On the Complexity of the Escape Problem for Linear Dynamical Systems over Compact Semialgebraic Sets

Julian D'Costa ORCID
Oxford University, United Kingdom

Engel Lefaucheux ORCID
Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany

Eike Neumann
Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany

Joël Ouaknine
Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany

James Worrell
Oxford University, United Kingdom

Abstract

We study the computational complexity of the Escape Problem for discrete-time linear dynamical systems over compact semialgebraic sets, or equivalently the Termination Problem for affine loops with compact semialgebraic guard sets. Consider the fragment of the theory of the reals consisting of negation-free $\exists\forall$-sentences without strict inequalities. We derive several equivalent characterisations of the associated complexity class which demonstrate its robustness and illustrate its expressive power. We show that the Compact Escape Problem is complete for this class.

2012 ACM Subject Classification

Keywords and phrases .

1 Introduction

EN: I just noticed that a lot of the above appears verbatim in your previous paper. This may have to be reformulated a bit more – e.g. not use the exact same idioms.

In ambient space $\mathbb{R}^n$, a *discrete linear dynamical system* is an orbit $(X_n)_{n\in\mathbb{N}}$ defined by an initial vector X_0 and a matrix A through the recursion $X_{n+1} = AX_n$. Linear dynamical systems are fundamental models in many different domains of science and engineering, and the computability and complexity of decision problems for linear dynamical systems are of both theoretical and practical interest.

In the study of dynamical systems, particularly from the perspective of control theory, considerable attention has been given to the study of *invariant sets*, *i.e.*, subsets of $\mathbb{R}^d$ from which no trajectory can escape; see, *e.g.*, [**?**, **?**, **?**, **?**]. Our focus in the present paper is on sets with the dual property that *no trajectory remains trapped*. Such sets play a key role in analysing *liveness* properties in cyber-physical systems (see, for instance, [1]): discrete progress is ensured by guaranteeing that all trajectories (*i.e.*, from any initial starting point) must eventually reach a point at which they "escape" (temporarily or permanently) the set in question, thereby forcing a discrete transition to take place.

More precisely, given a rational matrix A and a semialgebraic set $K \subseteq \mathbb{R}^d$, one may consider the *Discrete Escape Problem (DEP)* which asks whether, for all starting points X_0 in K, the corresponding orbit of the discrete linear dynamical system $(X_n)_{n\in\mathbb{N}}$ eventually

escapes K.[1]

The restriction of the DEP to the case when K is a *convex polytope*—phrased as "termination of linear programs" over the reals and the rationals respectively—was already studied and shown decidable in the seminal papers [**?**, **?**], albeit with no complexity bounds nor upper bounds on the number of iterations required to escape.

In this paper we study the *Compact Escape Problem (CEP)*, a version of the DEP where we additionally assume that the semialgebraic set K is compact. In practice, of course, this is usually not a burdensome restriction; in most cyber-physical systems applications, for instance, all relevant sets will be compact (see, *e.g.*, [1]).

The CEP was recently shown to be decidable for arbitrary compact semialgebraic sets in [12], however, no complexity was given.

The theory of the reals is the theory of the structure with universe $\mathbb{R}$ and signature $\langle \mathbb{Z}, +, \times, \leq, < \rangle$. By Tarski's theorem **JD:** cite this theory admits quantifier elimination, is recursively axiomatisable, and equal to the elementary theory of real closed fields. While this entails that the quantifier-free fragment of the theory is already as expressive as the whole theory, the complexity of quantifier elimination is non-negligible. The best-known practical methods based on Collins's technique of *Cylindrical Algebraic Decomposition* [8] have doubly exponential complexity in the number of quantifiers. Asymptotically faster but arguably impractical algorithms for the general decision problem were given by **EN:** Grioriev for decision, Renegar (?) for quantifier elimination. The running time of these algorithms is doubly exponential in the number of quantifier alternations, singly exponential in the dimension, and polynomial in the rest of the data.

This has motivated the introduction of complexity classes based on decision problems for fragments of the theory of the reals based on bounded quantifier alternations. The arguably best-known and best-studied such class is the existential theory of the reals **EN:** cite people, mention PSPACE decision problem, etc..

Main contributions. The goal of this paper is to establish the exact complexity of the Compact Escape Problem. Consider the fragment of the first-order theory of the reals composed of positive boolean combinations of non-strict polynomial inequalities prefixed by a single alternation of a block of existential and a block of universal quantifiers. Let us denote by $\exists\forall_{\leq}\mathbb{R}$ the complexity class of all problems reducible in polynomial time to the decision problem for this fragment. **EN:** I would avoid language like the below Using strong results from effective real algebraic geometry we prove that $\exists\forall_{\leq}\mathbb{R}$ is polynomial time equivalent to the decision problem for another fragment of $\exists\forall$-sentences where the quantifiers are restricted to range over compact sets, a result of independent interest. Finally, we leverage Diophantine approximation and algebraic number theory to show that the Compact Escape Problem is complete for this class.

1.1 Overview of the paper

We formally define the Compact Escape Problem (CEP) as the following decision problem:

Given as input

- A matrix $A \in \mathbb{Q}^{n \times n}$ with rational entries,
- A list $\mathcal{P}$ of polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$,

[1] By "escaping" K, we simply mean venturing outside of K—we are unconcerned whether the trajectory might re-enter K at a later time.

- A propositional formula $\Phi(x_1, \ldots, x_n)$ which combines atomic predicates of the form $P(x_1, \ldots, x_n) \leq 0$ with $P \in \mathcal{P}$ by means of the propositional connectives $\vee$ and $\wedge$,

subject to the promise that the set $K = \{x \in \mathbb{R}^n \mid \Phi(x)\}$ is compact, decide whether for all $x \in K$ there exists $k \in \mathbb{N}$ such that $A^k x \notin K$.

We assume that the polynomials P_j in the list $\mathcal{P}$ are encoded as lists $\langle(\alpha_{j,k}, c_{j,k})\rangle_{k=1,\ldots,s_j}$ of pairs of multi-indexes $\alpha_{j,k} \in \mathbb{N}^n$, whose entries are encoded in unary, and coefficients $c_{j,k} \in \mathbb{Z}$, encoded in binary, such that

$$P_j(x_1, \ldots, x_n) = \sum_{k=1}^{s_j} c_{j,k}(x_1, \ldots, x_n)^{\alpha_{j,k}}.$$

Note that the analogous problem for affine maps $x \mapsto Ax + b$ reduces to the CEP, for a point $x \in K$ escapes the compact set K under iterations of the affine map $Ax + b$ if and only if the point $(x, 1) \in K \times \{1\}$ escapes $K \times \{1\}$ under iterations of the linear map $B(x, z) = Ax + bz$.

We capture the computational complexity of this decision problem by showing that it is equivalent to the decision problem for a fragment of the theory of the reals.

Let $\exists\forall_{\leq}\mathbb{R}$ denote the decision problem for sentences of the form

$$\exists X \in \mathbb{R}^n . \forall Y \in \mathbb{R}^m . \left(\Phi_{0,\leq}(X, Y)\right), \tag{1}$$

where $\Phi_{0,\leq}$ is a positive boolean combination of non-strict polynomial inequalities. Evidently, this class lies between the existential fragment of the theory of the reals (without restriction on the types of inequalities) and the full $\exists\forall$-fragment.

The main result of this paper is the following:

▶ **Theorem 1.** *The compact escape problem is complete for the complexity class $\exists\forall_{\leq}\mathbb{R}$.*

The proof consists of three steps:

First, we show that for any sentence of the form

$$\exists X \in [-1, 1]^n . \forall Y \in [-1, 1]^m . \left(\Phi_{0,\leq}(X, Y)\right), \tag{2}$$

where $\Phi_{0,\leq}$ is a positive boolean combination of non-strict polynomial inequalities, one can compute a matrix $A \in \mathbb{Q}^{(n+2m)\times(n+2m)}$ and a compact set $K \subseteq \mathbb{R}^{n+2m}$ such that (A, K) is a negative instance of the compact escape problem if and only if (2) holds true.

Secondly, given any instance (A, K) with $A \in \mathbb{Q}^{n\times n}$ and $K \subseteq \mathbb{R}^n$ we can compute in polynomial time a sentence of the form

$$\exists X \in [-1, 1]^m . \forall Y \in [-1, 1]^\ell . \left(\Psi_{0,\leq}(Y) \to \Phi_{0,\leq}(X, Y)\right), \tag{3}$$

where $\Psi_{0,\leq}$ and $\Phi_{0,\leq}$ are a positive boolean combination of non-strict polynomial inequalities, such that (3) holds true if and only if (A, K) is a negative instance of the compact escape problem.

Finally, we prove that the decision problems for sentences of the form (1), (2), and (3) are all equivalent.

2 Preliminaries

2.1 Fragments of the theory of the reals

The statement and proof of Theorem 1 require complexity classes induced by decision problems for fragments of the the first-order theory of the reals. The main goal of this subsection is to formally define these complexity classes.

