part of the basis, too. When $e = 1$ we have that $\deg(R_1^t) \neq \deg(R_2^t)$ and $\deg(R_1^{t-1}) = \deg(R_2^{t-1})$. Again, we assume without loss of generality that $\deg(R_1^t) > \deg(R_2^t)$. We will show that there is a polynomial p_2 that is a product of homogeneous linear forms, such that $H(R_1^t) = p_2 \cdot H(R_1^{t'}) = p_2 \cdot H(R_1^{t-1})$. (The last equality holds since $t' = t-1$ in this case.) Since our inductive hypothesis states that $H(R_1^{t'})$ is a product of homogeneous linear forms, this will suffice to establish the case when $e = 1$. This is because $H(R_2^t)$ does not change significantly in this step, and we will choose p_1 to be merely a field element.

Since the degree increases at time t, it follows from Lemma 3.6 that the rule that is applied at time t is of type $3(a)$. Thus $H(R_1^t) = c \cdot x_j \cdot H(R_2^{t-1}) = (c \cdot x_j \cdot a) \cdot H(R_1^{t-1})$ for some c and a in $\mathbb{F}$, where the first equality follows from the definition of rule $3(a)$ and the second equality is from the basis case $e = 0$. This completes the proof of the

basis case $e = 1$.

Now, to complete the inductive argument, assume that the claim holds at time $t' + e - 1$, and consider what happens at time $t = t' + e$. Note that, by the way that time t' is chosen, we have $\deg(R_1^t) \neq \deg(R_2^t)$. Again, we assume without loss of generality that $\deg(R_1^t) > \deg(R_2^t)$. We need to show that there are polynomials p_1 and p_2, each a product of homogeneous linear forms, such that $H(R_1^t) = p_2 \cdot p_1 \cdot H(R_1^{t'})$ and $H(R_2^t) = p_1 \cdot H(R_1^{t'})$. (The fact that the inductive hypothesis holds at time t' thus suffices to establish the rest of the (inner and outer) inductive claims.)

If $\deg(P, t) = \deg(P, t-1)$, then the only rules that are possible at time t are of type 1, 2, and $4(a)$. These rules make no significant changes to $H(R_1)$ or $H(R_2)$, and thus the hypothesis holds in this case.

If $\deg(P, t) > \deg(P, t-1)$, then the rule at time t is either of type $3(a)$ or $3(b)$. Since $e > 1$, we have $\deg(R_1^{t-1}) \neq \deg(R_2^{t-1})$. The argument is symmetric for the two cases $\deg(R_1^{t-1}) > \deg(R_2^{t-1})$ and $\deg(R_1^{t-1}) < \deg(R_2^{t-1})$, so once again we present only the proof for the case $\deg(R_1^{t-1}) > \deg(R_2^{t-1})$. By the induction hypothesis, there are polynomials q_1 and q_2, each a product of homogeneous linear forms, such that $H(R_1^{t-1}) = q_2 \cdot q_1 \cdot H(R_1^{t'})$ and $H(R_2^{t-1}) = q_1 \cdot H(R_1^{t'})$.

If rule $3(a)$ is applied at time t, then $H(R_2^t)$ does not change significantly (it is multiplied by some field element b), whereas $H(R_1^t) = a \cdot H(R_1^{t-1}) + c \cdot x_j \cdot H(R_2^{t-1}) = a \cdot q_2 \cdot q_1 \cdot H(R_1^{t'}) + c \cdot x_j \cdot q_1 \cdot H(R_1^{t'}) = (a \cdot q_2 + c \cdot x_j) \cdot q_1 \cdot H(R_1^{t'})$. This satisfies the induction claim, by letting $p_1 = b \cdot q_1$ and $p_2 = (a/b) \cdot q_2 + (c/b) \cdot x_j$.

