LOWER BOUNDS FOR THE CIRCUIT SIZE OF PARTIALLY HOMOGENEOUS POLYNOMIALS

HÔNG VÂN LÊ

Abstract. In this paper we associate to each partially homogeneous multivariate polynomial $f$ over any field 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 also improve estimates in the normal homogeneous-form of an arithmetic circuit obtained by Raz in [9]. Our methods yield non-trivial lower bounds for the circuit size of several classes of multivariate homogeneous polynomials (Examples 4.6, 4.9).

AMSC: 03D15, 68Q17, 13P25

Contents

1. Introduction 2
2. $(s, r)$-weakly elusive polynomial mappings 4
3. How to prove that a polynomial mapping is $(s, r)$-weakly elusive 6
   3.1. Counting the dimension of the space of regular functions 6
   3.2. Recognizing the existence of $(s, r)$-weakly elusive subsets 8
4. Natural polynomial families of $m$-tuples of homogeneous polynomials associated with a partially homogeneous polynomial 12
5. An approach for obtaining lower bounds for the circuit size of the permanent 17
6. Appendix: Normal form of arithmetic circuits and universal circuit-graph 19
Acknowledgements 24
References 24

H.V.L. is supported by RVO: 67985840.
1. Introduction

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

$$\text{Per}_n([x_{ij}]) := \sum_{\sigma \in \Sigma_n} \prod_{i=1}^{n} x_{i\sigma(i)}.$$ 

Finding non-trivial lower bounds for the circuit size or formula size of the permanent $\text{Per}_n$ is a challenging problem in algebraic computational complexity theory, especially in understanding the $VP$ versus $VNP$ problem [2], [3], [12], [10]. It has been pointed out by Mulmuley-Sohoni [8] that a proof of $VP \neq VNP$ which is based on a generic property of $\text{poly}(n)$-definable polynomials will likely fall in the trap of the “natural proof”. On the other hand, proving that a sequence of polynomials of large circuit size (resp. formula size) is $\text{poly}(n)$-definable seems to be equally hard as proving a non-trivial lower bound for the circuit size (resp. the formula size) of the permanent, since the permanent is $VNP$-complete. 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 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 [11], [7], [8]. The determinantal complexity $c_{\text{det}}$, though better understood than the formula size, is still very complicated. The best lower bound $c_{\text{det}}(\text{Per}_n) \geq (n^2/2)$ has been obtained by Mignon and Ressayer [7]. To get the quadratic estimate, Mignon and Ressayer compared the second fundamental form of the hyper-surface $\{\text{det}_m(x) = 0\}$ with that of $\{\text{Per}_n(x) = 0\}$. Mulmuley and Sohoni suggested to use representation theory to obtain lower bounds for $c_{\text{det}}(\text{Per}_n)$ [8].

In [9] 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 $\hat{f} \in \mathbb{F}[x_1, \ldots, x_{3n}]$, whose degree linearly depends on $r$, such that the circuit size $L(\hat{f})$ of $\hat{f}$ is bounded from below by a function of $r$ and $s$. In [6] 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 partially homogeneous polynomial $\hat{f}$ (e.g. the permanent, see also Definition 4.1 below) we construct a polynomial family $P_{\lambda}(\hat{f})$ 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 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, toward to obtaining non-trivial lower bounds for the circuit size of the permanent.

The remainder of our paper is organized as follows. In section 2 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 2.4, Corollary 2.5). In section 3 we propose several algebraic methods for proving that a polynomial mapping is \((s, r)\)-weakly elusive (Proposition 3.1, Corollaries 3.2, 3.7) and consider related problems in commutative geometry (Problems 1, 2, 3, 4). In section 4 we associate to each partially homogeneous polynomial \(\tilde{f}\) 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 \(\tilde{f}\). We present non-trivial examples of our methods (Examples 4.6, 4.9). In section 5 we outline a program for obtaining non-trivial lower bounds for the circuit size of the permanent.

In the appendix we give an improved version of a normal form theorem (Theorem 6.5) as well as an improved version of the existence of a universal circuit-graph (Proposition 6.6), which are originally due to Raz, in the form that is needed for our paper. Our upper bounds for the size of a normal-homogeneous circuit and the size of a universal circuit-graph are considerably better than those ones obtained by Raz (Example 4.6, Lemma 4.7).

**Notations.** In our paper we assume that \(\mathbb{F}\) is an arbitrary field. The space of all (resp. homogeneous) polynomials of degree \(r\) in \(n\) variables over \(\mathbb{F}\) will be denoted by \(\text{Pol}^r(\mathbb{F}^n)\) (resp. \(\text{Pol}^r_{\text{hom}}(\mathbb{F}^n)\)), and the space of all ordered \(m\)-tuples of (resp. homogeneous) polynomials in \(\text{Pol}^r(\mathbb{F}^n)\) (resp. \(\text{Pol}^r_{\text{hom}}(\mathbb{F}^n)\)) will be denoted by \((\text{Pol}^r(\mathbb{F}^n))^m\) (resp. \((\text{Pol}^r_{\text{hom}}(\mathbb{F}^n))^m\)). We denote by \(\text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)\) (resp. \(\text{Pol}^r_{\text{hom}}(\mathbb{F}^n, \mathbb{F}^m)\)) 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 \(\text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)\) as \(\text{Pol}^r(\mathbb{F}^n)^*\). Clearly, there is a natural linear map \(\text{Pol}^r(\mathbb{F}^n) \rightarrow \text{Pol}^r(\mathbb{F}^n)^*\), which is an isomorphism if \(\mathbb{F}\) is a field of characteristic 0. We also note that there is a linear isomorphism \(\text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m) = (\text{Pol}^r(\mathbb{F}^n)^*)^m\). For \(\tilde{f} \in \text{Pol}^r(\mathbb{F}^n)\) we denote by \(\tilde{f}^*\)
2. \((s, r)-WEAKLY ELUSIVE POLYNOMIAL MAPPINGS\)

In this section we introduce the notion of an \((s, r)-weakly elusive polynomial mapping\) (Definition 2.1), which is slightly weaker than the notion of an \((s, r)-elusive polynomial mapping\) introduced by Raz (Example 2.2), see also Remark 3.8.2 in Section 3 for motivation. Then we show how this notion is useful for obtaining lower bounds for the circuit size of a polynomial family of \(m\)-tuples of homogeneous polynomials (Proposition 2.4, Corollary 2.5). The key notion is a polynomial family of \(m\)-tuples of homogeneous polynomials of equal degree (Definition 2.3).

**Definition 2.1.** (cf. [9, 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 [9, Definition 1.1] only in the requirement that \(\Gamma\) 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 2.2.**

1. Any \((s, r)-elusive polynomial mapping is \((s, r)-weakly elusive.\)

2. The curve \((1, x, \ldots, x^m) \in \mathbb{R}^{m+1}\) 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 is useful, when we want to verify, whether a polynomial family of \(m\)-tuples of homogeneous polynomials of equal degree has uniformly bounded circuit size.

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

**Definition 2.3.** 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 $P_\lambda$.

**Proposition 2.4.** Let $Z = \{z_1, \ldots, z_n\}$ be a set of variables and $1 \leq n, m \leq s$. Assume that $P_\lambda \in (\text{Pol}_{\text{hom}}(\mathbb{F}(\langle Z \rangle)))^m$, $\lambda \in \mathbb{F}^k$, is a polynomial family of $m$-tuples of homogeneous polynomials of degree $r$ such that for each $\lambda \in \mathbb{F}^k$ the circuit size of $P_\lambda$ is at most $L$. Then the associated polynomial mapping $f$ is not $(s, 2r - 1)$-weakly elusive for any $s \geq s_0 := 64 \cdot L^2 \cdot r^3$.