Thus, let $\mathcal{L}$ be the first-order language with signature $\langle \mathbb{Z}, +, \times, <, \leq \rangle$, propositional connectives, $\wedge$ and $\vee$, and quantifiers $\exists$ and $\forall$. For complexity purposes, we assume that integer constants are encoded in binary. See, *e.g.*, [15, 16] for an introduction to first-order logic. We interpret all formulas in $\mathcal{L}$ in the structure of real numbers. Thus, we say that two formulas are equivalent if their interpretations in $\mathbb{R}$ are equivalent. The restriction to the connectives $\vee$ and $\wedge$ is insubstantial, since formulas over the same signature that use the connectives "$\neg$" and "$\rightarrow$" can be efficiently converted into equivalent formulas in $\mathcal{L}$. We will make free use of the connectives $\neg$ and $\rightarrow$ throughout this paper, understanding them as syntactic sugar.

Let QFF denote the set of quantifier-free formulas in $\mathcal{L}$. Let $\mathrm{QFF}_{\leq}$ (resp. $\mathrm{QFF}_{<}$) denote the subset of QFF consisting of those formulas that do not contain the relational symbol "$<$" (resp. "$\leq$"). Note that the negation of a $\mathrm{QFF}_{\leq}$-formula is a $\mathrm{QFF}_{<}$-formula and vice versa.

We define the sets of formulas $\Sigma_{n,\leq}$ and $\Pi_{n,\leq}$ inductively as follows:

1. Let $\Sigma_{0,\leq} = \Pi_{0,\leq} = \mathrm{QFF}_{\leq}$.
2. A formula $\Psi(y_1, \ldots, y_s)$ belongs to $\Sigma_{n+1,\leq}$ if and only if it is of the form

$$\Psi(y_1, \ldots, y_s) = (\exists x_1) \ldots (\exists x_t).\Phi(x_1, \ldots, x_t, y_1, \ldots, y_s),$$

   where Φ belongs to $\Pi_{n,\leq}$.
3. Dually, a formula $\Psi(y_1, \ldots, y_s)$ belongs to $\Pi_{n+1,\leq}$ if and only if it is of the form

$$\Psi(y_1, \ldots, y_s) = (\forall x_1) \ldots (\forall x_t).\Phi(x_1, \ldots, x_t, y_1, \ldots, y_s),$$

   where Φ belongs to $\Sigma_{n,\leq}$.

We define $\Sigma_{n,<}$ and $\Pi_{n,<}$ (resp. Σ_n and Π_n) analogously, starting with $\mathrm{QFF}_{<}$-formulas (resp. QFF-formulas).

By convention we denote vectors of variables $X = (x_1, \ldots, x_t)$ by upper case letters and introduce the shorthand notations $\exists X$ and $\forall X$ for blocks of quantifiers $(\exists x_1) \ldots (\exists x_t)$ and $(\forall x_1) \ldots (\forall x_t)$. Recall that a first-order formula Φ is called a sentence if it does not contain any free variable.

The *decision problem* for a class $\mathcal{C}$ of first-order formulas in the language $\mathcal{L}$ is the following: Given a sentence that belongs to $\mathcal{C}$ decide whether the sentence holds true in the universe of real numbers.

It is natural to ask how the decision problems for the classes we have introduced above are related with respect to polynomial-time reductions. By taking the negation of formulas it is easy to see that the decision problem for Σ_n is equivalent to that of Π_n, the decision problem for $\Sigma_{n,\leq}$ is equivalent to that of $\Pi_{n,<}$, and the decision problem for $\Sigma_{n,<}$ is equivalent to that of $\Pi_{n,\leq}$. As such it suffices to consider the "Σ"-classes in the following.

By a standard trick, any QFF-formula $\Phi(X)$ with free variables X can be converted in polynomial time into an equivalent formula $\exists Y.f(X, Y) = 0$ where f is a single polynomial. It follows that:

1. If n is odd then the decision problems for the classes Σ_n and $\Sigma_{n,\leq}$ are polynomial-time equivalent.
2. If n is even then the decision problems for the classes Σ_n and $\Sigma_{n,<}$ are polynomial-time equivalent.

Of course, for $n = 0$ the decision problem is trivial for all three classes. For $n = 1$ we have the following remarkable result:

▶ **Theorem 2** ([14]). *The decision problems for Σ_1 and $\Sigma_{1,<}$ are polynomial-time equivalent.*

We thus have polynomial-time reductions for decision problems as indicated below:

$$(\Sigma_0 \equiv \Sigma_{0,\leq} \equiv \Sigma_{0,<}) \to (\Sigma_1 \equiv \Sigma_{1,\leq} \equiv \Sigma_{1,<}) \to \Sigma_{2,\leq} \to (\Sigma_2 \equiv \Sigma_{2,<}) \to \Sigma_{3,<} \to \dots$$

It is open to the best of our knowledge whether there exists a reduction of the decision problem for Σ_2 to that of $\Sigma_{2,\leq}$. The techniques from [14] do not seem to carry over to higher orders of quantifier alternations.

We study the decision problem for the class $\Sigma_{2,\leq}$ in greater detail. Let us denote by $\exists\forall_{\leq}\mathbb{R}$ the complexity class of all problems reducible in polynomial time to this decision problem. To demonstrate the robustness of this complexity class and gauge its computational power we give a number of equivalent characterisations. It turns out that, somewhat surprisingly, the decision problem for $\Sigma_{2,\leq}$-sentences is equivalent to the decision problem for exists-forall-sentences whose quantifiers are restricted to range over compact sets.

Let $X = (x_1, \dots, x_n)$ be a vector of variables. Let y be a variable or a constant. We write $|X| \leq y$ as an abbreviation for the formula $\bigwedge_{j=1}^{n} (-y \leq x_j \leq y)$. Of course, this syntactic construct will only have the intended semantics if our context ensures that $y \geq 0$, and we will only use it in such situations.

Write $I = [-1, 1]$. Let $\Phi_0(X, Y, Z)$ be a quantifier-free formula in $\mathcal{L}$. We introduce the syntactic abbreviation

$$\exists X \in I^n . \forall Y \in I^m . (\Phi_0(X, Y, Z))$$

for the formula

$$\exists X \in \mathbb{R}^n . \forall Y \in \mathbb{R}^m . (|Y| > 1 \vee (|X| \leq 1 \wedge \Phi_0(X, Y, Z)))$$

in the language $\mathcal{L}$.

We have the following result, whose proof is the focus of Section 3:

▶ **Theorem 3.** *The decision problems for the following three classes of sentences are equivalent with respect to polynomial-time reduction:*

1. *The class $\Sigma_{2,\leq}$, consisting of sentences of the form*

$$\exists X \in \mathbb{R}^m . \forall Y \in \mathbb{R}^n . (\Phi_{0,\leq}(X, Y)),$$

where $\Phi_{0,\leq}$ is a $\mathrm{QFF}_{\leq}$-formula.

2. *The class $\mathtt{b}\text{-}\Sigma_{2,\leq}$, consisting of sentences of the form*

$$\exists X \in I^m . \forall Y \in I^n . (\Phi_{0,\leq}(X, Y)),$$

where $\Phi_{0,\leq}$ is a $\mathrm{QFF}_{\leq}$-formula.

3. *The class $\mathtt{b}\text{-}\Sigma^{++}_{2,\leq}$, consisting of sentences of the form*

$$\exists X \in I^m . \forall Y \in I^n . (\Psi_{0,\leq}(Y) \to \Phi_{0,\leq}(X, Y)),$$

where $\Phi_{0,\leq}$ and $\Psi_{0,\leq}$ are $\mathrm{QFF}_{\leq}$-formulas.

It is obvious that the decision problem for $\mathtt{b}\text{-}\Sigma_{2,\leq}$-sentences reduces to that of $\mathtt{b}\text{-}\Sigma^{++}_{2,\leq}$-sentences. Note however that it is not clear that a reduction should exist in either direction between $\Sigma_{2,\leq}$ and $\mathtt{b}\text{-}\Sigma_{2,\leq}$. On the one hand, the latter class only allows for quantification over bounded sets, which seems to make it more restrictive. On the other hand, $\mathtt{b}\text{-}\Sigma_{2,\leq}$-sentences involve strict inequalities and hence do not belong to the class $\Sigma_{2,\leq}$. Let us denote

by $\mathtt{b}\text{-}\exists\forall_{\leq}\mathbb{R}$ and by $\mathtt{b}\text{-}\exists\forall^{++}_{\leq}\mathbb{R}$ the complexity classes induced respectively by the decision problem for $\mathtt{b}\text{-}\Sigma_{2,\leq}$-sentences and by the decision problem for $\mathtt{b}\text{-}\Sigma^{++}_{2,\leq}$-sentences.

