Sets of Linear Forms Which Are Hard to Compute

Michael Kaminski

Department of Computer Science, Technion – Israel Institute of Technology, Haifa, Israel

Igor E. Shparlinski

School of Mathematics and Statistics, University of New South Wales, Sydney, Australia

Abstract

We present a uniform description of sets of m linear forms in n variables over the field of rational numbers whose computation requires $m(n-1)$ additions. Our result is based on bounds on the height of the annihilating polynomials in the Perron theorem and an effective form of the Lindemann–Weierstrass theorem which is due to Sert (1999).

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory

Keywords and phrases Linear algorithms, additive complexity, effective Perron theorem, effective Lindemann–Weierstrass theorem

Digital Object Identifier 10.4230/LIPIcs.MFCS.2021.66

Funding *Igor E. Shparlinski*: During this work, the author was supported by Australian Research Council Grant DP180100201.

Acknowledgements The authors would like to thank Michel Waldschmidt for the suggestion to use the work of Sert [11] in their argument.

1 Introduction

Evaluating a set of a linear forms is a natural computation task that frequently appears in both theory and applications. For a matrix

$$\Delta = \begin{pmatrix} \delta_{1,1} & \delta_{1,2} & \cdots & \delta_{1,n} \\ \delta_{2,1} & \delta_{2,2} & \cdots & \delta_{2,n} \\ \vdots & \vdots & & \vdots \\ \delta_{m,1} & \delta_{m,2} & \cdots & \delta_{m,n} \end{pmatrix} \tag{1}$$

and a column vector

$$\boldsymbol{x} = (x_1, \ldots, x_n)^T \tag{2}$$

linear forms are presented as a matrix-vector product

$$\Delta\,\boldsymbol{x} = (\delta_{j,1}x_1 + \ldots \delta_{j,n}x_n)_{j=1}^{m} \tag{3}$$

in which the matrix entries $\delta_{s,t}$ are fixed values and the vector entries x_s are varying inputs and computations are by means of *linear* algorithms. As expected, the complexity of a linear algorithm is its number of additions and we are interested in sets of linear forms of high complexity.

Obviously, the set of linear forms (3) can be computed in $m(n-1)$ additions. However, in finite fields, this trivial upper bound is not the best possible. Namely, over a finite field of q elements, it can be computed in $O(mn/\log_q m)$ additions, see [10, Theorem 1], where the implied constants are absolute. On the other hand (in finite fields), when $m = O(n)$, there exist $\delta_{s,t}$, $s = 1, \ldots, m$ and $t = 1, \ldots, n$, for which any computation of (3) requires $\Omega(mn/\log_q m)$ additions, cf. [10, Section 5]. In fact, this lower bound holds for almost all

$m \times n$ matrices with $m = O(n)$, see Appendix B.2 for the precise statement and the proof by a *counting argument*. Thus, for each pair of positive integers m and n such that $m = O(n)$, the entries of such a matrix can be effectively computed, but to describe them uniformly (in m and n) is a very difficult open problem. Even no example of a non-linear complexity is known from the literature.

The situation is quite different when the underlying field is infinite. By a *transcendence degree argument*, it is easy to see that, over the field of real numbers $\mathbb{R}$, say, when the coefficients of the linear forms are algebraically independent, the computation of (3) requires $m(n-1)$ additions (cf. [4, Section 5.2]). This leads to a natural question: what about the field of rational numbers $\mathbb{Q}$? Refining the transcendence degree argument we establish the existence of sets of linear forms (3) over $\mathbb{Q}$ whose computation requires $m(n-1)$ additions. Moreover, as it is shown in Appendix B.3, almost all sets of linear forms (3) are of such complexity. The main result of our paper is a uniform description of such a set.

Namely, we show that, if the entries of a matrix Δ are algebraically independent and Γ is "sufficiently close" to Δ, then computing $\Gamma \boldsymbol{x}$ also requires $m(n-1)$ additions. However, an estimate of the above "sufficiently close" and, as a corollary, uniform description of such matrices are based on very non-trivial number-theoretic tools [11] and also involves lengthy and somewhat tedious calculations. Furthermore, we believe that some of our results, such as bounds on the height of the annihilating polynomials in the Perron theorem, are of independent interest and may find further applications.

This paper is organized as follows. In Section 2 we present the definition of a linear algorithm and its associated graph and in Section 3, we normalize linear algorithms and state some simple basic complexity results. In Section 4, we prove the existence of a set of linear forms of the maximal complexity over $\mathbb{Q}$. Then, in Section 5, we present an alternative proof of the existence of such a set and outline an example. In Section 6 we estimate the height of the polynomial[1] appearing in the alternative proof and in Section 7 we recall an effective version of the *Lindemann-Weierstrass theorem* of Sert [11], which makes the existence proof constructive.[2] Finally, in Section 8, we present an example of a set of m linear forms in n variables over $\mathbb{Q}$ whose computation requires $m(n-1)$ additions.

To shorten the calculations and to simplify the final result, we use very crude estimates routinely applying inequalities of the form $N^N + N \leqslant 2N^N$, $e^{N^N} < N^{N^{N^2}}$ and similar. Nevertheless these estimation are still sufficient to make the point and to illustrate the approach.

Throughout the paper we adhere the convention that our main results are called *"Theorems"*, our auxiliary results are *"Propositions"*, while all previously known results (regardless of their depth and importance) are called *"Lemmas"*.

2 Linear algorithms and their associated graphs

A *linear algorithm* over a field $\mathbb{F}$ in *indeterminates* $x_1, x_2, \ldots, x_n$ consists of a sequence of operations $u_i \leftarrow \alpha_i u_{j_i} + \beta_i u_{k_i}$, $i = 1, \ldots, C$, where

- $\alpha_i, \beta_i \in \mathbb{F}^*$ are the algorithm coefficients;
- u_i is the algorithm *variable* that does not appear in a previous step;

[1] That is, the maximum of the absolute values of the polynomial coefficients.

[2] The Lindemann–Weierstrass theorem states that if algebraic numbers $\alpha_1, \ldots, \alpha_N$ are linearly independent over $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_N}$ are algebraically independent.

- u_{j_i} and u_{k_i} are either indeterminates or the algorithm variables appearing in a previous step (that is, if u_{j_i} and u_{k_i} are the algorithm variables appearing at step i, then $j_i, k_i < i$).

With each algorithm variable u in a linear algorithm we associate the following linear form $\ell(u)$:

- if u is an indeterminate x_t, then $\ell(u)$ is x_t;
- if u is the left-hand side of an operation $u \leftarrow \alpha v + \beta w$, then $\ell(u)$ is the linear form $\alpha\ell(v) + \beta\ell(w)$.

A linear algorithm *computes* a linear form $\ell(x_1, \ldots, x_n)$, if there is a variable, or an indeterminate, u of the algorithm and a *constant* $\gamma \in \mathbb{F}$ such that $\ell(x_1, \ldots, x_n) = \gamma\ell(u)$ (thus, linear algorithms compute linear forms up to scaling by a constant) and a linear algorithm computes a set linear forms

$$\mathcal{L}(x_1, \ldots, x_n) = \{\ell_s(x_1, \ldots, x_n) : \ s = 1, \ldots, m\}$$

if it computes each form $\ell_s(x_1, \ldots, x_n) \in \mathcal{L}(x_1, \ldots, x_n)$.

The number n of the variables and the number m of linear forms are fixed throughout this paper.

▶ **Definition 1.** *The complexity $|\mathcal{A}|$ of a linear algorithm $\mathcal{A}$ is the length C of its sequence of operations.*

▶ **Definition 2.** *The (additive) complexity of a set of linear forms is the minimal complexity of a linear algorithm that computes the set and algorithms of that minimal complexity are called optimal.*

It is known from [13] that if a set of linear forms over an infinite field can be computed in C additions by a *straight-line* algorithm (see [1, Section 12.2]), then it also can be computed in C additions by a linear algorithm. In other words, multiplications and divisions "cannot replace additions".

With a linear algorithm $\mathcal{A}$ we associate a labelled directed acyclic graph $G_{\mathcal{A}}(V_{\mathcal{A}}, E_{\mathcal{A}})$, whose set of vertices is the union of $\{x_1, \ldots, x_n\}$ and the set of the variables of $\mathcal{A}$ and there is an edge from vertex v to vertex u, if there is an operation of the form $u \leftarrow \alpha v + \beta w$ or the form $u \leftarrow \alpha w + \beta v$. In the former case, the edge is labelled α and, in the latter case, it is labelled β. We denote the label of edge e by $\lambda(e)$.

By definition, $|V_{\mathcal{A}}| = n + |\mathcal{A}|$ and the number of vertices of $G_{\mathcal{A}}$ of the in-degree 2 is $|\mathcal{A}|$.

Let $\pi = e_1, \ldots, e_k$ be a path of edges in $G_{\mathcal{A}}$. The *weight* $w(\pi)$ of π is defined, recursively, as follows.

- If π is of length zero, then $w(\pi) = 1$;
- $w(\pi, e) = w(\pi)\lambda(e)$, where π, e is the path π extended with edge e.

The following correspondence between linear algorithms and their associated graphs is well-known from the literature.

▶ **Lemma 3** (See, e.g., [4, Remark 13.19].). *Let*

$$\mathcal{A} = \{u_i \leftarrow \alpha_i u_{j_i} + \beta_i u_{k_i} : \ i = 1, \ldots, C\}$$

be a linear algorithm and let $\Pi_{\mathcal{A}}(x_t, u_i)$ denote the set of all paths of edges from the indeterminate x_t to the algorithm variable u_i in $G_{\mathcal{A}}$. Then

$$\ell(u_i) = \sum_{t=1}^{n} \left(\sum_{\pi \in \Pi_{\mathcal{A}}(x_t, u_i)} w(\pi) \right) x_t, \qquad i = 1, \ldots, C. \tag{4}$$

3 Normalized linear algorithms

In this section we introduce a subclass of linear algorithms called *normalized* linear algorithms. These algorithms have the same computation power, but are more convenient for dealing with complexity issues.