**Proof.** Let $s$ be an integer as in Proposition 2.4. To prove Proposition 2.4 it suffices to show the existence of a homogeneous polynomial mapping of degree $(2r - 1)$

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

such that

$$
(2.1) \quad f(\mathbb{F}^k) \subset \Gamma_G(\mathbb{F}^s).
$$

We shall construct a polynomial mapping $\Gamma_G$ satisfying (2.1) with help of Proposition 6.6. By Proposition 6.6, 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 $y_1, \ldots, y_s$, where $s \leq s_0$. We label the other edges of $G_{L,r,n,m}$ with the field element 1, see Remark 6.7. Now we define $\Gamma_G$ to be the polynomial mapping in the variables $y_1, \ldots, y_s$ such that

$$
(\alpha_1, \ldots, \alpha_s) = (g_1, \ldots, g_m)
$$

where $(g_1, \ldots, g_m)$ 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 $i \in [1, s]$. (Thus $\Gamma_G$ depends only on $l$ variables.) An examination $\Gamma_G$ based on the description of $G_{s,r,n,m}$ in the proof of Theorem 6.5 using the same argument in the proof of [9, Proposition 3.2]) for the special case $m = n$, shows that the polynomial mapping $\Gamma_G$ is homogeneous of degree $2r - 1$. (More precisely, for a node $v \in G_{L,r,n,m}$ denote the polynomial $g_v \in \mathbb{F}[z_1, \ldots, z_n, y_1, \ldots, y_s]$ that is computed by the node $v$ and is regarded as polynomial in $[z_1, \ldots, z_n]$ with coefficients in $\mathbb{F}[y_1, \ldots, y_s]$. Then $g_v$ is homogeneous of degree $2r_v - 1$ in variables $y_1, \ldots, y_s$ if $v$ is a sum-gate of syntactic degree $r_v$; and $g_v$ is homogeneous of degree $2r_v - 2$ in variables $y_1, \ldots, y_s$ if $v$ is a product-gate of syntactic degree $r_v$.) By the assumption of Proposition 2.4 for any $\lambda \in \mathbb{F}^k$, the circuit size of $f(\lambda)$ is at most $L$. Taking into account Proposition 6.6 there exists $\alpha \in \mathbb{F}^s$ such that $f(\lambda) = \Gamma_G(\alpha)$. This proves (2.1) and completes the proof of Proposition 2.4. \qed
Corollary 2.5. Let \( P_\lambda \in (\text{Pol}_{\text{hom}}(\mathbb{F}^n))^m \), \( \lambda \in \mathbb{F}^k \), be a polynomial family of \( m \)-tuples of homogeneous polynomials of degree \( r \) and \( f : \mathbb{F}^k \to (\text{Pol}_{\text{hom}}(\mathbb{F}^n))^m \) its associated polynomial mapping. Assume that \( f \) is \((s, 2r - 1)\)-weakly elusive. Then \( P_\lambda \) has a member with circuit size greater than or equal to \( \sqrt{\frac{7}{8r^3}} \).

Proposition 2.4 crystallizes some arguments in Raz’s proof of [9, Proposition 3.7]. In Proposition 4.4 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 2.4 or its equivalent version Corollary 2.5 for estimating from below the circuit size \( L(\tilde{f}) \).

3. How to prove that a polynomial mapping is \((s, r)\)-weakly elusive

Given \( f \in \text{Pol}^k(\mathbb{F}^n, \mathbb{F}^m) \) 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 3.1, Corollaries 3.2, 3.7). 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 \( \text{Pol}^p_{\text{hom}}(\mathbb{F}^n, \mathbb{F}^m) \) (Theorem 3.10). We also pose some problems in commutative algebra (Problems 1, 2, 3, 4) whose solutions would advance the proposed methods.

3.1. Counting the dimension of the space of regular functions.
For a given quadruple \((s, r, m, d)\) with \( s \leq m - 1 \) let us denote by

- \( L_{\text{hom}}(s, r, m, d) \) the set of all homogeneous polynomials \( \tilde{g} \) on \( \mathbb{F}^s \) which can be written as

\[
\tilde{g} = \Gamma^s(\tilde{f}) \quad \text{(i.e., } \tilde{g}(y) = \tilde{f}(\Gamma(y)) \text{ for all } y \in \mathbb{F}^s)\),
\]

for some \( \tilde{f} \in \text{Pol}^d_{\text{hom}}(\mathbb{F}^m) \) and for some \( \Gamma \in \text{Pol}^r_{\text{hom}}(\mathbb{F}^s, \mathbb{F}^m) \).
- \( L_{\text{hom}}(s, r, m, d) \) the subset in \( L(s, r, m, d) \) consisting of those \( g \) defined by (3.1) where \( f \in \text{Pol}^d_{\text{hom}}(\mathbb{F}^m) \);
- \( l_{\text{hom}}(s, r, m, d) := \max\{\dim \Gamma^s(\text{Pol}^d_{\text{hom}}(\mathbb{F}^m)) | \Gamma \in \text{Pol}^r_{\text{hom}}(\mathbb{F}^s, \mathbb{F}^m)\} \).
**Pol** \(_d\) \(_{hom}(\mathbb{F}^s)\) the linear space of all homogeneous polynomials \(g\) of degree \(rd\) in \((x_1, \cdots, x_s)\).

In this subsection we assume that \(f\) is a polynomial mapping from \(\mathbb{F}^n\) to \(\mathbb{F}^m\), where \(m \geq n + 1 \geq 2\). Denote by \(A_{hom}^d(f)\) the quotient space \(Pol_{hom}^d(\mathbb{F}^m)/I_{hom}^d(f(\mathbb{F}^n))\), where \(I_{hom}^d(f(\mathbb{F}^n))\) consists of all homogeneous polynomials of degree \(d\) in the ideal \(I(f(\mathbb{F}^n))\). If \(f\) is homogeneous, then \(\dim A_{hom}^d(f)\) is the value of the Hilbert function of the projectivization of \(f(\mathbb{F}^n)\) at \(d\).

**Proposition 3.1.** Assume that for some \(d \geq 1\) we have \(\dim A_{hom}^d(f) \geq l_{hom}(s, r, m, n) + 1\). Then \(f\) is \((s, r)\)-weakly elusive.

**Proof.** Assume that \(f\) satisfies the condition of Proposition 3.1. 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 \(\Gamma\). 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

\[(3.2) \quad I_{hom}(\Gamma(\mathbb{F}^s)) \subset I_{hom}(f(\mathbb{F}^n)).\]

Let \(I_{hom}^{\perp, d}(f(\mathbb{F}^n))\) be a complement of the subspace \(I_{hom}^d(f(\mathbb{F}^n))\) in \(Pol_{hom}^d(\mathbb{F}^m)\).