A remark is in order on the robustness of our definition of the class $\exists\forall_{\leq}\mathbb{R}$ under different encodings of polynomials. In practice it is common to encode a polynomial P as a list $\langle(\alpha_j, c_j)\rangle_{j=1,\dots,m}$ where $\alpha_j \in \mathbb{N}^n$ is a multi-index and $c_j \in \mathbb{Z}$ such that

$$P(x_1, \dots, x_n) = \sum_{j=1}^{m} c_j (x_1, \dots, x_n)^{\alpha_j}. \tag{4}$$

This is the encoding we have chosen in the definition of the CEP. By contrast, the polynomials that occur in atomic predicates of a formula in the language $\mathcal{L}$ are encoded as terms over the signature $\langle \mathbb{Z}, +, \times \rangle$. While one can translate the encoding (4) to a term over the signature $\langle \mathbb{Z}, +, \times \rangle$ in polynomial time, a term of size N can encode a polynomial whose number of non-zero coefficients grows exponentially in N, so that a polynomial-time translation in the other direction is not possible in general. One may hence raise the justified objection that the reduction of the CEP to the decision problem for $\Sigma_{2,\leq}$ sentences could hide an exponential overhead in the encoding of the polynomials. Moreover, in order to show $\exists\forall_{\leq}\mathbb{R}$-hardness of the CEP we need to convert a compact set which is encoded as a $\mathrm{QFF}_{\leq}$-formula into an equivalent formula whose atoms use the encoding (4). We show in Theorem 18 that we can efficiently convert any $\Sigma_{2,\leq}$-sentence into an equivalent one whose atoms have degree at most 4. This resolves the issue, for a uniform bound on the degrees allows one to translate back and forth in polynomial time between the two encodings of polynomials. While an analogous result for Σ_2-sentences (and, *e.g.*, $\mathrm{QFF}_{\leq}$-formulas) is straightforward (see *e.g.* [14, Lemma 3.2] or the proof of Theorem 18 below for a proof idea), the argument becomes much more involved for $\Sigma_{2,\leq}$-sentences. It relies on many of the results that are established in the sequel. Thus, for the majority of this paper we have to insist on our specific choice of encoding.

2.2 Mathematical tools

Our characterisation of the complexity class $\exists\forall_{\leq}\mathbb{R}$ requires two strong results from effective real algebraic geometry: Singly exponential quantifier elimination and a doubly exponential bound on a ball meeting all components of a semialgebraic set. We use the following singly exponential quantifier elimination result given in [2]. For a historic overview on this type of result see [2, Chapter 14, Bibliographical Notes].

▶ **Theorem 4** ([2, Theorem 14.16]). *Let $\mathcal{P}$ be a set of at most s polynomials with integer coefficients, each of degree at most d, in $k + n_1 + \cdots + n_\ell$ variables. Let τ be a bound on the bitsize of the coefficients of all $P \in \mathcal{P}$. Let*

$$\Phi_\ell(Y) = (Q_1 X_1). \dots . (Q_\ell X_\ell). \left(\Psi_0(Y, X_1, \dots, X_\ell)\right),$$

where $Q_j \in \{\exists, \forall\}$ are alternating blocks of quantifiers, be a formula over the language $\mathcal{L}$, all of whose atoms involve polynomials contained in $\mathcal{P}$. Assume that the size of the block of variables Y is k and that the size of the block of variables X_j is n_j.

Then there exists an equivalent quantifier-free formula

$$\omega_0(Y) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} \bigvee_{m=1}^{M_{i,j}} P_{i,j,m}(Y) \bowtie_{i,j,m} 0.$$

over $\mathcal{L}$, where:

1. $I \leq s^{(n_1+1)\cdot\cdots\cdot(n_\ell+1)(k+1)} d^{O(n_1\cdot\cdots\cdot n_\ell\cdot k)}$.
2. $J_i \leq s^{(n_1+1)\cdot\cdots\cdot(n_\ell+1)} d^{O(n_1\cdot\cdots\cdot n_\ell)}$.
3. $M_{i,j} \leq d^{O(n_1\cdot\cdots\cdot n_\ell)}$.
4. *The degrees of the polynomials* $P_{i,j,m}$ *are bounded by* $d^{O(n_1\cdot\cdots\cdot n_\ell)}$.
5. *The bitsize of the coefficients of the polynomials* $P_{i,j,m}$ *is bounded by* $\tau d^{O(n_1\cdot\cdots\cdot n_\ell\cdot k)}$.

Recall that a *sign condition* on a family $\mathcal{P}$ of polynomials in n variables is a mapping $\sigma\colon \mathcal{P} \to \{-1, 0, 1\}$. The *realisation* of a sign condition σ in $\mathbb{R}^n$ is the set

$$\mathrm{Reali}(\sigma) = \{X \in \mathbb{R}^n \mid \forall P \in \mathcal{P}.\, \mathrm{sign}(P(X)) = \sigma(P)\}\,.$$

A sign condition σ is called *realisable* if its realisation is non-empty. Equivalently, a sign condition is a formula over the language $\mathcal{L}$ involving only conjunctions.

The next theorem is due to Vorobjov [17]. See also [9, Lemma 9] and [3, Theorem 4].

▶ **Theorem 5.** *There exists an integer constant* β' *with the following property: Let* $\mathcal{P}$ *be a set of* s *polynomials with integer coefficients in* n *variables of degree at most* $d \geq 2$*. Assume that the bit-size of the coefficients of each polynomial in* $\mathcal{P}$ *is at most* τ*. Then there exists a ball centred at the origin of radius at most*

$$2^{\tau d^{\beta'(n+1)}}$$

which intersects every connected component of every realisable sign condition on $\mathcal{P}$ *in* $\mathbb{R}^n$*.*

Our proof of $\exists\forall_{\leq}\mathbb{R}$-completeness of the CEP combines spectral methods with two well-known but nontrivial results on algebraic numbers. We require a version of Kronecker's theorem on simultaneous Diophantine approximation. See [13, Corollary 3.1] for a proof.

▶ **Theorem 6.** *Let* $(\lambda_1, \ldots, \lambda_m)$ *be complex algebraic numbers of modulus* 1*. Consider the free Abelian group*

$$L = \{(n_1, \ldots, n_m) \in \mathbb{Z}^m \mid \lambda_1^{n_1} \cdot \cdots \cdot \lambda_m^{n_m} = 1\}\,.$$

Let $(\beta_1, \ldots, \beta_s)$ *be a basis of* L*. Let* $\mathbb{T}^m = \{(z_1, \ldots, z_m) \in \mathbb{C}^m \mid |z_j| = 1\}$ *denote the complex unit* m*-torus. Then the closure of the set* $\{(\lambda_1^k, \ldots, \lambda_m^k) \in \mathbb{T}^m \mid k \in \mathbb{N}\}$ *is the set* $S = \{(z_1, \ldots, z_m) \in \mathbb{T}^m \mid \forall j \leq s.(z_1, \ldots, z_m)^{\beta_j} = 1\}$*.*

Moreover, for all $\varepsilon > 0$ *and all* $(z_1, \ldots, z_m) \in S$ *there exist infinitely many indexes* k *such that* $|\lambda_j^k - z_j| < \varepsilon$ *for* $j = 1, \ldots, n$*.*

Moreover, the integer multiplicative relations between given complex algebraic numbers in the unit circle can be elicited in polynomial time. For a proof see [6, 10]. We assume the standard encoding of algebraic numbers, see [7] for details.

▶ **Theorem 7.** *Let* $(\lambda_1, \ldots, \lambda_m)$ *be complex algebraic numbers of modulus* 1*. Consider the free Abelian group*

$$L = \{(n_1, \ldots, n_m) \in \mathbb{Z}^m \mid \lambda_1^{n_1} \cdot \cdots \cdot \lambda_m^{n_m}\}\,.$$

Then one can compute in polynomial time a basis $(\beta_1, \ldots, \beta_s) \in (\mathbb{Z}^m)^s$ *for* L*. Moreover, the integer entries of the basis elements* β_j *are bounded polynomially in the size of the encodings of* $\lambda_1, \ldots, \lambda_m$*.*

3 Proof of Theorem 3

Our proof of Theorem 3 will use Theorems 4 and 5. The latter are formulated in terms of the algebraic complexity of a family of polynomials. We will reformulate them in terms of the bitsize of a formula in the language $\mathcal{L}$.

The *matrix size* μ of a first-order formula

$$\Psi(Y) = (Q_1 X_1). \dots . (Q_\ell X_\ell). \left(\Phi_0(Y, X_1, \dots, X_\ell)\right),$$

where $Q_j \in \{\exists, \forall\}$ is the number of bits required to write down the quantifier-free part $\Phi_0(Y, X_1, \dots, X_\ell)$. The *dimensions* of the formula $\Psi(Y)$ are the numbers $m, n_1, \dots, n_\ell$, where m is the dimension of Y. The *size* σ of the formula $\Psi(Y)$ is the number of bits required to write down the whole formula. Note that we have $\sigma = O(m + n_1 + \dots + n_\ell + \mu)$.