If rule $3(b)$ is applied at time t, then $H(R_1^t)$ does not change significantly (it is multiplied by some field element a), whereas $H(R_2^t) = c \cdot x_j \cdot H(R_1^{t-1}) = c \cdot x_j \cdot q_2 \cdot q_1 \cdot H(R_1^{t'})$. This satisfies the induction claim, by letting $p_1 = (c/a) \cdot x_j$ and $p_2 = a \cdot q_2 \cdot q_1$. □

The following theorem is the main contribution of this section. It presents serious limitations of the expressive power of $\mathrm{IMM}_{2,n}$ when restricted to (inherently) non-singular matrices. Subsequent sections will deal with the limitations that are encountered when also incorporating singular matrices.

THEOREM 3.9. *Let $f(\overline{x})$ be a polynomial of total degree at least two whose highest-degree homogeneous part is irreducible. Then $f(\overline{x})$ is*

not computable by $\mathbb{H}_{2\times 2} \cap$ *Indg.*

PROOF. The proof is by contradiction. Suppose that there is some $\mu_{\mathbb{H}_{2\times 2}\cap \text{Indg}}$-SLP P for $f(\overline{x})$. By Corollary 3.5, we may assume that P has a nondecreasing degree sequence. By definition, $f = R_1^{|P|}$. However, by Lemma 3.8, $H(R_1^{|P|})$ factors completely into a product of homogeneous linear forms, in contradiction to our hypothesis that $H(f)$ is irreducible. □

3.3. Limitation of $\mu_{\mathbb{H}_{2\times 2}}$-SLPs. In the previous section, we saw that potentially-degenerate matrices are essential, if one wants to express irreducible polynomials of degree greater than one as projections of $\text{IMM}_{2,n}$. The limitations of incorporating potentially-degenerate matrices ultimately come down to the following simple observation:

OBSERVATION 3.10. *If a nonzero polynomial $f(\overline{x})$ 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 $f(\overline{x})$. □

Our goal in this section is to show that certain polynomials of the form $\sum_{i=1}^{k} x_{2i-1}x_{2i}$ cannot be expressed as projections of $\text{IMM}_{2,n}$. We note that some of the lemmas apply to more general polynomials f as well. To avoid repeating the conditions that f must satisfy, we introduce the following convention:

Convention: All of the polynomials f considered in this and later sections satisfy the property that $f|_p(\overline{x}) \neq 0$ for any regular projection of size at most four. Any straight-line program P that we consider computes such a polynomial f.

Recall in this regard that, by Proposition 2.6, any regular projection p of size at most four can be extended to a well-formed regular

projection p' of size at most eight, with the property that

$$H((\sum_{i=1}^{k} x_{2i-1}x_{2i})|_{p'})$$

is irreducible if $k \geq 6$ (by Proposition 2.7).

Given a projection p and a straight-line program $P = \{m_P^i \mid 1 \leq i \leq |P|\}$ computing a polynomial $f(\overline{x})$, 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 $f(\overline{x})|_p$. Note that this definition applies for any type of projections.

Our conventions imply some limitations on the type of potentially-degenerate matrices that we can utilize:

LEMMA 3.11. *There does not exist a matrix in P such that all of its entries belong to $\mathbb{H}$. This implies that 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 $f(\overline{x})|_p$ is nonzero while $P|_p$ contains $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, in contradiction to Observation 3.10. □

LEMMA 3.12. *For any matrix $m \in P$ that belongs to $\mathbb{H}_{2\times 2} \cap$ 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 3.11, $\det(m)$ contains at most three variables. This gives us the projection promised in the first claim. Proposition 2.6 implies the correctness of the second claim. □

DEFINITION 3.13. *We call such a well-formed homogeneous projection q as in Lemma 3.12 a* degenerating projection *for the potentially degenerate matrix m. (If m is an inherently degenerate matrix, then we consider the* empty *projection to be a degenerating projection for m This is justified by Proposition 3.14, which tells us that it is no loss of generality to consider only inherently degenerate matrices that contain no variables.)*

PROPOSITION 3.14. *If a matrix $m \in \mathbb{H}_{2\times 2} \cap Idg$ 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 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 $w \in \mathbb{F}$.