Since \(\Gamma\) is homogeneous of degree \(r\) we have

\[(3.3) \quad \dim \Gamma^*(I_{hom}^{\perp, d}(f(\mathbb{F}^n))) \leq \dim \Gamma^*(Pol_{hom}^d(\mathbb{F}^m)) \leq \dim Pol_{hom}^d(\mathbb{F}^s).\]

Taking into account \(\ker \Gamma^* \cap Pol_{hom}^d(\mathbb{F}^m) = I_{hom}(\Gamma(\mathbb{F}^s))\), (3.2) implies that

\[(3.4) \quad \dim \Gamma^*(I_{hom}^{\perp, d}(f(\mathbb{F}^n))) = \dim A_{hom}^d(f).\]

Clearly (3.3) and (3.4) contradict the assumption of our Proposition. This proves that \(f\) is \((s, r)\)-weakly elusive. □

**Corollary 3.2.** Assume that for some \(d, s, r, n, m \geq 1\) we have \(\dim A_{hom}^d(f) \geq \dim Pol_{hom}^d(\mathbb{F}^s)\). Then \(f\) is \((s, r)\)-weakly elusive.

**Example 3.3.** Let us consider the Veronese mapping \(\nu_k : \mathbb{C}^n \to \mathbb{C}^{(n-1+k)^k} = Pol_{hom}^k(\mathbb{C}^n)\) of degree \(k\):

\[\nu_k(x_1, \cdots, x_n) = (x_1^k, x_1 x_2^{k-1}, \cdots, x_n^k).\]

It is known that \(A_{hom}^d(\nu_k)\) is equal to \(Pol_{hom}^d(\mathbb{C}^n)\), see e.g. [4, Example 13.4]. By Proposition 3.1, \(\nu_k\) is \((s, r)\)-weakly elusive, if

\[(3.5) \quad \binom{dk + n - 1}{dk} \geq \binom{rd + s - 1}{rd} + 1 \quad \text{for some } d.\]
Remark 3.4. The method presented in this subsection formalizes a Raz’s argument in his proof of Lemma 4.1 in [9]. Using a statement, which is a prototype of Corollary 3.2, Raz constructed \((s, r)-elusive\) polynomial mappings \(f : \mathbb{F}^n \rightarrow \mathbb{F}^n^2\) of degree less than \((\ln n)/20\), where \(s = n^c, r = n^d\) and \(0 < c, d < 1\). As a consequence, Raz obtained non-trivial lower bounds for the size of arithmetic circuits with constant depth computing certain homogeneous polynomials [9, Corollary 4.6]. Proposition 3.1 has limitation (in particular, the \((s, r)-elusiveness\) of the polynomial mappings obtained by Raz are not strong enough to obtain a non-trivial lower bound for the circuit size of considered polynomials), because, in particular, the dimension of \(\text{Pol}_{\text{hom}}^d(\mathbb{F}^n)\) is larger than the dimension of \(\text{Pol}_{\text{hom}}^d(\mathbb{F}^m)\) for the parameters \((n, m, s, r)\) we are interested in, namely for obtaining non-trivial lower bounds for the circuit size of the permanent, as we shall explain in the next section. One also verifies that, (3.5) does not imply a non-trivial lower bound for the circuit size of associated polynomials based on the methods in [9].

Problem 1. Find upper bounds for \(l_{\text{hom}}(r, s, d, m)\) that are better than \(\text{dim Pol}_{\text{hom}}^d(\mathbb{F}^r)\).

Problem 2. For a given \(f \in \text{Pol}_{\text{hom}}^k(\mathbb{F}^n, \mathbb{F}^m)\) find lower bound for \(\text{dim } A^d(f)\).

3.2. Recognizing the existence of \((s, r)-weakly elusive subsets.\)

In this subsection, following [6], we reduce the problem of verifying whether a polynomial mapping \(f : \mathbb{F}^n \rightarrow \mathbb{F}^m\) 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 3.5. 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 \(\Gamma : \mathbb{F}^s \rightarrow \mathbb{F}^m\) 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 \(\Gamma : \mathbb{F}^s \rightarrow \mathbb{F}^m\) of degree \(r.\) We identify a \(k\)-tuple \(S_k = (b_1, \cdots, b_k), b_i \in \mathbb{F}^m,\) with the point \(\bar{S}_k \in \mathbb{F}^{mk}\) via the identification \(\mathbb{F}^m \times_k \mathbb{F}^m = \mathbb{F}^{mk}.\)

Recall that we identify \(\text{Pol}_{\text{hom}}^r(\mathbb{F}^s, \mathbb{F}^m)\) with \((\text{Pol}_{\text{hom}}^r(\mathbb{F}^s))^m.\)

Proposition 3.6. (cf. [6, Lemma 2.4]) A tuple \(S_k\) of \(k\) points in \(\mathbb{F}^m\) is \((s, r)-weakly elusive, if and only if \(\bar{S}_k\) does not belong to the image
of the evaluation map

\[
Ev^r_{s,m,k} : (\text{Pol}_{\text{hom}}^r(F_s)^*)^m \times (F^s)^k \to F^{mk},
\]

(3.6) \( (\tilde{f}_1^*, \ldots, \tilde{f}_m^*, (a_1, \ldots, a_k)) \mapsto (\tilde{f}_1^*(a_1), \ldots, \tilde{f}_m^*(a_k)). \)

Proposition 3.6 is proved in the same way as [6, 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 is slightly different from that one in [6].)

Corollary 3.7. (cf. [6, Corollary 2.5]) A polynomial mapping \( f : F^n \to F^m \) contains an \((s, r)\)-weakly elusive \( k \)-tuple, if and only if the subset

\[ \hat{f}^k := f(F^n) \times_{k \text{ times}} f(F^n) \subset F^{mk} \]

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.

Remark 3.8. Our introduction of the notion of weakly elusive functions is motivated by the fact that the associated evaluation map in Proposition 3.6 is bi-homogeneous and easier to handle than the evaluation mapping associated with elusive functions.

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

Once we find a “witness” \( W \) in \( \ker(Ev^r_{s,m,k})^* \), we could check if \( (f \times_{k \text{ times}} f)^r(W) = 0 \). 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 \( \overline{Ev^r_{s,m,k}} \subset (F^m)^k \), which could be sufficient for proving the weak elusiveness of some concrete polynomial mappings \( f \), using Corollary 3.7. For instance, we could study

Problem 4. Find an upper bound for the minimal degree of a polynomial in \( \ker(Ev^r_{s,m,k})^* \). (We can get abound for degree of the image of the evaluation mapping using the discussion below).

Let us describe the ideal of \( \overline{Ev^r_{s,m,k}} \subset (F^m)^k \). We identify \( F^{mk} \) with \( \text{Mat}_{mk}(F) \). Formula (3.7) 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
Using the monomial basis for \( Pol_{\text{hom}}^k(\mathbb{F}^s) \) we represent \( \tilde{f}_i \) in coordinates as \((\tilde{f}_i^s), \alpha \in [1, \binom{s+r+s-1}{r}] \). We also represent \( \alpha \) as a multi-index \( \alpha = \alpha_1 \cdots \alpha_s \) where \( \sum_{q=1}^s \alpha_q = r \). We write \( a_j = (a_j^p), p \in [1, s] \).

Then
\[
\tilde{f}_i^{s, \alpha_1 \cdots \alpha_s}(a_j) = \sum_{\alpha} \tilde{f}_i^{s, \alpha_1 \cdots \alpha_s}(a_j^1)^{\alpha_1} \cdots (a_j^s)^{\alpha_s}.
\]

For \( r = 1 \) we have \( Pol_{\text{hom}}^1(\mathbb{F}^s) = \mathbb{F}^s \) and the evaluation mapping is a quadratic map and the above representation of \( Ev_{s,1,m}^k \) is the usual matrix multiplication \( \text{Mat}_{ms}(\mathbb{F}) \times \text{Mat}_{sk}(\mathbb{F}) \rightarrow \text{Mat}_{mk}(\mathbb{F}) \).

