Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 139 (2014)

LOWER BOUNDS FOR THE CIRCUIT SIZE OF PARTIALLY HOMOGENEOUS POLYNOMIALS

HÔNG VÂN LÊ

Abstract. In this paper we associate to each multivariate polynomial f that is homogeneous relative to a subset of its variables a series of polynomial families $P_\lambda(f)$ of m-tuples of homogeneous polynomials of equal degree such that the circuit size of any member in $P_\lambda(f)$ is bounded from above by the circuit size of f. This provides a method for obtaining lower bounds for the circuit size of f by proving (s,r)-(weak) elusiveness of the polynomial mapping associated with $P_\lambda(f)$. We discuss some algebraic methods for proving the (s,r)-(weak) elusiveness. We also improve estimates in the normal homogeneous-form of an arithmetic circuit obtained by Raz in [12] which results in better lower bounds for circuit size (Lemma 6.7, Remark 6.8). Our methods yield non-trivial lower bound for the circuit size of several classes of multivariate homogeneous polynomials (Corollary 6.9, Example 6.10).

To my Teacher Anatoly Timofeevich Fomenko

Contents

2010 *Mathematics Subject Classification.* Primary 03D15, 68Q17, 13P25.
H.V.L. is supported by RVO: 67985840.

ISSN 1433-8092

1. Preface

I had a fortune to study under the guidance of Anatoly Timofeevich for almost all the time I spent at the Lomonosov Moscow State University. I am greatly indebted to Anatoly Timofeevich for his support and encouragement, for his lessons in mathematics and beyond. During my time at the Lomonosov Moscow University Anatoly Timofeevich led, except regular seminars on topology and differential geometry, also a seminar on computer geometry. My present contribution in computational complexity reflects, in particular, interests I acquired in Moscow under the influence of Anatoly Timofeevich. I wish him good health, happiness and more success for the coming years.

2. Introduction

Let $\mathbb{F}$ be a field. Recall that the permanent $Per_n(\mathbb{F}) \in \mathbb{F}[x_{ij} | \, 1 \leq i, j \leq n]$ is defined by

$$Per_n([x_{ij}]) := \sum_{\sigma \in \Sigma_n} \Pi_{i=1}^n x_{i\sigma(i)}.$$

Finding non-trivial lower bounds for the circuit size or formula size of the permanent Per_n is a challenging problem in algebraic computational complexity theory, especially in the VP versus VNP problem [2], [4], [17], [15]. It has been pointed out by Mulmuley-Sohoni [10] that a proof of $VP \neq VNP$ which is based on a generic property of $poly(n)$-definable polynomials will likely fall in the trap of the "natural proof" [13]. Up to now, there is no known tool for obtaining a non-trivial lower bound for the circuit size of the permanent. The only known non-trivial lower bound for the formula size of the permanent is due to Kalorkoti [7], which says that over any field, the formula size of $Per_n(\mathbb{F})$ is at least $\Omega(n^3)$. (Kalorkoti proved the same lower bound for the formula size of the determinant, and Pavel Hrubeš told me that Kalorkoti's proof works also for the formula size of the permanent.) Another tool for obtaining a non-trivial lower bound for the formula size of the permanent exploits the Valiant theorem on the relation between the formula size and the determinantal complexity of the permanent [16], [9], [10]. The determinantal complexity c_{det}, though better understood than the formula size, is still very complicated. The best lower bound $c_{det}(Per_n) \geq (n^2/2)$ has been obtained by Mignon and Ressayer [9]. To get the quadratic estimate, Mignon and Ressayer compared the second fundamental form of the hyper-surface $\{\det_m(x) = 0\}$ with that of $\{Per_n(x) = 0\}$. Mulmuley and Sohoni suggested to use representation theory to obtain lower bounds for $c_{det}(Per_n)$ [10]. We also like to mention the recent paper [3] on reduction to circuits of depth 4.

In [12] Raz introduced new exciting ideas to the study of lower bounds for the circuit size of multivariate polynomials. He proposed a method of elusive functions to construct polynomials of large circuit size. Namely from an (s, r)-elusive polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$, for certain values of

(s, r, n, m), he obtained a multivariate polynomial $\tilde{f} \in \mathbb{F}[x_1, \cdots, x_{3n}]$, whose degree linearly depends on r, such that the circuit size $L(\tilde{f})$ of $\tilde{f}$ is bounded from below by a function of r and s. In [8] we developed further Raz's ideas, showing the effectiveness of his method for fields $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$.

In this paper we develop Raz's ideas in a somewhat different direction. From a given polynomial $\tilde{f}$ that is homogeneous relative to a subset of its variables (e.g. the permanent, see Definition 6.1 below) we construct a polynomial family $P_\lambda(\tilde{f})$ of m-tuples of homogeneous polynomials of degree r such that the $(s, 2r-1)$-weak elusiveness of the polynomial mapping associated with $P_\lambda(\tilde{f})$ would imply a lower bound for the circuit size of $\tilde{f}$ in terms of s and r. We propose several algebraic methods for verifying whether a homogeneous polynomial mapping is (s, r)-(weakly) elusive. We show that our methods yield non-trivial lower bounds for a large class of homogeneous polynomials. We discuss some problems in commutative algebra related with our method.

The remainder of our paper is organized as follows. In Section 3 we recall basic notions in the theory of arithmetic circuits that are needed in our paper. Then we give a slightly extended version of the Raz normal form theorem (Theorem 3.5) as well as an improved version of the Rax existence of a universal circuit-graph (Theorem 3.6) in the form that is needed in Proposition 4.4, Corollary 4.6 and Lemma 6.7. Lemma 6.7 is an improvement of a previous result by Raz, see Remark 6.8. In section 4 we relate the notion of (weakly)-elusive polynomial mappings with the circuit size of a polynomial family of m-tuples of homogeneous polynomials of equal degree (Proposition 4.4, Corollary 4.6). In section 5 we propose several algebraic methods for proving the (s, r)-(weak) elusiveness of a polynomial mapping (Proposition 5.1, Remark 5.2, Corollaries 5.3, 5.10, Examples 5.4, 5.6). We also consider related problems in commutative algebra (Problems 1,2,3). In section 6 we associate to each polynomial $\tilde{f}$ that is homogeneous relative to a subset of its variables a series of polynomial families $P_\lambda(\tilde{f})$ of m-tuples of homogeneous polynomials of equal degree such that the circuit size of any member in $P_\lambda(\tilde{f})$ is bounded from above by the circuit size $L(\tilde{f})$ of $\tilde{f}$ (Proposition 6.4). We present non-trivial examples of our methods (Examples 6.6. 6.10). We also suggest a method for obtaining non-trivial lower bounds for the circuit size of the permanent (Lemmas 6.12, 6.13).

Notations. In our paper we assume that $\mathbb{F}$ is an arbitrary field, if not specified otherwise. The space of all (resp. homogeneous) polynomials of degree r in n variables over $\mathbb{F}$ will be denoted by $Pol^r(\mathbb{F}^n)$ (resp. $Pol^r_{hom}(\mathbb{F}^n)$), and the space of all ordered m-tuples of (resp. homogeneous) polynomials in $Pol^r(\mathbb{F}^n)$ (resp. $Pol^r_{hom}(\mathbb{F}^n)$) will be denoted by $(Pol^r(\mathbb{F}^n))^m$ (resp. $(Pol^r_{hom}(\mathbb{F}^n))^m$). We denote by $Pol^r(\mathbb{F}^n, \mathbb{F}^m)$ (resp. $Pol^r_{hom}(\mathbb{F}^n, \mathbb{F}^m)$) the space of polynomial mappings (resp. homogeneous

polynomial mappings) of degree r from $\mathbb{F}^n$ to $\mathbb{F}^m$. If $m = 1$ then we abbreviate $Pol^r(\mathbb{F}^n, \mathbb{F})$ as $Pol^r(\mathbb{F}^n)^*$. Clearly, there is a natural linear map $Pol^r(\mathbb{F}^n) \to Pol^r(\mathbb{F}^n)^*$, which is an isomorphism if $\mathbb{F}$ is a field of characteristic 0. We also note that there is a linear isomorphism $Pol^r(\mathbb{F}^n, \mathbb{F}^m) = (Pol^r(\mathbb{F}^n)^*)^m$. For $\tilde{f} \in Pol^r(\mathbb{F}^n)$ we denote by $\tilde{f}^*$ the image of $\tilde{f}$ under the linear map $Pol^r(\mathbb{F}^n) \to Pol^r(\mathbb{F}^n)^*$. For $\lambda \in \mathbb{F}$ we also denote $\tilde{f}^*(\lambda)$ by $\tilde{f}(\lambda)$.

3. Normal form of arithmetic circuit and their universal circuit-graph

In this section we recall some necessary definitions related to arithmetic circuits. We formulate a version of the Raz theorem on normal-homogeneous circuit (Theorem 3.5) and a version of the Raz theorem on the existence of a universal circuit-graph (Theorem 3.6). These results are needed in Proposition 4.4, Corollary 4.6 that relate the (s, r)-weak elusiveness with a lower bound for the circuit size of an arithmetic circuit. This results in a better estimate on the circuit size than that of Raz, see Lemma 6.7 and Remark 6.8.

Definition 3.1. (cf. [12, §1.1]) *An arithmetic circuit* is a finite directed acyclic graph whose nodes are divided into four types: *an input-gate* is a node of in-degree 0 labelled with an input variable; *a simple gate* is a node of in-degree 0 labelled with the field element 1; *a sum-gate* is a node labelled with $+$; *a product-gate* is a node labelled with $\times$; *an output-gate* is node of out-degree 0 giving the result of the computation. Every edge (u, v) in the graph is labelled with a field element α. It computes the product of α with the polynomial computed by u. A product-gate (resp. a sum-gate) computes the product (resp. the sum) of polynomials computed by the edges that reach it. We say that a polynomial $g \in \mathbb{F}[x_1, \cdots, x_n]$ is computed by a circuit if it is computed by one of the circuit output-gates. If a circuit has m output-gates, then it computes an m-tuple of polynomials $g^i \in \mathbb{F}[x_1, \cdots, x_n]$, $i \in [1, m]$. The *fanin* of a circuit is defined to be the maximal in-degree of a node in the circuit, that is, the maximal number of children that a node has.

Definition 3.2. ([12, §2]) *A circuit-graph* G is the underlying graph G_Φ of an arithmetic circuit Φ together with the labels of all nodes. This is the entire circuit, except for the labels of the edges. We call $G = G_\Phi$ *the circuit graph* of Φ. The *size* of an arithmetic circuit Φ is defined to be the number of edges in Φ, and is denoted by $Size(\Phi)$. The *depth* of a circuit Φ is defined to be the length of the longest directed path in Φ, and is denoted by $Depth(\Phi)$. The *circuit size* $L(P)$ of an m-tuple P of polynomials $g^1, \cdots, g^m \in \mathbb{F}[x_1, \cdots, x_n]$ is the minimal size of an arithmetic circuit computing P.

