Electronic Colloquium on Computational Complexity, Report No. 140 (2014)

CONSTRUCTING ELUSIVE FUNCTIONS WITH HELP OF EVALUATION MAPPINGS

HÔNG VÂN LÊ

ABSTRACT. We develop a method to construct elusive functions using techniques of commutative algebra and algebraic geometry. The key notions of this method are elusive subsets and evaluation mappings. We also develop the effective elimination theory combined with algebraic number field theory in order to construct concrete points outside the image of a polynomial mapping. Using the developed methods, for $\mathbb{F} = \mathbb{C}$ or $\mathbb{R}$, we construct examples of (s, r)-elusive functions whose monomial coefficients are algebraic numbers, which give polynomials with algebraic number coefficients of large circuit size.

AMSC: 03D15, 68Q17, 13P25

Contents

1. Introduction

In computational algebraic complexity theory we investigate different complexity classes of sequences (f_n) of polynomials over a field $\mathbb{F}$. We also search lower or upper bounds of complexities on a given polynomial.

Supported by RVO: 67985840.

ISSN 1433-8092

Two most important complexities of a multivariate polynomial f are the circuit complexity $L(f)$ and the formula size $L_e(f)$. These complexities measure the minimal size of certain arithmetic circuits computing f. Arithmetic circuits are the standard computational model for computing polynomials. *An arithmetic circuit*, as defined, e.g., in [14, §1.1], is a finite directed acyclic graph whose nodes are divided into four types: nodes of in-degree 0 (input gates) labeled with an input variable or the field element 1, nodes labelled with + (sum gates), node labeled with × (product gates), and nodes of out-degree 0 (output gates) giving the result of the computation. Every edge (u, v) in the graph is labeled 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 $f \in \mathbb{F}[X_1, \cdots, X_n]$ 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 a m-tuple of polynomials $f^i \in \mathbb{F}[X_1, \cdots, X_n]$, $i \in [1, m]$. In what follows we consider only ordered m-tuples of polynomials resulting from a numeration of the output gates of an arithmetic circuit; so an m-tuple is understood as an ordered m-tuple. Further, assuming in this note that $\mathbb{F}$ is a field of characteristic 0, we also identify an m-tuple of polynomials in n variables with a polynomial mapping from $\mathbb{F}^n$ to $\mathbb{F}^m$. Let us denote by $Pol^r(\mathbb{F}^n, \mathbb{F}^m)$ the space of all polynomial mapping of degree at most r from $\mathbb{F}^n$ to $\mathbb{F}^m$ and set $Pol(\mathbb{F}^n, \mathbb{F}^m) := \cup_{r=0}^{\infty} Pol^r(\mathbb{F}^n, \mathbb{F}^m)$.

We define *the size of a circuit* as the number of its edges, and *the circuit complexity* $L(f)$ of a polynomial mapping f to be the minimum size of an arithmetic circuit computing f [14]. *The formula size* $L_e(f)$ *of a polynomial mapping* f is defined as the minimum size of an arithmetic circuit computing f, which is a directed tree, i.e., all vertices have outdegree at most 1.

The formula size and the circuit complexity of polynomial mappings do not have clear geometric or algebraic structure. In [18] Valiant suggested to "approximate" the formula size of a polynomial by the determinantal complexity, observing that on the one hand, the determinantal complexity is a lower bound for the formula size, and on the other hand, the determinantal complexity has a clear algebraic and geometric interpretation. Geometric and algebraic properties of the determinantal complexity of a polynomial have been employed by Mignon-Ressayre [12] and by Mulmuley-Sohoni [13] to study lower bounds on the determinantal complexity, and to attack the problem VP versus VNP.

In [14] Raz proposed a geometric approach to obtain a lower bound on the circuit complexity of a polynomial by introducing a polynomial mapping associated with a universal graph of a given arithmetic circuit. Using his method Raz has constructed explicit polynomials whose constant depth circuit size is large [14, Lemma 4.1], see also Remark 4.10.

Raz's method of constructing elusive functions is combinatorial, and it is not clear how to apply his method to find other examples of elusive functions. In this paper we develop an algebraic-geometric method for construction of elusive functions. The key notion of this method are elusive subsets and evaluation mappings.

The structure of our paper is as follows. In section 2 we recall the notion of a (s, r)-elusive function introduced by Raz in [14]. To study (s, r)-elusive functions we introduce the notion of a (s, r)-elusive subset (Definition 2.2) and we characterize polynomial mappings whose image contains an (s, r)-elusive subset consisting of k points (Corollary 2.5). This construction leads to the notions of a (s, r, k)-elusive function and of a strong (s, r)-elusive function (Definitions 2.2, 2.9). We compare these notions, using an interpolation formula for polynomial mappings (Proposition 2.6, Remark 2.10). In section 3 we develop the method invented by Kumar-Lokam-Patankar-Sarma [9] that uses the effective elimination theory combined with algebraic number field theory in order to find concrete points b which lie outside the image of a polynomial mapping g, if g is defined over $\mathbb{Q}$, such that the coordinates of b are algebraic numbers (Proposition 3.5). Note that our method is close to the Strassen-Schnorr-Heintz-Sieveking method of constructing polynomials with algebraic coefficients which are hard to compute, but our method and their method yield different polynomials which are hard to compute in different complexity classes (Remark 3.8.1). In section 4 we construct examples of (s, r)-elusive functions (Proposition 4.5). Using this, for $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$, we construct explicit examples of sequences of polynomials $f_n : \mathbb{F}^{2n} \to \mathbb{F}^n$ of degree $5r + 1$ whose coefficients are algebraic numbers such that any depth r arithmetic circuit for f_n is of size greater than $n^2/50r^2$ (Proposition 4.7). We compare our results with previously obtained results (Remark 4.10). We also construct (s, r)-elusive functions whose monomial coefficients are algebraic numbers, which give polynomials of large circuit size (Proposition 4.12, Corollary 4.14).

Finally we note that our results in effective elimination theory are applicable for similar complexities of the same nature, e.g. the determinantal complexity, the rank of tensors and the rigidity of matrices.

2. Elusive functions and associated polynomial mappings

In this section we recall the notion of a (s,r)-elusive function introduced by Raz in [14] for constructing sequences of multivariate polynomials of high circuit complexity (Definition 2.1). To study (s,r)-elusive functions we introduce the notion of a (s,r)-elusive subset (Definition 2.2) and we find a condition for a polynomial mapping whose image contains a (s,r)-elusive subset (Corollary 2.5). We also introduce the notion of a (s,r,k)-elusive function (Definition 2.2) and the notion of a strongly (s,r)-elusive functions (Definition 2.9). We compare (s,r)-elusive functions with (s,r,k)-elusive functions and strongly (s,r)-elusive functions, using an interpolation formula for polynomial mappings over $\mathbb{F}$ and an evaluation mapping (Proposition 2.6, Remark 2.10).

Definition 2.1 ([14], p. 2)**.** A polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$ is called (s,r)-*elusive*, if for every polynomial mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r, we have $f(\mathbb{F}^n) \not\subset \Gamma(\mathbb{F}^s)$.

Using the existence of elusive functions Raz has constructed polynomials of large circuit size [14, §3.4]. Raz's construction of elusive functions is based on a certain combinatoric property of the coefficients of a special polynomial mapping [14, Lemma 4.1]. Our approach to elusive functions is based on the concept of an (s,r)-elusive subset.

Definition 2.2. A k-tuple S_k of k points in $\mathbb{F}^m$ is called (s,r)-*elusive*, if for every polynomial mapping $\Gamma : \mathbb{F}^s \to \mathbb{F}^m$ of degree r, we have $S_k \not\subset \Gamma(\mathbb{F}^s)$. A polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$ is called (s,r,k)-*elusive*, if there is a k-tuple of points in the image $f(\mathbb{F}^n)$ which is (s,r)-elusive.

Clearly any (s,r,k)-elusive function is (s,r)-elusive.

Example 2.3. (cf. [14]) A polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$ is $(m-1,1)$-elusive, if and only if the image $f(\mathbb{F}^n)$ does not belong to any hyperplane in the affine space $\mathbb{F}^m$. Equivalently, a $(m-1,1)$-elusive polynomial is $(m-1,1,m+1)$-elusive. For example, the moment curve $f : \mathbb{C} \to \mathbb{C}^m$, $t \mapsto (t, t^2, \cdots, t^m)$ is $(m-1,1)$-elusive, since the image of the moment curve contains $m+1$ points $b_0 := f(0) = 0, \cdots, b_i := f(a_i) \in \mathbb{C}^m$, $1 \le i \le m$, satisfying the following condition. The values $a_i \in \mathbb{F}^n$ are chosen to be distinct such that $b_1, \cdots, b_m$ are linear independent vectors in $\mathbb{C}^n$. Clearly the $(m+1)$-tuple $(0, b_1, \cdots, b_m)$ is $(m-1,1)$-elusive, which implies that f is $(m-1,1,m+1)$-elusive, see Corollary 2.7 for a detailed explanation.