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 3.9.** If \( s \leq \min(k, m) \) then the image of \( Ev_{s,m,k}^1 \) consists of exactly of matrices of rank at most \( s \) in \( \text{Mat}_{mk}(\mathbb{F}) \). If \( s \geq \min(k, m) \) then \( Ev_{s,m,k}^1 \) is surjective.

Proposition 3.9 tells us that the image of \( Ev_{s,m,k}^1 \) is a determinantal variety if \( s \leq \min(k, m) \). The generators of the ideal \( I(Ev_{s,m,k}^1(\text{Mat}_{m}^k \times \text{Mat}_{s}^k)) \) are minors of rank \((s+1) \times (s+1)\).

Now let us consider the case \( r \geq 1 \). Note that
\[
Ev_{s,m,k}^r(f^s, a) = Ev_{s,m,k}^1(id, \nu_r^k)(f^s, a),
\]
where \( f^s \in (Pol_{\text{hom}}^r(\mathbb{F}^s)^*)^m, a \in (\mathbb{F}^s)^k \) and \( \nu_r^k \) is the sum of \( k \) copies of the Veronese map \( \nu_r \):
\[
\nu_r^k : (\mathbb{F}^s)^k \rightarrow (F^{(s+r-1)})^k, (a_1, \cdots, a_k) \mapsto (\nu_r(a_1), \cdots, \nu_r(a_k)).
\]

Let us describe the ideal of the image of the polynomial mapping \( (id, \nu_r^k) \). It is known that (see e.g. [1], p. 23)
\[
I(\nu_r(\mathbb{F}^s)) = \langle (x_1^{\alpha_1} \cdots x_s^{\alpha_s} \cdot x_1^{\beta_1} \cdots x_s^{\beta_s} - x_1^{\gamma_1} \cdots x_s^{\gamma_s} x_1^{\delta_1} \cdots x_s^{\delta_s}) \mid X^{\alpha} X^{\beta} = X^{\gamma} X^{\delta} \rangle_{F[x_1^{\alpha_1} \cdots x_s^{\alpha_s}]}
\]
where \( X^{\alpha} \) denotes the monomial \( x_1^{\alpha_1} \cdots x_s^{\alpha_s} \) corresponding to the multi-index \( \alpha = \alpha_1 \cdots \alpha_s \) and \( \{x_1^{\alpha_1} \cdots x_s^{\alpha_s}\} \) is a basis of \( \mathbb{F}^{(s+r-1)} \). Next, we observe that
\[
I(id, \nu_r^k)((Pol_{\text{hom}}^r(\mathbb{F}^s)^*)^m, (\mathbb{F}^s)^k) = \langle \bigoplus_{i=1}^k I_i(\nu_r(\mathbb{F}^s)) \rangle.
\]

We regard elements of \( (Pol_{\text{hom}}^r(\mathbb{F}^s)^*)^m \) 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
\[
\ker Ev_{s,m,k}^r = \{ \tilde{g} \in Pol_{\text{hom}}^r(\text{Mat}_{mk}(\mathbb{F})) \mid \tilde{g}([f_j^{s,l_{1,\cdots,l_s}}] \cdot [x_i^{l_{1,\cdots,l_s}}]) \in I(id, \nu_r^k)((Pol_{\text{hom}}^r(\mathbb{F}^s)^*)^m, (\mathbb{F}^s)^k) \}
\]

(3.10)
In what follows we show the effectiveness of the recognizing method in the sense that, using it, we could discover many weakly elusive homogeneous polynomial mappings.

**Theorem 3.10.** Assume that $s \leq m - 1$ and

$$\binom{n + p - 1}{p} \geq \frac{m(s + r - 1)}{m - s}. \quad (3.11)$$

If $\text{char}(\mathbb{F}) = 0$ or $p \leq \text{char}(\mathbb{F}) - 1$, then the image of almost every (i.e., except a subset of codimension at least 1) homogeneous polynomial mapping $P \in \text{Pol}_p^{\text{hom}}(\mathbb{F}^n, \mathbb{F}^m)$ 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 $\text{char}(\mathbb{F}) = 0$ or $p \leq \text{char}(\mathbb{F}) - 1$. In [6, Corollary 2.8] we provided a linear isomorphism

$$I_{n,m}^p : \text{Pol}_p^{\text{hom}}(\mathbb{F}^n, \mathbb{F}^m) \to \mathbb{F}^m(n + p - 1),$$

using the interpolation formula [6, Proposition 2.6], which has the following property. Let $S_{n,p,m} \in \mathbb{F}^m(n + p - 1)$ be identified with the associated tuple $S_{n,p,m}$ of $(n + p - 1)$ points in $\mathbb{F}^m$ as above. Then the image of the polynomial mapping $(I_{n,m}^p)^{-1}(S_{n,p,m})$ in $\mathbb{F}^m$ contains the associated tuple $S_{n,p,m}$ of $(n + p - 1)$ points in $\mathbb{F}^m$. Thus, to prove Theorem 3.10 it suffices to show that almost every (up to a subset of codimension at least 1) tuple $S_{n,p,m}$ of $(n + p - 1)$ points in $\mathbb{F}^m$ is $(s, r)$-weakly elusive, if $\text{char}(\mathbb{F}) = 0$ or $p \leq \text{char}(\mathbb{F}) - 1$.

Next, we note that

$$\dim[(\text{Pol}_r^{\text{hom}}(\mathbb{F}^s)^s) \times (\mathbb{F}^s)^k] \leq m\binom{s + r - 1}{r} + k \cdot s. \quad (3.12)$$

The equality in (3.12) holds if $\text{char}(\mathbb{F}) = 0$ or $r \leq \text{char}(\mathbb{F}) - 1$. Since the evaluation mapping $E_{s,m,k}$ is bi-homogeneous of degree $(1, r)$, we derive from (3.12) that the image of the evaluation map $E_{s,m,k}^k$ is a subset of codimension at least 1, if we have

$$m\binom{s + r - 1}{r} + k \cdot s \leq mk. \quad (3.13)$$

Now assume that $\text{char}(\mathbb{F}) = 0$ or $p \leq \text{char}(\mathbb{F}) - 1$. Then for $k = \binom{n + p - 1}{p}$, the condition (3.13) holds. Hence, almost every (except a subset of codimension at least 1) point $S_{n,p,m} \in \mathbb{F}_m(n + p - 1)$ lies outside the image of the evaluation mapping.
map $E_{r,m}$, or equivalently, by Proposition 3.6, $S_{n,p,m}$ is an $(s,r)$-weakly elusive tuple of points in $\mathbb{F}^m$. This completes the proof of Theorem 3.10.

4. Natural polynomial families of $m$-tuples of homogeneous polynomials associated with a partially homogeneous polynomial

In this section we introduce the notion of a partially homogeneous multivariate polynomial (Definition 4.1, Example 4.2). We associate with each partially homogeneous polynomial $\tilde{f}$ 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 4.4, Example 4.3). As a consequence, we estimate from below the circuit size of a partially homogeneous polynomial $\tilde{f}$ in terms of the weak elusiveness of the associated polynomial mapping (Corollary 4.5). For a large class of homogeneous polynomials, our estimates are non-trivial (Examples 4.6, 4.9.)