Observe that if $\Phi(X)$ is a QFF-formula of (matrix) size μ and $P(X) \bowtie 0$ is an atom of Φ then P has degree at most μ and its coefficients are bounded in bitsize by μ. The following is an immediate corollary to Theorem 4:

▶ **Theorem 8.** *There exists a constant α with the following property:*
Let

$$(Q_1 X_1). \dots . (Q_\ell X_\ell). \Phi_0(Y, X_1, \dots, X_\ell)$$

be a first-order formula in the language $\mathcal{L}$ of matrix size μ and with dimensions m, $n_1, \dots, n_\ell$. Then there exists an equivalent quantifier-free formula $\Psi_0(Y)$ of size at most

$$\mu^{\alpha^{\ell+1}((m+1)\cdot(n_1+1)\cdot\dots\cdot(n_\ell+1))}.$$

Theorem 5 entails the following:

▶ **Corollary 9.** *There exists a constant β with the following property: Let $\Phi_0(X)$ be a quantifier-free formula in the language $\mathcal{L}$ of matrix size μ and dimension $n \geq 1$. Then the sentence $\exists X \in \mathbb{R}^n. \left(\Phi_0(X)\right)$ is equivalent to the sentence*

$$\exists X. \left(|X| \leq 2^{\mu^{\beta(n+1)}} \wedge \Phi_0(X)\right)$$

Proof. The proof is straightforward. It is deferred to Appendix A. ◀

We will frequently make use of the following standard trick:

▶ **Lemma 10.** *Given an integer N in unary and a sentence*

$$(Q_1 X_1).(Q_2 X_2). \dots . (Q_s X_s). \Phi_0(X_1, \dots, X_s),$$

we can in polynomial time in the size of the sentence and N compute a sentence

$$\exists B \in [-1, 1]^{N+1}. (Q_1 X_1; |X_1| \leq 1).(Q_2 X_2; |X_2| \leq 1). \dots . (Q_s X_s; |X_s| \leq 1). \Psi_0(B, X_1, \dots, X_s)$$

which is equivalent to the sentence

$$(Q_1 X_1; |X_1| \leq 2^{2^N}).(Q_2 X_2; |X_2| \leq 2^{2^N}). \dots . (Q_s X_s; |X_s| \leq 2^{2^N}). \Phi_0(X_1, \dots, X_s).$$

Here, the notation $(Q_j; |X_j| \leq c)$ indicates that the quantifier is restricted to the set

$$\left\{ X_j \in \mathbb{R}^{n_j} \;\middle|\; |X_{j,1}| \leq c, \dots, |X_{j,n_j}| \leq c \right\}.$$

Further, if Φ_0 is a $\mathrm{QFF}_{\leq}$-formula then so is Ψ_0.

Proof. See Appendix B ◀

3.1 Showing $\exists\forall_{\leq}\mathbb{R} \subseteq \mathtt{b}\text{-}\exists\forall_{\leq}\mathbb{R}$

We now show that the decision problem $\exists\forall_{\leq}\mathbb{R}$ reduces to $\mathtt{b}\text{-}\exists\forall_{\leq}\mathbb{R}$ in polynomial time.

We first bound the existential quantifier. This bound does not yet require the quantifier-free part of the sentence to involve only non-strict inequalities.

▶ **Lemma 11.** *Let $\exists X \in \mathbb{R}^n.\forall Y \in \mathbb{R}^m.\,(\Phi_0(X,Y))\,.$ be a sentence over the language $\mathcal{L}$ of matrix size μ. Then, denoting $I = [-1,1]$, we can compute in polynomial time an equivalent sentence of the form*

$$\exists X \in I^{n+N}.\forall Y \in \mathbb{R}^m.\,(\Psi_0(X,Y))\,.$$

Proof. Consider the formula

$$\chi_1(X) = \forall Y \in \mathbb{R}^m.\,(\Phi_0(X,Y))\,.$$

By Theorem 8 this formula is equivalent to a quantifier-free formula $\chi_0(X)$ of size at most $\mu^{\alpha^2(n+1)(m+1)}$. By Corollary 9 the sentence $\exists X \in \mathbb{R}^n.\,(\chi_0(X))$ is equivalent to the sentence

$$\exists X \in \mathbb{R}^n.\,\left(|X| \leq 2^{\mu^{\alpha^2\beta(n+1)^2(m+1)}} \wedge \chi_0(X)\right).$$

Hence, our original sentence is equivalent to the sentence

$$\exists X \in \mathbb{R}^n.\forall Y \in \mathbb{R}^m.\,\left(|X| \leq 2^{\mu^{\alpha^2\beta(n+1)^2(m+1)}} \wedge \Phi_0(X,Y)\right).$$

Now, we can compute in polynomial time a positive integer N in unary such that we have $\mu^{\alpha^2\beta(n+1)^2(m+1)} \leq 2^N$. By (the proof of) Lemma 10 we obtain an equivalent sentence as claimed. ◀

Next we derive a similar bound for the universal quantifier in terms of the bound for the existential one. This will require the assumption that all inequalities are non-strict. The reason for this is the following simple continuity property of $\mathrm{QFF}_{<}$-formulas, which can fail for general formulas in the language $\mathcal{L}$:

▶ **Proposition 12.** *Let $\Phi_0(X)$ be a $\mathrm{QFF}_{<}$-formula with a vector of n free variables X. Assume that $x \in \mathbb{R}^n$ is such that $\Phi_0(x)$ holds true. Then there exists $\varepsilon > 0$ such that $\Phi_0(\tilde{x})$ holds true for all $\tilde{x} \in \mathbb{R}^n$ with $|x - \tilde{x}| < \varepsilon$.*

Proof. By structural induction on the formula Φ. The base case follows from the fact that polynomials are continuous functions. The induction steps are easy. ◀

▶ **Lemma 13.** *Let $B \in \mathbb{N}$ be a positive integer constant. Let*

$$\Psi = \forall X \in \mathbb{R}^n.\exists Y \in \mathbb{R}^m.\,(|X| > B \vee \Phi_0(X,Y))$$

be a $\Pi_{2,<}$-sentence. Then the sentence Ψ holds true over the reals if and only if the sentence

$$\Psi' = \exists C \in \mathbb{R}.\forall X \in \mathbb{R}^n.\exists Y \in \mathbb{R}^m.\,(|X| > B \vee (Y \leq C \wedge \Phi(X,Y)))$$

holds true over the reals.

Proof. Clearly, Ψ' implies Ψ, so that if Ψ is false then Ψ' is false.

Suppose now that Ψ is true. Let $K = \{X \in \mathbb{R}^n \mid |X| \leq B\}$. Then, by assumption, for all $X \in K$ there exists $Y(X) \in \mathbb{R}^m$ such that $\Phi(X, Y(X))$ holds true. It follows from

Proposition 12 that there exists $\varepsilon(X) > 0$ such that $\Phi(X', Y(X))$ holds true for all X' with $|X - X'| < \varepsilon(X)$. The set $\{\mathsf{Ball}(X, \varepsilon(X)) \mid X \in K\}$, where $\mathsf{Ball}(X, c)$ denotes the ball of radius c centered at X, is an open cover of K. The set K is compact, so that this cover has a finite subcover $\mathsf{Ball}(X_1, \varepsilon(X_1)), \ldots, \mathsf{Ball}(X_s, \varepsilon(X_s))$. It follows that for all $X \in K$ there exists $j \in \{1, \ldots, s\}$ such that $\Phi(X, Y(X_j))$ holds true. Thus, the formula Ψ' holds true with $C = \max\{|Y(X_1)|, \ldots, |Y(X_s)|\}$. ◀

Note that the conclusion of Lemma 13 does not hold true in general for $\Pi_{2,\leq}$-formulas. For instance, the formula

$$\forall x \in [-1, 1].\exists y \in \mathbb{R}.\left(x^2\,(1 - xy) \leq 0\right)$$

is clearly true, but the formula

$$\exists C \in \mathbb{R}.\forall x \in [-1, 1].\exists y \in [-C, C].\left(x^2\,(1 - xy) \leq 0\right)$$

is clearly false.

▶ **Lemma 14.** *Given a sentence of the form*

$$\exists X \in I^n.\forall Y \in \mathbb{R}^m.\,(\Phi_{0,\leq}(X, Y))\,,$$

where $\Phi_{0,\leq}$ is a $\mathrm{QFF}_{\leq}$-formula, we can compute in polynomial time an equivalent $\mathtt{b}$-$\Sigma_{\leq}$-sentence

$$\exists X \in I^n.\forall Y \in I^{n+M}.\,(\Psi_{0,\leq}(X, Y))\,.$$

Proof. The proof combines Lemma 13 with proof ideas similar to those used in the proof of Lemma 11. It is given in Appendix C. ◀

Lemmas 11 and 14 together yield the inclusion $\exists\forall_{\leq}\mathbb{R} \subseteq \mathtt{b}\text{-}\exists\forall_{\leq}\mathbb{R}$.

3.2 Showing $\mathtt{b}\text{-}\exists\forall_{\leq}\mathbb{R} \subseteq \exists\forall_{\leq}\mathbb{R}$

We next establish the inclusion $\mathtt{b}\text{-}\exists\forall_{\leq}\mathbb{R} \subseteq \exists\forall_{\leq}\mathbb{R}$. The key lemma is the following:

▶ **Lemma 15.** *Let*

$$\exists \varepsilon > 0.(Q_1 X \in \mathbb{R}^n).(Q_2 Y \in \mathbb{R}^m).\,(\Phi_0(\varepsilon, X, Y))$$

be a sentence over the language $\mathcal{L}$ of matrix size μ. If this sentence holds true, then there exists $\varepsilon > 2^{-\mu^{4\alpha^3\beta(n+1)(m+1)}}$ witnessing the existential quantifier.