Note that $\begin{bmatrix} a\cdot x_i & 0 \\ w & 0 \end{bmatrix} = \begin{bmatrix} x_i & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & 0 \\ w & 0 \end{bmatrix}$ and $\begin{bmatrix} a\cdot x_i & 0 \\ b\cdot x_j & 0 \end{bmatrix} = \begin{bmatrix} x_i & 0 \\ 0 & x_j \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$. 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. □

NOTE 3.15. *The statement of Proposition 3.14 can be generalized for matrices in $\mathbb{S}_{2\times 2} \cap Idg$ and $\mathbb{R}_{2\times 2} \cap Idg$ with almost the same proof. Hence, we can assume that for any $\mu_{\mathbb{S}_{2\times 2}}$-SLP ($\mu_{\mathbb{R}_{2\times 2}}$-SLP, respectively) P and any inherently degenerate matrix m in P, the entries of m all belong to $\mathbb{F}$.*

LEMMA 3.16. *Let $f(\overline{x})$ be a polynomial 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 a (potentially or inherently) 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 either $R_1^t(P') \neq 0$ or $R_2^t(P') \neq 0$, and for all $i \in \{1,2\}$, if $R_i^t(P') \neq 0$, then for all $j \in \{1,2\}$ and for all t' such that $t \leq t' \leq |P|$, it holds that $R_j^{t'}(P')$ is a multiple of $R_i^t(P')$ (and, in particular, $R_i^t(P')$ divides $f(\overline{x})|_p$).

PROOF. Note first that it cannot be the case that both $R_1^t(P') = 0$ and $R_2^t(P') = 0$, as this would imply that $f|p = 0$, contrary to our convention. 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 $c \neq 0$. Let h and g be the polynomials given by $R_1^{t-1}(P')$ and $R_2^{t-1}(P')$, respectively. Thus $R_1^t(P') = ah + cg$ and $R_2^t(P') = (b/c)(ah + cg)$. Thus $R_2^t(P')$ is a multiple of $R_1^t(P')$ (and vice-versa), 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 $f(\overline{x})|_p$).

If $c = 0$, then $ab = 0$, so either $a = 0$ or $b = 0$. If $a = 0$ then $R_1^t(P') = 0$ and $R_2^t(P') = (dh + bg)$. An easy induction shows that any register from that point on will be a multiple of $R_2^t(P')$. The case when $b = 0$ is similar. □

COROLLARY 3.17. *If $f(\overline{x})|_p$ is a nonzero irreducible polynomial and the other hypotheses of Lemma 3.16 hold, then $R_i^t(P') = c \cdot f(\overline{x})|_p$ for some $c \in \mathbb{F}^*$.*

DEFINITION 3.18. *Let $f(\overline{x})$, P, m_P^t and P' satisfy the conditions of Lemma 3.16. If there is an $i \in \{1,2\}$ such that $R_i^t(P')$ is a polynomial of degree at least one, then we call p a* finishing projection for m_P^t in P. *Otherwise, we call p a* cutting projection for m_P^t in P.

The motivation for these names comes from the fact that we can essentially terminate the straight line program P' at time t if p is a finishing projection, whereas we can essentially cut off the start of P' if p is a cutting projection. The following observation makes this precise.