▶ **Definition 4.** *A linear algorithm is normalized if in each its operation*

$$u_i \leftarrow \alpha_i u_{j_i} + \beta_i u_{k_i}$$

the coefficient α_i of u_{j_i} is 1. The coefficient β_i of u_{j_k} is called a proper *coefficient.*

We say that a label is *proper* if it is a proper coefficient of the algorithm.

The result below immediately follows from Definition 4 and the definition of the associated graph $G_{\mathcal{A}}$ of an algorithm $\mathcal{A}$.

▶ **Proposition 5.** *The additive complexity of a normalized linear algorithm $\mathcal{A}$ equals to the number of proper labels of its associated graph $G_{\mathcal{A}}$.*

Furthermore, we also have the following results.

▶ **Proposition 6.** *For each linear algorithm there is a normalized linear algorithm of the same complexity that computes the same set of linear forms.*

Proof. Let

$$\mathcal{A} = \{u_i \leftarrow \alpha_i u_{j_i} + \beta_i u_{k_i} : \; i = 1, \dots, C\}$$

be a linear algorithm. It suffices to show that there exists a normalized linear algorithm

$$\widetilde{\mathcal{A}} = \{\widetilde{u}_i \leftarrow \widetilde{u}_{j_i} + \widetilde{\beta}_i \widetilde{u}_{k_i} : i = 1, \dots, C\}$$

and constants $\gamma_i \in \mathbb{F}$, $i = 1, \dots, C$, such that $\ell(u_i) = \gamma_i \ell(\widetilde{u}_i)$, $i = 1, \dots, C$.

We convert $\mathcal{A}$ to $\widetilde{\mathcal{A}}$ and define the constants γ_i by recursion on $i = 1, \dots, C$.

The first addition of $\mathcal{A}$ is $u_1 \leftarrow \alpha_1 x_s + \beta_1 x_t$, implying $\ell(u_1) = \alpha_1 x_s + \beta_1 x_t$. We put

$$\widetilde{\beta}_1 = \frac{\beta_1}{\alpha_1} \qquad \text{and} \qquad \gamma_1 = \alpha_1.$$

Then

$$\ell(u_1) = \alpha_1 x_s + \beta_1 x_t = \alpha_1 \left(x_s + \frac{\beta_1}{\alpha_1} x_t \right) = \gamma_1 (x_s + \widetilde{\beta}_1 x_t) = \gamma_1 \ell(\widetilde{u}_1).$$

The $(i+1)$-st addition of $\mathcal{A}$ is $u_{i+1} \leftarrow \alpha_{i+1} u_{j_{i+1}} + \beta_{i+1} u_{k_{i+1}}$, implying

$$\ell(u_{i+1}) = \alpha_{i+1} \ell(u_{j_{i+1}}) + \beta_{i+1} \ell(u_{k_{i+1}}).$$

We put

$$\widetilde{\beta}_{i+1} = \frac{\beta_{i+1} \gamma_{k_{i+1}}}{\alpha_{i+1} \gamma_{j_{i+1}}} \qquad \text{and} \qquad \gamma_{i+1} = \alpha_{i+1} \gamma_{j_{i+1}}.$$

Then

$$\begin{aligned}
\ell(u_{i+1}) &= \alpha_{i+1} \ell(u_{j_{i+1}}) + \beta_{i+1} \ell(u_{k_{i+1}}) \\
&= \alpha_{i+1} \gamma_{j_{i+1}} \ell(\widetilde{u}_{j_{i+1}}) + \beta_{i+1} \gamma_{k_{i+1}} \ell(\widetilde{u}_{k_{i+1}}) \\
&= \alpha_{i+1} \gamma_{j_{i+1}} \ell(\widetilde{u}_{j_{i+1}} + \frac{\beta_{i+1} \gamma_{k_{i+1}}}{\alpha_{i+1} \gamma_{j_{i+1}}} \widetilde{u}_{k_{i+1}}) \\
&= \gamma_{i+1} \ell(\widetilde{u}_{j_{i+1}} + \widetilde{\beta}_{i+1} \widetilde{u}_{k_{i+1}}) \\
&= \gamma_{i+1} \ell(\widetilde{u}_{i+1}),
\end{aligned}$$

which concludes the proof. ◀

From now on, we assume that all linear algorithms under consideration are over $\mathbb{R}$ and by Proposition 6, we assume that they are normalized.

We represent a linear from $\ell(x_1,\dots,x_n)=\sum_{t=1}^{n}\delta_t x_t$ by the product $(\delta_1,\dots,\delta_n)\boldsymbol{x}$, where $\boldsymbol{x}$ is the (column) vector of the indeterminates $x_1,\dots,x_n$ as in (2). Similarly, we represent a set of linear forms

$$\ell_s(x_1,\dots,x_n)=\sum_{t=1}^{n}\delta_{s,t}x_t\,,\qquad s=1,\dots,m,$$

by a matrix-vector product $\Delta\boldsymbol{x}$, where the sth row of the matrix Δ is the row vector $(\delta_{s,1},\dots,\delta_{s,n})$ of the coefficients of $\ell_s(x_1,\dots,x_n)$, see (3).

4 Computation of linear forms over $\mathbb{R}$ and $\mathbb{Q}$

In this section we prove the existence of a matrix $\Delta\in\mathbb{Q}^{m\times n}$ such that computing the set of linear forms $\Delta\boldsymbol{x}$ requires $m(n-1)$ additions. As a preliminary step, we consider matrices with entries from $\mathbb{R}$.

▶ **Theorem 7** (Cf. [4, Theorem 13.10]). *If all the coefficients of the linear forms* (3) *are algebraically independent, then the additive complexity of* (3) *is* $m(n-1)$.[3]

Proof. Let $\mathcal{A}$ be a linear algorithm that computes (3) and let $G_{\mathcal{A}}=(V_{\mathcal{A}},E_{\mathcal{A}})$ be its associated labelled graph.

Let u_{i_s} and γ_s, $s=1,\dots,m$, be the algorithm variables and the respective constants such that

$$\ell_s(x_1,\dots,x_n)=\sum_{t=1}^{n}\delta_{s,t}x_t=\gamma_s\ell(u_{i_s}).$$

Then, by Lemma 3,

$$\delta_{s,t}=\gamma_s\sum_{\pi\in\Pi_{\mathcal{A}}(x_t,u_{i_s})}w(\pi)=P_{s,t}\left(\gamma_s,\beta_1,\dots,\beta_{|\mathcal{A}|}\right)$$

for some polynomials $P_{s,t}\left(Y_s,X_1,\dots,X_{|\mathcal{A}|}\right)$, $s=1,\dots,m$ and $t=1,\dots,n$.

If the number $|\mathcal{A}|$ of the proper labels is less than $m(n-1)$, then the total number of β and γ variables is less than mn, implying that these mn polynomials are algebraically dependent, see Proposition 5.

Let $P(Z_{1,1},\dots,Z_{m,n})$ be a polynomial over $\mathbb{Q}$ such that

$$P\left(P_{1,1}\left(Y_1,X_1,\dots,X_{|\mathcal{A}|}\right),\dots,P_{m,n}\left(Y_m,X_1,\dots,X_{|\mathcal{A}|}\right)\right)=0. \tag{5}$$

Then

$$P\left(P_{1,1}\left(\gamma_1,\beta_1,\dots,\beta_{|\mathcal{A}|}\right),\dots,P_{m,n}\left(\gamma_m,\beta_1,\dots,\beta_{|\mathcal{A}|}\right)\right)=0,$$

implying

$$P\left(\delta_{1,1},\dots,\delta_{m,n}\right)=0. \tag{6}$$

That is, the matrix entries $\delta_{s,t}$ are algebraically dependent, in contradiction with the condition of the theorem. ◀

[3] In [4] this result is attributed to [16], but the proof in [16] is very implicit.

Recall that we aim to find an $m \times n$ matrix over $\mathbb{Q}$ that defines the set of linear forms of complexity $m(n-1)$. The existence of such a matrix is shown below (see Theorem 15), but to describe its entries is not straightforward at all and we do this in Section 8.

To proceed with our proof of existence we first need to introduce a number of definitions and auxiliary results.

▶ **Definition 8.** *We say that $P(Z_1, \ldots, Z_N) \in \mathbb{Z}[Z_1, \ldots, Z_N]$ is an annihilating polynomial of $P_k(X_1, \ldots, X_{N-1}) \in \mathbb{Z}[X_1, \ldots, X_{N-1}]$, $k = 1, \ldots, N$, if P is a non-zero polynomial and*

$$P\left(P_1\left(X_1, \ldots, X_{N-1}\right), \ldots, P_N\left(X_1, \ldots, X_{N-1}\right)\right) = 0.$$

▶ **Definition 9.** *We say that the polynomial $P_{s,t}\left(Y_s, X_1, \ldots, X_{|\mathcal{A}|}\right)$, $s = 1, \ldots, m$ and $t = 1, \ldots, n$, defined in the proof of Theorem 7 is associated with the (s,t)-th entry of Δ via $\mathcal{A}$.*

▶ **Definition 10.** *We say that a polynomial P is (m,n)-associated if for some $m \times n$ matrix Δ, some $s = 1, \ldots, m$, some $t = 1, \ldots, n$ and some algorithm $\mathcal{A}$ with $|\mathcal{A}| < m(n-1)$ that computes (3), P is associated with the (s,t)-th entry of Δ via $\mathcal{A}$.*

▶ **Proposition 11.** *The set of (m,n)-associated polynomials is finite.*

Proof. By (4), the coefficients of $P_{s,t}\left(Y_s, X_1, \ldots, X_{|\mathcal{A}|}\right)$ are zero or one and, by definition, $|\mathcal{A}| < m(n-1)$. Therefore

$$\deg P_{s,t}\left(Y_s, X_1, \ldots, X_{|\mathcal{A}|}\right) < m(n-1),$$

where $s = 1, \ldots, m$ and $t = 1, \ldots, n$, and the result follows. ◀

▶ **Definition 12.** *The polynomial $P\left(Z_{1,1}, \ldots, Z_{m,n}\right) \in \mathbb{Q}[Z_{1,1}, \ldots, Z_{m,n}]$ satisfying (5), that is, an annihilating polynomial of*

$$P_{1,1}\left(Y_1, X_1, \ldots, X_{|\mathcal{A}|}\right), \ldots, P_{m,n}\left(Y_m, X_1, \ldots, X_{|\mathcal{A}|}\right),$$

is called an $\mathcal{A}$-Δ-annihilating polynomial.