**Definition 4.1.** A multivariate polynomial $\tilde{f} \in \mathbb{F}[x_1, \cdots, x_n]$ will be called *partially homogeneous*, if there exists a non-empty proper subset $Z$ of the set of variables $(x_1, \cdots, x_n)$ such that $\tilde{f}$ is homogeneous in $Z$.

**Example 4.2.** 1. For $i \in [1,n]$ let $Z_i := \{x_{ij} | j \in [1,n]\}$. Then the permanent $P_n$ is homogeneous in $Z$ of degree 1.

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

3. The polynomial $\tilde{f} = x^2 + y^2$ is not partially homogeneous.

Now assume that $\tilde{f} \in \mathbb{F}[x_1, \cdots, x_n]$ is a partially homogeneous polynomial that is homogeneous of degree $r$ in 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

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

Note that $Z^\perp$ 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

- $Y := Z^\perp \setminus X$;
THE CIRCUIT SIZE OF PARTIALLY HOMOGENEOUS POLYNOMIALS

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

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

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

where $\tilde{f}_q \in \text{Pol}^*(\mathbb{F}(Y))$. We define a polynomial mapping $f : \mathbb{F}^k \to \text{Pol}_{\text{hom}}^r(\mathbb{F}(Z))$ by

$$(4.1) \quad f(\lambda) := \sum_{q=1}^{m} \tilde{f}_q(\lambda) h(q).$$

Case 2. Assume that $X$ is not empty, i.e. $p \geq 1$. Let us enumerate the polynomials in the set $\{ \frac{\partial}{\partial x}, x \in X \}$ by $\tilde{f}_1, \ldots, \tilde{f}_p$. For $j \in [1, p]$, we write $\tilde{f}_j \in \text{Pol}^*(\mathbb{F}(Y, Z))$ as follows

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

where $\tilde{f}_{j,q} \in \text{Pol}^*(\mathbb{F}(Y))$. We define a polynomial mapping $f : \mathbb{F}^k \to (\text{Pol}_{\text{hom}}^r(\mathbb{F}(Z)))^p$ by

$$(4.2) \quad f(\lambda) := (\sum_{q=1}^{m'} \tilde{f}_{1,q}(\lambda) h(q), \ldots, \sum_{q=1}^{m'} \tilde{f}_{p,q}(\lambda) h(q)) \in (\text{Pol}_{\text{hom}}^r(\mathbb{F}(Z)))^p.$$

Example 4.3. Let $n$ be a basis parameter. We shall apply the above construction to the permanent $\text{Per}_n$. 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 $\text{Per}_n$ 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 $m' := \dim \text{Pol}_{\text{hom}}^{n-t}(\mathbb{F}(Z)) = \binom{n-t(n+1)-1}{n-t}$.
- Set $m := n \cdot m'$.
Let \( h : [1, m'] \to \text{Pol}_{\text{hom}}^{n-t}(\mathbb{F}(Z)) \) be an ordering of the monomial basis.

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

\[
\text{Per}_n([x_{ij}]) = \sum_{i=1}^{n} x_{1i} P_{n-1,i}(Y, Z),
\]

where \( P_{n-1,i}(Y, Z) = \frac{\partial \text{Per}_n}{\partial x_{1i}}. \) 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 \( \tilde{f}_{n-1,i,q} \in \text{Pol}_{\text{hom}}^{n-1}(\mathbb{F}(\langle Y \rangle)). \) Note that \(#(Y) = (t-1)n. \) We define a polynomial mapping

\[
f : \mathbb{F}^{(t-1)n} \to (\text{Pol}_{\text{hom}}^{n-t}(\mathbb{F}(Z)))^n
\]

by determining its \( i \)-th component \( f_i \in \text{Pol}_{\text{hom}}^{n-t}(\mathbb{F}(Z)), \) for all \( i \in [1, n], \) as follows (cf. 4.2)

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

Now we make another partition of the set of variables \( \{x_{ij}, 1 \leq i, j \leq n\} \) of the permanent \( \text{Per}_n \) 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 attach to the permanent \( \text{Per}_n \) another family of polynomial mappings \( f : \mathbb{F}^{tn} \to \text{Pol}_{\text{hom}}^{n-t}(\mathbb{F}(Z')), \) using the recipe in [1,2]:

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

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

\[
\text{Per}_n(Y', Z') = \sum_{j=1}^{m'} \tilde{f}_{n,j}(Y') h(j).
\]
The following Proposition shows that the circuit size of the polynomial families of tuples of homogeneous polynomials of equal degree associated with a partially homogeneous polynomial $P$ is bounded by the circuit size of $P$.

**Proposition 4.4.** 1. Let $f : \mathbb{F}^k \rightarrow Pol_{\text{hom}}^r(\mathbb{F}(\langle Z \rangle))$ be the polynomial mapping in (4.1). Then for each $\lambda \in \mathbb{F}^k$ the circuit size of the polynomial $f(\lambda)$ is at most $L(\tilde{f})$.

2. Let $f : \mathbb{F}^k \rightarrow (Pol_{\text{hom}}^r(\mathbb{F}(\langle Z \rangle)))^p$ be the polynomial mapping in (4.2). 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 (4.1). Note that for each $\lambda \in \mathbb{F}^k$, we have $f(\lambda) = \tilde{f}(\lambda, Z) \in Pol_{\text{hom}}^r(\mathbb{F}(\langle Z \rangle))$. 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 $\Phi$ of size less than $5L(\tilde{f})$ that computes the $p$-tuple $\\{\frac{\partial \tilde{f}}{\partial x} | x \in X\} = \{\tilde{f}_i(Y, Z) \in Pol^r(\mathbb{F}^*(\langle Y, Z \rangle)) | i = [1, p]\}$. Note that for any value $\lambda \in \mathbb{F}^k$ we have $f(\lambda) = (\tilde{f}_1(\lambda, Z), \ldots, \tilde{f}_p(\lambda, Z))$, which is an $p$-tuple of polynomials in $Z$ of circuit size less than or equal to $\text{Size}(\Phi)$. Since $\text{Size}(\Phi) < 5L(\tilde{f})$, we obtain $L(f(\lambda)) < 5L(\tilde{f})$ for all $\lambda \in \mathbb{F}^k$.

This completes the proof of Proposition 4.4. □

Combining Proposition 4.4 with Corollary 2.5, we obtain immediately

**Corollary 4.5.** 1. Assume that the polynomial mapping $f$ defined by the recipe in (4.1) is $(s, 2r-1)$-weakly elusive. Then the circuit size $L(\tilde{f})$ of the associated polynomial tildef satisfies

$$L(\tilde{f}) > \frac{\sqrt{s}}{8 \cdot r^{3/2}}.$$  

2. Assume that the polynomial mapping $f$ defined in (4.2) is $(s, 2r-1)$-weakly elusive. Then the circuit size $L(\tilde{f})$ of the associated polynomial
\[ \tilde{f} \text{ satisfies } \]
\[ L(\tilde{f}) > \frac{\sqrt{s}}{40 \cdot r^{3/2}}. \]

**Example 4.6.** Let us consider an example from [9, §3.3, §3.4], which motivates our construction in (4.2). 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 \( h : [1, m'] \rightarrow Pol_{\text{hom}}^r(\mathbb{F}^n) \) be an ordering of the monomial basis of \( Pol_{\text{hom}}^r(\mathbb{F}[x_1, \cdots, x_n]) \). For \( i \in [1, n] \) we define \( \tilde{f}_i \in \mathbb{F}[x_1, \cdots, x_n, z_1, \cdots, z_n] \) by
\[ \tilde{f}_i(x_1, \cdots, x_n, z_1, \cdots z_n) := \sum_{q=1}^{m'} f_{q,i}(x_1, \cdots, x_n) h(q). \]