Definition 3.3. For a circuit-graph G, we define *the syntactic-degree of a node in* G inductively as follows [12, §2]. The syntactic-degree of a simple

gate is 0, and the syntactic-degree of an input-gate is 1. The syntactic-degree of a sum-gate is the maximum of the syntactic-degrees of its children. The syntactic-degree of a product-gate is the sum of the syntactic-degrees of its children. For an arithmetic circuit Φ and a node $v \in \Phi$, we define the syntactic-degree of v to be its syntactic-degree in the circuit-graph G_Φ. The degree of a circuit is the maximal syntactic-degree of a node in the circuit.

Definition 3.4. ([12, Definitions 2.1, 2.2]) A circuit-graph G is called *homogeneous*, iff for every arithmetic circuit Φ such that $G = G_\Phi$ and every gate v in Φ, the polynomial computed by the gate v is homogeneous. Further, we say that a homogeneous graph is *in normal form*, if it satisfies the following conditions.

(1) There is no simple gate.
(2) All edges from the input-gates are to sum-gates.
(3) All output-gates are sum-gates.
(4) The gates of G are alternating. That is, if v is a product-gate (resp.a sum-gate) and (u, v) is an edge, then u is a sum-gate (resp. a product-gate or an input-gate.)
(5) The in-degree of every product-gate is exactly 2.
(6) The out-degree of every sum-gate is at most 1.

We say that an arithmetic circuit is *in a normal-homogeneous form*, if the circuit graph G_Φ is in a normal-homogeneous form.

Let $N(\Phi)$ denote the number of gates in Φ.

Theorem 3.5. *(cf.* [12, Proposition 2.3]*) Let Φ be an arithmetic circuit of size s that computes an m-tuple P of homogeneous polynomials $g_1, \cdots, g_m \in Pol^r_{hom}(\mathbb{F}^n)$ where $r \geq 1$. Then there exists an arithmetic circuit Ψ for the polynomials $g_1, \cdots, g_m$ such that Ψ is in a normal homogeneous form with $N(\Psi) < 16s(r+1)^2 + 5m + 4n$.*

Proof. Theorem 3.5 is almost identical with [12, Proposition 2.3] except that Raz assumed that $m = n$. The proof presented here uses the Raz algorithm in the proof of [12, Proposition 2.3]. The Raz algorithm transforms an arithmetic circuit Φ that computes P into an arithmetic circuit Ψ in normal homogeneous form which also computes P and, moreover, satisfies the condition of Theorem 3.5. We shall write the proof of Theorem 3.5 in detail, since it will be needed for the proof of Proposition 3.6 later.

Step 1. If a (sum- or product-) gate in Φ has in-degree 1, then we remove its and connect its only child directly to all its parents. The size of the new circuit is less than the size of the old circuit. Hence we can assume that Φ has *no gate of in-degree 1.* (This property is necessary for the next step and needs not be preserved under later steps).

Step 2. We transform Φ to Φ_1, which satisfies *the condition (5)* of Definition 3.4, by replacing any product-gate of in-degree larger than 2 with a tree of product-gates of in-degree 2 such that each new born product-gate has out-degree one, and by replacing any sum-gate of in-degree larger than

2 with a tree of sum-gates of in-degree 2 such that each new born sum-gate has out-degree one. It is easy to check that $Size(\Phi_1) \leq 2s$.

Step 3. We transform Φ_1 to Φ_2 such that G_{Φ_2} also *satisfies the condition (5), and moreover, is homogeneous.* The nodes of Φ_2 are obtained by splitting each node $v \in \Phi_1$ into $(r+1)$ nodes $v_0, \cdots, v_r$, where the node v_i computes the homogeneous part of degree i of the polynomial computed by the node v. We ignore monomials of degree larger than r. If the original node $v \in \Phi_1$ is a sum-gate, we replace the sub-circuit in Φ_1 connecting v with its children $u^1, \cdots, u^t$ by the circuits that compute $v_i = u^1_i + \cdots + w^t_i$ for all $i \in [0, r]$. If $v \in \Phi_1$ is a product-gate, we replace the sub-circuit in Φ_1 connecting v with its children u^1, u^2 by the sub-circuits that compute $v_i = \sum_{j=0}^{i} u^1_j \times u^2_{i-j}$ for all $i \in [0, r]$. Clearly Φ_2 also computes P, moreover Φ_2 is homogeneous, satisfies the condition (5) in Definition 3.4. By the construction

$$Size(\Phi_2) \leq r(r+1)Size(\Phi_1) \leq 2s(r+1)^2. \tag{3.1}$$

Step 4. We transform Φ_2 to a homogeneous circuit Φ_3 which computes P and satisfies *the conditions (1), (5)* in Definition 3.4 by removing every node of syntactic-degree 0 as follows. Let $u \in \Phi_2$ be a node of syntactic degree 0. We assume that u has out-degree at least 1, otherwise we can remove u without affecting the functionality of the circuit. Let v be a parent of u. If v is a sum-gate, noting that Φ_2 is homogeneous, v computes a field element α_v. Then we replace the sub-circuit computing v from its children by a simple gate and label the corresponding edge by α_v. If v is a product-gate, then v has the only two children u and w, so we replace the sub-circuit consisting of v together with all edges connecting with v by edges with appropriate label connecting w with the parents of v. Repeating this process we get the desired circuit Φ_3 with no newly created gate and $Size(\Phi_3) \leq Size(\Phi_2)$.

Step 5. We transform Φ_3 to a homogeneous circuit Φ_4 which computes P and satisfies *the conditions (1), (5) and (4).* This is done as follows. For any edge (u, v) such that u, v are both product-gates we add a dummy sum-gate in between them. For any edge (u, v) such that u, v are both sum-gates we connect all the children of u directly to v. Clearly $Size(\Phi_4) \leq 2\, Size(\Phi_3)$.

Step 6. We transform Φ_4 to a homogeneous circuit Φ_5 which computes P and satisfies *the conditions (1), (5), (4) and (3)* by connecting every product output-gate to a new dummy sum-gate. Clearly

$$Size(\Phi_5) \leq Size(\Phi_4) + m \leq 2\, Size(\Phi_2) + m.$$

Step 7. We transform Φ_5 to a homogeneous circuit Φ_6 which computes P and satisfies *the conditions (1), (5), (4), (3) and (2)* by adding a dummy sum-gate in the middle of any edge from an input-gate to a product gate. This step also transforms a formula Φ_5 to the formula Φ_6. Clearly

$$Size(\Phi_6) \leq 2Size(\Phi_5) - m \leq 4\, Size(\Phi_2) + m.$$

Step 8. We transform Φ_6 to a homogeneous circuit Φ_7 which computes P and satisfies all the conditions in Theorem 3.5 by duplicating q-times any sum-gate of out-degree $q > 1$. The resultant Φ_7 may have large circuit size, since we do not have a control over the number of edges outgoing from product-gate. Thus we are restrict ourself with the following estimate

$$N(\Phi_7) \leq 3N(\Phi_6) \leq 2(Size(\Phi_6) + n + m) \leq 8\, Size(\Phi_2) + 5m + 4n.$$

Taking into account (3.1), this completes the proof of Theorem 3.5. □

Theorem 3.6. *cf.* [12, Proposition 2.8] *Assume that a quadruple (s, r, n, m) satisfies $n, m \leq s$, $1 \leq r$. Then there is a circuit-graph $G_{s,r,n,m}$, in a normal-homogeneous form that is universal for n-inputs and m-outputs circuits of size s that computes homogeneous polynomials of degree r, in the following sense.*

Let $\mathbb{F}$ be a field. Assume that a m-tuple $P := (g_1, \cdots, g_m) \in (Pol^r_{hom}(\mathbb{F}^n))^m$ is of circuit size s. Then there exists an arithmetic circuit Ψ that computes P such that $G_\Psi = G_{s,r,n,m}$.

Furthermore, the number of the edges leading to the sum-gates in $G_{s,r,n,m}$ is less than $256 \cdot s^2(r+2)^6$.

Proof. Theorem 3.6 differs from Proposition 2.8 in [12] only in two instances. Firstly, Raz assumed that $m = n$. Secondly, we have an estimate on the number of the edges leading to the sum-gates in $G_{s,r,n,m}$. This estimate, combined with Remark 3.7 below, yields a better lower bound for the circuit size of partially homogeneous polynomials in considerations, see Remark 6.8. The idea of the proof of Theorem 3.6, due to Raz [12], is to produce a circuit-graph $G_{s,r,n,m}$ with sufficient nodes and edges so that the circuit-graph of any normal-homogeneous circuit Φ computing P can be embedded into $G_{s,r,n,m}$.

Set $N := N(s, r, n, m) = 16\, s(r+1)^2 + 5m + 4n$.

The circuit-graph $G_{s,r,n,m}$ is constructed based on Theorem 3.5 as follows. First we describe how to partition the nodes of $G_{s,r,n,m}$ into $2r$ levels.

- The level-1 contains n input-gates, and the last level-$2r$ contains m output-gates.
- For every $i \in \{2, ..., r\}$, the level-$2i$ contains N sum-gates of syntactic-degree i.
- For every $i \in \{2, ..., r\}$, the level-$(2i-1)$ contains product-gates of syntactic-degree i.
- Every product-gate in level-$(2i-1)$ is assigned a type $j \in [1, i-1]$.
- For each pair (i, j) such that $1 \leq j \leq i-1 \leq r-1$ there are exactly N product-gates of syntactic degree i and of type j.

Now describe the edges of the circuit-graph $G_{s,r,n,m}$. First we connect each sum-gate in level-$(2i)$ with all product-gates in level-$(2i-1)$. Then we connect each product-gate of type j in level-$(2i-1)$ with one sum-gate in level-$(2j)$ and with one sum-gate in level-$(2i-2j)$ inductively using an

ordering the set $\{(i,j)|\ 1 \leq j \leq i-1 \leq r-1\}$, such that the out-degree of every sum-gate is at most 1.

Clearly the constructed circuit-graph $G_{s,r,n,m}$ is in a normal-homogeneous form.

Let $P := (g_1, \cdots, g_m) \in (Pol^r_{hom}(\mathbb{F}^n))^m$ have a circuit size s and Ψ an arithmetic circuit in normal homogeneous form that computes P as described in the proof in Theorem 3.5; in particular $Size(P) \leq 16\, s(r+1)^2 + 5m + 4n$. We will show how to embed G_Ψ into $G_{s,r,n,m}$.