▶ **Definition 13.** *We say that a set of polynomials $\mathfrak{Q}$ is (m,n)-complete if for each $m \times n$ matrix Δ and each algorithm $\mathcal{A}$ with $|\mathcal{A}| < m(n-1)$ that computes (3), $\mathfrak{Q}$ contains an $\mathcal{A}$-Δ-annihilating polynomial.*

For our specific example we shall look for a common non-zero of all polynomials in an (m,n)-complete set. This resembles the approach in [14], see also [4, Section 9.4].

▶ **Proposition 14.** *Let $\mathfrak{Q}$ be a minimal with respect to inclusion (m,n)-complete set of polynomials. Then $\mathfrak{Q}$ is finite.*

Proof. This is because number of polynomials in $\mathfrak{Q}$ does not exceed the number of all k-tuples, $k < m(n-1)$ of (m,n)-associated polynomials and by Proposition 11 the number of such tuples is finite. ◀

In what follows, for a matrix A we denote by $|A|$ its *Frobenius norm*, that is, the square root of the sum of squares of its entries. Similarly, for a vector $\boldsymbol{\alpha}$ we use $|\boldsymbol{\alpha}|$ to denote its *Euclidean norm.*

▶ **Theorem 15.** *There exists an $m \times n$ matrix over $\mathbb{Q}$ that defines the set of linear forms of complexity $m(n-1)$.*

Proof. Let $\Delta_1, \Delta_2, \dots$, be a sequence of $m \times n$ matrices over $\mathbb{Q}$ that converges (in the Frobenius norm) to the matrix $\Delta = (\delta_{s,t})$ from the proof of Theorem 7. That is, $\lim_{i\to\infty} |\Delta_i - \Delta| = 0$.

Let $\Delta_i = (\delta_{s,t,i})$, $i = 1, 2, \dots$. Then

$$\lim_{i\to\infty} \delta_{s,t,i} = \delta_{s,t} \quad s = 1, \dots, m \text{ and } n = 1, \dots, n. \tag{7}$$

Assume to the contrary that for each $i = 1, 2, \dots$, there is an algorithm $\mathcal{A}_i$, $|\mathcal{A}_i| < m(n-1)$, that computes $\Delta_i \boldsymbol{x}$. Let $\mathfrak{Q}$ be a finite (m,n)-complete set provided by Proposition 14. Then, like in the proof of Theorem 7, it can be shown that for each $i = 1, 2, \dots$, there is an $\mathcal{A}_i$-Δ_i-annihilating polynomial $P_i(Z_{1,1}, \dots, Z_{m,n}) \in \mathfrak{Q}$ such that $P_i(\delta_{1,1,i}, \dots, \delta_{m,n,i}) = 0$.

Thus, there is a subsequence $\widetilde{\Delta}_1, \widetilde{\Delta}_2, \dots$ of $\Delta_1, \Delta_2, \dots$ with the same annihilating polynomial $P(Z_{1,1}, \dots, Z_{m,n})$, implying $P\left(\widetilde{\delta}_{1,1,i}, \dots, \widetilde{\delta}_{m,n,i}\right) = 0$, $i = 1, 2, \dots$, which, by (7), implies (6). However, the latter contradicts the algebraic independence of the entries of Δ. ◀

5 An alternative proof of Theorem 15 and an outline of an example

Here we present an alternative and more constructive approach of the existence of a set of m linear forms in n variables over $\mathbb{Q}$ of complexity $m(n-1)$ and outline our example. To simplify the calculations, we look for a matrix Γ defining such a set in the ball of radius 1 centered at Δ. We show in Section 7 that this condition is redundant.

Theorem 16 below is in the background of our example of linear forms which are hard to compute.

▶ **Theorem 16.** *Let $\mathfrak{Q}$ be an (m,n)-complete set of polynomials. Let $\Gamma = (\gamma_{s,t})$ and $\Delta = (\delta_{s,t})$ be $m \times n$ matrices, where $\delta_{s,t}$, $s = 1, \dots, m$ and $t = 1, \dots, n$, are algebraically independent and $|\Delta - \Gamma| < 1$. Let $\boldsymbol{\gamma} = (\gamma_{1,1}, \dots, \gamma_{m,n})$ and let $\boldsymbol{\delta} = (\delta_{1,1}, \dots, \delta_{m,n})$. If*

$$|\boldsymbol{\delta} - \boldsymbol{\gamma}| < \min_{Q\in\mathfrak{Q}} \min_{|\boldsymbol{\mu}|<1} \left\{ \frac{|Q(\boldsymbol{\delta})|}{|\nabla Q(\boldsymbol{\delta} + \boldsymbol{\mu})|} \right\}, \tag{8}$$

then computing $\Gamma\boldsymbol{x}$ requires $m(n-1)$ additions.

The proof of Theorem 16 is based on the following lemma.

▶ **Lemma 17** (The *mean value theorem for several variables*, see, e.g., [2, Chapter 12, Example 1].). *Let $F : \mathbb{R}^N \to \mathbb{R}$ be a differentiable function and $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 \in \mathbb{R}^N$. Then, for some $\vartheta \in [0,1]$,*

$$F(\boldsymbol{\alpha}_2) - F(\boldsymbol{\alpha}_1) = \nabla F(\boldsymbol{\alpha}_1 + \vartheta(\boldsymbol{\alpha}_2 - \boldsymbol{\alpha}_1)) \cdot (\boldsymbol{\alpha}_2 - \boldsymbol{\alpha}_1),$$

where ∇F denotes the gradient of F.

Proof of Theorem 16. Assume to the contrary that the set of linear forms $\Gamma\boldsymbol{x}$ can be computed in less than $m(n-1)$ additions by an algorithm $\mathcal{A}$. Then, since $\mathfrak{Q}$ is (m,n)-complete, there is an $\mathcal{A}$-Γ-annihilating polynomial $Q \in \mathfrak{Q}$ such that $Q(\boldsymbol{\gamma}) = 0$.

By Lemma 17, for some $\vartheta \in [0,1]$

$$Q(\boldsymbol{\delta}) - Q(\boldsymbol{\gamma}) = \nabla Q(\boldsymbol{\gamma} + \vartheta(\boldsymbol{\delta} - \boldsymbol{\gamma})) \cdot (\boldsymbol{\delta} - \boldsymbol{\gamma}). \tag{9}$$

Since

$$\boldsymbol{\gamma} + \vartheta(\boldsymbol{\delta} - \boldsymbol{\gamma}) = \vartheta\boldsymbol{\delta} + (1-\vartheta)\boldsymbol{\gamma} = \vartheta\boldsymbol{\delta} + (1-\vartheta)(\boldsymbol{\delta} + \boldsymbol{\gamma} - \boldsymbol{\delta}) = \boldsymbol{\delta} + (1-\vartheta)(\boldsymbol{\gamma} - \boldsymbol{\delta})$$

and $|(1-\vartheta)(\boldsymbol{\gamma}-\boldsymbol{\delta})|<1$, by (9), for $\boldsymbol{\mu}=(1-\vartheta)(\boldsymbol{\gamma}-\boldsymbol{\delta})$, we have

$$Q(\boldsymbol{\delta}) = \nabla Q(\boldsymbol{\delta}+\boldsymbol{\mu})\cdot(\boldsymbol{\delta}-\boldsymbol{\gamma}) \tag{10}$$

because $Q(\boldsymbol{\gamma})=0$. It follows from (10), by the Cauchy–Schwarz inequality, that

$$|Q(\boldsymbol{\delta})| \le |\nabla Q(\boldsymbol{\delta}+\boldsymbol{\mu})|\,|\boldsymbol{\delta}-\boldsymbol{\gamma}|\,,$$

which contradicts (8). ◀

Note that, since the components of $\boldsymbol{\delta}$ are algebraically independent, $Q(\boldsymbol{\delta})\neq 0$. Thus, for a finite (m,n)-complete set of polynomials $\mathfrak{Q}$, the right-hand side of (8) is positive.

Using the trivial inequality

$$|\boldsymbol{\delta}-\boldsymbol{\gamma}| \le \sqrt{mn}\max\{|\delta_{s,t}-\gamma_{s,t}|:\ s=1,\dots,m,\ t=1,\dots,n\}$$

we see that Theorem 16 yields the corollary below.

▶ **Corollary 18.** *Let $\mathfrak{Q}$ be an (m,n)-complete set of polynomials. Let $\Gamma=(\gamma_{s,t})$ and $\Delta=(\delta_{s,t})$ be $m\times n$ matrices, where $\delta_{s,t}$, $s=1,\dots,m$ and $t=1,\dots,n$, are algebraically independent and $|\Delta-\Gamma|<1$. Let $\boldsymbol{\gamma}=(\gamma_{1,1},\dots,\gamma_{m,n})$ and $\boldsymbol{\delta}=(\delta_{1,1},\dots,\delta_{m,n})$. If*

$$\max\{|\delta_{s,t}-\gamma_{s,t}|:\ s=1,\dots,m \text{ and } t=1,\dots,n\} < \frac{1}{\sqrt{mn}}\min_{Q\in\mathfrak{Q}}\min_{|\boldsymbol{\mu}|<1}\left\{\frac{|Q(\boldsymbol{\delta})|}{|\nabla Q(\boldsymbol{\delta}+\boldsymbol{\mu})|}\right\},$$

then computing $\Gamma\boldsymbol{x}$ requires $m(n-1)$ additions.