To treat (s,r)-elusive k-tuples we consider the following evaluation map

$$Ev^k_{r,s,m} : Pol^r(\mathbb{F}^s, \mathbb{F}^m) \times (\mathbb{F}^s)^k \to (\mathbb{F}^m)^k, \tag{2.1}$$
$$(f_1, \cdots, f_m)(a_1, \cdots, a_k) \mapsto (f_1(a_1), \cdots, f_m(a_k)),$$

where $f_j \in Pol^r(\mathbb{F}^s)$ for $1 \le j \le m$ and $a_i \in \mathbb{F}^s$ for $1 \le i \le k$.

We identify a k-tuple $S_k = (b_1, \cdots, b_k)$, $b_i \in \mathbb{F}^m$, with the point $\overline{S_k} \in (\mathbb{F}^m)^k$ whose coordinate $\overline{S_k}^{i,j}$, $1 \le i \le k$, $1 \le j \le m$, is equal to the i-th coordinate b^i_j of $b_j \in \mathbb{F}^m$.

Lemma 2.4. *A k-tuple $S_k \subset \mathbb{F}^m$ is (s,r)-elusive, if and only if $\overline{S_k}$ does not belong to the image of $Ev^k_{r,s,m}$.*

Proof. Assume that $\overline{S_k}$ belongs to the image of $Ev^k_{s,r,m}$. Then there are a polynomial mapping $f \in Pol^r(\mathbb{F}^s, \mathbb{F}^m)$ and a point $a \in \mathbb{F}^{sk}$ such that

$$Ev^k_{r,s,m}(f, a) = \overline{S_k}. \tag{2.2}$$

We write $S_k = (b_1, \cdots, b_k)$, $b_i \in \mathbb{F}^m$, and $a = (a_1, \cdots, a_k)$, $a_i \in \mathbb{F}^s$. The equation (2.2) implies

$$f(a_i) = b_i. \tag{2.3}$$

Thus $S_k \subset f(\mathbb{F}^s)$. This proves the "only if" assertion of Lemma 2.4.

Conversely, assume that $S_k \subset f(\mathbb{F}^s)$ for some $f \in Pol^r(\mathbb{F}^s, \mathbb{F}^m)$. Then there are points $a_i \in \mathbb{F}^s$, $i = \overline{1,k}$, such that (2.3) holds for all i. Since (2.3) is equivalent to (2.2), it follows that $\overline{S_k}$ belongs to the image of $Ev^k_{r,s,m}$. This completes the proof of Lemma 2.4. □

Corollary 2.5. *A polynomial map $f : \mathbb{F}^n \to \mathbb{F}^m$ is (s,r,k)-elusive, if and only if the subset $\hat{f}^k := f(\mathbb{F}^n) \times \cdots_{k\,times} \times f(\mathbb{F}^n) \subset \mathbb{F}^{mk}$ does not belong to the image of the evaluation mapping $Ev^k_{s,r,m}$.*

Now we are going to find a sufficient condition for a polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$ to be (s,r,k)-elusive using an interpolation formula for a polynomial mapping.

Interpolation of a function in many variables by a polynomial mapping has been investigated for a long time, but there are many interesting and unsolved questions [8]. One of the main differences between interpolation of a function in one variable and interpolation of a function in many variables is that in the former case an interpolable set, i.e., the set at which the value of an interpolating polynomial function (resp. a polynomial mapping) must coincide with the value of a given interpolable function, can be arbitrary, but in the later case cannot be arbitrary. The interpolation formula given below is likely unknown, though possibly, there are some similar formulas. Our interpolable set is a lattice in a simplex in $\mathbb{F}^n$.

Note that a monomial $X_1^{i_1}\cdots X_s^{i_s} \in Pol^r(\mathbb{F}^s)$ can be identified with an ordered s-tuple $(i_1, \cdots, i_s)$ of non-negative integers i_j, $1 \le j \le s$, such that $i_1 + \cdots + i_s \le r$. The following formula is well-known

$$\dim Pol^r(\mathbb{F}^s) = \binom{s+r}{s}. \tag{2.4}$$

By (2.4) there exists a 1-1 mapping H_s^r from the set Mon_s^r of all monomials $X_1^{i_1}\ldots X_s^{i_s} \in Pol^r(\mathbb{F}^s)$ to the set $S_{s,r}$ of $\binom{s+r}{r}$ points $(i_1, \cdots, i_s) \in \mathbb{F}^s$. (The mapping H_s^r induces a linear isomorphism $H_{s,m}^r : Pol^r(\mathbb{F}^s, \mathbb{F}^m) \to (\mathbb{F}^s)^m$, $k = m\binom{s+r}{r}$.) For a set $S_{s,r,m}$ of $\binom{s+r}{r}$ points in $\mathbb{F}^m$ we enumerate the points in $S_{s,r,m}$ by $b_{i_1,\cdots,i_s}$, where $i_s \in \mathbb{N}$ and $\sum_s i_s \le r$.

Now we are ready to prove

Proposition 2.6. *Given a tuple $S_{s,r,m}$ of $\binom{\mathrm{s+r}}{\mathrm{r}}$ points $b_{i_1,\cdots,i_s}$ in $\mathbb{F}^m$, $i_j \in \mathbb{N}$ and $\sum_{j=1}^s i_j \le r$, there exists an algorithmically constructed polynomial mapping $f_{S_{s,r,m}} : \mathbb{F}^s \to \mathbb{F}^m$ of degree r such that*

$$f_{S_{s,r,m}}(i_1, \cdots, i_s) = b_{i_1,\cdots,i_s}, \tag{2.5}$$

for all $(i_1, \cdots, i_s) \in \mathbb{N}^s \subset \mathbb{F}^s$ satisfying $\sum_{j=1}^s i_j \le r$.

Proof. Let f^i (resp. b^i) denote the i-th coordinate of a polynomial mapping $f : \mathbb{F}^s \to \mathbb{F}^m$ (resp. of a point $b \in \mathbb{F}^m$), i.e., $f = (f^1, \cdots, f^m)$. Note that (2.5) is equivalent to the following system of equations

$$f^i_{S_{s,r,m}}(i_1, \cdots, i_s) = b^i_{i_1,\cdots,i_s}, \text{ for } i \in [1, m] \tag{2.6}$$

and for all $(i_1, \cdots, i_s) \in \mathbb{N}^s \subset \mathbb{F}^s$ satisfying $\sum_s i_s \le r$. Since the system (2.6) consists of independent subsystems each of which corresponds to an upper index $i \in [1, m]$, it suffices to prove Proposition 2.6 for the case $m = 1$.

We construct $f_{S_{s,r,1}}$ by induction on s. Note that the case $s = 1$ is well-known. Given an $(r+1)$-tuple $(b_0, \cdots, b_r)$ of elements $b_i \in \mathbb{F}$, there is a polynomial $f_{S_{1,r,1}} \in \mathbb{F}[X]$ taking values in $(b_0, \cdots, b_r)$. The Newton interpolation formula defines $f_{S_{s,r,1}}$ by the following formula

$$f_{S_{1,r,1}}(X) := \lambda_0 + \lambda_1 X + \lambda_2 X(X-1) + \cdots + \lambda_r X(X-1)\cdots(X-r), \tag{2.7}$$

where the coefficients $\lambda_k \in \mathbb{F}$ are defined inductively on k by solving the system of the following linear equations with coefficients in $\mathbb{N}$

$$\lambda_0 = b_0,$$

$$\lambda_0 + \lambda_1 = b_1,$$

$$\cdots$$

$$\lambda_0 + \lambda_1 \cdot k + \cdots + \lambda_k \cdot k! = b_k, \tag{2.8}$$

etc.

Next, let us assume that $s_0 \geq 2$ and Proposition 2.6 is valid for $s \leq s_0 - 1$. Now we show how to construct the required polynomial $f_{S_{s_0,r,1}}$. Recall that $f_{S_{s_0,r,1}} : \mathbb{F}^{s_0} \to \mathbb{F}$ is required to satisfy the following equation

$$f_{S_{s_0,r,1}}(i_1, i_2, \cdots, i_{s_0}) = b_{i_1,\cdots i_{s_0}} \in S_{s_0,r,1} \subset \mathbb{F} \tag{2.9}$$

$$\text{for all } (i_1, \cdots, i_{s_0}) \text{ such that } X_1^{i_1} \cdots X_s^{i_{s_0}} \in Mon_{s_0}^r.$$

We set

$$f_{S_{s_0,r,1}}(X_1, \cdots, X_{s_0}) := P^r(X_1, \cdots, X_{s_0-1}) + X_{s_0} P^{r-1}(X_1, \cdots, X_{s_0-1}) + \cdots$$
$$+ X_{s_0}(X_{s_0} - 1) \cdots (X_{s_0} - r + 1) P^0(X_1, \cdots, X_{s_0-1}). \tag{2.10}$$

To determine the polynomials $P^k(X_1, \cdots, X_{s_0-1})$ entered in (2.10) for $0 \leq k \leq r$ we exploit the following canonical injective map

$$Mon_{s-1}^r \to Mon_s^r,\ X_1^{i_1} \cdots X_{s-1}^{i_{s-1}} \mapsto X_1^{i_1} \cdots X_{s-1}^{i_{s-1}}, \tag{2.11}$$

as well as the following canonical inclusions

$$Mon_{s-1}^r \supset Mon_{s-1}^{r-1} \supset Mon_{s-1}^{r-2} \supset Mon_{s-1}^{r-3} \supset \cdots. \tag{2.12}$$