Let \( W := \{w_1, \cdots, w_n\} \) be an additional set of variables. We define \( \bar{f} \in \mathbb{F}[x_1, \cdots, x_n, z_1, \cdots, z_n, w_1, \cdots w_n] \) as follows
\[ \bar{f}(x_1, \cdots, x_n, y_1, \cdots, y_n, z_1, \cdots, z_n) := \sum_{i=1}^{n} w_i \tilde{f}_i(x_1, \cdots, x_n, z_1, \cdots, z_n). \]

Note that \( \tilde{f} \) is homogeneous of degree \( r \) in 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 \( f : \mathbb{F}^n \rightarrow \mathbb{F}^m \) according to the receipt (4.2):
\[ f(\lambda) := (\sum_{q=1}^{m'} f_{q,1}(\lambda), \cdots, \sum_{q+1}^{m'} f_{q,n}(\lambda)). \]

Corollary 4.5.2 implies immediately

**Lemma 4.7.** (cf. [9, Corollary 3.8]) Let \( 1 \leq r \leq n \leq s \) and \( m = n \cdot \binom{n+r-1}{r} \) be integers. Let \( f : \mathbb{F}^n \rightarrow \mathbb{F}^m \) be a polynomial mapping. If \( f \) is \((s, 2r-1)\)-weakly elusive, then the circuit size of \( \tilde{f} \) is at least \( \frac{\sqrt{s}}{40 \cdot r^{3/2}} \).

Lemma 4.7 is an improvement of [9, Corollary 3.8] where Raz, under the assumption that \( f \) is \((s, 2r-1)\) elusive, obtained the lower bound \( \Omega(\sqrt{s}/r^4) \) for the circuit size of \( \tilde{f} \) which is weaker than our lower bound \( \Omega(\sqrt{s}/r^{3/2}) \). This is due to our upper bound \( 64 \cdot s^2 r^3 \) for the number of edges leading to the sum-gates in the universal circuit-graph \( G_{s,r,n,m} \), see Proposition 6.6, which is better than the upper bound \( \Omega(s^2 \cdot r^8) \) obtained by Raz in [9, Proposition 3.3], based on his upper bound \( \Omega(s \cdot r^4) \) in [9, Proposition 2.8] for the number of the nodes in the universal graph-circuit \( G_{s,r,n,n} \).
Corollary 4.8. Let \( \text{char}(\mathbb{F}) = 0 \). Assume that \( r \) grows much slower than \( n \), e.g. \( r = \text{const} \) or \( r = \ln \ln n \). Let \( p = (r-1)(2r-1) \). Then there are sequences of polynomials \( \tilde{f}_n \in \text{Pol}_{\text{hom}}^{p+r+1}(\mathbb{F}^{3n}) \) whose coefficients are algebraic numbers, such that
\[
L(\tilde{f}_n) \geq \Omega(\frac{n^{(r-3)}r^{r-3}}{(r-1)^{r-3}r^{n/2}}).
\]

Corollary 4.8 is almost identical with Corollary 4.12 in [6], except that the estimate in Corollary 4.8 is better than that one in Corollary 4.12 [6] (the dominator contains \( r^{3/2} \) vs \( r^4 \)). This improvement is due to Lemma 4.7. We omit the proof of Corollary 4.8.

Example 4.9. Let \( X, Y \) be a set of variables and \( n_X = \#(X) \), \( n_Y = \#(Y) \). We denote by \( \text{Pol}_{\text{hom}}^{p,q}(\mathbb{F}\langle X,Y \rangle) \) the linear subspace of \( \text{Pol}_{\text{hom}}^{p+q}(\mathbb{F}\langle X,Y \rangle) \) 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 \( \text{Pol}_{\text{hom}}^{t,n-t}(\mathbb{F}\langle Y'\rangle, \mathbb{F}\langle Z'\rangle) \), where \( Y', Z' \) are defined in Example 4.3. Then each polynomial \( \tilde{f} \in \text{Pol}_{\text{hom}}^{p,q}(\mathbb{F}\langle X,Y \rangle) \) is associated uniquely by recipe of (4.1) with a homogeneous polynomial mapping \( f \in \text{Pol}_{\text{hom}}^{p}(\mathbb{F}\langle X \rangle, \text{Pol}_{\text{hom}}^{q}(\mathbb{F}\langle Y \rangle)) \). Now assume that \( s + 1 \leq \binom{n_Y+q-1}{q} \) and
\[
\left( \frac{n_X + p - 1}{p} \right) \geq \frac{s^{(s+2q-2)}}{q^{(n_Y+q-1)}} - s.
\]

Theorem 3.10 implies that, if \( \text{char}(\mathbb{F}) = 0 \) or \( p \leq \text{char}(\mathbb{F}) - 1 \), almost all polynomial \( \tilde{f} \) in \( \text{Pol}_{\text{hom}}^{p}(\mathbb{F}\langle X \rangle, \text{Pol}_{\text{hom}}^{q}(\mathbb{F}\langle Y \rangle)) \) is \((s,2q-1)\)-elusive, and hence, by Corollary 4.5.1 we have
\[
L(\tilde{f}) \geq \frac{\sqrt{s}}{8q^{n/2}}.
\]

Furthermore, assume that \( \text{char}(\mathbb{F}) = 0 \). Then using Proposition 4.5 in [6], adapted to our case of weakly elusive homogeneous polynomial mappings, it is easy to show explicitly infinitely many bi-homogeneous polynomials \( \tilde{f} \in \text{Pol}_{\text{hom}}^{p,q}(\mathbb{F}\langle X,Y \rangle) \) whose monomials coefficients are algebraic numbers and \( \tilde{f} \) satisfies (4.7), if (4.6) holds. We refer the reader to the proof of Proposition 4.5 in [6] for the method of proof.

5. AN APPROACH FOR OBTAINING LOWER BOUNDS FOR THE CIRCUIT SIZE OF THE PERMANENT

In this section we assume that \( \text{char}(\mathbb{F}) = 0 \). We outline an approach for obtaining lower bounds for the circuit size of the permanent \( P_n \),
using Corollary 4.5. Here, we restrict ourself to consideration of lower bounds associated with the mappings $f$ defined in 4.3 corresponding to the Case 1. We keep the notations used in Example 4.3. Recall that $Z$ is a rectangular matrix of size $(n-t)n$. Denote by $\bar{\text{Per}}(Z)$ the linear subspace of $\text{Pol}_{l,r}^{n-t}(\mathbb{F}(Z))$ which is generated by the (minor) permanents of size $(n-t) \times (n-t)$ of the matrix $Z$. Clearly $\dim \bar{\text{Per}}(Z) = \binom{n}{n-t}$. Let us denote by $\text{Per}(Y,Z)$ the linear subspace in $\text{Pol}_{l,r}^{n-t}(\mathbb{F}(Y,Z))$ consisting of all polynomial $P$ whose associated polynomial mapping $\bar{P}$ takes values in $\text{Per}(Z)$.