Following the above existence proof, for an example of a rational $m\times n$ matrix defining a set of linear forms of complexity $m(n-1)$ we need a set of algebraically independent numbers $\delta_{s,t}$, $s=1,\dots,m$ and $t=1,\dots,n$, for which the right-hand side of (8) can be effectively estimated. Such a set is provided by an effective version of the Lindemann-Weierstrass theorem due to Sert [11], see Lemma 26 in Section 7.

6 The degree and the height of annihilating polynomials

In this section we estimate the denominator of the right-hand side of (8). For this we need to estimate the degree and the height of (m,n)-polynomials which are defined as follows.

▶ **Definition 19.** *A polynomial P is called an (m,n)-polynomial if for some $m\times n$ matrix Δ and some algorithm $\mathcal{A}$, $|\mathcal{A}|<m(n-1)$, that computes (3), P is $\mathcal{A}$-Δ-annihilating.*

Recall that these polynomials arise from linear algorithms of the complexity less than $m(n-1)$ and satisfy (5).

We start with the following result, that is essentially due to Perron.

▶ **Lemma 20** ([8], see also [9, Theorem 1.1] for a self-contained proof.). *Let*

$$P_k(X_1,\dots,X_{N-1})\in\mathbb{Z}[X_1,\dots,X_{N-1}]$$

with $\deg P_k(X_1,\dots,X_{N-1})=d_k$*, $k=1,\dots,N$. Then there exists an annihilating polynomial $P(Z_1,\dots,Z_N)\in\mathbb{Z}[Z_1,\dots,Z_N]$ of $P_1,\dots,P_N$ such that*

$$\deg P \le \frac{d_1\times\cdots\times d_N}{\min\{d_1,\dots,d_N\}}.$$

Actually, in [8], the polynomial $P(Z_1,\dots,Z_N)$ has rational coefficients, but, multiplying them by their common denominator, we obtain a polynomial over $\mathbb{Z}$.

In the case of (m,n)-polynomials, $N = mn$ and $d_s \le m(n-1)$, $i = 1,\dots,N$. Therefore, by Lemma 20, we may assume that the degree of (m,n)-polynomials under consideration does not exceed N^{N-1}.

Next, we are going to estimate the minimum height $h(P)$ of the polynomial $P(Z_1,\dots,Z_N)$ provided by Lemma 20. This can be done by solving a system of linear homogeneous equations, see [14, Lemma2.2], [4, Lemma 9.28] or [9, Property 1.2].

We need some auxiliary results first. We start with recalling the following well-known upper bound on the height of a polynomial product.

▶ **Lemma 21** (See, e.g., [5, Lemma 1.2(1)(b)], where the logarithmic height $\ln h(P)$ is used.)**.** *Let $P_k \in \mathbb{Z}[X_1,\dots,X_{N-1}]$, $k = 1,\dots,\ell$. Then*

$$h\left(\prod_{k=1}^{\ell} P_k\right) \le N^{\sum\limits_{k=1}^{\ell} \deg P_k} \prod_{k=1}^{\ell} h(P_k).$$

We also recall the classical *Siegel lemma*.

▶ **Lemma 22** ([12, Page 213, Hilfssatz], see also [3, 15] for further improvements and generalizations.)**.** *If a system of J linear homogeneous equations in $I > J$ variables*

$$\sum_{i=1}^{I} b_{i,j} z_i = 0, \qquad j = 1,\dots,J,$$

with $B = (b_{i,j})_{i,j=1}^{I,J} \in \mathbb{Z}^{I\times J}$, has a nonzero solution, then it has a nonzero integer solution $\boldsymbol{v} = (v_1,\dots,v_I)$ with

$$h(\boldsymbol{v}) \leqslant 1 + (I h(B))^{J/(I-J)},$$

where

$$h(B) = \max\{|b_{i,j}| : \ i = 1,\dots,I, \ j = 1,\dots,J\}$$

and

$$h(\boldsymbol{v}) = \max\{|v_i| : \ i = 1,\dots,I\}. \tag{11}$$

We are now ready to estimate the height of an annihilating polynomial. More precisely we establish the following result.

▶ **Proposition 23.** *Let $P(Z_1,\dots,Z_N) \in \mathbb{Z}[Z_1,\dots,Z_N]$ be an annihilating polynomial of*

$$P_k(X_1,\dots,X_{N-1}) \in \mathbb{Z}[X_1,\dots,X_{N-1}], \qquad k = 1,\dots,N.$$

There exists another annihilating polynomial $Q(Z_1,\dots,Z_N) \in \mathbb{Z}[Z_1,\dots,Z_N]$ of $P_1,\dots,P_N$ of degree and height

$$\deg Q \leqslant \deg P,$$
$$h(Q) \leqslant 1 + \left(\binom{\deg P + N}{N} N^{d_{\max}\deg P} h_{\max}^{\deg P}\right)^{\binom{\deg P+N}{N}-1},$$

respectively, where

$$d_{\max} = \max\{\deg P_k : \ k = 1,\dots,N\},$$
$$h_{\max} = \max\{h(P_k) : \ k = 1,\dots,N\}.$$

Proof. We employ the following notation:

- $\boldsymbol{X} = (X_1, \dots, X_{N-1})$ and $\boldsymbol{Z} = (Z_1, \dots, Z_N)$ are vectors of variables;
- $\boldsymbol{i} = (i_1, \dots, i_N)$ and $\boldsymbol{j} = (j_1, \dots, j_{N-1})$ are vectors of non-negative integers;
- $\boldsymbol{X}^{\boldsymbol{j}} = \prod_{s=1}^{N-1} X_s^{j_s}$ and $\boldsymbol{Z}^{\boldsymbol{i}} = \prod_{k=1}^{N} Z_k^{i_k}$ are multivariate monomials.

We search for a polynomial Q in the form

$$Q(Z_1, \dots, Z_N) = \sum_{\boldsymbol{i}\colon i_1+\ldots+i_N \le \deg P} v_{\boldsymbol{i}} \boldsymbol{Z}^{\boldsymbol{i}}, \tag{12}$$

with unknown coefficients $v_{\boldsymbol{i}}$ to be determined.

To find the coefficients $v_{\boldsymbol{i}}$ of $Q(Z_1, \dots, Z_N)$, we substitute the polynomials $P_k(X_1, \dots, X_{N-1})$ for Z_k, $k = 1, \dots, N$, in (12), obtaining

$$\begin{aligned} &Q\left(P_1(X_1, \dots, X_{N-1}), \dots, P_N(X_1, \dots, X_{N-1})\right) \\ &\qquad = \sum_{\boldsymbol{i}\colon i_1+\ldots+i_N \le \deg P} v_{\boldsymbol{i}} \prod_{k=1}^{N} P_k^{i_k}(X_1, \dots, X_{N-1}) = 0. \end{aligned} \tag{13}$$

Let

$$\prod_{k=1}^{N} P_k^{i_k}(X_1, \dots, X_{N-1}) = \sum_{\boldsymbol{j}\colon j_1+\ldots+j_{N-1} \leqslant d_{\max} \deg P} \mathbf{c}_{\boldsymbol{i},\boldsymbol{j}} \boldsymbol{X}^{\boldsymbol{j}}.$$

Then, it follows from (13) that

$$\begin{aligned} &\sum_{\boldsymbol{i}\colon i_1+\ldots+i_N \le \deg P} v_{\boldsymbol{i}} \sum_{\boldsymbol{j}\colon j_1+\ldots+j_{N-1} \leqslant d_{\max} \deg P} \mathbf{c}_{\boldsymbol{i},\boldsymbol{j}} \boldsymbol{X}^{\boldsymbol{j}} \\ &\qquad = \sum_{\boldsymbol{j}\colon j_1+\ldots+j_{N-1} \leqslant d_{\max} \deg P} \boldsymbol{X}^{\boldsymbol{j}} \left(\sum_{\boldsymbol{i}\colon i_1+\ldots+i_N \le \deg P} \mathbf{c}_{\boldsymbol{i},\boldsymbol{j}} v_{\boldsymbol{i}} \right) = 0. \end{aligned}$$

That is, we have a system of linear homogeneous equations

$$\sum_{\boldsymbol{i}\colon i_1+\ldots+i_N \le \deg P} \mathbf{c}_{\boldsymbol{i},\boldsymbol{j}}\, v_{\boldsymbol{i}} = 0, \qquad \boldsymbol{j}:\ j_1 + \ldots + j_{N-1} \leqslant d_{\max} \deg P \tag{14}$$

in

$$I = \binom{\deg P + N}{N} \tag{15}$$

unknowns $v_{\boldsymbol{i}}$ (the coefficients of $P(Z_1, \dots, Z_N)$).