OBSERVATION 3.19. *Let $f(\overline{x})$ be a polynomial such that under any well-formed homogeneous projection q of size at most six, $f(\overline{x})|_q$ is always a nonzero irreducible polynomial. Let P be a $\mu_{\mathbb{H}_{2\times 2}}$-SLP for $f(\overline{x})$, and let m_P^t, p and P' be as in Lemma 3.16. Depending on*

whether p is a cutting or finishing projection, we can obtain a $\mu_{\mathbb{H}_{2\times 2}}$-SLP for $f(\overline{x})|_p$ from P that either starts or ends at time t:

- *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 $f(\overline{x})|_p$.*

- *If p is a finishing projection for m_P^t in P, then there is some i such that $R_i^t(P') \neq 0$. Then by Lemma 3.16 and Corollary 3.17, $R_i^t(P')$ is a nonzero multiple of $f(\overline{x})|_p$ and moreover, $R_i^t(P') = a \cdot R_1^{t-1}(P') + b \cdot R_2^{t-1}(P')$, where $a, b \in \mathbb{H} \cup \mathbb{F}$, since by Lemma 3.12, all of the entries in $m_P^t|_p$ are field elements. One of a and b must be a unit, since $R_i^t(P') \neq 0$. Therefore, we can throw away the portion of P' after time t (including the t-th instruction) and generate the desired output, as follows:*

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

DEFINITION 3.20. *Let $f(\overline{x})$ be a polynomial and let P be one of its $\mu_{\mathbb{H}_{2\times 2}}$-SLPs. We classify the (potentially or inherently) 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*. (Of course, for inherently degenerate matrices, the only degenerating projection that needs to be considered is the empty projection.)*

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

OBSERVATION 3.21. *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 3.22. *If $k \geq 8$, then $f(\overline{x}) = \sum_{i=1}^{k} x_{2i-1}x_{2i}$ is not computable by $\mathbb{H}_{2\times 2}$. That is, for every n, $f(\overline{x})$ can not be obtained from $IMM_{2,n}$ under homogeneous projections.*

PROOF. We prove the theorem by contradiction. Suppose P is a $\mu_{\mathbb{H}_{2\times 2}}$-SLP for $f(\overline{x})$. 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 2.2, the highest-degree homogeneous part of $f(\overline{x})$ is irreducible, and by Theorem 3.9, we have reached a contradiction. Otherwise, let $t_B = \max(B)$. Note that, by Proposition 2.7, 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 $f(\overline{x})|_p$ it computes. Since the size of p is bounded by six, by Proposition 2.7, $f(\overline{x})|_p$ 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 3.19, we now have a $\mu_{\mathbb{H}_{2\times 2}\cap \text{Indg}}$-SLP for $f(\overline{x})|_p$ which is a contradiction to Theorem 3.9. Notice that by Proposition 2.7, the above arguments apply to any polynomial of the form $\sum_{i=1}^{k'} x_{2i-1}x_{2i} + l(\overline{x})$ where $l(\overline{x})$ is an arbitrary linear function, and $k' \geq 5$.

- 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 3.16 that, at time t_G, register R_1 computes a nonzero multiple of f. Hence by the second item of Observation 3.19 with $p = \emptyset$, we obtain a new $\mu_{\mathbb{H}_{2\times 2}}$-SLP for $f(\overline{x})$, 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 $f(\overline{x})|_p$ it computes. By the second item of Observation 3.19, we obtain a new $\mu_{\mathbb{H}_{2\times 2}}$-SLP P' for $f(\overline{x})|_p$ and furthermore, by Observation 3.21, P' does not contain any good matrices. Hence, this reduces us to the first case, since $f(\overline{x})|_p$ is of the form

$$\sum_{i=1}^{k'} x_{2i-1}x_{2i} + l(\overline{x})$$

  where $l(\overline{x})$ is an arbitrary linear function, and $k' \geq 5$. It is not hard to see that we will arrive at a contradiction for $f(\overline{x})|_p$, which completes our proof.

□

The proof of Theorem 3.22 leads to the following corollary.

COROLLARY 3.23. *If $k \geq 8$, then $f(\overline{x}) = \sum_{i=1}^{k} x_{2i-1}x_{2i} + l(\overline{x})$ is not computable by $\mathbb{H}_{2\times 2}$, where $l(\overline{x})$ 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 $\mathrm{IMM}_{2,n}$, 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 3.9 holds in the setting of simple projections, we first show that, for nondegenerate matrices, the simple case reduces to the homogeneous case.