Using (2.11) and (2.12) we denote the restriction of H_s^r to $Mon_{s_0-1}^{r-k}$ by $H_{s_0-1}^{r-k}$. The image $H_{s_0-1}^{r-k}(Mon_{s_0-1}^{r-k})$ is a set $S_{s_0-1,r-k}$ of $\binom{s_0-1+r-k}{r-k}$ elements in $\mathbb{F}^{s_0-1} \subset \mathbb{F}^{s_0}$. Clearly, for $0 \leq k \leq r$

$$S_{s_0-1,r-k} = \{(i_0, \cdots, i_{s_0-1}, k) |\, i_j \in \mathbb{N} \text{ and } \sum_{j=1}^{s-)} i_j \leq r - k\} \subset S_{s_0,r}.$$

Next we decompose

$$S_{s_0,r,1} := \{b_{i_0,i_1,\cdots,i_{s_0}} |\, i_j \in \mathbb{N} \text{ and } \sum_{j=1}^{s_0} i_j \leq r\} \subset \mathbb{F}$$

as a union of its disjoint subsets

$$S_{s_0,r,1} = S_{s_0-1,r,1} \cup S_{s_0-1,r-1,1} \cup \cdots \cup S_{s_0-1,0,1},$$

where for $0 \leq k \leq r$

$$S_{s_0-1,r-k,1} := \{b_{i_0,\cdots,i_{s_0-1},k} |\, i_j \in \mathbb{N} \text{ and } \sum_{j=1}^{s} i_j \leq r - k\} \subset S_{s_0,r,1}.$$

Substituting $X_{s_0} = 0$ into (2.10), taking into account (2.9), we observe that the polynomial $P^r(X_1, \cdots, X_{s_0-1})$ satisfies the following equation

$$P^r(i_1, \cdots, i_{s_0-1}) = b_{i_0,\cdots,i_{s_0-1},0} \in S_{s_0-1,r,1} \subset \mathbb{F} \tag{2.13}$$

$$\text{for all } (i_1, \cdots, i_{s_0}) \text{ such that } (X_1^{i_1} \cdots X_{s_0-1}^{i_{s_0-1}}) \in Mon^r_{s_0-1}.$$

The induction assumption implies that $P^r(X_0, \cdots, X_{s_0-1})$ can be defined algorithmically such that (2.13) holds.

Now we will construct polynomials P^{r-1}, $P^{r-2}, \cdots, P^0$ inductively from (2.9), (2.10) and (2.13). Assume this has been done for all $P^r, \cdots, P^{r-k+1}$, $1 \le k \le r+1$. Substituting $X_{s_0} = k$ into (2.10) and comparing this with (2.9), we obtain the following defining equation for $P^{r-k} : \mathbb{F}^{s_0-1} \to \mathbb{F}$

$$f_{S_{s_0,r}}(i_1, \cdots, i_{s_0-1}, k) = P^r(i_1, \cdots, i_{s_0-1}) + kP^{r-1}(i_1, \cdots, i_{s_0-1}) + \cdots$$

$$+k!P^{r-k}(i_1, \cdots, i_{s_0-1}) = b_{i_1,\cdots,i_{s_0-1},k}. \tag{2.14}$$

$$\Longleftrightarrow P^{r-k}(i_1, \cdots, i_{s_0-1}) = \beta^{r-k}_{i_1,\cdots,i_{s_0-1}} \in \mathbb{F} \tag{2.15}$$

for all$(i_1, \cdots, i_{s_0-1})$ such that $(X_1^{i_1} \cdots X_{s_0-1}^{i_{s_0-1}}) \in Mon^r_{s_0-1}$ and for

$$\beta^{r-k}_{i_1,\cdots,i_{s_0-1}} := \frac{1}{k!}[b_{i_1,\cdots,i_{s_0-1},k} - (P^r(i_1, \cdots, i_{s_0-1}) +$$

$$+kP^{r-1}(i_1, \cdots, i_{s_0-1}) + \cdots + k!P^{r-k+1}(i_1, \cdots, i_{s_0-1}))].$$

By the induction assumption P^{r-k} can be algorithmically constructed using (2.15). This completes the induction step. Hence Proposition 2.6 is valid for all s. □

Corollary 2.7 (cf. Example 2.3)**.** *Assume that $\{b_1, \cdots, b_m\}$ are linearly independent vectors in $\mathbb{F}^m$. Then there exists a polynomial map $f : \mathbb{F} \to \mathbb{F}^m$ of degree m whose image contains the points $b_0 = 0, b_1, \cdots, b_m$. In other words, f is is $(m-1, 1)$-elusive.*

Let us consider the interpolation problem for homogeneous polynomial mappings. Since each homogeneous polynomial $f \in Pol^r_{hom}(\mathbb{F}^{n+1}, \mathbb{F}^m)$ $\subset Pol^r(\mathbb{F}^{n+1}, \mathbb{F}^m)$ is defined uniquely by the value of its restriction to the hyperplane $b^{n+1} = 1$ in $\mathbb{F}^{n+1}$, we get immediately from Proposition 2.6

Corollary 2.8. *1. Given a tuple $S_{s,r,m}$ of $\binom{s+r}{r}$ points $b_{i_1,\cdots,i_s}$ in $\mathbb{F}^m$, where $i_j \in \mathbb{N}$ and $\sum_{j=1}^s i_j \le r$, there exists an algorithmically constructed homogeneous polynomial mapping $f_{S_{s,r,m}} : \mathbb{F}^{s+1} \to \mathbb{F}^m$ of degree r such that*

$$f_{S_{s,r,m}}(i_1, \cdots, i_s, 1) = b_{i_1,\cdots,i_s} \tag{2.16}$$

for all $(i_1, \cdots, i_s)$ *satisfying* $i_j \in \mathbb{N}$ *and* $\sum_{j=1}^s i_j \le r$.

2. Let us abbreviate $\binom{s+r}{r}$ *by* $b(s,r)$. *Proposition 2.6 and the formulas in its proof give a linear isomorphism*

$$I_m^{b(s,r)} : \mathbb{F}^{mb(s,r)} \to Pol^r(\mathbb{F}^s, \mathbb{F}^m), \tag{2.17}$$

which associates any point $\overline{S_{s,r,m}} \in \mathbb{F}^{mb(s,r)}$ *with a polynomial mapping* $f_{S_{s,r,m}} \in Pol^r(\mathbb{F}^s, \mathbb{F}^m)$.

Proposition 2.6 motivates the following

Definition 2.9. A mapping $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ is called *strongly* (s,r)-*elusive*, if the set $\{f(i_1, \cdots, i_n) | i_j \in \mathbb{N}$ and $\sum_{j=1}^n i_j \le p\}$ is (s,r)-elusive.

Remark 2.10. 1. By Lemma 2.4, a polynomial mapping $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ is strongly (s,r)-elusive, if and only if the point in $\mathbb{F}^{mb(s,r)}$ associated with the tuple $(f(i_1, \cdots, i_n) | i_j \in \mathbb{N}$ and $\sum_{j=1}^n i_j \le p)$ does not belong to the image of the evaluation mapping $Ev_{r,s,m}^{b(p,n)}$.

2. A strongly (s,r)-elusive polynomial mapping $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ is (s,r,k)-elusive for any $k \ge \binom{n+p}{p}$, and, hence, it is (s,r)-elusive.

3. If $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ is (strongly) (s,r)-elusive, then it is (strongly) (s', r)-elusive for any $s' \le s$.

3. Zariski closure of the image of a polynomial mapping, effective elimination theory and algebraic number field theory

Remark 2.10 asserts that a verification of the strong (s,r)-elusiveness of a polynomial mapping f can be reduced to the following problem. Given a polynomial map $\tilde{f} : \mathbb{F}^n \to \mathbb{F}^m$ and given a point $b \in \mathbb{F}^m$, verify whether b belongs to the image $\tilde{f}(\mathbb{F}^m)$. This problem is in fact a part of the elimination theory, which we discuss in this section (Lemma 3.1, Corollary 3.2). We develop the method invented by Kumar-Lokam-Patankar-Sarma [9] that uses effective elimination theory combined with algebraic number field theory in order to get concrete points b which do not belong to the Zariski closure of the image of a polynomial mapping $\tilde{f}$, if $\tilde{f}$ is defined over $\mathbb{Q}$, such that the coordinates of b are algebraic numbers (Proposition 3.5). This result will be used in the next section to find a sufficient condition for a polynomial mapping f to be strongly (s,r)-elusive. As a consequence, we will construct in the next section concrete polynomial mappings and multivariate polynomials whose circuit size is large. We note that the idea to use algebraic numbers to construct polynomials which are hard to compute first appeared in the works by Strassen-Schnorr and Heintz-Sieveking (Remark 3.8.1).