We also note that for the coefficients $\mathbf{c}_{\boldsymbol{i},\boldsymbol{j}}$ of the system of linear equations (14) we have

$$\max_{\boldsymbol{i},\boldsymbol{j}} |\mathbf{c}_{\boldsymbol{i},\boldsymbol{j}}| \leqslant \max_{i_1+\ldots+i_N \le \deg P} h\left(\prod_{k=1}^{N} P_k^{i_k} \right),$$

where $\boldsymbol{i}$ and $\boldsymbol{j}$ run through the vectors with $i_1 + \ldots + i_N \le \deg P$ and $j_1 + \ldots + j_{N-1} \leqslant d_{\max} \deg P$, respectively

Hence, by Lemma 21 with $\ell = \deg P$,

$$\max_{\boldsymbol{i},\boldsymbol{j}} |\mathbf{c}_{\boldsymbol{i},\boldsymbol{j}}| \le N^{d_{\max} \deg P} h_{\max}^{\deg P}. \tag{16}$$

Since, by our assumption on the polynomial Q, this system has a non-zero solution, we can select at most $J \leqslant I-1$ linear equations forming a system of linear homogeneous equations, which is equivalent to (14). Hence combining the bound (16) with Lemma 22, we derive that (14) has a solution with

$$\max\{v_{\boldsymbol{i}} :\ \boldsymbol{i}=(i_1,\ldots,i_N) \text{ with } i_1+\ldots+i_N \le \deg P\} \leqslant 1+\left(IN^{d_{\max}\deg P} h_{\max}^{\deg P}\right)^{I-1},$$

where I is given by (15), which concludes the proof. ◀

In what follows we renumber the (m,n)-associated polynomials $P_{s,t}$, $s=1,\ldots,m$ and $t=1,\ldots,n$, in (5) as $P_1,\ldots,P_N$, that is, we write

$$\{P_1,\ldots,P_N\}=\{P_{s,t} :\ s=1,\ldots,m,\ t=1,\ldots,n\}. \tag{17}$$

We remark that by Lemma 20, we can assume $\deg P \leqslant d_{\max}^{N-1}$ in the notation of Proposition 23. Furthermore, as we have noticed in the proof of Proposition 11, in the special case of (m,n)-associated polynomials we have

$$d_{\max}=N \qquad \text{and} \qquad h_{\max}=1. \tag{18}$$

Thus, by Lemma 20, we can assume

$$\deg P \le N^{N-1}. \tag{19}$$

▶ **Corollary 24.** *For any $N=mn \geqslant 4$ and polynomials (17), there exists an (m,n)-polynomial $Q(Z_1,\ldots,Z_N)$ of degree and height satisfying*

$$\deg Q \leqslant N^{N-1} \qquad \textit{and} \qquad h(Q) \leqslant N^{2N^{N^2}}, \tag{20}$$

respectively.

Proof. The bound on the degree follows directly from (19). Using the well known estimate

$$\binom{q}{r} \leqslant \frac{q^r}{r!} \leqslant (eq/r)^r,$$

which holds for arbitrary integers integers $q \geqslant r \geqslant 1$, we derive

$$\binom{N^{N-1}+N}{N} \leqslant \left(e\left(N^{N-2}+1\right)\right)^N = e^N N^{N(N-2)}\left(1+1/N^{N-2}\right)^N \leqslant e^{N+1}N^{N^2-2N}.$$

Since for $N \geqslant 4$ we have $e^{N+1} < N^N$, we now obtain

$$\binom{N^{N-1}+N}{N} < N^{N^2-N}.$$

Substituting (18) and (19) in Proposition 23 and using the above estimate, we see that

$$h(Q) \leqslant 1+\left(N^{N^N+N^2-N}\right)^{N^{N^2-N}} = 1+N^{\left(N^N+N^2-N\right)N^{N^2-N}}.$$

We now use the crude estimate $N^N+N^2-N < 2N^N$ and obtain

$$h(Q) < 1+N^{2N^{N^2}}.$$

Since $h(Q)$ is an integer, this concludes the proof. ◀

Let $\mathfrak{Q}_{m,n}$ denote the class of annihilating (m,n)-polynomials Q with the degree and height satisfying 20, where $N = mn$. By Corollary 24, we see that for $N = mn \geqslant 4$, $\mathfrak{Q}_{m.n} \neq \emptyset$. Clearly, $\mathfrak{Q}_{m,n}$ is (m,n)-complete and, therefore, Corollary 18 can be applied with $\mathfrak{Q} = \mathfrak{Q}_{m,n}$.

We remark that the case of $N = mn \leqslant 3$ is trivial, as then $m = 1$ or $n = 1$. Hence the condition $N \geqslant 4$, which stems from Corollary 24, is not restrictive.

We also recall the definition of the naive height in (11).

▶ **Corollary 25.** *For any $N = mn \geqslant 4$ and $\boldsymbol{\delta} \in \mathbb{R}^N$, we have*

$$\max_{Q \in \mathfrak{Q}_{m,n}} \max_{|\boldsymbol{\mu}|<1} |\nabla Q(\boldsymbol{\delta} + \boldsymbol{\mu})| < N^{3N^{N^2}} (h(\boldsymbol{\delta}) + 1)^{N^{N-1}}.$$

Proof. First we estimate

$$\frac{\partial Q}{\partial Z_k}(\boldsymbol{\delta} + \boldsymbol{\mu}), \qquad k = 1, \ldots, N.$$

The polynomial $\partial Q / \partial Z_k$ is of degree

$$\deg \partial Q / \partial Z_k < \deg Q \leqslant N^{N-1}$$

and thus, by Corollary 24, of height

$$h\left(\partial Q / \partial Z_k\right) \leqslant N^{N-1} h(Q) \leqslant N^{2N^{N^2}+N-1}.$$

The number of monomials in N variables of degree less than N^{N-1} is less than N^{N^2-N}. Thus, for $|\boldsymbol{\mu}| \leqslant 1$ we have

$$\begin{aligned} \left| \frac{\partial Q}{\partial Z_k}(\boldsymbol{\delta} + \boldsymbol{\mu}) \right| &\leqslant N^{N^2-N} h\left(\partial Q / \partial Z_k\right) (h(\boldsymbol{\delta}) + 1)^{N^{N-1}} \\ &\leqslant N^{2N^{N^2}+N^2-1} (h(\boldsymbol{\delta}) + 1)^{N^{N-1}} < N^{3N^{N^2}} (h(\boldsymbol{\delta}) + 1)^{N^{N-1}}, \end{aligned}$$

and the result follows. ◀

7 Effective Lindemann–Weierstrass theorem

In this section we estimate the numerator of the right-hand side of (8). This, together with the estimation of the denominator of the right-hand side of (8) in the previous section, would make Theorem 16 constructive. The estimation of the numerator is based on an effective version of the Lindemann-Weierstrass theorem due to Sert [11] stated below. We precede the statement of the theorem with the necessary definitions and notations.

- K is a number field of degree D.
- M_K is the set of normalized absolute values of K, that is, the extensions onto K all the values on $\mathbb{Q}$ (Archimedean and p-adic).
- The *absolute height* $\mathfrak{h}_a(\boldsymbol{\alpha})$ of an s-tuple $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in K^s$ is defined by

  $$\mathfrak{h}_a(\boldsymbol{\alpha}) = \prod_{\nu \in M_K} \max_{1 \leq k \leq s} \{1, |\alpha_k|_\nu\}^{D_\nu / D},$$

  where D_ν is the local degree of K_ν, that is, the dimension of the ν-completion of K over $\mathbb{R}$, if ν is Archimedean, or the ν-completion of K over $\mathbb{Q}_p$, if ν is p-adic.
- Let $\{\beta_1, \ldots, \beta_L\}$ be the set of all coefficients of a polynomial $P(x_1, \ldots, x_N)$ over K. We denote by Δ_P the discriminant of $\mathbb{Q}(\beta_1, \ldots, \beta_L)$.

- The *absolute height* of a multi-variate polynomial P is the absolute height of the tuple of the polynomial coefficients.

Our main technical tool is the following result of Sert.

▶ **Lemma 26** ([11, Theorem 3]). *Let $P \in K[Z_1, \dots, Z_N]$ be of degree $d \geq 1$ and of absolute height H and let $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_N) \in K^N$ be linearly independent over $\mathbb{Q}$. Then*

$$\begin{aligned} &\ln |P(e^{\alpha_1}, \dots, e^{\alpha_N})| \\ &\quad \geq \quad -c_0 d^N \left(\ln H + \frac{39}{328D} \ln |\Delta_P| + \exp\left(c_1 d^N + c_2 d^N \ln d + 72 \max\{1, \mathfrak{h}_a(\boldsymbol{\alpha})\}\right) \right), \end{aligned}$$

where

$$\begin{aligned} c_0 &= 41 \times 3^{2N} 2^{-N+1} D^{N+1} N^N, \\ c_1 &= 2^{2-N} 3^{2N+1} D^{N+1} N^N + (1+6D) 2^{4-N} 3^{2N} D^N N^N \ln(9DN) \\ &\qquad\qquad + 2^{4-N} 3^{2N} D^{N+1} N^N (1+6N) \ln \mathfrak{h}_a(\boldsymbol{\alpha}), \\ c_2 &= (1+6D) 2^{4-N} 3^{2N} D^N N^N. \end{aligned}$$

▶ Remark 27. As noticed by Sert [11, Page 100], if the coefficients of $P(Z_1, \dots, Z_N)$ are rational integers, then, in Lemma 26, we replace H with the ordinary height $h(P)$ of P and replace $\ln |\Delta_P|$ with zero.

The result below follows from Lemma 26 and Remark 27 by a straightforward substitution.

▶ **Corollary 28.** *Let $Q(Z_1, \dots, Z_N) \in \mathfrak{Q}_{m,n}$ and let $\alpha_1, \dots, \alpha_N$ be algebraic numbers linearly independent over $\mathbb{Q}$. Then, for $N \geqslant 4$,*

$$|Q(e^{\alpha_1}, \dots, e^{\alpha_N})| > \exp\left(-N^{2^{5N} D^{N+1} N^{N^2+2} (D + \max\{1, \mathfrak{h}_a(\boldsymbol{\alpha})\})} \right)$$

where D is the degree of the number field $\mathbb{Q}(\alpha_1, \dots, \alpha_N)$.

The proof of this corollary is presented in Appendix A.1.

Now, the substitution of the bound of Corollaries 28 and 25 for the numerator and the denominator of the right-hand side of (8), respectively, makes Theorem 16 constructive.

Finally, for the uniform example of a set of m linear forms in n variables over $\mathbb{Q}$ of complexity $m(n-1)$ in the next section we need the estimation below.