Since $N(\Psi) \leq N = N(s,r,m,n)$, we can embed all the product-gates of syntactic degree i and of type j of the circuit graph G_Ψ into the product-gates of type j in level $(2i-1)$ of $G_{s,r,n,m}$. Since the in-degree of each product-gate in Ψ as well as in $G_{s,r,n,m}$ is two, we embed all the sum-gates of Ψ into the sum-gate of $G_{s,r,n,m}$ so that the edges leading to the product-gates in Ψ are also edges leading to the product-gates in $G_{s,r,n,m}$. Since each sum-gate in level-$(2i)$ is connected with each product-gate in level-$(2i-1)$ the edges leading to the sum-gates in Ψ can be embedded into the edges leading to the sum-gates in $G_{s,r,n,m}$. This completes the proof of the first assertion of Theorem 3.6.

To prove the last assertion of Theorem 3.6 we note that for $i \in [1,r]$ there are at most $(r-1)N$ product-gates on level-$(2i-1)$ and there are exactly N sum-gates on level-$(2i)$ of the universal circuit-graph $G_{s,r,n,m}$. Hence the total number of the edges leading to the sum-gates in $G_{s,r,n,m}$ is at most $r \cdot (r-1)N \cdot N < 256\, s^2(r+2)^6$. This completes the proof of Theorem 3.6. □

Remark 3.7. ([12, 3.2]) Assume that Φ is a normal homogeneous arithmetic circuit that computes a m-tuple $P \in (Pol^r_{hom}(\mathbb{F}^n)^m)$. Then there is an arithmetic circuit Ψ of the same circuit-graph as Φ that computes P such that the label of any edge leading to a product-gate in Ψ is 1.

4. (s,r)-WEAKLY ELUSIVE POLYNOMIAL MAPPINGS

In this section we introduce the notion of an (s,r)-weakly elusive polynomial mapping (Definition 4.1), which is slightly weaker than the notion of an (s,r)-elusive polynomial mapping introduced by Raz (Example 4.2), see also Remark 5.9 in Section 3 for motivation. Then we show how this notion is useful for obtaining lower bounds for the circuit size of elements in a polynomial family of m-tuples of homogeneous polynomials (Proposition 4.4, Corollary 4.6). The key geometric structures here are polynomial families of m-tuples of homogeneous polynomials of equal degree (Definition 4.3).

Definition 4.1. (cf. [12, Definition 1.1]) A polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$ is called (s,r)-*weakly elusive*, if its image does not belong to the image of any homogeneous polynomial mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r.

This definition differs from the Raz definition [12, Definition 1.1] only in the requirement that Γ must be homogeneous. This is a minor difference,

as we will see in the example below, but it will be technical simpler in some situations.

Example 4.2.
(1) Any (s,r)-elusive polynomial mapping is (s,r)-weakly elusive.
(2) The curve $(1, x, \cdots, x^m) \in \mathbb{R}^{m+1}$ is $(m,1)$-weakly elusive, since its image does not belong to any hyper-surface through the origin of $\mathbb{R}^{m+1}$. On the other hand, this curve is not $(m,1)$-elusive, since it lies on the affine hyper-surface $x_1 = 1$ in $\mathbb{R}^{m+1}$.
(3) If $f : \mathbb{F}^n \to \mathbb{F}^m$ is $(s+1,r)$-weakly elusive, then f is (s,r)-elusive.

The notion of (s,r)-weakly elusive polynomial mappings aims to verify, whether elements in a polynomial family of m-tuples of homogeneous polynomials of equal degree have uniformly bounded circuit size.

Given a set S of variables $x_1, \cdots, x_l$ we denote by $Pol^r(\mathbb{F}\langle S\rangle)$ (resp. $Pol^r_{hom}(\mathbb{F}\langle S\rangle)$) the space of polynomials (resp homogeneous polynomials) of degree r in variables $x_1, \cdots, x_s$ over $\mathbb{F}$.

Definition 4.3. A family $P_\lambda \in (Pol^r_{hom}(\mathbb{F}^n))^m$, $\lambda \in \mathbb{F}^k$, will be called *a polynomial family of m-tuples of homogeneous polynomials of equal degree*, if there exists a polynomial mapping $f : \mathbb{F}^k \to \mathbb{F}^N = (Pol^r_{hom}(\mathbb{F}^n))^m$, such that $P_\lambda = f(\lambda)$ for all $\lambda \in \mathbb{F}^k$. The polynomial mapping f will be called *associated with the family P_λ*.

Proposition 4.4. *Let $Z = \{z_1, \cdots, z_n\}$ be a set of variables and $1 \leq n, m \leq s$. Assume that $P_\lambda \in (Pol^r_{hom}(\mathbb{F}(\langle Z\rangle))^m$, $\lambda \in \mathbb{F}^k$, is a polynomial family of m-tuples of homogeneous polynomials in n variables of degree r such that for each $\lambda \in \mathbb{F}^k$ the circuit size of P_λ is at most L. Then the associated polynomial mapping f is not $(s, 2r-1)$-weakly elusive for any $s \geq s_0 := 256 \cdot L^2 \cdot (r+2)^6$.*

Proof. Let s be an integer as in Proposition 4.4. To prove Proposition 4.4 it suffices to show the existence of a homogeneous polynomial mapping of degree $(2r-1)$

$$\Gamma_G : \mathbb{F}^s \to (Pol^r_{hom}(\mathbb{F}\langle Z\rangle))^m$$

such that

$$f(\mathbb{F}^k) \subset \Gamma_G(\mathbb{F}^s). \tag{4.1}$$

We shall construct a homogeneous polynomial mapping Γ_G satisfying (4.1) with help of Proposition 3.6. By Theorem 3.6, the universal circuit-graph $G_{L,r,n,m}$ has at most s_0 edges leading to the sum-gates. We label these edges with $y_1, \cdots, y_{\bar{s}}$, where $\bar{s} \leq s_0$. We label the other edges of $G_{L,r,n,m}$ with the field element 1, see Remark 3.7. Now we define Γ_G to be the polynomial mapping in the variables $y_1, \cdots, y_s$ such that

$$\Gamma_G(\alpha_1, \cdots, \alpha_s) = (g_1, \cdots, g_m)$$

where $(g_1, \cdots, g_m)$ are the m output-gates of the circuit $\Phi_{G_{L,r,n,m}}$ obtained from $G_{L,r,n,m}$ by replacing the label y_i with the field element $\alpha_i \in \mathbb{F}$ for all $i \in [1, \bar{s}]$. In particular, Γ_G depends only on $\bar{s}$ variables.

Lemma 4.5. *(cf.* [12, Proposition 3.2]*)* Γ_G *is a homogeneous polynomial mapping of degree* $2r-1$.

Proof. We apply the argument in the Raz proof of [12, Proposition 3.2], which is a special case of Lemma 4.5 with $m = n$. For a node $v \in G_{L,r,n,m}$ denote the polynomial $g_v \in \mathbb{F}[z_1, \cdots, z_n, y_1, \cdots, y_s]$ that is computed by the node v and is regarded as polynomial in $[z_1, \cdots, z_n]$ with coefficients in $\mathbb{F}[y_1, \cdots, y_s]$. If v is a product-gate, with children v_1, v_2 (that are sum-gates), then, by induction, the coefficients in the polynomials g_{v_1}, g_{v_2} are homogeneous polynomials of degree $2r_{v_1} - 1$, $2r_{v_2} - 1$, respectively, (in the labels $y_1, \cdots, y_s$). By Remark 3.7 (v_1, v) and (v_2, v) are labelled by 1, the coefficients in the polynomial g_v are homogeneous polynomials of degree $2r_{v_1} - 1 + 2r_{v_2} - 1 = 2r_v - 2$ (in the labels $y_1, \cdots, y_s$). If v is a sum-gate, then, by induction, the coefficients in the polynomial g_u, for every child u of v, are homogeneous polynomials of degree $2r_u - 2 = 2r_v - 2$ (in the labels $y_1, \cdots, y_s$). Since the edge (u, v) is labelled by an element of $\{y_1, \cdots, y_s\}$, the coefficients in the polynomial g_v are homogeneous polynomials of degree $2r_v - 1$ (in the labels $y_1, \cdots, y_s$). □

By the assumption of Proposition 4.4, for any $\lambda \in \mathbb{F}^k$, the circuit size of $f(\lambda)$ is at most L. Taking into account Theorem 3.6, there exists $\alpha \in \mathbb{F}^s$ such that $f(\lambda) = \Gamma_G(\alpha)$. This proves (4.1) and completes the proof of Proposition 4.4. □

Corollary 4.6. *Let* $P_\lambda \in (Pol^r_{hom}(\mathbb{F}^n))^m$, $\lambda \in \mathbb{F}^k$, *be a polynomial family of* m*-tuples of homogeneous polynomials of degree* r *and* $f : \mathbb{F}^k \to (Pol^r_{hom}(\mathbb{F}^n))^m$ *its associated polynomial mapping. Assume that* f *is* $(s, 2r-1)$*-weakly elusive. Then* P_λ *has a member with circuit size greater than or equal* $\frac{\sqrt{s}}{16(r+2)^3}$.

Proposition 4.4 crystallizes some arguments in Raz's proof of [12, Proposition 3.7]. In Proposition 6.4 below we shall see that for each multivariate partially homogeneous polynomial $\tilde{f}$ there are many polynomial families $P_\lambda(\tilde{f})$ of m-tuples of homogeneous polynomials of equal degree associated with $\tilde{f}$ such that the circuit size of any member in the family $P_\lambda(\tilde{f})$ is bounded by the circuit size of $\tilde{f}$. Then we can apply Proposition 4.4, or its equivalent version Corollary 4.6, for estimating from below the circuit size $L(\tilde{f})$.

5. How to prove the (s, r)-weak elusiveness

In this section we assume that $\mathbb{F}$ is a field of characteristic 0, or the size of $\mathbb{F}$ is sufficiently large, so that $Pol^k_{hom}(\mathbb{F}^n, \mathbb{F}^m) = (Pol^k_{hom}(\mathbb{F}^n))^m$.

Given $f \in Pol^k(\mathbb{F}^n, \mathbb{F}^m)$ and two numbers s, r, it is generally hard to know whether f is (s,r)-weakly elusive or (s,r)-elusive. In this section we propose some algebraic methods to establish the (s,r)-(weak) elusiveness of f (Proposition 5.1, Remark 5.2, Corollaries 5.3, 5.10, Examples 5.4, 5.6). Under "algebraic methods" (resp. "algebraic characteristics") we mean operations on f (resp. properties like the dimension of vector spaces associated with f), which are related with techniques developed in commutative algebra. We show that, for appropriate parameters (s, r, n, m, p), the subset of (s,r)-(weakly) elusive homogeneous polynomial mappings is everywhere dense with respect to the Zariski topology in the space $Pol^p_{hom}(\mathbb{F}^n, \mathbb{F}^m)$ (Theorem 5.12). We also pose some problems in commutative algebra (Problems 1, 2, 3) whose solutions would advance the proposed methods.