LEMMA 4.1. *Every matrix in $\mathbb{S}_{2\times 2}\cap$Indg can be represented by a product of matrices in $\mathbb{H}_{2\times 2}\cap$ 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 $m \in \mathbb{S}_{2\times 2}\cap$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 $m \in \mathbb{H}_{2\times 2} \cap$ Indg.

2. If there are at least three distinct variables occurring in m, then $\det(m)$ is a nonzero polynomial and $m \in$ Pdg, a contradiction to our assumption.

3. If there is only a single variable x_k occurring in m, then x_k has either two or four occurrences in m (since otherwise $m \notin$ Indg) 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 $(c_{2,2}w_{1,1} - c_{2,1}w_{1,2})x_k + (w_{1,1}w_{2,2} - w_{1,2}w_{2,1})$. Thus since $m \in$ Indg, $c_{2,2}w_{1,1} - c_{2,1}w_{1,2} = 0$. If $w_{1,1} = w_{1,2} = 0$, then $m \in$ Idg, a contradiction to our assumption. If exactly one of them is equal to zero, then this contradicts our assumptions that $c_{2,1} \neq 0, c_{2,2} \neq 0$, and $c_{2,2}w_{1,1} - c_{2,1}w_{1,2} = 0$. Hence, we can assume that $\frac{c_{2,2}}{c_{2,1}} = \frac{w_{1,2}}{w_{1,1}} = d \neq 0$. Thus,

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

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

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

This verifies that m is a product of matrices in $\mathbb{H}_{2\times 2} \cap$ 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 $m \in$ 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 second matrix belongs to Indg because its determinant belongs to $\mathbb{F}^*$. By the first subcase, the first matrix is a product of matrices in $\mathbb{H}_{2\times 2} \cap$ Indg, and hence so is m.

4. If there are exactly two distinct variables x_k and x_l occurring in $m \in$ Indg, 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 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 $\mathbb{S}_{2\times 2} \cap$ Indg is equal to a product of matrices in $\mathbb{H}_{2\times 2} \cap$ Indg. □

The preceding lemma, together with Theorem 3.9, immediately yield the following corollary:

COROLLARY 4.2. *Let $f(\overline{x})$ be a polynomial whose highest-degree homogeneous part is irreducible. Then $f(\overline{x})$ is not computable by $\mathbb{S}_{2\times 2} \cap$ 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 4.3. *Let $l(\overline{x})$ be an arbitrary linear function. If $k \geq 8$, then $f(\overline{x}) = \sum_{i=1}^{k} x_{2i-1}x_{2i} + l(\overline{x})$ is not computable by $\mathbb{S}_{2\times 2}$, namely, for any n, $f(\overline{x})$ can not be obtained from $IMM_{2,n}$ under simple projections.*

PROOF. We prove the theorem via contradiction. Suppose there is a $\mu_{\mathbb{S}_{2\times 2}}$-SLP P for $f(\overline{x})$.

Similar to Lemma 3.11, we prove the following lemma.

LEMMA 4.4. *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_is are all distinct. Consider the projection $p = \{x_i \leftarrow \frac{w_i}{c_i} \mid 1 \leq i \leq 4\}$. Then $f(\overline{x})|_p$ is nonzero while $P|_p$ contains $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. By Proposition 2.6 and Proposition 2.7, $f(\overline{x})$ is nonzero under any regular projection of size at most four. Thus by Observation 3.10, we have reached a contradiction. □

A direct consequence of Lemma 4.4 is an analogue of Lemma 3.12. The proof of the following lemma proceeds in the same way as that of Lemma 3.12, so we omit it here.