**Lemma 5.1.** The linear span of $f(\mathbb{F}(Y))$ is $\bar{\text{Per}}(Z)$. 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 $\bar{\text{Per}}(Z)$. Now we complete the proof of Lemma 5.1 by observing that all the basis of $\bar{\text{Per}}(Z)$ lies on the image of $f$. \hfill \Box

Next we need the following simple

**Lemma 5.2.** 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 $\pi \circ i = \text{Id}$. 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 5.2 \hfill \Box

We set $m(t) := \binom{n}{n-t}$ and we regard $f$ as a homogeneous polynomial mapping of degree $t$ into $\mathbb{F}^{m(t)}$. Using the same argument as in Example 4.9 we obtain that if $s \in \mathbb{N}$ satisfies

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

(5.1)
then almost all homogeneous polynomials in $Per(Y,Z)$ has the circuit size at least $\frac{\sqrt{s}}{8(n-t)^3}$. For instant, the following values $n, t, s$ satisfy (5.1)

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

for sufficiently large $N \in \mathbb{N}$, since in this case (5.1) is a consequence of the following inequality

$$\left(\frac{N^7}{N^3}\right) \geq 2\left(\frac{N^{4k} + 2N}{2N}\right),$$

whose validity can be verified using the Stirling approximation.

The next step in our approach is to solve Problem 2 for the aforementioned $f$ and use a solution of Problem 1 to obtain the $(s, n - t)$-weak elusiveness of $f$. Alternatively, using Corollary 3.7, we need to find a solution of Problem 3 for proving the desired $(s, n - t)$-weak elusiveness of $f$.

6. Appendix: Normal form of arithmetic circuits and universal circuit-graph

In this Appendix we reformulate a Raz’s theorem on normal-homogeneous circuit (Theorem 6.5), improving an estimate in his original assertion and giving one extra estimate on the size of arithmetic circuits in a normal-homogeneous form. Using these estimates, we reformulate Raz’s theorem on the existence of a universal circuit-graph (Proposition 6.6), improving a Raz’s estimate on the size of a universal circuit-graph. These estimates play important role in the previous sections.

First we recall some necessary definitions.

**Definition 6.1.** (cf. [2, §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 $\alpha$. It computes the product of $\alpha$ 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 $g \in F[x_1, \cdots, x_n]$ 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 $g^i \in F[x_1, \cdots, x_n], i \in [1, m]$. 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 6.2. ([9 §2]) A circuit-graph $G$ is the underlying graph $G_\Phi$ of an arithmetic circuit $\Phi$ 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 $\Phi$. The size of an arithmetic circuit $\Phi$ is defined to be the number of edges in $\Phi$, and is denoted by $\text{Size}(\Phi)$. The depth of a circuit $\Phi$ is defined to be the length of the longest directed path in $\Phi$, and is denoted by $\text{Depth}(\Phi)$. The circuit size $L(P)$ of a $m$-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 6.3. For a circuit-graph $G$, we define the syntactic-degree of a node in $G$ inductively as follows [9 §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 $\Phi$ and a node $v \in \Phi$, we define the syntactic-degree of $v$ to be its syntactic-degree in the circuit-graph $G_\Phi$. The degree of a circuit is the maximal syntactic-degree of a node in the circuit.

Definition 6.4. ([9 Definitions 2.1, 2.2]) A circuit-graph $G$ is called homogeneous, iff for every arithmetic circuit $\Phi$ such that $G = G_\Phi$ and every gate $v$ in $\Phi$, the polynomial computed by the gate $v$ is homogeneous. Further, we say that a homogeneous graph is in normal form, if it satisfies

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. 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 $G_\Phi$ is in a normal-homogeneous form.

Let $N_j^\Sigma(\Phi)$ (resp. $N_j^\Pi(\Phi)$) denote the number of sum-gates (resp. product-gates and input-gates) of syntactic degree $j$ in an arithmetic circuit $\Phi$ and set $N(\Phi) := \sum_j (N_j^\Sigma(\Phi) + N_j^\Pi(\Phi))$.

Theorem 6.5. cf. [9 Proposition 2.3] Let $\Phi$ be an arithmetic of size $s$ that computes an $m$-tuple $P$ of homogeneous polynomials $g_1, \cdots, g_m \in \text{Pol}_\text{hom}^r(\mathbb{F}^n)$ where $r \geq 1$. Then there exists an arithmetic circuit $\Psi$ for
the polynomials $g_1, \cdots, g_m$ such that $\Psi$ is in a normal homogeneous form with $N_j^x(\Psi) \leq 8s$ for all $1 \leq j \leq r$ and $N(\Psi) < 24sr$.

**Proof.** Theorem 6.5 differs from [9, Proposition 2.3] in several points. Firstly, Raz assumed that $m = n$. Secondly, Raz obtained the upper bound $N(\Psi) \leq O(s \cdot r^2)$; he also did not estimate $N_j^x(\Psi)$. The proof presented here follows the Raz’s algorithm in the proof of [9, Proposition 2.3] that transforms an arithmetic circuit $\Phi$ that computes $P$ into an arithmetic circuit $\Psi$ in normal homogeneous form which also computes $P$ and, moreover, satisfies the condition of Theorem 6.5. Our new estimates on $N_j^x(\Psi)$ and $N_j^+(\Psi)$ will be needed for Proposition 6.6 below.

**Step 1.** If a (sum- or product-) gate in $\Phi$ 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 $\Phi$ 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 $\Phi$ to $\Phi_1$, which satisfies the condition (5) of Definition 6.4 by replacing any product-gate of in-degree larger 2 by a tree of product-gates of in-degree 2, and any sum-gate of in-degree larger than 2 by a tree of sum-gates of in-degree 2. It is easy to check that $\text{Size}(\Phi_1) \leq 2s$ and $N(\Phi_1) \leq 2\text{Size}(\Phi_1) \leq 4s$.

**Step 3.** We transform $\Phi_1$ to $\Phi_2$ such that $G_{\Phi_2}$ also satisfies the condition (5), and moreover, is homogeneous. The nodes of $\Phi_2$ 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 $\Phi_1$ connecting $v$ with its children $u^1, \cdots, u^t$ by the circuits that compute $v_i = u^1_i + \cdots + u^t_i$ for all $i \in [0, r]$. If $v \in \Phi_1$ is a product-gate, we replace the sub-circuit in $\Phi_1$ 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 $\Phi_2$ also computes $P$, moreover $\Phi_2$ is homogeneous, satisfies the condition (5) in Definition 6.4. By construction, for any $j \in [0, r]$, each product-gate $v \in \Phi_1$ contributes at most two product-gates of syntactic degree $j$ in $\Phi_2$. Hence $N_j^x(\Phi_2) \leq 2N(\Phi_1) \leq 8s$ for all $1 \leq j \leq r$.

**Step 4.** We transform $\Phi_2$ to a homogeneous circuit $\Phi_3$ which computes $P$ and satisfies the conditions (1), (5) in Definition 6.4 by removing every node of syntactic-degree 0. 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 \( \Phi_2 \) is homogeneous, \( v \) computes a field element \( \alpha_v \). Then we replace the sub-circuit computing \( v \) from its children by a simple gate and label the corresponding edge by \( \alpha_v \). 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 \( \Phi_3 \) with \( N_0(\Phi_3) = 0 \) and \( N_j^\times(\Phi_3) \leq N_j^\times(\Phi_2) \leq 8s \) for \( j \in [1, r] \), since no new gate is created.

**Step 5.** We transform \( \Phi_3 \) to a homogeneous circuit \( \Phi_4 \) 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 \( v \). Since no new product-gate is created, \( N_j^\times(\Phi_4) = N_j^\times(\Phi_3) \leq 8s \).