5.1. **Hilbert functions and (s,r)-weak elusiveness.** Let $\mathbb{F}P^{m-1}$ denote the projective space of dimension $(m-1)$ over field $\mathbb{F}$, that is $\mathbb{F}P^{m-1} = (\mathbb{F}^m \setminus \{0\})/(\mathbb{F} \setminus \{0\})$. Elements of $\mathbb{F}P^{m-1}$ are denoted by $[x_1, \cdots, x_m]$, where $x_i \in \mathbb{F}$. For $\Gamma = (\Gamma^1, \cdots, \Gamma^m) \in (Pol^r_{hom}(\mathbb{F}^s))^m = Pol^r_{hom}(\mathbb{F}^s, \mathbb{F}^m)$ and $g \in Pol^*_{hom}(\mathbb{F}^m)$ let

$$\Gamma^*(g) := g(\Gamma^1, \cdots, \Gamma^m) \in Pol^*_{hom}(\mathbb{F}^s),$$

$$\Gamma_{pr} := \{[\Gamma^1(\lambda), \cdots, \Gamma^m(\lambda)] \in \mathbb{F}P^{m-1}) |\, \lambda \in \mathbb{F}^s\}.$$

(Thus Γ_{pr} is the projective variety in $\mathbb{F}P^{m-1}$ that is associated with Γ.)

For a given quadruple (s, r, m, d) with $s \le m-1$ we set

$$l_{hom}(s, r, m, d) := \max\{\dim \Gamma^*(Pol^d_{hom}(\mathbb{F}^m)) |\, \Gamma \in (Pol^r_{hom}(\mathbb{F}^s))^m\}.$$

Let

- $I^d_{hom}(\Gamma(\mathbb{F}^s))$ denote the space consisting of all homogeneous polynomials of degree d in the ideal $I(\Gamma(\mathbb{F}^s))$,
- $A^d_{hom}(\Gamma)$ - the quotient space $Pol^d_{hom}(\mathbb{F}^m)/I^d_{hom}(\Gamma(\mathbb{F}^n))$.

Since $I^d_{hom}(\Gamma(\mathbb{F}^n)) = \ker \Gamma^* \cap Pol^d_{hom}(\mathbb{F}^m)$, we have

$$\dim \Gamma^*(Pol^d_{hom}(\mathbb{F}^m)) = \dim A^d_{hom}(\Gamma). \tag{5.1}$$

Note that $\dim A^d_{hom}(\Gamma)$ is equal to the value $h_\Gamma(d)$ of *the Hilbert function of the variety* Γ_{pr} *at* d, see for instance [6, Lecture 13]. Hence it follows from (5.1)

$$l_{hom}(s, r, m, d) = \max\{h_\Gamma(d) |\, \Gamma \in Pol^r_{hom}(\mathbb{F}^s, \mathbb{F}^m)\}. \tag{5.2}$$

Furthermore, we denote by $Pol^{rd}_{hom}(\mathbb{F}^s)$ the linear space of all homogeneous polynomials g of degree rd in $(x_1, \cdots, x_s)$. Then $\Gamma^*(Pol^d_{hom}(\mathbb{F}^m)) \subset Pol^{rd}_{hom}(\mathbb{F}^s)$ for all $\Gamma \in Pol^r_{hom}(\mathbb{F}^s, \mathbb{F}^m)$. Hence we obtain

$$l_{hom}(s, r, m, d) \le \dim Pol^{rd}_{hom}(\mathbb{F}^s) = \binom{rd+s-1}{rd}. \tag{5.3}$$

Problem 1. Find upper bounds for $l_{hom}(r, s, d, m)$ that are better than (5.3). Equivalently, we need to find better upper bounds for $h_\Gamma(d)$ for $\Gamma \in Pol^r_{hom}(\mathbb{F}^s, \mathbb{F}^m)$.

Now assume that f is a homogeneous polynomial mapping from $\mathbb{F}^n$ to $\mathbb{F}^m$, where $m \geq n+1 \geq 2$.

Proposition 5.1. *Let f be a homogeneous polynomial mapping from $\mathbb{F}^n$ to $\mathbb{F}^m$, where $m \geq n+1 \geq 2$. If there exist $s, r, d \geq 1$ such that $h_f(d) \geq l_{hom}(s, r, m, d) + 1$, then f is (s, r)-weakly elusive.*

Proof. Assume that f satisfies the condition of Proposition 5.1. We will show that for any homogeneous mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r the image of f does not lie on the image of Γ. Assume the opposite, i.e. there exists a homogeneous mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r such that $f(\mathbb{F}^n) \subset \Gamma(\mathbb{F}^s)$. Then

$$I_{hom}(\Gamma(\mathbb{F}^s)) \subset I_{hom}(f(\mathbb{F}^n)). \tag{5.4}$$

Let $I^{\perp,d}_{hom}(f(\mathbb{F}^n))$ be a complement of the subspace $I^d_{hom}(f(\mathbb{F}^n))$ in $Pol^d_{hom}(\mathbb{F}^m)$. Since Γ is homogeneous of degree r, using (5.2), we have

$$\dim \Gamma^*(I^{\perp,d}_{hom}(f(\mathbb{F}^n))) \leq \dim \Gamma^*(Pol^d_{hom}(\mathbb{F}^m)) \leq l_{hom}(s, r, m, d). \tag{5.5}$$

Taking into account $\ker \Gamma^* \cap Pol^*_{hom}(\mathbb{F}^m) = I_{hom}(\Gamma(\mathbb{F}^s))$, (5.4) implies that

$$\dim \Gamma^*(I^{\perp,d}_{hom}(f(\mathbb{F}^n))) = \dim A^d_{hom}(f) = h_f(d). \tag{5.6}$$

Clearly (5.5) and (5.6) contradict the assumption of our Proposition. This proves that f is (s, r)-weakly elusive. □

Remark 5.2. The above arguments also apply to the study of (s, r)-elusive functions. We set

$$l(s, r, m, d) := \max\{\dim \Gamma^*(Pol^d_{hom}(\mathbb{F}^m)) | \, \Gamma \in (Pol^r(\mathbb{F}^s))^m\}.$$

The argument in the proof of Proposition 5.1 implies the following assertion. Assume that f is a homogeneous polynomial mapping from $\mathbb{F}^n$ to $\mathbb{F}^m$. If for some $s, r, d \geq 1$ we have $h_f(d) \geq l(s, r, m, d) + 1$ then f is (s, r)-elusive.

We obtain immediately from Proposition 5.1 and Remark 5.2 the following

Corollary 5.3. *Assume that f is a homogeneous polynomial mapping from $\mathbb{F}^n$ to $\mathbb{F}^m$.*

1. If for some $d, s, r \geq 1$ we have $h_f(d) \geq \binom{rd+s-1}{rd}$, then f is (s, r)-weakly elusive.

2. If for some $d, s, r \geq 1$ we have $h_f(d) \geq \binom{rd+s}{rd}$, then f is (s, r)-elusive.

Now we redenote $\binom{n-1+k}{k}$ as $b(n-1+k, k)$.

Example 5.4. Let us consider the Veronese mapping $\nu_k : \mathbb{C}^n \to \mathbb{C}^{b(n-1+k)(k)} = Pol^k_{hom}(\mathbb{C}^n)$ of degree k:

$$\nu_k(x_1, \cdots, x_n) := (x_1^k, x_1^{k-1}x_2, x_1^{k-2}x_2^2, \cdots, x_n^k).$$

It is known that $A^d_{hom}(\nu_k)$ is equal to $Pol^{dk}_{hom}(\mathbb{C}^n)$, see e.g. [6, Example 13.4]. By Corollary 5.3, ν_k is (s, r)-weakly elusive, if for some d we have

$$\binom{dk+n-1}{dk} \geq \binom{rd+s-1}{rd} + 1. \tag{5.7}$$

To apply Corollary 5.3 to solving the question whether a homogeneous polynomial mapping f from $\mathbb{F}^n$ to $\mathbb{F}^m$ is (weakly) elusive, in the first step, we search for an intermediate lower bound for the value $h_f(d)$ of the Hilbert function h_f, where d is some appropriate integer. The following Lemma suggests a way to find such a lower bound.

Lemma 5.5. *Let f be a homogeneous polynomial mapping from $\mathbb{F}^n$ to $\mathbb{F}^m$. Assume that there exists a subspace $\mathcal{L} \subset Pol^d_{hom}(\mathbb{F}^m)$ such that $\ker f^* \cap \mathcal{L} = 0$. Then $h_f(d) \geq \dim \mathcal{L}$.*

Proof. As we have observed above,

$$h_f(d) = \dim f^*(Pol^d_{hom}(\mathbb{F}^m)) \geq \dim f^*(\mathcal{L}) = \dim \mathcal{L}.$$

The last equality holds since $\ker f^* \cap \mathcal{L} = 0$. This proves Lemma 5.5. □

Example 5.6. As an application of Corollary 5.3 and Lemma 5.5 we shall explain Raz's proof of (s,d)-elusiveness of functions constructed in [12, Lemma 4.1]. For an integer k, denote by $[k]$ the set $\{1, \cdots, k\}$. Let $m = n^2$. We identify the set $[m]$ with $[n] \times [n]$ by the lexicographic order. Let $1 \leq d \leq (\log_2 n)/100$ be an integer. Let $d' = 5d$. Let $X = \{x_{i,j}\}_{i \in [d'], j \in [n]}$ be a set of $n \cdot d'$ input variables. For every $(a,b) \in [n] \times [n] = [m]$, define a polynomial

$$f_{(a,b)}(x_{1,1}, \cdots, x_{d',n}) = \Pi_{i \in [d']} x_{i,a+i \cdot b}$$

where the sum $a + i \cdot b$ is taken modulo n. Let

$$f = (f_{(1,1)}, f_{(1,2)}, \cdots, f_{(n,n)}).$$

Raz proved that the polynomial mapping $f : \mathbb{F}^{n \cdot d'} \to \mathbb{F}^m$ is (s,d)-elusive, where $s = \lfloor n^{1+1/(2d)} \rfloor$. In his proof Raz introduced the notion of *a retrievable monomial in $Pol^r_{hom}(\mathbb{F}^m)$*, or equivalently, *a retrievable subset $Q \subset [n] \times [n]$ of size r*. We define a map $R : 2^{[n] \times [n]} \to \mathbb{F}[x_{1,1}, \cdots x_{d',n}]$ as follows

$$R(Q) = f_Q := \Pi_{(a,b) \in Q} f_{a,b} = \Pi_{(a,b) \in Q} \Pi_{i \in [d']} x_{i,a+ib}.$$

Let m_Q denote the monomial $\Pi_{(a,b) \in Q} x_{(a,b)} \in Pol^r_{hom}(\mathbb{F}^m)$. Then $R(Q) = f^*(m_Q)$. A subset $Q \subset [n] \times [n]$ is called *retrievable*, if $R^{-1}(R(Q)) = Q$, or equivalently $(f^*)^{-1}(f^*(m_Q)) = m_Q$. Raz proved the following

Claim R [12, Claim 4.2] The set of retrievable monomials m_Q of degree $r = \lfloor n^{1-1/(2d)} \rfloor$ is at least a half of the set of all monomials in $Pol^r_{hom}(\mathbb{F}^m)$.