Proof. Consider the formula

$$\chi_2(\varepsilon) = (Q_1 X \in \mathbb{R}^n).(Q_2 Y \in \mathbb{R}^m).\,(\Phi_0(\varepsilon, X, Y))\,.$$

By Theorem 8 this formula is equivalent to a quantifier-free formula $\chi_0(\varepsilon)$ of size at most $\mu^{2\alpha^3(n+1)(m+1)}$. Let $\chi_0'(\varepsilon)$ be the sentence that results from χ_0 by replacing each atom in $P(\varepsilon) \bowtie 0$ in χ_0, where P has degree d, with the atom $\varepsilon^d P(1/\varepsilon) \bowtie 0$. Then, evidently, a number $\varepsilon > 0$ satisfies $\chi_0(\varepsilon)$ if and only if $1/\varepsilon$ satisfies $\chi_0'(\varepsilon)$ and vice versa.

By Corollary 9 the sentence $\exists x \in \mathbb{R}.\,(x > 0 \wedge \chi_0'(x))$ is equivalent to the sentence

$$\exists x \in \mathbb{R}.\left(x > 0 \wedge |x| \leq 2^{\mu^{4\alpha^3\beta(n+1)(m+1)}} \wedge \chi_0'(x)\right).$$

The result follows. ◀

▶ **Theorem 16.** *Given a* $\mathtt{b}$-$\Sigma_{2,\leq}$*-sentence*

$$\exists X \in I^n.\forall Y \in I^m.\,(\Phi_{0,\leq}(X,Y))$$

we can compute in polynomial time an equivalent $\Sigma_{2,\leq}$*-sentence.*

Proof. The proof combines Lemma 15 and Proposition 12 with similar ideas as in the proof of Lemma 11. We give the full proof in Appendix D. ◀

3.3 Showing $\mathtt{b}$-$\exists\forall^{+\,+}_{\leq}\mathbb{R} \subseteq \mathtt{b}$-$\exists\forall_{\leq}\mathbb{R}$

Finally we show the inclusion $\mathtt{b}$-$\exists\forall^{+\,+}_{\leq}\mathbb{R} \subseteq \mathtt{b}$-$\exists\forall_{\leq}\mathbb{R}$.

We will in fact show a stronger but more technical result. Recall that the Hausdorff distance of two non-empty compact subsets K and L of a metric space X is given by

$$d(K,L) = \max\{\sup_{x\in K} d(x,L), \sup_{x\in L} d(x,K)\},$$

where, as usual, $d(x,K) = \inf_{y\in K} d(x,y)$. This distance function makes the non-empty compact subsets of a metric space into a metric space $\mathcal{F}(X)$ of its own.

▶ **Theorem 17.** *Consider a sentence of the form*

$$\exists X \in I^n.\forall Y \in I^m.\,(\Psi_{0,\leq}(X,Y) \to \Phi_{0,\leq}(X,Y))\,,$$

where $\Psi_{0,\leq}(X,Y)$ *and* $\Phi_{0,\leq}(X,Y)$ *are* $\mathrm{QFF}_{\leq}$*-formulas. Assume that the set-valued function* $F(X) = \{Y \in I^m \mid \Psi_{0,\leq}(X,Y)\}$ *either maps some* $X \in I^n$ *to the empty set or is continuous as a map of type* $I^n \to \mathcal{F}(I^m)$*. Then we can compute in polynomial time an equivalent* $\mathtt{b}$-$\Sigma_{2,\leq}$*-sentence.*

Proof. See Appendix E. ◀

The inclusion $\mathtt{b}$-$\exists\forall^{+\,+}_{\leq}\mathbb{R} \subseteq \mathtt{b}$-$\exists\forall_{\leq}\mathbb{R}$ follows from the special case of Theorem 17 where the formula $\Psi_{0,\leq}(Y)$ does not depend on X.

Theorem 17, in its general form, finally allows us to prove that the complexity class $\exists\forall_{\leq}\mathbb{R}$ is robust under different encodings of polynomials.

▶ **Theorem 18.** *Given a* $\mathcal{C}$*-sentence, where* $\mathcal{C} \in \{\Sigma_{2,\leq}, \mathtt{b}\text{-}\Sigma_{2,\leq}, \mathtt{b}\text{-}\Sigma^p_{2,\leq}\}$ *we can compute in polynomial time an equivalent* $\mathcal{C}$*-sentence whose atoms involve polynomials of degree at most four. In particular we can compute in polynomial time a sentence whose atoms involve polynomials encoded as in* (4)*.*

Proof. See Appendix F. ◀

4 The complexity of deciding the Compact Escape Problem

We show that the CEP is complete for the complexity class $\exists\forall_{\leq}\mathbb{R}$. Formally this is achieved by locating the CEP between the complexity classes $\mathtt{b}$-$\exists\forall_{\leq}\mathbb{R}$ and $\mathtt{b}$-$\exists\forall^{+\,+}_{\leq}\mathbb{R}$ and applying Theorem 3.

Let us first show that the CEP is $\exists\forall_{\leq}\mathbb{R}$-hard. As a preparation we need to construct in polynomial time an arbitrary finite number of irrational rotations with independent angles:

▶ **Lemma 19.** *Given* $n \in \mathbb{N}$ *in unary we can compute in polynomial time a set of points* $q_1,\ldots,q_n \in \mathbb{T}^1 \subseteq \mathbb{C}$ *with rational real and imaginary part such that the only integer solution* $(e_1,\ldots,e_n) \in \mathbb{Z}^n$ *to the equation* $q_1^{e_1}\cdot\cdots\cdot q_n^{e_n} = 1$ *is the zero vector.*

Proof. See Appendix G. ◀

▶ **Theorem 20.** *The Compact Escape Problem is $\exists\forall_{\leq}\mathbb{R}$-hard.*

Proof. By Theorem 3 the decision problem for $\mathtt{b}\text{-}\Sigma$-sentences is $\exists\forall_{\leq}\mathbb{R}$-complete. It hence suffices to reduce this problem to the CEP.

Thus, given a $\mathtt{b}\text{-}\Sigma_{2,\leq}$-sentence

$$\Psi_{2,\leq} = \exists x \in I^n . \forall y \in I^m . (\Phi_{0,\leq}(x, y))$$

we compute in polynomial time a compact set K and a rational matrix $A \in \mathbb{Q}^{(n+2m)\times(n+2m)}$ such that there exists a point $x \in K$ with $A^k x \in K$ for all $n \in \mathbb{N}$ if and only if $\Psi_{2,\leq}$ holds true.

By Theorem 18 we may assume that all polynomials that occur in $\Psi_{2,\leq}$ have degree at most 4.

Consider the compact set

$$K = \left\{(x, u_1, v_1, \ldots, u_m, v_m) \in I^n \times I^{2m} \;\middle|\; u_j^2 + v_j^2 = 1, \Phi_{0,\leq}(x, u_1, \ldots, u_m)\right\}.$$

Use Lemma 19 to compute rational numbers $a_1, \ldots, a_m, b_1, \ldots, b_m \in \mathbb{Q}$ such that the numbers $a_j + ib_j$ do not admit any non-trivial integer multiplicative relations. Denote by I_n the $(n \times n)$-identity matrix. Let $R \in \mathbb{Q}^{2m\times 2m}$ be defined as follows:

$$R = \begin{pmatrix} a_1 & -b_1 & & & \\ b_1 & a_1 & & & \\ & & \ddots & & \\ & & & a_m & -b_m \\ & & & b_m & a_m \end{pmatrix}$$

Let $A \in \mathbb{Q}^{(n+2m)\times(n+2m)}$ be defined as follows:

$$A = \begin{pmatrix} I_n & \\ & R \end{pmatrix}.$$

Then for all $x \in K$ we have by Theorem 6

$$\overline{\mathcal{O}_A(x)} = \{x\} \times \left\{(u_1, v_1, \ldots, u_m, v_m) \in I^{2m} \;\middle|\; u_j^2 + v_j^2 = 1\right\}.$$

It follows that $\overline{\mathcal{O}_A(x)} \subseteq K$ if and only if $\Phi_{0,\leq}(x, u_1, \ldots, u_m)$ holds true for all $u_1, \ldots, u_m \in I^m$.

Thus, the instance (A, K) of the CEP is a negative instance if and only if the sentence $\Psi_{2,\leq}$ holds true. We can compute (A, K) in polynomial time from $\Psi_{2,\leq}$. This is almost immediately obvious, except that the polynomial inequalities that represent K must be encoded as lists of coefficients, while the polynomial inequalities in $\Psi_{2,\leq}$ are given as terms over the signature $\langle \mathbb{Z}, +, \times \rangle$. But since the polynomials that occur in $\Psi_{2,\leq}$ have degree at most 4 we can efficiently compute a list of coefficients from the term representations. ◀

Conversely, we have:

▶ **Theorem 21.** *The Compact Escape Problem is contained in $\exists\forall_{\leq}\mathbb{R}$.*

Proof Sketch. The full proof is given in Appendix H. We will only briefly sketch the proof idea here.