LEMMA 4.5. *For any matrix $m \in P$ which belongs to $\mathbb{S}_{2\times 2} \cap Pdg$, 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. □

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 – denoted as $r(m)$ – of the subspace spanned by $\{l_{i,j} \mid i,j \in \{1,2\}\}$. In some sense $r(m)$ 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 4.6. *Let $l_1, l_2, \ldots, l_k$ be linearly independent homogeneous linear forms, and let $w_1, \ldots, w_k$ 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. □

Our next lemma is a generalization of Lemma 4.1.

LEMMA 4.7. *Every matrix m in $\mathbb{R}_{2\times 2} \cap$ Indg can be represented by a product of matrices in $\mathbb{H}_{2\times 2} \cap$ Indg.*

PROOF. If $r(m) = 0, 3$ or 4, then the proof is completely analogous to the cases 1 and 2 in Lemma 4.1, 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 4.1 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 4.8. *Any matrix having the following form can be expressed as the product of matrices in* $\mathbb{H}_{2\times 2} \cap$ *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 4.1.

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. □

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 4.1 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 $m \in$ Indg. □

The preceding lemma, together with Theorem 3.9, immediately yield the following corollary:

COROLLARY 4.9. *Let $f(\overline{x})$ be a polynomial whose highest-degree homogeneous part is irreducible. Then $f(\overline{x})$ is not computable by $\mathbb{R}_{2\times 2} \cap$ Indg.*

Now we are ready to prove our main theorem.

THEOREM 4.10 (Theorem 1.2 restated). *If $k \geq 8$, then*

$$f(\overline{x}) = \sum_{i=1}^{k} x_{2i-1}x_{2i}$$

is not computable by $\mathbb{R}_{2\times 2}$, namely, for any n, $f(\overline{x})$ can not be obtained from $IMM_{2,n}$ under regular projections.

PROOF. The proof is by contradiction. Suppose P is a $\mu_{\mathbb{R}_{2\times 2}}$-SLP for $f(\overline{x})$.

By Proposition 2.6 and Proposition 2.7, $f(\overline{x})$ is nonzero under any regular projection of size at most four, which leads to the following lemma.

LEMMA 4.11. *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 for all i and j in $\{1, 2\}$, $l_{i,j} = -w_{i,j}$. In other words, $m_P^t|_p = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. By Observation 3.10, this contradicts the property that $f(\overline{x})$ is nonzero under any regular projection of size at most four. □

LEMMA 4.12. *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. Note that $\det(m_P^t)$ is a polynomial of degree at least one. Let $\overline{\gamma}$ be a zero of $\det(m_P^t)$. By Lemma 4.11, we know that $r = r(m_P^t) \leq 3$. Let $l_1, \ldots, l_r$ be linearly-independent linear forms. Let $w_1 = l_1(\overline{\gamma}), \ldots, w_r = l_r(\overline{\gamma})$. By Lemma 4.6, there is a projection p of size r that satisfies the first part of the lemma. The second part of the claim follows from Proposition 2.6. □

By Lemma 4.12, we can define degenerating projections in terms of well-formed regular projections. Note that the proofs of Lemma 3.16 and Corollary 3.17 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 3.19.

OBSERVATION 4.13. *Let $f(\overline{x})$ be a polynomial such that under any well-formed regular projection q of size at most six, $f(\overline{x})|_q$ is always a nonzero irreducible polynomial. Let P be a $\mu_{\mathbb{R}_{2\times 2}}$-SLP for $f(\overline{x})$ 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 $f(\overline{x})|_p$.*

- *If p is a cutting projection for m_P^t in P, this case is identical to the first case in Observation 3.19.*

- *If p is a finishing projection for m_P^t in P, this case is identical to the second case in Observation 3.19.*

Now the remaining part of the 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. □

Acknowledgements

Discussions that the first author had with Meena Mahajan, Guillaume Malod, Christian Ikenmeyer, 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 Saptharishi and the anonymous referees for many helpful comments. We are grateful to Luke Friedman, Ramprasad Saptharishi, and Aniruddha Zalani for pointing out mistakes in earlier versions. Useful feedback was also provided by Maurice Jansen and Ran Raz. This research was supported in part by NSF Grants CCF-1064785, and CCF-0832787.