Now let $\mathcal{L} \subset Pol^r_{hom}(\mathbb{F}^m)$ be generated by retrievable monomials Q of degree $r = \lfloor n^{1-1/(2d)} \rfloor$. It is not hard to see that $\ker f^* \cap \mathcal{L} = 0$ [12, Claim 4.4]. Consequently, Lemma 5.5 and Claim R yield

$$h_f(r) \geq \dim \mathcal{L} \geq \frac{1}{2} \binom{m}{r}. \tag{5.8}$$

Furthermore, Raz get the following estimates

$$\frac{1}{2}\binom{m}{r} \geq s^r > \binom{rd+s}{rd}. \tag{5.9}$$

Using (5.8), (5.9) and Corollary 5.3.2 we obtain the (s,d)-elusiveness of f.

Thus, to apply the Hilbert function method to the study of (weak) elusiveness of homogeneous polynomial mappings, we need to investigate the following.

Problem 2. For a given $f \in Pol^k_{hom}(\mathbb{F}^n, \mathbb{F}^m)$ find a lower bound for $h_f(d)$.

Problems 1,2 are related to the problems of searching for lower bounds and upper bounds of Hilbert functions. We refer the reader to [14] for an overview of lower bounds and upper bounds of Hilbert functions.

5.2. **(s,r)-weakly elusive subsets and (s,r)-weakly elusive polynomial mappings.** In this subsection, adapting the methods of elusive subsets developed in [8], we reduce the problem of verifying whether a polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$ is (s,r)-weakly elusive, to verifying whether a subset A in the image of $f(\mathbb{F}^n)$ is (s,r)-weakly elusive.

Definition 5.7. A subset $A \subset \mathbb{F}^m$ will be called (s,r)-*weakly elusive*, if A does not lie on the image of any homogeneous polynomial mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r.

In order to prove that f is (s,r)-weakly elusive, it suffices to show the existence of a k-tuple of points in the image of $f(\mathbb{F}^n)$, which is (s,r)-weakly elusive, i.e. it does not lie on the image of any homogeneous polynomial mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r. We regard a k-tuple $S_k = (b_1, \cdots, b_k)$, $b_i \in \mathbb{F}^m$, as an element in $(\mathbb{F}^m)^k = \mathbb{F}^{mk}$.

Recall that we identify $Pol^r_{hom}(\mathbb{F}^s, \mathbb{F}^m)$ with $(Pol^r_{hom}(\mathbb{F}^s)^*)^m$.

Proposition 5.8. *(cf.* [8, Lemma 2.4]*) A tuple $S_k \in (\mathbb{F}^m)^k$ of k points in $\mathbb{F}^m$ is (s,r)-weakly elusive, if and only if S_k does not belong to the image of the evaluation map*

$$Ev^r_{s,m,k} : (Pol^r_{hom}(\mathbb{F}^s)^*)^m \times (\mathbb{F}^s)^k \to \mathbb{F}^{mk},$$

$$[(\tilde{f}_1^*, \cdots, \tilde{f}_m^*), (a_1, \cdots, a_k)] \mapsto (\tilde{f}_1^*(a_1), \cdots, \tilde{f}_m^*(a_k)). \tag{5.10}$$

Proposition 5.8 is proved in the same way as [8, Lemma 2.4], so we omit its proof. (Note that we use here a notation for the evaluation mapping $Ev^r_{s,m,k}$ which seems better than the notation $Ev^k_{r,s,m}$ in [8].)

Remark 5.9. Our introduction of the notion of weakly elusive functions is motivated by the fact that the evaluation map $Ev^r_{s,m,k}$ in Proposition 5.8 is bi-homogeneous with respect to the variables $(\tilde{f}_i^*)$ and the variables (a_i). So

it is easier to handle with the new evaluation map than with the evaluation mapping associated with elusive functions.

Corollary 5.10. *(cf.* [8, Corollary 2.5]*) A polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$ contains an (s,r)-weakly elusive k-tuple, if and only if the subset*

$$\hat{f}^k := f(\mathbb{F}^n) \underbrace{\times \cdots \times}_{k \text{ times}} f(\mathbb{F}^n) \subset \mathbb{F}^{mk}$$

does not belong to the image of the evaluation mapping $Ev^k_{s,r,m}$.

Clearly, the subset $\hat{f}^k$ does not belong to the image of the polynomial map $Ev^r_{s,m,k}$, if the Zariski closure $\overline{\hat{f}^k}$ of $\hat{f}^k$ does not belong to the Zariski closure $\overline{Ev^r_{s,m,k}}$ of the image of $Ev^r_{s,m,k}$. Thus we pose the following problem, whose solution is an important step in proving that a polynomial mapping f is (s,r)-weakly elusive.

Problem 3. Find elements of the ideal of $\overline{Ev^r_{s,m,k}} \subset (\mathbb{F}^m)^k$, i.e. elements in the kernel of the ring homomorphism: $(Ev^r_{s,m,k})^* : \mathbb{F}[x_1, \cdots, x_{mk}] \to \mathbb{F}[y_1, \cdots, y_N]$, $N = m \dim(Pol^r_{hom}(\mathbb{F}^s)^*) + ks$.

Once we find a "witness" W in $\ker(Ev^r_{s,m,k})^*$, we could check if $(f \times_{k\,times} f)^*(W) = 0$. If not, then the polynomial mapping f is (s,r)-weakly elusive.

Problem 3 seems very hard. At the first step we should study property of the ideal of $\overline{Ev^r_{s,m,k}} \subset (\mathbb{F}^m)^k$, which could be sufficient for proving the weak elusiveness of some concrete polynomial mappings f, using Corollary 5.10.

Let us describe the ideal of $\overline{Ev^r_{s,m,k}} \subset (\mathbb{F}^m)^k$. We identify $\mathbb{F}^{mk}$ with $Mat_{mk}(\mathbb{F})$. Formula (5.10) says that for $i \in [1,m]$, $j \in [1,k]$ the (ij)-component of the image of the evaluation mapping $Ev^r_{s,m,k}$ equals $\tilde{f}^*_i(a_j)$. Using the monomial basis for $Pol^r_{hom}(\mathbb{F}^s)$ we represent $\tilde{f}_i$ in coordinates as $(\tilde{f}^\alpha_i)$, $\alpha \in [1, \binom{r+s-1}{r}]$. We also represent α as a multi-index $\alpha = \alpha_1 \cdots \alpha_s$ where $\sum_{q=1}^s \alpha_q = r$. We write $a_j = (a^p_j)$, where $p \in [1,s]$ and $a^p_j \in \mathbb{F}$. Then

$$(\tilde{f}^{\alpha_1 \cdots \alpha_s}_i)^*(a_j) = \sum_\alpha (\tilde{f}^{\alpha_1 \cdots \alpha_s}_i)^*[(a^1_j)^{\alpha_1} \cdots (a^s_j)^{\alpha_s}]. \tag{5.11}$$

(For each j the coordinates $a^1_j, \cdots, a^s_j$ form a basis of $(\mathbb{F}^s)^* = Pol^1_{hom}(\mathbb{F}^s)$. Thus the monomials $\{(a^1_j)^{\alpha_1} \cdots (a^s_j)^{\alpha_s} | \sum_{q=1}^s \alpha_q = r\}$ form a basis of $Pol^r_{hom}(\mathbb{F}^s)$.)

For $r = 1$ we have $Pol^1_{hom}(\mathbb{F}^s)^* = \mathbb{F}^s$ and the evaluation mapping is a quadratic map. Furthermore, the above representation of $Ev^k_{s,1,m}$ is the usual matrix multiplication $Mat_{ms}(\mathbb{F}) \times Mat_{sk}(\mathbb{F}) \to Mat_{mk}(\mathbb{F})$.

The following Proposition is well-known; its proof is based on the fact that the rank of a matrix is equal to the rank of the span of its column vectors and equal to the rank of the span of its line vectors.

Proposition 5.11. *If $s \le \min(k,m)$ then the image of $Ev^1_{s,m,k}$ consists of exactly of matrices of rank at most s in $Mat_{mk}(\mathbb{F})$. If $s \ge \min(k,m)$ then $Ev^1_{s,m,k}$ is surjective.*

Proposition 5.11 tells us that the image of $Ev^1_{s,m,k}$ is a determinantal variety if $s \leq \min(k,m)$. The generators of the ideal $I(Ev^1_{s,m,k}(Mat^s_m \times Mat^s_k))$ are minors of rank $(s+1)\times(s+1)$.

Now let us consider the case $r \geq 1$. Note that

$$Ev^r_{s,m,k}(\tilde{f}^*, a) = Ev^1_{s,m,k} \circ (Id, \nu^k_r)(\tilde{f}^*, a), \tag{5.12}$$

where $\tilde{f}^* \in (Pol^r_{hom}(\mathbb{F}^s)^*)^m$, $a \in (\mathbb{F}^s)^k$ and ν^k_r is the direct sum of k copies of the Veronese map ν_r,

$$\nu^k_r : (\mathbb{F}^s)^k \to (F^{b(s+r-1,s)})^k, (a_1, \cdots, a_k) \mapsto (\nu_r(a_1), \cdots, \nu_r(a_k)).$$

Let us describe the ideal of the image of the polynomial mapping (Id, ν^k_r). It is known that (see e.g. [6, p. 23])

(5.13)

$$I(\nu_r(\mathbb{F}^s)) = \langle (x^{\alpha_1\cdots\alpha_s}x^{\beta_1\cdots\beta_s} - x^{\gamma_1\cdots\gamma_s}x^{\delta_1\cdots\delta_s}) |\, X^\alpha X^\beta = X^\gamma X^\delta \rangle_{\mathbb{F}[x^{\alpha_1\cdots\alpha_s}]}$$

where X^α denotes the monomial $x_1^{\alpha_1}\cdots x_s^{\alpha_s}$ corresponding to the multi-index $\alpha = \alpha_1\cdots\alpha_s$ and $\{x^{\alpha_1\cdots\alpha_s}\}$ is a basis of $\mathbb{F}^{b(s+r-1,s)}$. Next, we observe that

$$I(Id, \nu^k_r)((Pol^r_{hom}(\mathbb{F}^s)^*)^m, (\mathbb{F}^s)^k) = \langle \oplus^k_{i=1} I_i(\nu_r(\mathbb{F}^s)) \rangle.$$

We regard elements of $(Pol^r_{hom}(\mathbb{F}^s)^*)^m$ as matrices over $\mathbb{F}$ of size Sm, $S = \binom{s+r-1}{s}$, and elements of $(\mathbb{F}^S)^k$ as matrices over $\mathbb{F}$ of size Sk. Summarizing we have

$$\ker Ev^r_{s,m,k} = \{\tilde{g} \in Pol^*_{hom}(Mat_{mk}(\mathbb{F})) |\, \tilde{g}([f^{*,l_1\cdots l_s}_j]\cdot[x^{l_1,\cdots l_s}_t]) \in$$
$$I(Id, \nu^k_r)((Pol^r_{hom}(\mathbb{F}^s)^*)^m, (\mathbb{F}^s)^k)\}. \tag{5.14}$$

The identity (5.14) serves as a starting point for our future work on Problem 3.