Suppose we are given a matrix $A \in \mathbb{Q}^{n\times n}$ with rational entries and a family of polynomials $\mathcal{P}$ together with a negation-free propositional formula which encodes a compact set $K \subseteq \mathbb{R}^n$. We can compute in polynomial time from this data a $\mathrm{QFF}_{\leq}$-formula Φ which encodes K. We will show that the existence of a point in K that is trapped under A is expressible as a $\mathtt{b}\text{-}\Sigma^{++}_{2,\leq}$-sentence. Together with Theorem 3 this yields the result. Let us assume for the sake of simplicity that A is diagonalisable over the complex numbers. The general case employs the Jordan normal form. It is not more difficult but requires more cumbersome notation.

We compute the complex eigenvalues $\lambda_1, \ldots, \lambda_m, \lambda_{m+1}, \ldots, \lambda_{m+b}, \lambda_{m+b+1}, \ldots, \lambda_{m+b+s}$ of A, counted with multiplicity. The eigenvalues are labelled such that $\lambda_1, \ldots, \lambda_m$ have modulus 1, such that $\lambda_{m+1}, \ldots, \lambda_{m+b}$ have modulus strictly greater than 1, and such that $\lambda_{m+b+1}, \ldots, \lambda_{m+b+s}$ have modulus strictly smaller than 1. Using [5] we can compute in polynomial time base change matrices Q and Q^{-1} such that $D = Q^{-1}AQ$ is a diagonal matrix.

Let $x \in K$ be a starting point. If the complex vector $Q^{-1}x$ has a non-zero component $(Q^{-1}x)_j$ with $m+1 \leq j \leq m+b$ then the orbit of x under A is unbounded, and hence forced to leave the bounded set K.

Now assume that $(Q^{-1}x)_j = 0$ for all $m+1 \leq j \leq m+b$. All components $(Q^{-1}x)_j$ with $j \geq m+b+1$ converge to zero under the iteration of A in the sense that the sequence $(Q^{-1}(A^k x))_j$ converges to zero as $k \to \infty$. It follows that the closure of the orbit of x under A is equal to the range of the semialgebraic function

$$f(x,z) = Q\,\mathrm{diag}\,(z_1, \ldots, z_m, 0, \ldots, 0)\,Q^{-1}x,$$

where $z_1, \ldots, z_m$ range over the closure of the sequence $(\lambda_1^k, \ldots, \lambda_m^k)_k$ in the torus $\mathbb{T}^m$. By Theorem 6 the closure of this sequence is an algebraic subset of $\mathbb{T}^m$, cut out by the integer multiplicative relations between the eigenvalues $\lambda_1, \ldots, \lambda_m$. By Theorem 7 a $\mathrm{QFF}_{\leq}$-formula $\Psi(Z)$ encoding this algebraic set, up to identifying $\mathbb{T}^m$ with a subset of the real hypercube $I^{2m} \subseteq \mathbb{R}^{2m}$.

It follows that we can express the existence of a trapped point by the following "informal" sentence:

$$\exists X \in I^n . \forall Z \in I^{2n}.$$
$$\big(\Psi(Z) \to \big(X \in K \wedge \big((Q^{-1}X)_{m+1} = 0 \wedge \cdots \wedge (Q^{-1}X)_{m+b} = 0\big) \wedge f(X,Z) \in K\big)\big)\,.$$

Thanks to the polytime computability of Q and Q^{-1} we can compute in polynomial time formulas that express the relations $(Q^{-1}X)_j = 0$ for $j = m+1, \ldots, m+b$, and $f(X,Z) \in K$. This allows us to compute in polynomial time a $\mathtt{b}\text{-}\Sigma^{++}_{\leq}$-sentence which is equivalent to the above "informal" sentence. ◀

References

1. R. Alur. *Principles of Cyber-Physical Systems.* MIT Press, 2015.
2. Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry.* Springer, 2006.
3. Saugata Basu and Marie-Françoise Roy. Bounding the radii of balls meeting every connected component of semi-algebraic sets. *Journal of Symbolic Computation*, 45(12):1270 – 1279, 2010.
4. Z. I. Borevich and I.R. Shafarevich. *Number Theory.* Academic Press inc., 1966.
5. J.-Y. Cai. Computing Jordan normal forms exactly for commuting matrices in polynomial time. *Int. J. Found. Comput. Sci.*, 5(3/4):293–302, 1994.
6. J.-Y. Cai, R.J. Lipton, and Y. Zalcstein. The complexity of the A B C problem. *SIAM J. Comput.*, 29(6), 2000.

7 Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993.
8 George E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In H. Brakhage, editor, *Automata Theory and Formal Languages*, pages 134–183, Berlin, Heidelberg, 1975. Springer Berlin Heidelberg.
9 D. Yu. Grigoriev and N. N. Vorobjov (Jr). Solving systems of polynomial inequalities in subexponential time. *J. Symbolic Computation*, 5:37 – 64, 1988.
10 D. W. Masser. *Linear relations on algebraic groups*, page 248–262. Cambridge University Press, 1988.
11 Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag Berlin Heidelberg, 1992.
12 E. Neumann, J. Ouaknine, and J. Worrell. On ranking function synthesis and termination for polynomial programs. In *CONCUR'20*, volume 171 of *LIPIcs*, pages 15:1–15:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.
13 Joël Ouaknine and James Worrell. *Positivity Problems for Low-Order Linear Recurrence Sequences*, page 366–379. Society for Industrial and Applied Mathematics, USA, 2014.
14 M. Schaefer and D. Stefankovic. Fixed Points, Nash Equilibria, and the Existential Theory of the Reals. *Theory Comput. Syst.*, 60(2):172–193, 2017.
15 S.M. Srivastava. *A course on Mathematical Logic*. Springer, 2008.
16 Dirk van Dalen. *Logic and Structure*. Springer Berlin Heidelberg, fourth edition, 2004.
17 N. N. Vorobjov (Jr). Bounds of real roots of a system of algebraic equations. *Zap. Nauchn. Sem. LOMI*, 137:7 – 19, 1984. (in Russian).

A Proof of Corollary 9

We can write Φ_0 in disjunctive normal form to obtain an equivalent formula

$$\bigvee_{i=1}^{N} \left(\bigwedge_{j=1}^{s_i} P_{i,j}(X) \bowtie_{i,j} 0 \right),$$

with $\bowtie_{i,j} \in \{\leq, <, =\}$. The atoms $P_{i,j} \bowtie_{i,j} 0$ correspond to atoms of Φ_0. In particular, each polynomial $P_{i,j}$ has degree at most μ and coefficients bounded in bitsize by μ.

Now, the sentence $\exists X.\,(\Phi_0(X))$ is equivalent to the sentence

$$\bigvee_{i=1}^{N} \exists X. \left(\bigwedge_{j=1}^{s_i} P_{i,j}(X) \bowtie_{i,j} 0 \right).$$

The latter sentence is, by Theorem 5 equivalent to

$$\bigvee_{i=1}^{N} \exists X. \left(|X| \leq 2^{\mu^{\beta'(n+1)+1}} \wedge \bigwedge_{j=1}^{s_i} P_{i,j}(X) \bowtie_{i,j} 0 \right).$$

This is then, by distributivity, equivalent to

$$\exists X. \left(|X| \leq 2^{\mu^{\beta'(n+1)+1}} \wedge \left(\bigvee_{i=1}^{N} \bigwedge_{j=1}^{s_i} P_{i,j}(X) \bowtie_{i,j} 0 \right) \right).$$

which by construction of the disjunctive normal form is equivalent to

$$\exists X. \left(|X| \leq 2^{\mu^{\beta'(n+1)+1}} \wedge \Phi_0(X) \right).$$

The result follows if we let $\beta = \beta' + 1$.