Given a polynomial mapping $f \in Pol(\mathbb{F}^n, \mathbb{F}^{n+k})$, where $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$ and $k \geq 1$, we are interested in the image $f(\mathbb{F}^n) \subset \mathbb{F}^{n+k}$. There are also several available methods to detect whether a point b belongs to the Zariski closure $\overline{f(\mathbb{F}^n)}$ of $f(\mathbb{F}^n) \subset \mathbb{F}^{n+k}$, based on algebraic description of the ideal of the sub-variety $\overline{f(\mathbb{F}^n)}$. The polynomial mapping $f = (f^1, \cdots, f^{n+k})$ induces a ring homomorphism

$$f^* : \mathbb{F}[Y_1, \cdots, Y_{n+k}] \to \mathbb{F}[X_1, \cdots, X_n], \quad Y_i \mapsto f^i(X_1, \cdots, X_n).$$

Denote by $I(f(\mathbb{F}^n))$ the ideal of $f(\mathbb{F}^n)$ (i.e. the ideal of all polynomials on $\mathbb{F}^m$ which vanish on $f(\mathbb{F}^n)$).

Lemma 3.1. *(*[4, Proposition 15.30], [7, Lemma 1.8.16]*) Assume that f is a polynomial mapping from $\mathbb{F}^n$ to $\mathbb{F}^{n+k}$. Then*
1. $\ker f^* = I(f(\mathbb{F}^n)) = I(\overline{f(\mathbb{F}^n)})$.
2. Let I be the ideal in $\mathbb{F}[X_1, \cdots, X_n, Y_1, \cdots, Y_{n+k}]$ generated by $\{Y_1 - f^1, \cdots, Y_{n+k} - f^{n+k}\}$. Then

$$\ker f^* = I \cap \mathbb{F}[Y_1, \cdots, Y_{n+k}].$$

Remark 3.2. Let $f : \mathbb{F}^n \to \mathbb{F}^m$ and $g : \mathbb{F}^s \to \mathbb{F}^m$ be two polynomial mappings. Clearly, $f(\mathbb{F}^n) \not\subset g(\mathbb{F}^s)$, if $\overline{f(\mathbb{F}^n)} \not\subset \overline{g(\mathbb{F}^s)}$, equivalently by Lemma 3.1, if $\ker f^* \not\supset \ker g^*$.

In general it is hard to find explicitly an element in $\ker f^*$. We know only algorithms for determining the generators of $\ker f^* = I \cap \mathbb{F}[Y_1, \cdots, Y_{n+k}]$ based on Gröbner's basis or on resultants for determining a special element of $\ker f^*$ of the corresponding system of polynomials, see e.g. [7]. These algorithms are time-consuming, and they do not give us any partial knowledge of the generators of $\ker f^*$ at the first glance. In [9] Kumar, Lokam, Patankar and Sarma used a result in effective elimination theory to get partial knowledge of an element in $\ker f^*$ and combining this knowledge with algebraic number field theory they obtained concrete matrices with high rigidity. Our extension of their method also uses the same result in effective elimination theory, namely the following

Lemma 3.3. *(*[3, p.6 Theorem 4]*) Let $I = \langle f^1, \cdots, f^s \rangle$ be an ideal in the polynomial ring $\mathbb{F}[Y_1, \cdots, Y_m]$ over an infinite field $\mathbb{F}$. Let d be the maximum total degree of the generators f^i. Let $Z = \{Y_{i_1}, \cdots, Y_{i_l}\}$ be a subset of indeterminates $\{Y_1, \cdots, Y_m\}$. If $I \cap \mathbb{F}[Z] \neq 0$ then there exists a non-zero polynomial $g \in I \cap \mathbb{F}[Z]$ such that $g = \sum_{i=1}^s g^i f^i$*

with $g^i \in \mathbb{F}[Y_1, \cdots, Y_m]$ *and* $\deg(g^i f^i) \le (\mu+1)(m+2)(d^\mu+1)^{\mu+2}$ *for* $i \in [1, s]$*, where* $\mu = \min\{s, m\}$*.*

Set $D(m, r) = (m+1)(m+2)(r^m+1)^{m+2}$.

Remark 3.4. Applying Lemmata 3.1 and 3.3 to the ideal $I = \langle Y_1 - f^1, \cdots, Y_{n+k} - f^{n+k} \rangle$, and to $Z = \{Y_1, \cdots, Y_{n+k}\}$, observing that $I \cap \mathbb{F}[Z] \neq 0$ if $k \ge 1$, we obtain the existence of a polynomial $g \in \ker f^* = I \cap \mathbb{F}[Z]$ whose degree is less than or equal $D(n+k, \deg f)$. Here $\deg f$ is the total degree of the generators f^i. Thus, to prove that a point $b \in \mathbb{F}^{n+k}$ does not belong to the image $f(\mathbb{F}^n) \subset \mathbb{F}^{n+k}$ it suffices to show that $g(b) \neq 0$ for any $g \in Pol^{D(n+k, \deg f)}(\mathbb{F}^n)$.

To find such a point $b \in \mathbb{F}^{n+k}$ we use the algebraic number field theory, assuming $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$, and that f is defined over $\mathbb{Q}$, i.e., all polynomials f^i in question are defined over $\mathbb{Q}$. The following Proposition is a generalization of [9, Theorem 8].

Proposition 3.5. *Let* $s \le m-1$ *and* $f : \mathbb{F}^s \to \mathbb{F}^m$ *be a polynomial mapping over* $\mathbb{Q}$ *of degree* r*.*

1. Assume that $p_1, \cdots, p_{s+1}$ *are distinct prime numbers such that* $p_i \ge D(m, r) + 2$ *for all* i*. Set*

$$b^i := e^{\frac{2\pi\sqrt{-1}}{p_i}} \text{ and } \tilde{b}^i := \sum_{j=1}^{i} a^i_j b^j$$

where $a^i_j \in \mathbb{Q}$ *and* $a^i_i \neq 0$*. Then* $\tilde{b} = (\tilde{b}^1, \cdots, \tilde{b}^{s+1}, a^{s+2}, \cdots, a^m) \in \mathbb{C}^m$ *does not belong to the image of* f *for* $\mathbb{F} = \mathbb{C}$ *and for any* $(a^{s+2}, \cdots, a^m) \in \mathbb{Q}^{m-s}$*.*

2. Assume that $p_1, \cdots, p_{s+1}$ *are distinct prime numbers such that* $p_i \ge 2D(m, r) + 3$ *for all* i*. Set*

$$b^i := e^{\frac{2\pi\sqrt{-1}}{p_i}} \text{ and } \tilde{b}^i := \sum_{j=1}^{i} a^i_j (b^j + \overline{b^j})$$

where $a^i_j \in \mathbb{Q}$ *and* $a^i_i \neq 0$*. Then* $\tilde{b} = (\tilde{b}^1, \cdots, \tilde{b}^{s+1}, a^{s+2}, \cdots, a^m) \in \mathbb{R}^m$ *does not belong to the image of* f *for* $\mathbb{F} = \mathbb{R}$ *and for any* $(a^{s+2}, \cdots, a^m) \in \mathbb{Q}^{m-s}$*.*

Proof. Proposition 3.5 is a consequence of Lemmas 3.1, 3.3, Remark 3.4 and Proposition 3.6 below. □

Proposition 3.6. *Assume that* $p_1, \cdots, p_m$ *are distinct prime numbers such that* $p_i \ge D + 2$ *for all* i*. Set* $b^i := e^{\frac{2\pi\sqrt{-1}}{p_i}}$ *and* $\tilde{b}^i := \sum_{j=1}^{i} a^i_j b^j$*, where* $a^i_j \in \mathbb{Q}$ *and* $a^i_i \neq 0$*.*

1. Then for all $g \in Pol^D(\mathbb{Q}^m) \subset Pol^D(\mathbb{C}^m)$ we have

$$g(\tilde{b}^1, \cdots, \tilde{b}^m) \neq 0.$$

2. Then for all $g \in Pol^{\lfloor \frac{D+1}{2} \rfloor}(\mathbb{Q}^m) \subset Pol^{\lfloor \frac{D+1}{2} \rfloor}(\mathbb{R}^m)$ we have

$$g(Re(\tilde{b}^1), \cdots, Re(\tilde{b}^m)) \neq 0,$$

where $\lfloor \frac{D+1}{2} \rfloor$ denotes the integral part of $\frac{D+1}{2}$, and $Re(a)$ denotes the real part of $a \in \mathbb{C}$.

Proof. 1. Let us prove Proposition 3.6.1 by induction on m. For $m = 1$ this is trivial, since $[\mathbb{Q}(\tilde{b}^1) : \mathbb{Q}] = p_1 - 1 \geq D + 1$.