In what follows we show the existence of many weakly elusive homogeneous polynomial mappings.

Theorem 5.12. *Assume that $s \leq m-1$ and*

$$\binom{n+p-1}{p} \geq \frac{m\binom{s+r-1}{r}}{m-s}. \tag{5.15}$$

If $char(\mathbb{F}) = 0$ or $p \leq char(\mathbb{F}) - 1$, then the image of almost every (i.e., except a subset of codimension at least 1) homogeneous polynomial mapping $P \in Pol^p_{hom}(\mathbb{F}^n, \mathbb{F}^m)$ contains a k-tuple of points in $\mathbb{F}^m$ that is (s,r)-weakly elusive, where $k = \binom{n+p-1}{p}$.

Proof. Assume that $char(\mathbb{F}) = 0$ or $p \leq char(\mathbb{F}) - 1$. In [8, Corollary 2.8] we provided a linear isomorphism

$$I^p_{n,m} : Pol^p_{hom}(\mathbb{F}^n, \mathbb{F}^m) \to \mathbb{F}^{m\cdot b(n+p-1,p)},$$

using the interpolation formula [8, Proposition 2.6], which has the following property. Let $S_{n,p,m} \in \mathbb{F}^{m\cdot b(n+p-1,p)}$ be a tuple of $\binom{n+p-1}{p}$ points in $\mathbb{F}^m$.

Then $(I^p_{n,m})^{-1}(S_{n,p,m})$ is a homogeneous polynomial mapping of degree p from $\mathbb{F}^n$ to $\mathbb{F}^m$ whose image is an algebraic subset of $\mathbb{F}^m$ that contains all the $\binom{n+p-1}{p}$ points of the tuple $S_{n,m,p}$. Thus, to prove Theorem 5.12, it suffices to show that almost every (up to a subset of codimension at least 1) tuple $S_{n,p,m}$ of $\binom{n+p-1}{p}$ points in $\mathbb{F}^m$ is (s,r)-weakly elusive, if (5.15) holds.

We note that

$$\dim[(Pol^r_{hom}(\mathbb{F}^s)^*)^m \times (\mathbb{F}^s)^k] \leq m\binom{s+r-1}{r} + k \cdot s. \tag{5.16}$$

The equality in (5.16) holds if $char(\mathbb{F}) = 0$ or $r \leq char(\mathbb{F}) - 1$. Since the evaluation mapping $Ev^r_{s,m,k}$ is bi-homogeneous of degree $(1,r)$, we derive from (5.16) that the image of the evaluation map $Ev^k_{s,r,m}$ is a subset of codimension at least 1, if we have

$$m\binom{s+r-1}{r} + k \cdot s \leq mk. \tag{5.17}$$

Now assume that (5.15) holds. Then for $k = \binom{n+p-1}{p}$, the condition (5.17) holds. Hence, almost every (except a subset of codimension at least 1) point $\overline{S_{n,p,m}} \in \mathbb{F}^{m\cdot(n+p-1,p)}$ lies outside the image of the evaluation map $Ev^k_{s,r,m}$, or equivalently, by Proposition 5.8, $S_{n,p,m}$ is an (s,r)-weakly elusive tuple of points in $\mathbb{F}^m$. This completes the proof of Theorem 5.12. □

6. Applications

In this section we introduce the notion of a multivariate polynomial that is *homogeneous relative to a subset of its variables* (Definition 6.1, Example 6.2). We associate with each polynomial $\tilde{f}$ that is homogeneous relative to a subset of its variables a series of natural polynomial families of m-tuples of homogeneous polynomials, whose circuit size is bounded from above by the circuit size of $\tilde{f}$ (Proposition 6.4). As a consequence, we estimate from below the circuit size of $\tilde{f}$ in terms of the weak elusiveness of the associated polynomial mapping (Corollary 6.5). For a large class of polynomials $\tilde{f}$ our estimates are non-trivial (Examples 6.6, 6.10.) Using Corollary 6.5, we suggest a method for obtaining lower bounds for the circuit size of the permanent P_n over a field $\mathbb{F}$ of characteristic 0 (Lemmas 6.12, 6.13).

6.1. Polynomial families of m-tuples of homogeneous polynomials associated with a partially homogeneous polynomial.

Definition 6.1. A multivariate polynomial $\tilde{f} \in \mathbb{F}[x_1, \cdots, x_n]$ will be called *homogeneous of degree d relative to a non-empty proper subset $Z = \{x_{k+1}, \cdots, x_{k+l}\}$ of the set of variables $(x_1, \cdots, x_n)$* if

$$f(x_1, \cdots, x_k, \lambda x_{k+1}, \cdots, \lambda x_{k+l}, x_{k+l+1}, \cdots, x_n) = \lambda^d f(x_1, \cdots, x_{k+1}, \cdots, x_{k+l}, \cdots, x_n)$$

for all $\lambda \in \mathbb{F}$.

For a set Z of variables let us denote by $\mathbb{F}\langle Z\rangle$ the vector space over $\mathbb{F}$ whose coordinates are the variables in Z.

Example 6.2. 1. For $i \in [1,n]$ let $Z = Z_i := \{x_{ij} | \, j \in [1,n]\}$. Then the permanent Per_n is homogeneous of degree 1 relative to Z.

2. Let $\tilde{f} \in Pol^r_{hom}(\mathbb{F}\langle Z\rangle)$ and $\tilde{g} \in Pol^*(\mathbb{F}\langle Y\rangle)$. Then $\tilde{g}\cdot\tilde{f}$ is homogeneous of degree r relative to Z.

3. The polynomial $\tilde{f} = x^2 + y^2$ is not homogeneous relative to $Z = \{z\}$.

Now assume that $\tilde{f} \in \mathbb{F}[x_1, \cdots, x_n]$ is a polynomial that is homogeneous of degree r relative to a proper subset Z of its variables. We shall associate with $\tilde{f}$ a series of polynomial families $P_\lambda(\tilde{f})$ of m-tuples of homogeneous polynomials whose circuit size is controlled from above by the circuit size of $\tilde{f}$.

W.l.o.g. we assume that the circuit size $L(\tilde{f})$ of $\tilde{f}$ is larger than $\#(Z)$. Set

$$Z^\perp := \{x_1, \cdots, x_n\} \setminus Z.$$

Since Z is a proper subset, $Z^\perp$ is not empty. Let X be a subset of $Z^\perp$ such that for each $x_i \in X$ the polynomial P has exactly degree 1 in x_i. This set X may be empty and need not to be the subset of all variables x_j of degree 1 in P.

Let

- $Y := Z^\perp \setminus X$;
- $p := \#(X)$, $k := \#(Y)$ and $l := \#(Z)$;
- r: = the total degree of $\tilde{f}$ in Z;
- $m' := \dim Pol^r_{hom}(\mathbb{F}\langle Z\rangle) = \binom{l+r-1}{r}$;
- $m := m'$ if X is an empty set. If not, set $m := p\cdot m'$;
- $h : [1, m'] \to Pol^r_{hom}(\mathbb{F}\langle Z\rangle)$ an ordering of the monomial basis.

Regarding X as a parameter, we shall associate with $\tilde{f}$ a polynomial family of (p-tuples) of homogeneous polynomials in variables Z by specifying the associated polynomial mapping f as follows.

Case 1. Assume that X is an empty set, so $m = m'$. Then $\tilde{f}$ is a polynomial in variables Y, Z. Now we write $\tilde{f}$ as follows

$$\tilde{f}(x_1, \cdots, x_n) := \sum_{q=1}^{m} \tilde{f}_q(Y)h(q),$$

where $\tilde{f}_q \in Pol^*(\mathbb{F}\langle Y\rangle)$. We associate with $\tilde{f}$ the following polynomial mapping $f : \mathbb{F}^k \to Pol^r_{hom}(\mathbb{F}\langle Z\rangle)$:

$$f(\lambda) := \sum_{q=1}^{m} \tilde{f}_q(\lambda)h(q). \tag{6.1}$$

Case 2. Assume that X is not empty, i.e. $p \geq 1$. Let us enumerate the polynomials in the set $\{\frac{\partial\tilde{f}}{\partial x}, x \in X\}$ by $\tilde{f}_1, \cdots, \tilde{f}_p$. For $j \in [1,p]$, we write

$\tilde{f}_j \in Pol^*(\mathbb{F}\langle Y, Z\rangle)$ as follows

$$\tilde{f}_j(Y,Z) := \sum_{q=1}^{m'} \tilde{f}_{j,q}(Y)h(q),$$

where $\tilde{f}_{j,q} \in Pol^*(\mathbb{F}\langle Y\rangle)$. We associate with $\tilde{f}$ the following polynomial mapping $f : \mathbb{F}^k \to (Pol^r_{hom}(\mathbb{F}\langle Z\rangle))^p$:

$$f(\lambda) := (\sum_{q=1}^{m'} \tilde{f}_{1,q}(\lambda)h(q), \cdots, \sum_{q=1}^{m'} \tilde{f}_{p,q}(\lambda)h(q)) \in (Pol^r_{hom}(\mathbb{F}\langle Z\rangle))^p. \tag{6.2}$$

Example 6.3. Let n be a basis parameter. We shall apply the above construction to the permanent Per_n. We fix an additional parameter $2 \leq t \leq n-2$. Then we partition the set of variables $\{x_{ij}, 1 \leq i,j \leq n\}$ of the permanent Per_n into three subsets X, Y, Z as follows

$$X = \{x_{1i},\, i \in [1,n]\},$$

$$Y = \{x_{ui},\, 2 \leq u \leq t,\, i \in [1,n]\},$$

$$Z = \{x_{ui},\, t+1 \leq u \leq n,\, i \in [1,n]\}.$$

- Set $m' := \dim Pol^{n-t}_{hom}(\mathbb{F}\langle Z\rangle) = \binom{(n-t)(n+1)-1}{n-t}$.
- Set $m := n \cdot m'$.
- Let $h : [1,m'] \to Pol^{n-t}_{hom}(\mathbb{F}\langle Z\rangle)$ be an ordering of the monomial basis.