B Proof of Lemma 10

Introduce fresh variables $b_0, \ldots, b_N$. Let Ψ_0' be the formula that results from Φ_0 by replacing each atom

$$P(X_1, \ldots, X_s) \bowtie 0$$

in Φ_0, where $\bowtie \in \{\leq, <, =\}$, by the atom

$$b_N^{d_P} \cdot P(X_1/b_N, \ldots, X_s/b_N) \bowtie 0,$$

where d_P is the total degree of P. Let Ψ_0 be the formula

$$\Psi_0' \wedge 2b_0 = 1 \wedge b_1 = b_0^2 \cdots \wedge b_N = b_{N-1}^2.$$

C Proof of Lemma 14

We can compute in polynomial time a sentence

$$\forall X \in I^n . \exists Y \in \mathbb{R}^m . \left(\chi_{0,<}(X, Y)\right),$$

where $\chi_{0,<}$ is a $\mathrm{QFF}_<$-formula, which is equivalent to the negation of our original sentence. By Lemma 13 this sentence is equivalent to the sentence

$$\exists C \in \mathbb{R} . \forall X \in I^n . \exists Y \in \mathbb{R}^m . \left(|Y| \leq C \wedge \chi_{0,<}(X, Y)\right).$$

Consider the formula

$$\omega_2(C) = \forall X \in I^n . \exists Y \in \mathbb{R}^m . \left(|Y| \leq C \wedge \chi_{0,<}(X, Y)\right).$$

Let μ denote its matrix size. The number μ is clearly computable in polynomial time from our original sentence. By Theorem 8 the formula $\omega_2(C)$ is equivalent to a quantifier-free formula $\omega_0(C)$ of size at most $\mu^{2\alpha^3(n+1)(m+1)}$. By Corollary 9 the sentence

$$\exists C \in \mathbb{R} . \left(\omega_0(C)\right)$$

is equivalent to the sentence

$$\exists C \in \mathbb{R} . \left(|C| \leq 2^{\mu^{4\alpha^3\beta(n+1)(m+1)}} \wedge \omega_0(C)\right).$$

It follows that the negation of our original sentence is equivalent to the sentence

$$\exists C \in \mathbb{R} . \forall X \in I^n . \exists Y \in \mathbb{R}^m . \left(|C| \leq 2^{\mu^{4\alpha^3\beta(n+1)(m+1)}} \wedge |Y| \leq C \wedge \chi_{0,<}(X, Y)\right).$$

The latter is further equivalent to the sentence

$$\forall X \in I^n . \exists Y \in \mathbb{R}^m . \left(|Y| \leq 2^{\mu^{4\alpha^3\beta(n+1)(m+1)}} \wedge \chi_{0,<}(X, Y)\right).$$

Now, compute a positive integer N in unary such that $\mu^{4\alpha^3\beta(n+1)(m+1)} \leq 2^N$, and proceed as in the proof of Lemma 11 to obtain in polynomial time an equivalent sentence of the form

$$\forall X \in I^n . \exists Y \in I^{m+M} . \left(\chi_{0,<}(X, Y)\right).$$

The result follows by negating this sentence again.

D Proof of Theorem 16

The negation of the sentence is equivalent to a $\Pi_{2,<}$-sentence

$$\forall X \in I^n.\exists Y \in I^m.\left(\Psi_{0,<}(X,Y)\right). \tag{5}$$

We claim that this sentence is equivalent to the sentence

$$\exists \varepsilon > 0.\forall X \in I^n.\exists Y \in (-1+\varepsilon, 1-\varepsilon)^m.\left(\Psi_{0,<}(X,Y)\right).$$

Clearly, the latter sentence implies (5). Conversely, assume that (5) holds true. Then for all $X \in I^n$ there exists $Y(X) \in I^m$ such that $\Psi_{0,<}(X, Y(X))$ holds true. By Proposition 12 there exists for each $X \in I^n$ a number $\varepsilon(X) > 0$ such that the sentence $\Psi_{0,<}(\widetilde{X}, \widetilde{Y})$ holds true for all $\widetilde{X}$ and all $\widetilde{Y}$ satisfying $|\widetilde{X} - X| < \varepsilon(X)$ and $|\widetilde{Y} - Y(X)| < \varepsilon(X)$. Since I^n is compact, the cover $\{\mathsf{Ball}(X, \varepsilon(X)) \mid X \in I^n\}$ admits a finite subcover $\mathsf{Ball}(X_1, \varepsilon_1), \ldots, \mathsf{Ball}(X_s, \varepsilon_s)$. Let $X \in I^n$. Then $X \in \mathsf{Ball}(X_j, \varepsilon_j)$ for some $j \in \{1, \ldots, s\}$. It follows that $\Psi_{0,<}(X, Y)$ holds true for a $Y \in (-1+\varepsilon_j/2, 1-\varepsilon_j/2)^m$. Thus, the number $\min\{\varepsilon_1/2, \ldots, \varepsilon_s/2\}$ witnesses the existential quantifier in the latter sentence.

By Lemma 15 we can compute in polynomial time a positive integer $N \in \mathbb{N}$ in unary such that (5) is equivalent to the sentence

$$\forall X \in I^n.\exists Y \in \mathbb{R}^m.\left(|Y| < 1 - 2^{-2^N} \wedge \Psi_{0,<}(X,Y)\right).$$

This sentence is further equivalent to the sentence

$$\forall b_0 \in \mathbb{R}. \ldots \forall b_N \in \mathbb{R}.\forall X \in \mathbb{R}^n.\exists Y \in \mathbb{R}^m.$$
$$\left(\left(|X| \leq 1 \wedge 2b_0 - 1 = 0 \wedge b_1 - b_0^2 = 0 \wedge \cdots \wedge b_N - b_{N-1}^2 = 0\right) \to \left(|Y| < 1 - b_N \wedge \Psi_{0,<}(X,Y)\right)\right).$$

This last sentence is a $\Pi_{2,<}$-sentence, so that by negating again we obtain a $\Sigma_{2,\leq}$-sentence equivalent to our original one.

E Proof of Theorem 17

We begin with three simple preparatory observations.

▶ **Lemma 22.** *Given a sentence of the form*

$$\exists X \in I^n.\forall Y \in I^m.\left(H(X,Y) > 0\right),$$

where H is a multivariate polynomial with integer coefficients we can compute in polynomial time an equivalent $\mathtt{b}$-$\Sigma_{2,\leq}$-sentence.

Proof. The sentence is equivalent to the sentence

$$\exists \varepsilon > 0.\exists X \in I^n.\forall Y \in I^m.\left(H(X,Y) \geq \varepsilon\right).$$

By Lemma 15 this sentence is equivalent to the sentence

$$\exists \varepsilon \in I.\exists X \in I^n.\forall Y \in I^m.\left(\varepsilon \geq 2^{\mu^{4\alpha^3\beta(n+1)(m+1)}} \wedge H(X,Y) \geq \varepsilon\right),$$

where μ is the size of h. Compute in polynomial time an integer N such that $\mu^{4\alpha^3\beta(n+1)(m+1)} \leq 2^N$ and apply Lemma 10 to obtain the result. ◀

▶ **Lemma 23.** *Let $P \in \mathbb{Z}[X]$ be a polynomial in n variables, encoded by a term T over the signature $\langle \mathbb{Z}, +, \times \rangle$. Then we can compute in polynomial time an integer N (in binary) such that $|P(I^n)| \leq N$.*

Proof. We can view T as a tree whose nodes are elements of the set $\{+, \times\}$ and whose leaves are either variables or constants. Let $c_1, \ldots, c_s \in \mathbb{Z}$ denote the integer constants that occur in T. Let $M = \max\{2, |c_1|, \ldots, |c_s|\}$.

Let S be the tree which is obtained by substituting M for all leaves in T. Then S encodes a positive integer B. This integer B is clearly an upper bound for the absolute value of P over I^n. By an easy induction argument B is bounded by M^{N_T}, where N_T is the number of nodes of T. The number M^{N_T} can be computed using at most N_T arithmetic operations. Its bitsize is bounded by $N_T\tau$, where τ is a bound on the bitsizes of the numbers $c_1, \ldots, c_s$. ◀

▶ **Proposition 24.** *Let $\Phi(X)$ be a quantifier-free formula over the language $\mathcal{L}$ whose atoms consist of equalities only. Then we can compute in polynomial time a polynomial $Q \in \mathbb{Z}[X]$ such that $\Phi(X)$ is equivalent to the formula $Q(X) = 0$.*

Proof. Construct a new formula $\Phi'(X)$ that results from $\Phi(X)$ by replacing each atom $P(X) = 0$ in $\Phi(X)$ by the atom $P(X)^2 = 0$.

Now construct a polynomial $Q_{\Phi'}$ by structural induction on Φ' as follows:

1. If $\Phi'(X) \equiv (P(X) = 0)$ then let $Q_{\Phi'} = P$.
2. If $\Phi'(X) \equiv \Psi(X) \vee \omega(X)$ then let $Q_{\Phi'} = Q_\Psi \cdot Q_\omega$.
3. If $\Phi'(X) \equiv \Psi(X) \wedge \omega(X)$ then let $Q_{\Phi'} = Q_\Psi + Q_\omega$.

It is easy to see that $Q_{\Phi'}$ can be computed in polynomial time from Φ. It has the desired property by construction. ◀

We are now in a position to prove Theorem 17.

Proof of Theorem 17. The proof is a reduction to Lemma 22.

As a preparation we assign to every $\mathrm{QFF}_{\leq}$-formula Φ a continuous function f_Φ such that $\Phi(X)$ holds true if and only if $f_\Phi(X) \leq 0$:

1. If $\Phi(X) = (P(X) \leq 0)$ then let $f_\Phi(X) = P(X)$.
2. If $\Phi(X) = \Psi(X) \vee \chi(X)$ then let $f_\Phi(X) = \min\{f_\Psi(X), f_\chi(X)\}$.
3. If $\Phi(X) = \Psi(X) \wedge \chi(X)$ then let $f_\Phi(X) = \max\{f_\Psi(X), f_\chi(X)\}$.