Now suppose that the statement is true when the number of variables of a polynomial g is strictly less than m. Assume that the statement is not true for m, i.e. there exists $g \in Pol^D(\mathbb{Q}^m) \subset Pol^D(\mathbb{C}^m)$ such that

$$g(\tilde{b}^1, \cdots, \tilde{b}^m) = 0. \tag{3.1}$$

Let us write

$$g(Y_1, \cdots, Y_m) = \sum_{i=0}^{d} g_i(Y_1, \cdots, Y_{m-1}) Y_m^{d-i},$$

where $g_i \in \mathbb{Q}[Y_1, \cdots, Y_{m-1}]$, since g is defined over $\mathbb{Q}$. If g does not depend on Y_m, or equivalently $g_i = 0$ for $i \in [0, d-1]$, the induction assumption implies that the induction statement is also valid for m, since $g = g_d \in Pol^D(\mathbb{Q}^{m-1}) \subset Pol^D(\mathbb{C}^{m-1})$ satisfies

$$g(\tilde{b}^1, \cdots, \tilde{b}^m) \neq 0.$$

Thus, we can assume that Y_m enters in g. Hence

$$g(\tilde{b}^1, \cdots, \tilde{b}^{m-1})(x) \neq 0 \in \mathbb{Q}(\tilde{b}^1, \cdots, \tilde{b}^{m-1})[x].$$

Clearly, (3.1) implies that $\tilde{b}^m$ is a root of a non-zero polynomial in one variable of degree D over the extension $\mathbb{Q}(\tilde{b}^1, \cdots, \tilde{b}^{m-1})$.Thus

$$[\mathbb{Q}(\tilde{b}^1, \cdots, \tilde{b}^m) : \mathbb{Q}(\tilde{b}^1, \cdots, \tilde{b}^{m-1})] \leq D. \tag{3.2}$$

Since $\tilde{b}^i = \sum_{j=1}^{i} a_j^i b^j$, where $a_j^i \in \mathbb{Q}$ and $a_i^i \neq 0$, we have

$$\mathbb{Q}(\tilde{b}^1, \cdots, \tilde{b}^k) = \mathbb{Q}(b^1, \cdots, b^k) \text{ for all } k \leq m.$$

Thus (3.2) implies that

$$[\mathbb{Q}(b^1, \cdots, b^m) : \mathbb{Q}(b^1, \cdots, b^{m-1})] \leq D. \tag{3.3}$$

Since $\mathbb{Q}(b^m)$ is a Galois extension of $\mathbb{Q}$, applying [10, Theorem 1.12 p. 266] we obtain

$$[\mathbb{Q}(b^1, \cdots, b^m) : \mathbb{Q}(b^1, \cdots, b^{m-1})] = [\mathbb{Q}(b^m) : \mathbb{Q}] = p_m - 1 \geq D + 1.$$

Thus, (3.3) does not hold. The contradiction implies that Proposition 3.6.1 is also valid for m. This completes the proof of Proposition 3.6.1.

2. Now let us prove Proposition 3.6.2. Repeating the argument in the proof of Proposition 3.6.1 we derive Proposition 3.6.2 from the following

Lemma 3.7. *For $1 \leq i \leq m$, $\mathbb{Q}(Re(\tilde{b}^i))$ is a Galois extension of $\mathbb{Q}$ and $[\mathbb{Q}(Re(\tilde{b}^i)) : \mathbb{Q}] \geq \lfloor \frac{D+1}{2} \rfloor$.*

Proof. Since $\mathbb{Q}(Re(\tilde{b}^i))$ is a subfield of the Galois extension $\mathbb{Q}(b^i)$, whose Galois group is cyclic, $\mathbb{Q}(Re(\tilde{b}^i))$ is also a Galois extension. Note that the Galois group $G_{\mathbb{Q}(Re(\tilde{b}^i))}$ of $\mathbb{Q}(Re(\tilde{b}^i))$ is $\mathbb{Z}_{p_i-1}/\mathbb{Z}_2$. Hence

$$[Q(Re(\tilde{b}^i)) : \mathbb{Q}] \geq \#(G_{\mathbb{Q}(Re(\tilde{b}^i))}) = \frac{p_i - 1}{2} \geq \lfloor \frac{D+1}{2} \rfloor.$$

This proves Lemma 3.7. □

This completes the proof of Proposition 3.6. □

Remark 3.8. 1. One of the main ideas of the Kumar-Lokam-Patankar-Sarma method, adapted and developed to our case, is to relate the separable degree of the field extension $\mathbb{Q}(\alpha_1, \cdots, \alpha_n)$, where α_i are algebraic numbers, with the complexity of polynomials and polynomial mappings whose monomial coefficients are α_i. This idea has been invented before by Strassen-Schnorr and Heintz-Sieveking. We refer the reader to [2, Chapter 9] for exposition of their methods. Their technique is used to construct polynomials P_n in one variable of degree n of multiplicity complexity with lower bound of type n^a, $a < 1$, where the coefficients of P_n are algebraic numbers. Our technique is used, in particular, to construct (*poly*(n)-definable) multivariate polynomial mappings and polynomials of constant degree, whose (constant-depth) circuit size is high (Propositions 4.7, 4.12, Corollaries 4.9, 4.14).

2. Let $f : \mathbb{F}^n \to \mathbb{F}^m$ be a mapping. The question whether f is a polynomial mapping defined over $\mathbb{Q}$ depends on the choice of a basis $(V_1, \cdots, V_n)$ of $\mathbb{F}^n$ as well as on the choice of a basis $(W_1, \cdots, W_m)$ of $\mathbb{F}^m$. Assume that $f : \mathbb{F}^n \to \mathbb{F}^m$ is a polynomial mapping defined over $\mathbb{Q}$ with respect to a basis $(V_1, \cdots, V_n)$ of $\mathbb{F}^n$ and a basis $(W_1, \cdots, W_m)$ of $\mathbb{F}^m$. Then f is also a polynomial mapping defined over $\mathbb{Q}$ with respect a basis $(V_1', \cdots, V_n')$ of $\mathbb{F}^n$ and a basis $(W_1', \cdots, W_m')$ of $\mathbb{F}^m$, if $V_i' = \sum_j A_{ij} V_j$, $W_i' = \sum B_{i'l} W_l$ and $A_{ij}, B_{i'l}$ are rational numbers. In other words, the basis (V_i') (resp. (W_j')) is obtained from the basis (V_i) (resp. (W_j)) by a linear transformation over $\mathbb{Q}$.

3. The set of all transformations $(a^i_j) \in Mat_n(\mathbb{Q})$ with $a^i_j = 0$ if $j > i$ and $a^i_i \neq 0$, which enter in Proposition 3.5, forms the solvable group $B_n(\mathbb{Q})$.

4. Examples and applications

In this section, using the methods developed in the previous sections, we construct concrete examples of (s,r)-elusive functions (Proposition 4.5, 4.12). As a result, we construct a sequence of $poly(n)$-definable polynomial mappings $P_n : \mathbb{F}^{2n} \to \mathbb{F}^n$ of constant degree $5r+1$ whose depth-r circuit size is greater than $n^2/(50r^2)$, and consequently, a sequence of multivariate $poly(n)$-definable polynomials of constant degree $5r+2$ whose depth-$\lfloor r/3 \rfloor$ circuit size is greater than $n^2/250r^2$ (Proposition 4.7, Corollary 4.9). We compare this result with similar results (Remark 4.10). We also construct a sequence of elusive polynomial mappings, whose monomial coefficients are algebraic numbers, which give polynomials with algebraic number coefficients such that their circuit size is very large (Corollary 4.14).

To apply the effective elimination theory to elusive functions, we need to estimate the degree of the evaluation mapping.

Lemma 4.1. *The evaluation map $Ev^k_{r,s,m}$, defined in (2.1), is of total degree $r+1$, it is also defined over $\mathbb{Q}$.*

Proof. Let us compute the degree of the evaluation map $Ev^k_{r,s,m}$. Let $\{V_j,\, 1 \le j \le s\}$ be a basis of $\mathbb{F}^s$. Let $\{(X_1^{i_1}\cdots X_s^{i_s})|\ \sum_{j=1}^s i_j \le r\}$ be the basis consisting of monomials in $Pol^r(\mathbb{F}^s)$. Let $f = (f^1, \cdots, f^m) \in Pol^r(\mathbb{F}^s, \mathbb{F}^m)$ where

$$f^l := \sum_{0 \le i_1 + \cdots + i_s \le r} a_{i_1\cdots i_s,l}(X_1^{i_1}\cdots X_s^{i_s}).$$

Let $b = (b_1, \cdots, b_k) \in (\mathbb{F}^s)^k$ where

$$b_i = \sum_j b_i^j V_j \in \mathbb{F}^s.$$

Then

$$Ev^k_{r,s,m}(f,b) = (f(\sum_{j=1}^s b_1^j V_j), \cdots, f(\sum_{j=1}^s b_k^j V_j)) \in (\mathbb{F}^m)^k. \tag{4.1}$$

Clearly $Ev^k_{r,s,m}$ is a polynomial mapping, whose degree does not depend on k or on m. Note that for $k=1$ and $m=1$ we have

$$Ev^1_{r,s,1}(f,b) = \sum_{0 \le i_1 + \cdots + i_s \le r} a_{i_1\cdots i_s}(b_1^1)^{i_1}\cdots(b_1^s)^{i_s} \in \mathbb{F}. \tag{4.2}$$

(4.2) implies that $Ev^1_{r,s,1}$ is of degree 1 on f and of maximal degree r on b. This proves the second assertion of Lemma 4.1. □

Next, we need a choice of a basis of the space $Pol^r(\mathbb{F}^n)$ which is not monomial.

Definition 4.2. A polynomial $(X - i)(X - i + 1) \cdots X \in \mathbb{F}[X]$ is called *a pseudo-monomial*, if $i \in \mathbb{N}$. A constant is also called a pseudo-monomial. A polynomial $f \in \mathbb{F}[X_1, \cdots, X_n]$ is called *a pseudo-monomial*, if $f = f^1 \cdots f^n$, where, for $1 \le i \le n$, $f^i \in \mathbb{F}[X_i]$ and f^i is a pseudo-monomial.