Since $\#(X) = n \geq 1$, we are in the Case 2. We represent the permanent as follows

$$Per_n([x_{ij}]) = \sum_{i=1}^{n} x_{1i} P_{n-1,i}(Y,Z), \tag{6.3}$$

where $P_{n-1,i}(Y,Z) = \frac{\partial Per_n}{\partial x_{1i}}$. For each $i \in [1,n]$ there is a unique decomposition

$$P_{n-1,i}(Y,Z) = \sum_{q=1}^{m'} \tilde{f}_{n-1,i,q}(Y)h(q),$$

where $\tilde{f}_{n-1,i,q} \in Pol^{t-1}_{hom}(\mathbb{F}(\langle Y\rangle))$. Note that $\#(Y) = (t-1)n$. We now associate with the permanent Per_n and with the partition of the variables of Per_n the following polynomial mapping

$$f : \mathbb{F}\langle Y\rangle \to (Pol^{n-t}_{hom}(\mathbb{F}\langle Z\rangle))^n \tag{6.4}$$

by the above recipe. Its i-th component $f_i \in Pol^{n-t}_{hom}(\mathbb{F}\langle Z\rangle)$, for $i \in [1,n]$, is defined as follows (cf. 6.2):

$$f_i(\lambda_{21}, \cdots, \lambda_{tn}) := \sum_{q=1}^{m'} \tilde{f}_{n-1,i,q}(\lambda_{21}, \cdots, \lambda_{tn})h^{-1}(q). \tag{6.5}$$

Now we make another partition of the set of variables $\{x_{ij}, 1 \leq i, j \leq n\}$ of the permanent Per_n into three subsets X', Y', Z', where X' is the empty; in other words, we are in the Case 1. Let

$$Y' := \{x_{ui} | 1 \leq u \leq t,\, i \in [1,n]\},$$
$$Z' := \{x_{ui} |\, u+1 \leq i \leq n,\, i \in [1,n]\}.$$

Note that $\#(Y') = tn$. We associate with the permanent Per_n another family of polynomial mappings $f : \mathbb{F}^{tn} \to Pol^{n-t}_{hom}(\mathbb{F}\langle Z'\rangle)$, using the recipe in (6.1):

$$f(\lambda_{11}, \cdots, \lambda_{tn}) := \sum_{q=1}^{m} \tilde{f}_q(\lambda_{11}, \cdots, \lambda_{tn}) h(q). \tag{6.6}$$

Here $\tilde{f}_q \in Pol^{n-t}_{hom}(\mathbb{F}\langle Y'\rangle)$ is defined uniquely from the equation

$$Per_n(Y', Z') = \sum_{j=1}^{m'} \tilde{f}_{n,j}(Y') h(j).$$

The following Proposition shows that the circuit size of each member in the polynomial families of tuples of homogeneous polynomials of equal degree that is associated with a polynomial f which is homogeneous relative to a subset of its variables is bounded by the circuit size of P.

Proposition 6.4. *1. Let $f : \mathbb{F}^k \to Pol^r_{hom}(\mathbb{F}\langle Z\rangle)$ be the polynomial mapping in (6.1). Then for each $\lambda \in \mathbb{F}^k$ the circuit size of the polynomial $f(\lambda)$ is at most $L(\tilde{f})$.*

2. Let $f : \mathbb{F}^k \to (Pol^r_{hom}(\mathbb{F}\langle Z\rangle)^p$ be the polynomial mapping in (6.2). Then for each $\lambda \in \mathbb{F}^k$ the circuit size of the p-tuple $f(\lambda)$ of homogeneous polynomials of degree r is at most $5L(\tilde{f})$.

Proof. 1. Let us consider the case that f is defined by (6.1). Note that for each $\lambda \in \mathbb{F}^k$, we have

$$f(\lambda)(Z) = \tilde{f}(\lambda, Z) \in Pol^r_{hom}(\mathbb{F}\langle Z\rangle).$$

It follows that the circuit size $L(f(\lambda))$ is at most $L(\tilde{f})$, what is required to prove.

2. By the Baur-Strassen result [1], there exists an arithmetic circuit Φ of size less than $5L(\tilde{f})$ that computes the p-tuple

$$\{\frac{\partial \tilde{f}}{\partial x} |\, x \in X\} = \{\tilde{f}_i(Y, Z) \in Pol^*(\mathbb{F}^*(\langle Y, Z\rangle)) |\, i = [1,p]\}.$$

Note that for any value $\lambda \in \mathbb{F}^k$ we have

$$f(\lambda) = (\tilde{f}_1(\lambda, Z), \cdots, \tilde{f}_p(\lambda, Z)),$$

which is an p-tuple of polynomials in Z of circuit size less than or equal to $Size(\Phi)$. Since $Size(\Phi) < 5L(\tilde{f})$, we obtain

$$L(f(\lambda)) < 5L(\tilde{f}) \text{ for all } \lambda \in \mathbb{F}^k.$$

This completes the proof of Proposition 6.4. □

Combining Proposition 6.4 with Corollary 4.6, we obtain immediately

Corollary 6.5. *1. Assume that the polynomial mapping f defined by the recipe in (6.1) is $(s, 2r-1)$-weakly elusive. Then the circuit size $L(\tilde{f})$ of the associated polynomial $\tilde{f}$ satisfies*

$$L(\tilde{f}) > \frac{\sqrt{s}}{16 \cdot (r+2)^3}.$$

2. Assume that the polynomial mapping f defined in (6.2) is $(s, 2r-1)$-weakly elusive. Then the circuit size $L(\tilde{f})$ of the associated polynomial $\tilde{f}$ satisfies

$$L(\tilde{f}) > \frac{\sqrt{s}}{80 \cdot (r+2)^3}.$$

Example 6.6. Let us consider an example from [12, §3.3, §3.4], which motivates our construction in (6.2). Let $m' := \binom{n+r-1}{r}$ and $m = n \cdot m'$. Assume that we are given $f_{q,i} \in \mathbb{F}[x_1, \cdots, x_n]$, where $q \in [1, m']$ and $i \in [1, n]$. As before, let $h : [1, m'] \to Pol^r_{hom}(\mathbb{F}^n)$ be an ordering of the monomial basis of $Pol^r_{hom}(\mathbb{F}\langle z_1, \cdots, z_n\rangle)$. For $i \in [1, n]$ we define $\tilde{f}_i \in \mathbb{F}[x_1, \cdots, x_n, z_1, \cdots, z_n]$ by

$$\tilde{f}_i(x_1, \cdots, x_n, z_1, \cdots z_n) := \sum_{q=1}^{m'} f_{q,i}(x_1, \cdots, x_n) h(q). \tag{6.7}$$

Let $W := \{w_1, \cdots, w_n\}$ be an additional set of variables. We define $\tilde{f} \in \mathbb{F}[x_1, \cdots, x_n, z_1, \cdots, z_n, w_1, \cdots w_n]$ as follows

(6.8)

$$\tilde{f}(x_1, \cdots, x_n \cdots, y_1, \cdots y_n, z_1, \cdots, z_n) := \sum_{i=1}^{n} w_i \tilde{f}_i(x_1, \cdots x_n, z_1, \cdots, z_n).$$

Note that $\tilde{f}$ is homogeneous of degree r relative to the proper subset $Z := \{z_1, \cdots, z_n\}$. Next we note that $\tilde{f}_i = \frac{\partial \tilde{f}}{\partial w_i}$. Now we construct $f : \mathbb{F}^n \to \mathbb{F}^m$ according to the recipe (6.2):

$$f(\lambda) := (\sum_{q=1}^{m'} f_{q,1}(\lambda), \cdots, \sum_{q+1}^{m'} f_{q,n}(\lambda)).$$

Corollary 6.5.2 implies immediately

Lemma 6.7. *(cf* [12, Corollary 3.8]*) Let $1 \leq r \leq n \leq s$ and $m = n \cdot \binom{n+r-1}{r}$ be integers. Let $f : \mathbb{F}^n \to \mathbb{F}^m$ be a polynomial mapping. If f is $(s, 2r-1)$-weakly elusive, then the circuit size of the polynomial $\tilde{f}$ defined by (6.8) and (6.7) is at least $\frac{\sqrt{s}}{80 \cdot (r+2)^3}$.*

Remark 6.8. Lemma 6.7 is an improvement of [12, Corollary 3.8], which, under the assumption of Lemma 6.7, provides the lower bound $\Omega(\sqrt{s}/r^4)$ for the circuit size of $\tilde{f}$. This lower bound is weaker than our lower bound $(\frac{\sqrt{s}}{80\cdot(r+2)^3})$. Our improvement is due to our upper bound $256 \cdot s^2(r+2)^6$ for the number of of edges leading to the sum-gates in the universal circuit-graph $G_{s,r,n,m}$, see Proposition 3.6, which is better than the upper bound $\Omega(s^2 \cdot r^8)$ obtained by Raz in [12, Proposition 3.3] for the number of the nodes in the universal graph-circuit $G_{s,r,n,n}$.

Corollary 6.9. *Let $char(\mathbb{F}) = 0$. Assume that r grows much slower than n, e.g. $r = const$ or $r = \ln\ln n$. Let $p = (r-1)(2r-1)$. Then there are sequences of polynomials $\tilde{f}_n \in Pol^{p+r+1}_{hom}(\mathbb{F}^{3n})$ whose coefficients are algebraic numbers, such that*

$$L(\tilde{f}_n) \geq (\frac{\lfloor \frac{n}{r(r-1)} \rfloor^{\frac{r-3}{2}}}{80(r+2)^3}).$$

Corollary 6.9 and its proof are almost identical with Corollary 4.12 and its proof in [8], except that the estimate in Corollary 6.9 is better than the one in Corollary 4.12 in [8] (the dominator contains $(r+2)^3$ vs r^4). This improvement is due to Lemma 6.7, which replaces Corollary 3.8 in [12] in the proof of Corollary 4.12 in [8]. We refer the reader to [8] for the proof of [8, Corollary 4.12] and omit the proof of Corollary 6.9.