▶ **Proposition 29.** *Let α be a positive integer such that $[\mathbb{Q}(\alpha^{1/N}) : \mathbb{Q}] = N$, where $N = mn \geqslant 4$ and $N > \alpha > 1$, and let $\gamma_{s,t}$, $s = 1, \dots, m$ and $t = 1, \dots, n$, be such that*

$$\left| e^{\alpha^{((s-1)n+t)/N}} - \gamma_{s,t} \right| < \exp\left(-N^{N^{3N^2}} \right). \tag{21}$$

Then, for $\Gamma = (\gamma_{s,t})$, computing $\Gamma \boldsymbol{x}$ requires $m(n-1)$ additions.

The proof of this proposition is presented in Appendix A.2.

8 An example

An example of an integer matrix $\Omega \in \mathbb{Z}^{m \times n}$ such that computing $\Omega \boldsymbol{x}$ requires $m(n-1)$ additions is based on Proposition 29 with $\alpha = 2$. We precede the example with a series of auxiliary calculations for which we need the propositions below.

Throughout we assume that $N \geqslant 4$.

We recall the definition of binomial coefficients for real arguments:

$$\binom{r}{i} = \frac{r(r-1)\cdots(r-i+1)}{i!}.$$

▶ **Proposition 30.** *For $r \in (0,1)$ and a non-negative integer j,*

$$\left|2^r - \sum_{i=0}^{j} \binom{r}{i}\right| < \frac{1}{j+1}$$

Proof. For $x > 0$, the Taylor expansion (with the Lagrange remainder) of $(1+x)^r$ is

$$(1+x)^r = \sum_{i=0}^{j} \binom{r}{i} x^i + \binom{r}{j+1} \Theta^{j+1} \tag{22}$$

for some $\Theta \in (0,x)$. Substituting 1 for both x and Θ in (22), we obtain

$$\left|2^r - \sum_{i=0}^{j} \binom{r}{i}\right| < \left|\binom{r}{j+1}\right| = \frac{|r(r-1)(r-2)\cdots(r-j)|}{(j+1)!} < \frac{j!}{(j+1)!} < \frac{1}{j+1},$$

and the result follows. ◀

By Proposition 30, we approximate $2^{((s-1)n+t)/N}$ by

$$r_{s,t} = \sum_{i=0}^{j} \binom{((s-1)n+t)/N}{i} \qquad s = 1,\ldots,m,\ t = 1,\ldots,n,$$

for an appropriate j, to be chosen later.

▶ **Proposition 31.** *For $x \in (1,2)$ and $k \geqslant 6$,*

$$e^x - \sum_{i=0}^{k} \frac{x^i}{i!} < \frac{1}{k+1}.$$

Proof. For $x > 0$, the Taylor expansion (with the Lagrange remainder) of e^x is

$$e^x = \sum_{i=0}^{k} \frac{x^i}{i!} + \frac{\Theta^{k+1}}{(k+1)!}$$

for some $\Theta \in (0,x)$. Thus, using $k! \geqslant 2^{k+1}$ for $k \geqslant 6$, we obtain

$$e^x - \sum_{i=0}^{k} \frac{x^i}{i!} = \frac{\Theta^{k+1}}{(k+1)!} < \frac{2^{k+1}}{(k+1)!} < \frac{1}{k+1},$$

which concludes the proof. ◀

By Proposition 31, we approximate $e^{r_{s,t}}$ by

$$\gamma_{s,t} = \sum_{i=0}^{k} \frac{r_{s,t}^i}{i!}, \qquad s = 1,\ldots,m,\ t = 1,\ldots,n,$$

for an appropriate k, to be chosen later.

Our last auxiliary estimation is as follows.

▶ **Proposition 32.** *Let $x \leq 2$ and $\varepsilon \in (-1,1)$. Then*

$$\left|e^x - e^{x+\varepsilon}\right| < 42\varepsilon.$$

Proof. By Lemma 17,

$$\left|e^x - e^{x+\varepsilon}\right| < \left|e^{x-|\varepsilon|} - e^{x+|\varepsilon|}\right| = 2\varepsilon e^{x+\Theta}$$

for some $\Theta \in (-\varepsilon, \varepsilon)$. Thus, $|e^x - e^{x+\varepsilon}| < 2e^3\varepsilon < 42\varepsilon$. ◀

To simplify the expressions in our example, recalling the bound of Proposition 29 it is now convenient to denote

$$E = \exp\left(N^{N^{3N^2}}\right). \tag{23}$$

We contend that for

$$j \geq 126E \qquad \text{and} \qquad k \geq 3E \tag{24}$$

we have the inequality

$$\left|e^{2^{((s-1)n+t)/N}} - \gamma_{s,t}\right| < \frac{2}{3E}. \tag{25}$$

Indeed, first we note that, by Propositions 31 and 32, we have

$$\begin{aligned}\left|e^{2^{((s-1)n+t)/N}} - \gamma_{s,t}\right| &= \left|e^{2^{((s-1)n+t)/N}} - \sum_{i=0}^{k} \frac{r_{s,t}^i}{i!}\right| \\ &\leq \left|e^{r_{s,t}} - \sum_{i=0}^{k} \frac{r_{s,t}^i}{i!}\right| + \left|e^{2^{((s-1)n+t)/N}} - e^{r_{s,t}}\right| \\ &< \frac{1}{k+1} + 42\left|2^{((s-1)n+t)/N} - r_{s,t}\right|.\end{aligned}$$

Now using Proposition 30 and recalling the choice of j and k in (24), we derive

$$42\left|2^{((s-1)n+t)/N} - r_{s,t}\right| \leqslant \frac{42}{j+1} \leqslant \frac{1}{3E} \qquad \text{and} \qquad \frac{1}{k+1} \leqslant \frac{1}{3E}$$

and (25) follows.

Thus, by (25) and Proposition 29, computing $\Gamma \boldsymbol{x}^T$, where

$$\Gamma = (\gamma_{s,t}) \in \mathbb{Q}^{m\times n}$$

requires $m(n-1)$ additions.

Of course, all of the above also holds for computations over $\mathbb{C}$ and unbounded algorithm coefficients, whereas in [7] the algorithm coefficients are bounded by 1.

Even though,

$$\gamma_{s,t} \leqslant e^{2^{((s-1)n+t)/N}} + \frac{2}{3E} \leq e^2 + 1/6 < 8 \tag{26}$$

the numerator and the denominator of $\gamma_{s,t}$ are very large. The matrix

$$\widetilde{\Gamma} = (\widetilde{\gamma}_{s,t}) \in \mathbb{Q}^{m\times n} \tag{27}$$

with "smaller" entries such that computing $\widetilde{\Gamma}\boldsymbol{x}^T$ requires $m(n-1)$ additions is defined by

$$\widetilde{\gamma}_{s,t} = \frac{\lfloor 3\lfloor E+1\rfloor \gamma_{s,t}\rfloor}{3\lfloor E+1\rfloor}, \qquad s = 1,\ldots,m, \ t = 1,\ldots,n. \tag{28}$$

For the proof, by Proposition 29, it suffices to show that

$$\left|e^{2^{((s-1)n+t)/N}} - \widetilde{\gamma}_{s,t}\right| < \frac{1}{E},$$

which is indeed so, because

$$\begin{aligned}\left|e^{2^{((s-1)n+t)/N}} - \widetilde{\gamma}_{s,t}\right| &= \left|e^{2^{((s-1)n+t)/N}} - \frac{\lfloor 3\lfloor E+1\rfloor\gamma_{s,t}\rfloor}{3\lfloor E+1\rfloor}\right| \\ &= \left|e^{2^{((s-1)n+t)/N}} - \gamma_{s,t} - \frac{\{3\lfloor E+1\rfloor\gamma_{s,t}\}}{3\lfloor E+1\rfloor}\right| \\ &\leq \left|e^{2^{((s-1)n+t)/N}} - \gamma_{s,t}\right| + \frac{\{3\lfloor E+1\rfloor\gamma_{s,t}\}}{3\lfloor E+1\rfloor} \\ &\leq \frac{2}{3E} + \frac{1}{3\lfloor E+1\rfloor} \leq \frac{1}{E}.\end{aligned}$$

By definition, the matrix

$$\Omega = 3\lfloor E+1\rfloor\widetilde{\Gamma} \in \mathbb{Z}^{m\times n}, \tag{29}$$

where $\widetilde{\Gamma}$ is defined by (28), has integer entries and computing $\Omega\boldsymbol{x}^T$ also requires $m(n-1)$ additions. Thus we have the following.

▶ **Theorem 33.** *Let $N = mn \geqslant 4$. The matrix*

$$\Omega = (\omega_{s,t}) \in \mathbb{Z}^{m\times n},$$

given by (29) *defines the set of linear forms of complexity $m(n-1)$ and has elements of size*

$$0 \leqslant \omega_{s,t} \leqslant 25\exp\left(N^{N^{3N^2}}\right).$$

Proof. From the above discussion it only remains to estimate the size of elements of Ω. From (26) we conclude that

$$0 \leqslant \omega_{s,t} \leqslant 8(3E+1) \leqslant 25E,$$

where E is defined by (23). As one easily verifies that under our assumption we have $E \geqslant 24$. ◀

It seems to be of interest to find an integer matrix with smaller entries, that defines the set of linear forms of the same complexity.

References

1 Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, MA, 1974.

2 Tom M. Apostol. *Mathematical Analysis*. Addison-Wesley, Reading, MA, 1963. Second edition.

3 Enrico Bombieri and Jeffrey. D. Vaaler. On Siegel's lemma. *Inventiones Mathematicaea*, 73:11–32, 1983.

4 Peter Bürgisser, Michael Clausen, and Amin Shokrollahi. *Algebraic Complexity Theory*. Springer, Berlin, 1997.

5 Teresa Krick, Luis M. Pardo, and Martín Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Mathematical Journal*, 9:354–364, 2001.

6 Serge Lang. *Algebraic Number Theory*. Addison-Wesley, Reading, MA, 1970.

7 Jacques Morgenstern. Note on a lower bound on the linear complexity of the fast Fourier transform. *Journal of the ACM*, 20:305–306, 1973.