Remark 4.3. 1. According to the lexicographical ordering in $Pol^p(\mathbb{F}^n)$ the linear transformation $Pol^p(\mathbb{F}^n) \to Pol^p(\mathbb{F}^n)$ sending the basis consisting of pseudo-monomials to the standard basis of monomials is an element of the solvable group $B_{\binom{n+p}{p}}(\mathbb{Q})$. In particular, any polynomial $f \in Pol^p(\mathbb{F}^n)$ can be written in a unique way as a linear combination of pseudo-monomials.

2. The notion of pseudo-monomials is motivated by the interpolation formulas (2.7), (2.8), (2.9), (2.15), (2.16) for polynomial mappings. Using these formulas we have defined the coefficients $\lambda^i_{i_1,\cdots i_n}$ of the pseudo-monomials $(X_1 - i_1)(X_1 - i_1 + 1) \cdots X_1 (X_2 - i_2) \cdots X_2 \cdots (X_n - i_n) \cdots X_n$ in the component f^i of a polynomial mapping $f : \mathbb{F}^n \to \mathbb{F}^m$ as a rational linear combination of the coordinates of the given points $b_{i_1 \cdots i_m} \in \mathbb{F}^m$.

Next, we need the following

Lemma 4.4. *Assume that $1 \le s < m$. Then there exists a (s, r)-elusive K-tuple in $\mathbb{F}^m$, if*

$$K \ge \frac{m\binom{s+r}{s} + 1}{m - s}. \tag{4.3}$$

Proof. Note that

$$\dim(Pol^r(\mathbb{F}^s, \mathbb{F}^m) \times (\mathbb{F}^s)^K) = m\binom{s+r}{s} + sK.$$

It follows that the image of the evaluation map $Ev^K_{s,r,m}$ is a proper subset of co-dimension at least 1 in $\mathbb{F}^{mK}$ if K satisfies (4.3). Taking into account Lemma 2.4, we obtain immediately Lemma 4.4. □

Using the interpolation formula in Proposition 2.6 we shall construct from (s, r)-elusive K-tuples in $\mathbb{F}^m$ (s, r)-elusive polynomial mappings

$f : \mathbb{F}^n \to \mathbb{F}^m$. Given K satisfying (4.3), let us assume that two positive integers n, p satisfy the following conditions

$$\binom{n+p}{n} \geq K \geq \frac{m\binom{s+r}{s}+1}{m-s}. \tag{4.4}$$

By Proposition 2.6, the first inequality in (4.4) is a sufficient condition for the existence of a polynomial mapping $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ such that the image $f(\mathbb{F}^n)$ contains a given K-tuple in $\mathbb{F}^m$.

Proposition 4.5. *Assume that n, p satisfy (4.4) with $K = \binom{n+p}{n}$. Let $\mathcal{B}$ be either the monomial basis or the pseudo-monomial basis of the space $Pol^p(\mathbb{R}^n) \subset Pol^p(\mathbb{C}^n)$.*

1. Assume that $f^1, \cdots, f^m$ are polynomials in $Pol^p(\mathbb{C}^n)$ such that the coefficients of each f^j w.r.t. the basis $\mathcal{B}$, according to the lexicographical ordering, and beginning with the smallest term, are

$$e^{\frac{2\pi\sqrt{-1}}{p_1^j}}, \cdots, e^{\frac{2\pi\sqrt{-1}}{p_K^j}}$$

where $\{p_i^j, 1 \leq i \leq K, 1 \leq j \leq m\}$ are distinct prime numbers such that $p_i^j \geq D(m,r)+2$. Then the polynomial mapping $f = (f^1, \cdots, f^m) : \mathbb{C}^n \to \mathbb{C}^m$ is (s,r)-elusive.

2. Assume that $f^1, \cdots, f^m$ are polynomials in $Pol^p(\mathbb{R}^n)$ such that the coefficients of each f^j w.r.t. the basis $\mathcal{B}$, according to the lexicographical ordering, and beginning with the smallest term, are

$$Re(e^{\frac{2\pi\sqrt{-1}}{p_1^j}}), \cdots, Re(e^{\frac{2\pi\sqrt{-1}}{p_K^j}}),$$

where $\{p_i^j, 1 \leq i \leq K, 1 \leq j \leq m\}$ are distinct prime numbers such that $p_i^j \geq 2D(m,r)+3$. Then the polynomial mapping $f = (f^1, \cdots, f^m) : \mathbb{R}^n \to \mathbb{R}^m$ is (s,r)-elusive.

Proof. It suffices to show that the polynomial mappings f defined in Proposition 4.5 are strongly (s,r)-elusive. Equivalently, we need to show that the set

$$S_K := \{f(i_1, \cdots, i_n) | \, i_j \in \mathbb{N} \text{ and } \sum_{j=1}^n i_j \leq p\} \subset \mathbb{F}^m,$$

$\mathbb{F} = \mathbb{C}$ or $\mathbb{F} = \mathbb{R}$, is a (s,r)-elusive K-tuple. We will show that the associated point $\overline{S_K} \in (\mathbb{F}^m)^K$ does not belong to the image of the evaluation map $Ev^K_{r,s,m}$. By Lemma 4.1 the evaluation map $Ev^K_{r,s,m}$ is a polynomial mapping of degree $(r+1)$, moreover it is defined over $\mathbb{Q}$. Remarks 3.8 and 4.3.2 imply that Lemma 4.1 also holds with respect to the basis of $(\mathbb{F}^m)^K = (\mathbb{F}^K)^m = Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ that is induced from the basis of pseudo-monomials in $Pol^p(\mathbb{F}^n)$. Now we will apply Proposition

3.5 to show that $\overline{S_K}$ does not belong to the image of $Ev^k_{r,s,m}$; more precisely, we will verify that the coordinates of $\overline{S_K}$ with respect to the pseudo-monomial basis in $(\mathbb{F}^K)^m = Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ satisfy the conditions of Proposition 3.5. Using Remarks 3.8.2 and 4.3.1 it suffices to consider the case of $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ whose pseudo-monomial coefficients are given by the recipe in Proposition 4.5.

By the assumption of Proposition 4.5 the first m coordinates of $\overline{S_K} \in (\mathbb{F}^K)^m = Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ are the smallest pseudo-monomials according to the lexico-graphical ordering, i.e., they are field elements. These field elements are numbers

$$e^{\frac{2\pi\sqrt{-1}}{p_1^1}} \cdots, e^{\frac{2\pi\sqrt{-1}}{p_1^m}},$$

if $\mathbb{F} = \mathbb{C}$. (The case $\mathbb{F} = \mathbb{R}$ is similar). Now assume that the conditions of Proposition 3.5 hold for the first lm-coordinates of $\overline{S_K} \in (\mathbb{F}^K)^m = Pol^r(\mathbb{F}^n, \mathbb{F}^m)$, for $l \geq 1$. The interpolation formula (2.15) for the $(l+1)j$ coordinate $(S_K)^j_{l+1}$ of $\overline{S_K}$, $1 \leq j \leq m$, if $\mathbb{F} = \mathbb{C}$, has the following form

$$(\overline{S_K})^{l+1}_j = a^{l+1}_j e^{\frac{2\pi\sqrt{-1}}{p^j_{l+1}}} + \sum_{1 \leq k \leq l} a^{l+1,k}_j e^{\frac{2\pi\sqrt{-1}}{p^j_k}},$$

where $a^{l+1,k}_j \in \mathbb{Q}$ and $a^{l+1}_j \neq 0$. (The case $\mathbb{F} = \mathbb{R}$ is similar). Thus the conditions in Proposition 3.5 also hold for first $(l+1)m$-coordinates of $\overline{S_K} \in (\mathbb{F}^K)^m = Pol^r(\mathbb{F}^n, \mathbb{F}^m)$. This completes the proof of Proposition 4.5. □

In [14, §3.4] Raz proposed a method for constructing polynomials of large complexity using (s, r)-elusive functions. Propositions 4.6, 4.7 below are sample applications of Raz's method.

Given a tuple of n^2 function $f_{ij} \in \mathbb{F}[X_1, \cdots, X_n]$, $1 \leq i, j \leq n$, we define an n-tuple of polynomials $\tilde{f}_i \in \mathbb{F}[X_1 \cdots, X_n, Z_1, \ldots, Z_n]$, $i \in [1, n]$, as follows (cf. [14, §3.3])

$$\tilde{f}_i(X_1, \cdots, X_n, Z_1, \cdots, Z_n) := \sum_{j=1}^{n} f_{ji}(X_1, \cdots, X_n) Z_j \tag{4.5}$$

Proposition 4.6. [14, Proposition 3.11] *Let $n, r \leq s$ be integers. Let $f : \mathbb{F}^n \to \mathbb{F}^{n^2}$ be a polynomial mapping. If f is (s, r)-elusive, then any depth-r arithmetic circuit over $\mathbb{F}$ for the n-tuple $\{\tilde{f}_i : \mathbb{F}^{2n} \to \mathbb{F}, i \in [1, n]\}$ of polynomials defined by (4.5) is of size greater than s.*

Using Proposition 4.6 and our construction of (s, r)-elusive functions in Proposition 4.5, we shall construct sequences of polynomials with large constant-depth circuit size.