**Step 6.** We transform \( \Phi_4 \) to a homogeneous circuit \( \Phi_5 \) which computes \( P \) and satisfies the conditions (1), (5), (4) and (3) by connecting every product output-gate to a new dummy sum-gate. Since no new product-gate is created, \( N_j^\times(\Phi_5) = N_j^\times(\Phi_4) \leq 8s \) for all \( j \in [0, r] \).

**Step 7.** We transform \( \Phi_5 \) to a homogeneous circuit \( \Phi_6 \) which computes \( P \) and satisfies the conditions (1), (5), (4), (3) and (2) by adding a dummy sum-gate in between any edge from an input-gate to a product gate. Note that \( N_j^\times(\Phi_6) = N_j^\times(\Phi_5) \leq 8s \) for all \( j \in [0, r] \).

**Step 8.** We transform \( \Phi_6 \) to a homogeneous circuit \( \Phi_7 \) which computes \( P \) and satisfies all the conditions in Theorem 6.5 by duplicating \( q \)-times any sum-gate of out-degree \( q > 1 \). We also note that \( N_j^\times(\Phi_7) = N_j^\times(\Phi_6) \leq 8s \). Since \( \Phi_7 \) satisfies the conditions (3), (4), (5), (6), we obtain for \( r \geq 2 \)

\[
\sum_{j=1}^{r-1} N_j^+(\Phi_7) = 2 \sum_{j=2}^{r} N_j^\times(\Phi_7) < 16s(r - 1).
\]

Since \( N_r^+(\Phi_7) = m < s \) and \( n < s \), we obtain immediately \( N(\Phi_7) \leq 24sr \) for \( r \geq 2 \). If \( r = 1 \), then obviously \( N(\Phi_7) \leq 2s < 24s \). Setting \( \Psi := \Phi_7 \), this completes the proof of Theorem 6.5.

**Proposition 6.6.** cf. [9 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 $P := (g_1, \ldots, g_m) \in (Pol_{hom}(\mathbb{F}^n))^m$ is of circuit size $s$. Then, there exists an arithmetic circuit $\Psi$ 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 $64 \cdot s^2 r^3$.

Proof. Proposition 6.6 differs from Proposition 2.8 in [9] only in three instances. Firstly, Raz assumed that $m = n$. Secondly, he obtained $N(G_{s,r,n,n}) \leq O(s r^4)$ and we use a finer estimate on the number of nodes of $G_{s,r,n,m}$. We also 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 6.7 below, yields a better lower bound for the circuit size of partially homogeneous polynomials in considerations, see Example 4.6.

The idea of the proof of Proposition 6.6, due to Raz [9], 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 $\Phi$ computing $P$ can be embedded into $G_{s,r,n,m}$.

The circuit-graph $G_{s,r,n,m}$ is constructed based on Theorem 6.5 as follows. First, we divide the nodes of $G_{s,r,n,m}$ into $2r$ levels. The first level contains $n$ input-gates, and the last level contains $m$ output-gates. The even-enumerated level $(2i)$ contains preliminarily $16sr$ sum-gates and the odd-enumerated level $(2i - 1)$ contains at most $4si$ product-gates or input-gates, see the description below. The levels $2i$ and $(2i - 1)$ contain gates of the same syntactic degree $i$. By (2) below, every product-gate in level $(2i - 1)$ has exactly two children, one is a sum-gate in level $(2j)$ for some $1 \leq j \leq \lfloor \frac{i}{2} \rfloor$ and the other is a sum-gate in level $(2i - 2j)$. So we partition the product-gates in level $(2i - 1)$ into $\lfloor \frac{i}{2} \rfloor$ types according to the smaller-level of their children. Each of these types contains exactly $8s$ nodes. Thus we have at most $4si$ nodes in each odd-enumerated level $(2i - 1)$.

Now we shall define the edges of $G_{s,r,n,m}$ such that $G_{s,r,n,m}$ has the following properties.

1. The two children of each product-gate of type $j$ in level $(2i - 1)$ are a sum-gate in level $(2j)$ and a sum-gate in level $(2i - 2j)$.
2. The out-degree of every sum-gate is at most 1.
3. The only sum-gates of out-degree 0 are the output-gates.

On each even-enumerated level $(2i)$ we choose preliminary $16sr$ sum-gates. This number is sufficient to achieve (1), (2) listed above, since each odd-numbered level of $G_{s,r,n,m}$ has at most $8s$ product-gates of $i$-type. Then we erase all sum-gates of out-degree 0 that are not the output-gates. In this way we define all the edges of $G_{s,r,n,m}$ leading from sum-gates to product-gates. Then we connect each sum-gate in
level \((2i)\) with all product-gates in level \((2i - 1)\). Clearly the constructed circuit-graph \(G_{s,r,n,m}\) satisfies \((1)\), \((2)\), \((3)\) and is in a normal-homogeneous form.

Let \(\Psi\) be an arithmetic circuit in normal homogeneous form that computes \(P\) as described in the proof in Theorem 6.5. We will show how to embed \(G_{\Psi}\) into \(G_{s,r,n,m}\).

Since \(N_{i}^{x}(\Psi) \leq 8s\), we can embed all the product-gates of syntactic degree \(i\) of the circuit graph \(G_{\Psi}\) into the product-gates of level \((2i - 1)\) of \(G_{s,r,n,m}\). Since \(\Psi\) is of normal-homogeneous form, the embedding of the product-gates of \(G_{\Psi}\) into \(G_{s,r,n,m}\) extends to an embedding of the whole graph-circuit \(G_{\Psi}\) into \(G_{s,r,n,m}\), because we have enough sum-gates on each level \((2i)\) of \(G_{s,r,n,m}\). This completes the first assertion of Proposition 6.6.

The last assertion of Proposition 6.6 follows from the estimate that the even-enumerated level \((2i)\) of \(G_{s,r,n,m}\) contains at most \(16sr\) nodes and the odd-enumerated level of \(G_{s,r,n,m}\) contains at most \(4sr\) nodes. This completes the proof of Proposition 6.6.

We end this appendix with the following remark on universal circuits, which is needed in the main body of our note.

**Remark 6.7.** ([9, 3.2]) Assume that \(\Phi\) is a normal homogeneous arithmetic circuit that computes a \(m\)-tuple \(P \in (\text{Pol}_{\text{hom}}(F^{n}))^{m}\). Then there is an arithmetic circuit \(\Psi\) of the same circuit-graph as \(\Phi\) that computes \(P\) such that the label of any edge leading to a product-gate in \(\Psi\) is 1.

**Acknowledgements**

The author would like to thank Pavel Pudlak for his stimulating discussions and criticism, and Ngô Viêt Trung for his illuminating discussion on related problems in commutative algebra. 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] J. zur Gathen, Feasible Arithmetic Computations: Valiant’s Hypothesis, J. Symbolic Computation (1987) 4, 137-172.
[4] J. Harris, Algebraic Geometry, A First Course, Springer-Verlag, 1993.
[5] G.-M. Greuel and G. Pfister, A SINGULAR Introduction to Commutative Algebra, Springer-Verlag, (2007).
[6] H. V. Lê, Constructing elusive functions with help of evaluation mappings, arXiv:1011.2887
[7] T. Mignon and N. Ressayre, A quadratic bound for the Determinant and Permanent Problem, IMRN 79 (2004), 4241-4253.
[8] 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.
[9] R. Raz, Elusive Functions and Lower Bounds for Arithmetic Circuits, Theory Of Computing Vol. 6, article 7 (2010).
[10] 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).
[11] 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.
[12] 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 l’Enseignement Mathemathique, (1982), 365-380.

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