References

M. AGRAWAL, E. ALLENDER & S. DATTA (2000). On TC^0, AC^0, and Arithmetic Circuits. *Journal of Computer and System Sciences* **60**, 395–421.

M. AGRAWAL, R. GURJAR, A. KORWAR & N. SAXENA (2015). Hitting-Sets for ROABP and Sum of Set-Multilinear Circuits. *SIAM J. Comput.* **44**(3), 669–697.

E. ALLENDER (2004). Arithmetic Circuits and Counting Complexity Classes. In *Complexity of Computations and Proofs*, J. KRAJÍČEK, editor, volume 13 of *Quaderni di Matematica*, 33–72. Seconda Università di Napoli.

A. AMBAINIS, E. ALLENDER, D. A. M. BARRINGTON, S. DATTA & H. LÊTHANH (1999). Bounded Depth Arithmetic Circuits: Counting and Closure. In *Proc. ICALP*, number 1644 in Lecture Notes in Computer Science, 149–158. Springer.

D. A. BARRINGTON (1985). Width-3 Permutation Branching Programs. Technical Report Technical Memorandum MIT/LCS/TM-293, MIT.

M. BEN-OR & R. CLEVE (1988). Computing Algebraic Formulas Using a Constant Number of Registers. In *Proc. ACM Symp. on Theory of Computing (STOC)*, 254–257.

M. BEN-OR & R. CLEVE (1992). Computing Algebraic Formulas Using a Constant Number of Registers. *SIAM Journal on Computing* **21**(1), 54–58.

H. CAUSSINUS, P. MCKENZIE, D. THÉRIEN & H. VOLLMER (1998). Nondeterministic NC^1 computation. *Journal of Computer and System Sciences* **57**, 200–212.

M. J. JANSEN, M. MAHAJAN & B. V. RAGHAVENDRA RAO (2013). Resource trade-offs in syntactically multilinear arithmetic circuits. *Computational Complexity* **22**(3), 517–564.

H. JUNG (1985). Depth efficient transformations of arithmetic into Boolean circuits. In *Proc. FCT*, number 199 in Lecture Notes in Computer Science, 167–173. Springer.

R. LIPTON & Y. ZALCSTEIN (1977). Word problems solvable in logspace. *Journal of the ACM* **24**, 522–526.

M. MAHAJAN & B. V. RAGHAVENDRA RAO (2013). Small Space Analogues of Valiant's Classes and the Limitations of Skew Formulas. *Computational Complexity* **22**(1), 1–38.

MEENA MAHAJAN, NITIN SAURABH & KARTEEK SREENIVASAIAH (2012). Counting paths in planar width 2 branching programs. In *Proc. 18th Computing: The Australasian Theory Symposium, (CATS 2012)*, volume 128 of *CRPIT*, 59–68. Australian Computer Society.

N. NISAN (1991). Lower Bounds for Non-Commutative Computation (Extended Abstract). In *Proc. ACM Symp. on Theory of Computing (STOC)*, 410–418.

D. ROBINSON (1993). *Parallel algorithms for group word problems*. Ph.D. thesis, Univ. of California, San Diego.

C. SAHA, R. SAPTHARISHI & N. SAXENA (2009). The Power of Depth 2 Circuits over Algebras. In *Proc. Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS)*, 371–382.

CHANDAN SAHA (2011). Private communication.

L. VALIANT (1979). Completeness classes in algebra. In *Proc. ACM Symp. on Theory of Computing (STOC)*, 249–261.

Manuscript received 28 August 2013

ERIC ALLENDER
Department of Computer Science
Rutgers University
Piscataway, NJ 08855, USA
allender@cs.rutgers.edu

FENGMING WANG
Airbnb Inc.
888 Brannan St.,
San Francisco, CA 94103, USA
wfengm@gmail.com