Proposition 4.7. *Let $\mathbb{F} = \mathbb{C}$ or $\mathbb{F} = \mathbb{R}$, and $1 \le r \in \mathbb{N}$ a constant. There are infinitely many sequences of poly(n)-definable polynomial mappings $\tilde{f}_{n,r} \in Pol^{5r+1}(\mathbb{F}^{2n}, \mathbb{F}^n)$, which satisfy the following properties. All the coefficients of $\tilde{f}_{n,r}$ are algebraic numbers, and any (unbounded fanin) depth-r arithmetic circuit over $\mathbb{F}$ for $\tilde{f}_{r,n}$ is of size greater than $\frac{n^2}{50r^2}$.*

Proof. Let $n' \ge r^2$ be an integer, and set

$$n := 5n'r,\ p := 5r,\ m := (n')^2,\ s := \lfloor (n')^2/2 \rfloor.$$

First we will show that the chosen values (n, p, m, s) satisfy Condition (4.4). Since $(m - s) \ge m/2$ it suffices to show

$$\binom{5n'r + 5r}{5r} \ge 2\frac{(n')^2\binom{\lfloor\frac{(n')^2}{2}\rfloor + r}{r} + 1}{(n')^2}. \tag{4.6}$$

Clearly (4.6) is a consequence of Lemma 4.8, which we now prove.

Lemma 4.8. *We have*

$$\binom{5n'r + 5r}{5r} \ge 2[\binom{\lfloor\frac{(n')^2}{2}\rfloor + r}{r} + 1]. \tag{4.7}$$

Proof. We rewrite the LHS of (4.7) as

$$\Pi_{k=0}^{r-1}\frac{(5n'r + 5k + 1)(5n'r + 5k + 2)\cdots(5n'r + 5k + 5)}{(5k + 1)(5k + 2)\cdots(5k + 5)}, \tag{4.8}$$

and RHS of (4.7) as

$$2(\Pi_{k=1}^{r}\frac{\lfloor\frac{(n')^2}{2}\rfloor + k}{k} + 1). \tag{4.9}$$

Using (4.8) and (4.9), taking into account the following inequalities

$$2(\Pi_{k=1}^{r}\frac{\lfloor\frac{(n')^2}{2}\rfloor + k}{k} + 1) \le \Pi_{k=1}^{r}(\frac{(n')^2 + 2k}{k} + 2) \le ((n')^2 + 4)^r,$$

$$\frac{(5n'r + 5k + 1)(5n'r + 5k + 2)\cdots(5n'r + 5k + 5)}{(5k + 1)(5k + 2)\cdots(5k + 5)} \ge (\frac{5n'r + 5k + 5}{5k + 5})^5$$

$$\ge (\frac{(n' + 1)r}{r})^5 \text{ (since } k + 1 \le r),$$

to prove Lemma 4.8 it suffices to establish the following inequality

$$(n' + 1)^5 \ge (n')^2 + 4. \tag{4.10}$$

Clearly (4.10) holds, since $n' \ge 1$. This completes the proof of Lemma 4.8. □

Since (4.6) is fulfilled, Proposition 4.5 implies that there exists a (s, r)-elusive function $f'_{n,r} \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$.

We extend $f'_{n,r}$ to a polynomial mapping, denoted by $f_{n,r}$, from $\mathbb{F}^n$ to $\mathbb{F}^{n^2}$ by composing $f_{n,r}$ with the canonical embedding $\mathbb{F}^{(n')^2} \to \mathbb{F}^{n^2}$. Clearly $f_{n,r}$ is also (s, r)-elusive. Since r is fixed and all the coefficients of $f_{n,r}$ are given, $f_{n,r}$ is $poly(n)$-definable. Let $\tilde{f}_{n,r} : \mathbb{F}^{2n} \to \mathbb{F}^n$ be the polynomial mapping obtained from $f_{n,r} : \mathbb{F}^n \to \mathbb{F}^{n^2}$ by recipe (4.5). Set

$$\tilde{f}_{n,r} := ((\tilde{f}_{n,r})^1, \cdots, (\tilde{f}_{n,r})^n),$$

where $(\tilde{f}_{n,r})^i$, $i \in [1, n]$, is the i-th coordinate of the polynomial mapping $\tilde{f}_{n,r}$. Since $f_{n,r} \in Pol^{5r}(\mathbb{F}^n, \mathbb{F}^{n^2})$, we have $\tilde{f}_{n,r} \in Pol^{5r+1}(\mathbb{F}^{2n}, \mathbb{F}^n)$. Furthermore, $(\tilde{f}_{n,r})^i, 1 \leq i \leq n$, is $poly(n)$-definable, since r is fixed. Taking into account Proposition 4.6 this completes the proof of Proposition 4.7. □

Corollary 4.9. *Let $\tilde{f}_{n,r} := ((\tilde{f}_{n,r})^1, \cdots, (\tilde{f}_{n,r})^n) \in Pol^{5r+1}(\mathbb{F}^{2n}, \mathbb{F}^n)$ be the polynomial mappings defined in Proposition 4.7. Let $\hat{f}_{n,r} : \mathbb{F}^{2n} \times \mathbb{F}^n \to \mathbb{F}$ be defined by*

$$\hat{f}_{n,r}(X_1, \cdots, X_n, Z_1, \cdots, Z_n, Y_1, \cdots, Y_n) := \sum_{i=1}^{n} (\tilde{f}_{n,r})_i(X_1, \cdots, Z_n) Y_i.$$

Then any depth-$\lfloor r/3 \rfloor$ arithmetic circuit for $\hat{f}_{n,r}$ is of size greater than $\frac{n^2}{250r^2}$.

Proof. We use Raz' argument in [14, Corollary 4.6]. Baur and Strassen proved that if a polynomial $\hat{f}$ can be computed by an arithmetic circuit of size s and depth d, then all partial derivatives of that polynomial can be computed by one arithmetic circuit of size $5s$ and depth $3d$. □

Remark 4.10. In [14, Lemma 4.1] Raz proposed a combinatoric method to construct a $([n^{1+1/(2r)}], r)$-elusive function of degree $5r$ from $\mathbb{F}^{5nr}$ to $\mathbb{F}^{n^2}$, if n is prime and $1 \leq r \leq (\log_2 n)/100$. As a result, Raz obtained a lower bound $n^{1+1/(2r)}$ for the size of any depth-r arithmetic circuit computing $\tilde{f}_n \in Pol^{5r+1}(\mathbb{F}^{n(5r+1)}, \mathbb{F}^n)$ [14, Corollary 4.5] and a lower bound $n^{1+1/(2r)}/5$ for any depth-$\lfloor r/3 \rfloor$ arithmetic circuit computing $\hat{f}_n \in Pol^{5r+1}(\mathbb{F}^{n(5r+2)})$ [14, Corollary 4.6]. Note that his polynomials $\tilde{f}_i$ have coefficients taking values in $\{0, 1\}$. Raz's results is an improvement of Shoup's and Smolensky's result [16], which gives a lower bound of $\Omega(dn^{1+1/d})$ for depth d arithmetic circuits, for explicit polynomials of degree $O(n)$ over $\mathbb{C}$. Shoup and Smolensky used algebraic independent numbers and a sequence of rapidly growing integers of the form $2, 2^n, \cdots, 2^{n^{n-1}}$ to construct such polynomials. We also like to mention better lower bounds for depth four homogeneous circuits, see e.g. [5], but these constant deep circuits have lower bound on the fanin at the bottom layer of product gates (and ours do not have such a bound).

Raz also generalized his construction of polynomials of large circuit size in Proposition 4.6 as follows [14, §3.1, 3.3]. We fix m' to be the number of monomials of total degree exactly r in n variables, that is, $m' = \binom{n+r-1}{r}$ and we fix $m = m' \cdot n$. Let M be the set of all monomials of total degree exactly r in the variables $\{z_1, \cdots, z_n\}$. Let $h : M \to [1, m']$ be the lexicographic order of monomials. Let us denote by $Pol^p_{hom}(\mathbb{F}^n, \mathbb{F}^m)$ the space of homogeneous polynomial mappings of degree p from $\mathbb{F}^n$ to $\mathbb{F}^m$. Given a homogeneous polynomial mapping $f = (f_{1,1}, \cdots, f_{m',n}) \in Pol^p_{hom}(\mathbb{F}^n, \mathbb{F}^m) = (Pol^p_{hom}[x_1, \cdots, x_n])^m$ we define an n-tuple of polynomials $\tilde{f}_1, \cdots, \tilde{f}_n \in \mathbb{F}[x_1, \cdots, x_n, z_1, \cdots, z_n]$ as follows (cf. (4.5))

$$\tilde{f}_i(x_1, \cdots, x_n, z_1, \cdots z_n) := \sum_{g \in M} f_{h(g),i}(x_1, \cdots, x_n) \cdot g =$$

$$= \sum_{j=1}^{m'} f_{j,i}(x_1, \cdots, x_n) h^{-1}(j). \tag{4.11}$$

Now we define a polynomial $\tilde{f} \in \mathbb{F}[x_1, \cdots, x_n, z_1, \cdots, z_n, w_1, \cdots, w_n]$ using (4.11) and the following formula (cf. the formula in Corollary 4.9)

$$\tilde{f} = \sum_{i=1}^{n} w_i \cdot \tilde{f}_i. \tag{4.12}$$

Lemma 4.11. *(*[14, Corollary 3.8]*) Let $1 \le r \le n \le s$, and $m = n \cdot \binom{n+r-1}{r}$ be integers. Let $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ be a polynomial mapping. If f is $(s, 2r-1)$-elusive, then any arithmetic circuit for the polynomial $\tilde{f} : \mathbb{F}^{3n} \to \mathbb{F}$ constructed by recipe (4.12) is of size $\ge \Omega(\sqrt{s}/r^4)$.*

In [14] Raz did not specify the value $\Omega(\sqrt{s}/r^4)$ but it is not hard to find that value using Raz's results in [14]. In [11] we developed Raz's method, in particular we specified the lower bound for the circuit size of $\tilde{f}$, see e.g. [11, Proposition 4.3] for a slightly generalized assertion.