Example 6.10. Let X, Y be a set of variables and $n_X = \#(X)$, $n_Y = \#(Y)$. We denote by $Pol^{p,q}_{hom}(\mathbb{F}\langle X, Y\rangle)$ the linear subspace of $Pol^{p+q}_{hom}(\mathbb{F}\langle X, Y\rangle)$ consisting of all polynomials which are homogeneous of degree p in X and homogeneous of degree q in Y. For example, the permanent P_n belongs to $Pol^{t,n-t}_{hom}(Y', Z')$, where Y', Z' are defined in Example 6.3. Then each polynomial $\tilde{f} \in Pol^{p,q}_{hom}(X, Y)$ is associated uniquely by the recipe of (6.1) with a homogeneous polynomial mapping $f \in Pol^{p}_{hom}(\mathbb{F}\langle X\rangle, Pol^{q}_{hom}(\mathbb{F}\langle Y\rangle))$. Now assume that $s+1 \leq \binom{n_Y+q-1}{q}$ and

$$\binom{n_X+p-1}{p} \geq \frac{\binom{n_Y+q-1}{q}\binom{s+2q-2}{2q-1}}{\binom{n_Y+q-1}{q} - s}. \tag{6.9}$$

Theorem 5.12 implies that, if $char(\mathbb{F}) = 0$ or $p \leq char(\mathbb{F}) - 1$, almost all polynomial $\tilde{f}$ in $Pol^{p}_{hom}(\mathbb{F}\langle X\rangle, Pol^{q}_{hom}(\mathbb{F}\langle Y\rangle))$ is $(s, 2q-1)$-elusive, and hence, by Corollary 6.5.1 we have

$$L(\tilde{f}) \geq \frac{\sqrt{s}}{16(q+2)^3}. \tag{6.10}$$

Furthermore, assume that $char(\mathbb{F}) = 0$. Then using Proposition 4.5 in [8], adapted to our case of weakly elusive homogeneous polynomial mappings, it is easy to exhibit explicitly infinitely many bi-homogeneous polynomials $\tilde{f} \in Pol^{p,q}_{hom}(\mathbb{F}\langle X, Y\rangle)$ whose monomials coefficients are algebraic numbers

such that $\tilde{f}$ satisfies (6.10), if (6.9) holds. We refer the reader to the proof of Proposition 4.5 in [8] for the method of the proof of this assertion.

6.2. **An approach for obtaining lower bounds for the circuit size of the permanent.** In this subsection we suggest a method for obtaining lower bounds of $L(Per_n)$ using the mappings $f : \mathbb{F}\langle Y\rangle Y \to Pol_{hom}^{n-t}(\mathbb{F}\langle Z\rangle)$ defined in (6.6) that are associated with Per_n. We keep the notations in Example 6.3 and assume that $\mathbb{F}$ is a field of characteristic 0. Recall that Z is a rectangular matrix of size $(n-t)\times n$. Denote by $\bar{P}er_{n,t}(Z)$ the linear subspace of $Pol_{hom}^{n-t}(\mathbb{F}\langle Z\rangle)$ which is generated by the (minor) permanents of size $(n-t)\times(n-t)$ of the matrix Z. Clearly $\dim \bar{P}er_{n,t}(Z) = \binom{n}{n-t}$. Let us denote by $Per_{n,t}(Y,Z)$ the linear subspace in $Pol_{hom}^{t,n-t}(\mathbb{F}\langle Y,Z\rangle)$ consisting of all polynomials P whose associated polynomial mapping $\tilde{P}$ takes values in $\bar{P}er_{n,t}(Z)$. The following Lemma 6.11 infers that to study the weak elusiveness of the polynomial mapping f we need to know the smallest linear subspace in $Pol_{hom}^{n-t}(\mathbb{F}\langle Z\rangle)$ that contains the image of f.

Lemma 6.11. *Assume that $f : \mathbb{F}^n \to \mathbb{F}^m$ is $(s,1)$-weakly elusive and not $(s+1,1)$-weakly elusive, i.e. the linear span of the image of $f(\mathbb{F}^n)$ is a linear subspace $\mathbb{F}^{s+1}$ in $\mathbb{F}^m$. Let $\pi : \mathbb{F}^m \to \mathbb{F}^{s+1}$ be a projection. Then f is (l,r)-weakly elusive, if and only if $\pi\circ f : \mathbb{F}^n \to \mathbb{F}^{s+1}$ is (l,r)-weakly elusive.*

Proof. First let us prove the "only if" assertion. Assume that f is (l,r)-weakly elusive and $\pi\circ f$ is not (l,r)-elusive. Then there exists a homogeneous polynomial mapping $\Gamma : \mathbb{F}^l \to \mathbb{F}^{s+1}$ of degree r such that $\pi\circ f(\mathbb{F}^n)$ lies on the image of $\Gamma(\mathbb{F}^l)$. Let $i : \mathbb{F}^{s+1} \to \mathbb{F}^m$ be the embedding, such that $\pi\circ i = Id$. It follows that $f(\mathbb{F}^n)$ lies on the image of the map $i\circ\Gamma(\mathbb{F}^l)$ of degree r, which contradicts our assumption. This proves the "only if" assertion.

Now let us prove the "if" assertion. Assume that f is not (l,s)-weakly elusive, i.e. the image $f(\mathbb{F}^n)$ belongs to the image $\Gamma(\mathbb{F}^l)$ for some homogeneous polynomial mapping $\Gamma : \mathbb{F}^l \to \mathbb{F}^m$ of degree r. Then the image $\pi\circ f(\mathbb{F}^m)$ belongs to the image of $\pi\circ\Gamma : \mathbb{F}^l \to \mathbb{F}^{s+1}$. Hence $\pi\circ f$ is not (l,s)-elusive. This completes the proof of Lemma 6.11. □

The following Lemma exhibits the smallest linear subspace in $Pol_{hom}^{n-t}(\mathbb{F}\langle Z\rangle)$ that contains the image of f.

Lemma 6.12. *The linear span of $f(\mathbb{F}(\langle Y\rangle)$ is $\bar{P}er_{n,t}(Z)$. Hence f is $(s,1)$-weakly elusive for $s = \binom{n}{n-t} - 1$.*

Proof. Note that the linear span of $f(\mathbb{F}(\langle Y\rangle)$ belongs to $\bar{P}er_{n,t}(Z)$. Now we complete the proof of Lemma 6.12 by observing that all the basis of $\bar{P}er(Z)$ lies on the image of f. □

Let n,t,s be defined as follows

$$n-t = N,\ t = N^3(N-1),\ n = N^4,\ k = constant,\ s = n^k = N^{4k}. \tag{6.11}$$

To obtain a lower bound for the circuit size of Per_n we might prove the weak elusiveness of f associated with $Per_n \in Per_{n,t}(Y,Z)$. The following Lemma says that the polynomial mappings associated with "generic" polynomials in $Per_{n,t}(Y,Z)$ are $(s, n-t)$-weak elusive, and hence the "generic" polynomials have very large circuit size.

Lemma 6.13. *Given any k almost all homogeneous polynomials in $Per_{n,t}(Y,Z)$ has the circuit size at least*

$$\frac{\sqrt{s}}{16\,(n-t+2)^3}$$

if N is sufficient large, since their associated polynomial mappings are $(s, n-t)$ elusive.

Proof. For sufficiently large $N \in \mathbb{N}$, using the Stirling approximation $N! \sim \sqrt{2\pi N}(\frac{N}{e})^N$ we obtain

$$\binom{N^7}{N^3} \geq 2\binom{N^{4k}+2N}{2N}. \tag{6.12}$$

Let (n,t,s) are given as in (6.11). Then (6.12) implies the following inequality

$$\binom{nt+t-1}{t} \geq \frac{\binom{n}{n-t}\binom{s+2(n-t)-2}{2(n-t)}}{\binom{n}{n-t}-s}, \tag{6.13}$$

Theorem 5.12 implies that, the validity of (6.13) implies the density of homogeneous polynomials in $Per_{n,t}(Y,Z)$ that have the circuit size at least $\sqrt{s}/(16\,(n-t+2)^3)$ since their associated polynomial mappings are $(s, n-t)$-elusive. This proves Lemma 6.13. □

Acknowledgements

The author would like to thank Pavel Hrubeš, Partha Mukhopadhyay and Pavel Pudlak for their stimulating discussions, helpful remarks and suggestions, and Ngô Viêt Trung for his illuminating discussion on related problems in commutative algebra. She is grateful to the anonymous referee for valuable suggestions. A part of this paper has been conceived during the author's visit to VNU for Sciences and the Institute of Mathematics of VAST in Hanoi. She would like to thank these institutions for excellent working conditions and financial support.

References

[1] W. Baur, V. Strassen, The Complexity of Partial Derivatives. Theor. Comput. Sci. 22(1983), 317-330.

[2] P. Burgisser, M. Clausen and M. A. Shokrollali, Algebraic Complexity Theory, Springer -Verlag, (1997).

[3] H. Fournier, N. Limaye, G. Malod, and S. Srinivasan, Lower bounds for depth 4 formulas computing iterated matrix multiplication, Electronic Colloquium on Computational Complexity (ECCC), 20:100, 2013.

[4] J. zur Gathen, Feasible Arithmetic Computations: Valiant's Hypothesis, J. Symbolic Computation (1987) 4, 137-172.
[5] G.-M. Greuel and G. Pfister, A SINGULAR Introduction to Commutative Algebra, Springer-Verlag, (2007).
[6] J. Harris, Algebraic Geometry, A First Course, Springer-Verlag, 1993.
[7] K. Kalorkoti, A lower bound for the formula size of rational functions. SIAM Journal of Computing, 14(3):678-687, 1985.
[8] H. V. Lê, Constructing elusive functions with help of evaluation mappings, arXiv:1011.2887
[9] T. Mignon and N. Ressayre, A quadratic bound for the Determinant and Permanent Problem, IMRN 79 (2004), 4241-4253.
[10] K.D. Mulmuley and M. Sohoni, Geometric complexity theory, I, An approach to the P vs. NP and related problems, SIAM J Computing 31 (2001), n.2 , 496-526.
[11] N. Nisan and A. Wigderson, Hardness vs randomness, J. Comput. Syst. Sci., 49(2)(1994), 149-167.
[12] R. Raz, Elusive Functions and Lower Bounds for Arithmetic Circuits, Theory Of Computing Vol. 6, article 7 (2010).
[13] A., Razborov and S. Rudich, Natural proofs, J. Comput. System Sci. 55 (1997), no. 1, part 1, 24-35.
[14] M. Sombera, Bounds for the Hilbert function of polynomial Ideals and for the degrees in the Nullstellensatz, J. P. A. A., 117/118 (1997), 565-599.
[15] A. Shpilka and A. Yehudayoff, Arithmetic Circuits: a survey of recent results and open questions, Foundations and Trends in Theoretical Computer Science: Vol. 5: No 3-4, pp 207-388 (2010).
[16] L.G. Valiant, Completeness classes in algebra, Conference Record of the Eleventh Annual ACM Symposium on Theory of Computing (Atlanta, Ga, 1979), Association for Computing Machinery, New York, (1979), p. 249-261.
[17] L. G. Valiant, Reducibility by Algebraic Projections. In Logic and Algorithmic: an International Symposium held in honor of Ernst Specker, volume 30 of Monographies de lEnseignement Mathemathique, (1982), 365-380.

Institute of Mathematics of ASCR, Zitna 25, 11567 Praha, email: hvle@math.cas.cz

ECCC ISSN 1433-8092
http://eccc.hpi-web.de