8 Oskar Perron. *Algebra I* (*Die Grundlagen*). Walter de Gruyter, Berlin, 1927.

9 Arkadiusz Ploski. Algebraic dependence of polynomials after O. Perron and some applications. In Svetlana Cojocaru, Gerhard Pfister, and Victor Ufnarovski, editors, *Computational Commutative and Non-Commutative Algebraic Geometry*, volume 196 of *NATO Science Series, III: Computer and Systems Sciences*, pages 167–173. IOS Press, Amsterdam, 2005.

10 John E. Savage. An algorithm for the computation of linear forms. *SIAM Journal on Computing*, 3:150–158, 1974.

11 Alain Sert. Une version effective du théorème de Lindemann-Weierstrass par les déterminants d'interpolation. *Journal of Number Theory*, 76:94–119, 1999.

12 Carl L. Siegel. Über einige Anwendungen diophantischer Approximationen. *Abhandlungen der Preussischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse*, 1:209–266, 1929.

13 Volker Strassen. Vermeidung von Divisionen. *Journal für Reine und Angewandte Mathematik*, 264:184–202, 1973.

14 Volker Strassen. Polynomials with rational coefficients which are hard to compute. *SIAM Journal on Computing*, 3:128–149, 1974.

15 Jeffrey D. Vaaler. The best constant in Siegel's lemma. *Monatshefte für Mathematik*, 140:71–89, 2003.

16 Shmuel Winograd. On the number of multiplications necessary to compute certain functions. *Communications od Pure and Applied Mathematics*, XXIII:165–179, 1970.

A Proofs of Corollary 28 and Proposition 29

A.1 Proof of Corollary 28

We just substitute the upper bounds

$$d \leqslant N^{N-1} \qquad \text{and} \qquad h(P) \leqslant N^{2N^{N^2}}$$

from Corollary 24 on d and H, respectively, in the parameters of Lemma 26 and also recall Remark 27. We note that we use some crude inequalities to simplify the bound.

More precisely, one verifies that for $N \geqslant 4$ we have

$$41 \times 3^{2N} 2^{-N+1} N^{-1} \leqslant 2^{5N}.$$

Hence, in Lemma 26 we can now take

$$c_0 \leqslant 41 \times 3^{2N} 2^{-N+1} D^{N+1} N^{2N-1} \leqslant 2^{5N} D^{N+1} N^{2N}. \tag{30}$$

Furthermore, simple calculus shows that $\ln(9x) \leqslant x$ for $x \geqslant 4$, hence

$$\ln(9DN) \leqslant DN.$$

Using this and the trivial bounds

$$1 + 6D \leqslant 2^3 D \qquad \text{and} \qquad 1 + 6N \leqslant 2^3 N,$$

we now obtain

$$\begin{aligned} c_1 &= 2^{2-N}3^{2N+1}D^{N+1}N^N + (1+6D)2^{4-N}3^{2N}D^N N^N \ln(9ND) \\ &\qquad\qquad + 2^{4-N}3^{2N}D^{N+1}N^N(1+6N)\ln \mathfrak{h}_a(\boldsymbol{\alpha}), \\ &\leqslant 2^{2-N}3^{2N+1}D^{N+1}N^N + 2^{7-N}3^{2N}D^{N+2}N^{N+1} \\ &\qquad\qquad + 2^{7-N}3^{2N}D^{N+1}N^{N+1}\ln \mathfrak{h}_a(\boldsymbol{\alpha}), \\ &\leqslant \left(2^{2-N}3^{2N+1}D^{-1}N^{-1} + 2^{7-N}3^{2N}\right)D^{N+2}N^{N+1} \\ &\qquad\qquad + 2^{7-N}3^{2N}D^{N+1}N^{N+1}\ln \mathfrak{h}_a(\boldsymbol{\alpha}) \\ &\leqslant \left(2^{-N}3^{2N+1} + 2^{7-N}3^{2N}\right)D^{N+2}N^{N+1} \\ &\qquad\qquad + 2^{7-N}3^{2N}D^{N+1}N^{N+1}\ln \mathfrak{h}_a(\boldsymbol{\alpha}). \end{aligned}$$

Since, for $N \geqslant 4$, we have

$$2^{-N}3^{2N+1} + 2^{7-N}3^{2N} = (3+128)\,2^{-N}3^{2N} = 131 \times 2^{-N}3^{2N} \leqslant 2^{4N}$$

and certainly the same bound for just the second term $2^{7-N}3^{2N}$, we derive

$$c_1 \leqslant 2^{4N}D^{N+1}N^{N+1}\left(D + \ln \mathfrak{h}_a(\boldsymbol{\alpha})\right). \tag{31}$$

Finally, for c_2, using $1+6D \leqslant 8D$ we have

$$c_2 = 2^{7-N}3^{2N}D^{N+1}N^N \leqslant 2^{4N}D^{N+1}N^N. \tag{32}$$

We now collect (30), (31) and (32) and obtain

$$\begin{aligned} c_0 d^N &\leqslant 2^{5N}N^{2N}D^{N+1}N^{N(N-1)} = 2^{5N}D^{N+1}N^{N^2+N}, \\ c_1 d^N &\leqslant 2^{4N}N^{N+1}D^{N+1}\left(D + \ln \mathfrak{h}_a(\boldsymbol{\alpha})\right)N^{N(N-1)} \\ &\qquad\qquad = 2^{4N}D^{N+2}N^{N^2+1} + 2^{4N}D^{N+1}N^{N^2+1}\ln \mathfrak{h}_a(\boldsymbol{\alpha}), \\ c_2 d^N \ln d &\leqslant 2^{4N}N^N D^{N+1}N^{N(N-1)}(N-1)\ln N \leqslant 2^{4N}D^{N+1}N^{N^2+1}\ln N. \end{aligned}$$

Therefore, we have the inequality

$$\begin{aligned} & c_1 d^N + c_2 d^N \ln d + 72\max\{1, \mathfrak{h}_a(\boldsymbol{\alpha})\} \\ &\qquad \leqslant 2^{4N}D^{N+2}N^{N^2+1} + 2^{4N}D^{N+1}N^{N^2+1}\ln N \\ &\qquad\qquad + \left(2^{4N}D^{N+1}N^{N^2+1} + 72\right)\max\{1, \mathfrak{h}_a(\boldsymbol{\alpha})\}. \end{aligned} \tag{33}$$

We now observe that

$$2^{4N}D^{N+2}N^{N^2+1} + 2^{4N}D^{N+1}N^{N^2+1}\ln N \leqslant 2^{4N+1}D^{N+2}N^{N^2+2}\ln N$$

and

$$2^{4N}D^{N+1}N^{N^2+1} + 72 \leqslant 2^{4N+1}D^{N+1}N^{N^2+1} \leqslant 2^{4N+1}D^{N+1}N^{N^2+1}\ln N.$$

Hence, the inequality (33) simplifies as follows:

$$\begin{aligned} & c_1 d^N + c_2 d^N \ln d + 72\max\{1, \mathfrak{h}_a(\boldsymbol{\alpha})\} \\ &\qquad\qquad \leqslant 2^{4N+1}D^{N+1}N^{N^2+2}\left(D + \max\{1, \mathfrak{h}_a(\boldsymbol{\alpha})\}\right)\ln N, \end{aligned}$$

and thus,

$$\exp\left(c_1 d^N + c_2 d^N \ln d + 72\max\{1, \mathfrak{h}_a(\boldsymbol{\alpha})\}\right) \leqslant N^{2^{4N+1} D^{N+1} N^{N^2+2}(D+\max\{1,\mathfrak{h}_a(\boldsymbol{\alpha})\})}.$$

Finally

$$\ln H = \ln h(P) \leqslant 2N^{N^2} \ln N$$

and we conclude

$$\ln H + \exp\left(c_1 d^N + c_2 d^N \ln d + 72\max\{1, \mathfrak{h}_a(\boldsymbol{\alpha})\}\right) \\ \leqslant 2N^{2^{4N+1} D^{N+1} N^{N^2+2}(D+\max\{1,\mathfrak{h}_a(\boldsymbol{\alpha})\})}.$$

Therefore, combining this bound with the above bound on $c_0 d^N$, by Lemma 26 we have

$$\ln |Q(e^{\alpha_1}, \ldots, e^{\alpha_N})| \geqslant -2^{5N+1} D^{N+1} N^{N^2+N} N^{2^{4N+1} D^{N+1} N^{N^2+2}(D+\max\{1,\mathfrak{h}_a(\boldsymbol{\alpha})\})}.$$

Elementary calculus shows that for $N \geqslant 4$ we have

$$2^{5N+1} D^{N+1} N^{N^2+N} \leqslant N^{2^{4N+1} D^{N+1} N^{N^2+1}}.$$

Hence

$$\ln |Q(e^{\alpha_1} \ldots, e^{\alpha_N})| \geqslant -N^{2^{4N+2} D^{N+1} N^{N^2+2}(D+\max\{1,\mathfrak{h}_a(\boldsymbol{\alpha})\})} \\ \geqslant -N^{2^{5N} D^{N+1} N^{N^2+2}(D+\max\{1,\mathfrak{h}_a(\boldsymbol{\alpha})\})},$$

and the result follows.

A.2 Proof of Proposition 29

Since $[\mathbb{Q}(\alpha^{1/N}) : \mathbb{Q}] = N$, we see that $\alpha_k = \alpha^{k/N}$, $k = 1, \ldots, N$, are linearly independent over $\mathbb{Q}$ and $\mathbb{Q}(\alpha_1, \ldots, \alpha_N) = \mathbb{Q}(\alpha_N)$. Thus, for D in Corollary 28 we have $D = N$.

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_N)$. By definition, $h(\boldsymbol{\alpha}) = \alpha$. We contend that $\mathfrak{h}_a(\boldsymbol{\alpha}) = \alpha$ as well.