Now we shall apply Lemma 4.11 and our methods to construct polynomials with algebraic number coefficients with large circuit size. First we need the following

Proposition 4.12. *Given $4 \le r' \in \mathbb{N}$, for $n \in \mathbb{N}$ set*

$$s(n) := (\lfloor \frac{n}{(r'-1)r'} \rfloor)^{r'-3},\ m(n) := n \cdot \binom{n-1+r'}{r'},\ p = (r'-1)(2r'-1).$$

Then, for $\mathbb{F}=\mathbb{C}$ *or* $\mathbb{F}=\mathbb{R}$, *if* $n\ge 2(r'-1)r'$ *and* $(n+r-4)^4\ge r!$ *there exists a polynomial mapping* $f\in Pol^p(\mathbb{F}^n,\mathbb{F}^{m(n)})$ *such that* f *is* $(s(n),2r'-1)$*-elusive, moreover the monomial coefficients of* f *are algebraic numbers.*

Proof. Set $r:=2r'-1$. We will show that $(n,p,m=m(n),s,r)$ defined in Proposition 4.12 satisfy (4.4) for $K:=\binom{n+p}{p}$, i.e., we need to verify that

$$\binom{n+p}{n}\ge\frac{m\binom{s+r}{s}+1}{m-s}. \tag{4.13}$$

Since $(n+r-4)^4\ge r!$ we get

$$(r')!\cdot n^{r'-4}\le (n+r-4)^4\cdot n^{r'-4}<n\cdot(n+1)\cdot\dots\cdot(n+r'-1). \tag{4.14}$$

Since $4\le r'$ and $n\ge 2$, taking into account (4.14), we obtain

$$s(n)<n^{r'-3}\le\frac{n}{2}n^{r'-4}\le\frac{n}{2}\cdot\binom{n-1+r'}{r'}\le\frac{m+1}{2}. \tag{4.15}$$

Abbreviating $s(n)$ as s, we deduce from (4.15)

$$\frac{m\binom{s+r}{s}+1}{m-s}\le\frac{(m+1)\binom{s+r}{s}}{m-s}<\frac{(m+1)\binom{s+r}{s}}{m-\frac{m+1}{2}}\le 2(1+\frac{2}{m-1})\binom{s+r}{s}. \tag{4.16}$$

Clearly (4.13) follows from (4.16) and the following inequality

$$\binom{n+p}{n}\ge 2(1+\frac{2}{m-1})\binom{s+r}{s}, \tag{4.17}$$

which we now prove. We rewrite the LHS of (4.17) as

$$\Pi_{k=0}^{r-1}\frac{(n+(r'-1)k+1)(n+(r'-1)k+2)\cdots(n+(r'-1)(k+1))}{((r'-1)k+1)((r'-1)k+2)\cdots(r'-1)(k+1)}. \tag{4.18}$$

Since $p=(r'-1)(2r'-1)=(r'-1)r$, we rewrite the RHS of (4.17) as

$$2(1+\frac{2}{m-1})\Pi_{k=1}^{r}\frac{s+k}{k}. \tag{4.19}$$

Lemma 4.13. *For all* $0\le k\le r-1$ *we have*

$$\frac{(n+1)^{r'-1}}{(k+1)^{r'-1}}\ge 2\frac{s+k+1}{k+1}. \tag{4.20}$$

Proof. To prove Lemma 4.13 it suffices to establish the following inequality

$$(n+1)^{r'-1}\ge 2\cdot r^{r'-2}\cdot(s+2r'-1). \tag{4.21}$$

Since $r \geq 7$ we have

$$\frac{s+2r'-1}{r} < \frac{s}{2} = \frac{1}{2}(\lfloor \frac{n}{(r'-1)r'} \rfloor)^{r'-3} <$$

$$\frac{1}{2}(\frac{n}{(r'-1)r'})^{r'-1} < \frac{1}{2}(\frac{n+1}{r})^{r'-1}. \tag{4.22}$$

Clearly (4.22) implies (4.21). This completes the proof of Lemma 4.13. □

Using (4.18) and Lemma 4.13 we obtain

$$\binom{n+p}{n} \geq \Pi_{k=0}^{r-1} \frac{(n+1)^{r'-1}}{(k+1)^{r'-1}} \geq \Pi_{k=1}^{r}(2\frac{s+k}{k}). \tag{4.23}$$

Taking into account (4.19), we obtain (4.17) from (4.23). This proves (4.13).

Since (4.13)holds, we can apply Proposition 4.5 to get a (s,r)-elusive mapping $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$, whose monomial coefficients are algebraic numbers are $\exp(\frac{2\pi\sqrt{-1}}{p_j^i})$ or its real part.

This completes the proof of Proposition 4.12. □

Lemma 4.11 and Proposition 4.12 yield immediately

Corollary 4.14. *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 $f_n \in Pol^{p+r'+1}(\mathbb{F}^{3n})$, whose coefficients are algebraic numbers, such that*

$$L(f_n) \geq \Omega(\frac{\lfloor \frac{n}{r'(r'-1)} \rfloor^{\frac{r'-3}{2}}}{(r')^4}).$$

Proof. Taking into account Lemma 4.11 and Proposition 4.12, it suffices to prove that if $r' = \ln\ln n$ and n is sufficient large, then $(n+r-4)^4 \geq r!$. Clearly, $(n+r-4)^4 \geq r!$ follows from $r\ln r < \ln n$. Since $r > \ln r$ for sufficiently large r, it suffices to show that $r^2 < \ln n$, or equivalently $2\ln r < \ln\ln n$. The last inequality holds for large r, since $2\ln r < r = \ln\ln n$. □

Note that Corollary 4.14 yields a much better lower bound than that in Proposition 4.7, whose assertion we have compared with a similar result by Raz and with that one by Shoup and Smolensky. This demonstrates the effectiveness of our methods.

Acknowledgements

I am indebted to Pavel Pudlak for his support, stimulating helpful discussions and critical remarks. I am thankful to Gerhard Pfister for his explanation of their results in [7], to Ran Raz for his motivating lecture in Prague [15], and to Sasha Sivatsky for his helpful remarks and to Partha Mukhopadhyay for stimulating discussions. A part of this note has been written during my visit of MSRI, Berkeley, GIT, Atlanta, and ASSMS, Government College University, Lahore-Pakistan. I thank these institutions for their hospitality 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] A. Bernasconi, E. W. Mayr, M. Mnuk and M. Raab, Computing the Dimension of a Polynomial Ideal, http://www14.informatik.tu-muenchen.de/personen/raab/, (2002).

[4] D. Eisenbud, Commutative algebras with a view toward Algebraic geometry, Springer-Verlag, 1994.

[5] 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.

[6] J. zur Gathen, Feasible Arithmetic Computations: Valiant's Hypothesis, J. Symbolic Computation (1987) 4, 137-172.

[7] G.-M. Greuel and G. Pfister, A SINGULAR Introduction to Commutative Algebra, Springer-Verlag, (2007).

[8] M. Gasca and T. Sauer, Polynomial interpolation in several variables. Multivariate polynomial interpolation. Adv. Comput. Math. 12 (2000), no. 4, 377-410.

[9] A Kumar, S. V. Lokam, V.M. Patankar, J. Sarma, Using Elimination Theory to construct Rigid Matrices, arxiv/pdf/0910/0910.5301v1.pdf.

[10] S. Lang, Algebra, Springer, 2002.

[11] H. V. Lê, Lower bounds for the circuit size of partially homogeneous polynomials, arXiv:1302.3360.

[12] T. Mignon and N. Ressayre, A quadratic bound for the Determinant and Permanent Problem, IMRN 79 (2004), 4241-4253.

[13] 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.

[14] R. Raz, Elusive Functions and Lower Bounds for Arithmetic Circuits, Theory Of Computing Vol. 6, article 7 (2010).

[15] R. Raz, How to fool people to work on circuit lower bounds, lecture in the Fall school in Prague, (2009).

[16] V. Shoup and R. Smolensky, Lower Bounds for Polynomial Evaluation and Interpolation, Problems FOCS 1991: 378-383.

[17] A. Shpilka and A. Yehudauoff, Arithmetic Circuit: a survey of recent results an open questions, Foundations and Trends in Theoretical Computer Science, 5(2010), 207-388.

[18] 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.

[19] 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