Since all α_k, $k = 1, \ldots, N$, are algebraic integers, their p-adic norms are less than 1. Therefore,

$$\mathfrak{h}_a(\boldsymbol{\alpha}) = \prod_{\nu|\infty} \max_{1 \le k \le N} \{1, |\alpha_k|_\nu\}^{D_\nu/N},$$

where (in this context) ∞ denotes the Archimedean value on $\mathbb{Q}$.

Since for all $\nu \mid \infty$ and all $k = 1, \ldots, N$,

$$\max\{1, |\alpha_k|_\nu\} = \alpha_k = \alpha^{k/N}$$

and by [6, Corollary 1, Section II.1]

$$\sum_{\nu|\infty} D_\nu = N,$$

we derive

$$\mathfrak{h}_a(\boldsymbol{\alpha}) = \prod_{\nu|\infty} \alpha^{D_\nu/N} = \alpha.$$

Now, the result follows from Corollary 18 with $\mathfrak{Q} = \mathfrak{Q}_{m,n}$, Corollary 25 and Corollary 28 by simple calculations.

Indeed, let

$$\delta_{s,t} = e^{\alpha^{((s-1)n+t)/N}}, \qquad s = 1, \dots, m, \ t = 1, \dots, n.$$

be the components of the vector $\boldsymbol{\delta} \in \mathbb{R}^N$ (indexed by $(s-1)n+t$).

For any $Q \in \mathfrak{Q}$ and $\boldsymbol{\mu} \in \mathbb{R}^N$ with $|\boldsymbol{\mu}| < 1$, by Corollary 25 (in which we interpret $\boldsymbol{\delta}$ and $\boldsymbol{\mu}$ as N-dimensional vectors), we have

$$|\nabla Q(\boldsymbol{\delta} + \boldsymbol{\mu})| < N^{3N^{N^2}} (e^a + 1)^{N^{N-1}} \leqslant N^{3N^{N^2}} (e^{N-1} + 1)^{N^{N-1}} \leqslant N^{3N^{N^2}} e^{N^N} \leqslant N^{4N^{N^2}}.$$

On the other hand, recalling that $D = N$ and $h(\boldsymbol{\alpha}) = \alpha$, by Corollary 28 we have

$$\begin{aligned} |Q(\boldsymbol{\delta})| &> \exp\left(-N^{2^{5N} N^{N^2+N+3}(N+\alpha)}\right) \\ &\geqslant \exp\left(-N^{2^{5N} N^{N^2+N+3}(2N-1)}\right) \\ &\geqslant \exp\left(-N^{2^{5N+1} N^{N^2+N+4}}\right). \end{aligned}$$

Hence

$$\frac{|Q(\boldsymbol{\delta})|}{|\nabla Q(\boldsymbol{\delta} + \boldsymbol{\mu})|} \geqslant N^{-4N^{N^2}} \exp\left(-N^{2^{5N+1} N^{N^2+N+4}}\right) \geqslant \exp\left(-2N^{2^{5N+1} N^{N^2+N+4}}\right).$$

Furthermore, since $N \geqslant 4$, we have

$$2N^{2^{5N+1} N^{N^2+N+4}} \leqslant N^{2^{5N+2} N^{N^2+N+4}} \leqslant N^{2^{6N} N^{N^2+N+4}} \leqslant N^{N^{N^2+4N+4}} \leqslant N^{N^{3N^2}}.$$

Note that, by (21), the condition $|\Delta - \Gamma| < 1$ of Corollary 18 is redundant.

B Density of matrices defining sets of linear forms of maximal additive complexity

B.1 Complexity of matrices

For a matrix Δ and a vector $\boldsymbol{x} = (x_1, \dots, x_n)^T$ of n indeterminates as in (1) and (2), respectively, we denote the additive complexity of the set of linear forms $\Delta \boldsymbol{x}$ by $\mathcal{C}(\Delta)$ and call it the complexity of Δ.

B.2 The case of finite fields

Let $\mathbb{F}$ be a finite field of q elements. In this section we show that "almost all" $m \times n$ matrices over $\mathbb{F}$, are of high complexity.

We may assume that $m \leq \frac{q^n - 1}{q-1}$, because the number of non-zero linear forms in n indeterminates over $\mathbb{F}$ is $q^n - 1$ and each form can be scaled by $q - 1$ non-zero elements of $\mathbb{F}$.

The proof is by the counting argument similar to that of [10, Lemma, Section 5]. For the sake of completeness, we reproduce it below.

For a positive integers C, m and n we denote by $S(C, m, n)$ the set of all $m \times n$ matrices over $\mathbb{F}$ of complexity not exceeding C:

$$S_{\mathbb{F}}(C, m, n) = \{\Delta \in \mathbb{F}^{m \times n} : \ \mathcal{C}(\Delta) \leq C\}.$$

First we need a bound on the cardinality $\# S_{\mathbb{F}}(C, m, n)$ of this set.

▶ **Proposition 34.** *We have*

$$\#S_{\mathbb{F}}(C,m,n) < (C+n)^{2C+m}q^{C+m}.$$

Proof. For a positive integer m a linear algorithm in n indeterminates of length C defines at most

$$L_{\mathbb{F}}(C,m) = \binom{C}{m}$$

sets of m linear forms, each of which is associated with

$$M_{\mathbb{F}}(m) = (q-1)^m m!$$

matrices of the size $m \times n$. Namely, we have $(q-1)^m$ scalar multiplications and $m!$ permutations, respectively, of the matrix rows.

Next we are going to count the number of linear algorithms over $\mathbb{F}$ in n indeterminates of length C, denoted by $A_{\mathbb{F}}(C,n)$.

By definition,

- $A_{\mathbb{F}}(1,n) \le n^2(q-1)$ and
- $A_{\mathbb{F}}(C+1,n) \le A_{\mathbb{F}}(C,n)(C+n)^2(q-1)$,

where the factors $(C+n)^2$ and $(q-1)$ come from the last addition $u_{C+1} = v + \alpha w$ of the algorithm,

$$v, w \in \{x_1,\dots,x_n\} \cup \{u_1,\dots,u_C\}$$

and $\alpha \ne 0$. Recall that all algorithms under consideration are normalized.

Solving the above recursion, we obtain

$$A_{\mathbb{F}}(C,n) \le \left(\frac{(C+n-1)!}{(n-1)!}\right)^2 (q-1)^C.$$

Thus,

$$\begin{aligned}\#S_{\mathbb{F}}(C,m,n) &\leqslant A_{\mathbb{F}}(C,n)L_{\mathbb{F}}(C,m)M_{\mathbb{F}}(m)\\ &< \left(\frac{(C+n-1)!}{(n-1)!}\right)^2 (q-1)^C \binom{C}{m}(q-1)^m m!\\ &< (C+n)^{2C+m}(q-1)^{C+m} < (C+n)^{2C+m}q^{C+m},\end{aligned}$$

which concludes the proof. ◀

▶ **Theorem 35.** *Let $\varepsilon, \kappa > 0$ be such that $2\kappa + \varepsilon < 1$ and let*

$$C_{\kappa,m,n} = \frac{\kappa mn}{\log_q(mn)} - n.$$

Then

$$\lim_{\substack{n\to\infty\\ q^{\varepsilon n}\ge m}} \frac{\#S_{\mathbb{F}}(C_{\kappa,m,n},m,n)}{q^{mn}} = 0.$$

Proof. It suffices to show that

$$\lim_{\substack{n\to\infty\\ q^{\varepsilon n}\ge m}} \left(\log_q \#S_{\mathbb{F}}(C_{\kappa,m,n},m,n) - mn\right) = -\infty. \qquad (34)$$

By Proposition 34 we have

$$\log_q \#S_{\mathbb{F}}(C_{\kappa,m,n}, m, n) - mn < (2C_{\kappa,m,n} + m) \log_q(C_{\kappa,m,n} + n) + C_{\kappa,m,n} + m - mn.$$

Recalling the definition of $C_{\kappa,m,n}$ and that $\kappa \leqslant 1$, we obtain

$$\begin{aligned}
&\log_q \#S_{\mathbb{F}}(C_{\kappa,m,n}, m, n) - mn \\
&\qquad < \left(\frac{2\kappa mn}{\log_q(mn)} - 2n + m\right) \log_q\left(\frac{\kappa mn}{\log_q(mn)}\right) + \frac{\kappa mn}{\log_q(mn)} - n + m - mn \\
&\qquad \leqslant \left(\frac{2\kappa mn}{\log_q(mn)} + m\right) \log_q(mn) + \frac{mn}{\log_q(mn)} + m - mn \\
&\qquad = 2\kappa mn + m \log_q m + m \log_q n + \frac{mn}{\log_q(mn)} + m - mn.
\end{aligned}$$

Under the condition $q^{\varepsilon n} \geq m$, we now obtain

$$\begin{aligned}
\log_q \#S_{\mathbb{F}}(C_{\kappa,m,n}, m, n) - mn &< 2\kappa mn + \varepsilon mn + m \log_q n + \frac{mn}{\log_q(mn)} + m - mn \\
&= (2\kappa + \varepsilon - 1 + o(1))\, mn,
\end{aligned}$$

and since $2\kappa + \varepsilon < 1$, we have (34). ◀

B.3 The case of rationals

In this case matrices with rational entries, since the set of polynomials $\mathfrak{Q}_{m,n}$, defined by (20), is (m,n)-complete, for for each matrix (1) such that $\mathcal{C}(\Delta) < m(n-1)$,

$$Q_{m,n}(\delta_{1,1}, \ldots, \delta_{m,n}) = 0,$$

where $Q_{m,n} = \prod_{Q \in \mathfrak{Q}_{m,n}} Q$.

Hence the entries of $m \times n$ rational matrices of complexity $\mathcal{C}(\Delta) < m(n-1)$ form a very sparse set in $\mathbb{Q}^{mn}$ (after we represent them as mn-dimensional vector). Namely, this set is a hypersurface of dimension $mn - 1$. In particular, almost all rational matrices (in terms on natural density) are of the maximal complexity $m(n-1)$.