Now assume we are given a sentence

$$\exists X \in I^n . \forall Y \in I^m . (\Psi(X, Y) \to \Phi(X, Y)) \tag{6}$$

as above. The negation of this sentence is equivalent to the sentence

$$\forall X \in I^n . \exists Y \in I^m . (\Psi(X, Y) \wedge f_\Phi(X, Y) > 0) . \tag{7}$$

Let us for now assume that the set $K(X) = \{Y \in I^m \mid \Psi(X, Y)\}$ is non-empty for all $X \in I^n$. Then by assumption this set depends continuously on X in the Hausdorff metric. It follows by elementary calculus that the function $h(X) = \max_{Y \in K(X)} f_\Phi(X, Y)$ is well-defined and continuous.

We further have, by compactness of I^n, that the function $h(X)$ attains its minimum in I^n. By definition of f_Φ, the sentence (7) holds true if and only if $\min_{x \in I^n} h(x) > 0$ if and only if there exists $\varepsilon > 0$ such that $\min_{x \in I^n} h(x) > \varepsilon$. Thus, the sentence (7) is equivalent to the sentence

$$\exists \varepsilon > 0 . \forall X \in I^n . \exists Y \in I^m . (\Psi(X, Y) \wedge f_\Phi(X, Y) > \varepsilon) .$$

So far we have proved this equivalence under the assumption that the compact set $K(X) = \{Y \in I^m \mid \Psi(X,Y)\}$ is non-empty for all X. But if the set $K(X)$ is empty for some X then both (7) and the above sentence are false, so that the two sentences are certainly equivalent.

Let $\chi(X,Y)$ be the formula that results from Φ by swapping all occurrences of $\vee$ and $\wedge$ and by replacing all atoms $P(X,Y) \leq 0$ in Φ by the atom $P(X,Y) > \varepsilon$. One easily checks that the above sentence is further equivalent to the sentence

$$\exists \varepsilon > 0. \forall X \in I^n. \exists Y \in I^m. \left(\Psi(X,Y) \wedge \chi(X,Y)\right).$$

It follows from 11 that there exists a witness ε for the existential quantifier with $\varepsilon > 2^{-\mu^{4\alpha^3\beta(n+1)(m+1)}}$. We can compute in polynomial time an integer N such that we have $\mu^{4\alpha^3\beta(n+1)(m+1)} \leq 2^N$. Consider the formula $\chi(X,Y)$. By Lemma 23 we can compute in polynomial time an integer L such that $|P(X,Y)| \leq L$ for all $(X,Y) \in I^n \times I^m$. We can hence replace each atom $P(X,Y) > 0$ in $\chi(X,Y)$ with the equivalent formula

$$\exists u \in [-L,L]. \exists v \in [-2^{2^N}, 2^{2^N}]. \left(P(X,Y) = u^2 \wedge uv = 1\right),$$

where u and v are fresh variables. By Proposition 24 the formula $\chi(X,Y)$ is equivalent to a formula of the form

$$\exists U \in [-L,L]^s. \exists V \in [-2^{2^N}, 2^{2^N}]^s. \left(Q(X,Y,U,V) = 0\right)$$

where Q is computable in polynomial time from $\chi(X,Y)$ and s is the number of atoms in $\chi(X,Y)$.

Now, consider the formula $\Psi(X,Y)$. By Lemma 23 we can compute in polynomial time an integer M such that for all atoms $P(X,Y) \leq 0$ in $\Psi(Y)$ the polynomial P satisfies $|P(X,Y)| \leq M$ for all $(X,Y) \in I^n \times I^m$. The atom is hence equivalent to $\exists w \in [-M,M]. P(X,Y) = -w^2$, where w is a fresh variable. Again by Proposition 24, letting t denote the number of atoms in $\Psi(X,Y)$ we can hence compute in polynomial time a formula $\exists W \in [-M,M]^t. R(X,Y,W) = 0$, which is equivalent to $\Psi(X,Y)$.

In total the sentence (7) is equivalent to the sentence

$$\forall X \in I^n. \exists Y \in I^m. \exists U \in [-L,L]^s. \exists V \in [-2^{2^N}, 2^{2^N}]^s. \exists W \in [-M,M]^t. \\ \left(R(X,Y,W) + Q(X,Y,U,V) = 0\right).$$

In the above we have used that the functions R and Q admit only non-negative values by construction. We may assume that $2^{2^N} \geq \max\{L,M\}$. Arguing as in Lemma 10 we can introduce auxiliary variables $B \in I^{N+1}$ to obtain an equivalent sentence

$$\forall X \in I^n. \exists Y \in I^m. \exists U \in I^s. \exists V \in I^s. \exists W \in I^t. \exists B \in I^{N+1}. \left(H(X,Y,U,V,W,B) = 0\right)$$

which is computable in polynomial time from our original sentence (6).

The sentence (6) is hence equivalent to the sentence

$$\exists X \in I^n. \forall Y \in I^m. \forall U \in I^s. \forall V \in I^s. \forall W \in I^t. \forall B \in I^{N+1}. \left(H(X,Y,U,V,W,B) > 0\right).$$

Again, we have used that H only admits non-negative values by construction. The result now follows from Lemma 22. ◀

F Proof of Theorem 18

We prove the result for $\mathtt{b}\text{-}\Sigma_{2,\leq}$-sentences. The result for $\Sigma_{2,\leq}$ sentences follows by applying the reductions from Lemmas 11 and 13, bounding the degrees of the atoms of the resulting $\mathtt{b}\text{-}\Sigma_{2,\leq}$-sentence, and translating back to a $\Sigma_{2,\leq}$-sentence using Theorem 16. By inspecting the proof of Theorem 16 we observe that the degree does not increase by this translation, since we only add new constraints, all of which involve polynomials of degree at most 2. The result for $\mathtt{b}\text{-}\Sigma^{++}_{2,\leq}$-sentences is implicitly contained in the below proof.

To a term T over the signature $\langle \mathbb{Z}, +, \times \rangle$ we assign a variable z_T and a formula η_T, where η_T is inductively defined as follows:

1. If T is a variable x_j then $\eta_T = \langle z_T = x_j \rangle$.
2. If T is a constant c then $\eta_T = \langle z_T = c \rangle$.
3. If T is of the form $U \times V$, then $\eta_T = \langle \eta_U \wedge \eta_V \wedge z_T = z_U \times z_V \rangle$
4. If T is of the form $U + V$, then $\eta_T = \langle \eta_U \wedge \eta_V \wedge z_T = z_U + z_V \rangle$.

The formula η_T is computable in polynomial time from T. Its atoms have degree at most two.

Let $P(X,Y) \leq 0$ be an atom in $\Phi_{\leq}(X,Y)$, where P is encoded by a term T. Let η_T be the formula associated with T as above. Then the formula $P(X,Y) \leq 0$ is equivalent to the formula $\forall Z.(\eta_T(X,Y,Z) \to z_T \leq 0)$.

More generally, the sentence $\exists X \in I^n . \forall Y \in I^m . \Phi_{\leq}(X,Y)$ is equivalent to the sentence

$$\exists X \in I^n . \forall Y \in I^m . \forall Z \in \mathbb{R}^M . \left(\eta_{T_1}(X,Y,Z) \wedge \cdots \wedge \eta_{T_s}(X,Y,Z) \to \widehat{\Phi}_{\leq}(Z) \right),$$

where $T_1, \ldots, T_s$ are the term representations of the atoms in $\Phi_{\leq}(X,Y)$ and $\widehat{\Phi}_{\leq}(Z)$ is obtained from $\Phi_{\leq}(X,Y)$ by substituting each atom $P(X,Y) \leq 0$ with term representation T_j by the atom $z_{T_j} \leq 0$.

We can further compute in polynomial time an integer N in binary such that the above sentence is equivalent to

$$\exists X \in I^n . \forall Y \in I^m . \forall Z \in [-N,N]^M . \left(\eta_{T_1}(X,Y,Z) \wedge \cdots \wedge \eta_{T_s}(X,Y,Z) \to \widehat{\Phi}_{\leq}(Z) \right),$$

By the proof of Lemma 10 we can have Z range over $[-1,1]^M$ up to introducing further auxiliary variables and adding a conjunction of quadratic polynomial equations to the formula $\widehat{\Phi}$. For notational convenience, let us simply assume that the sentence is equivalent to

$$\exists X \in I^n . \forall Y \in I^m . \forall Z \in I^M . \left(\eta_{T_1}(X,Y,Z) \wedge \cdots \wedge \eta_{T_s}(X,Y,Z) \to \widehat{\Phi}_{\leq}(Z) \right).$$

This sentence involves polynomials of degree at most 2.

Let us write $\eta(X,Y,Z) = \bigwedge_{j=1}^{s} \eta_{T_j}(X,Y,Z)$. It remains to show that the set

$$\left\{ (Y,Z) \in I^m \times I^M \;\mid\; \eta(X,Y,Z) \right\}$$

depends continuously on X in the Hausdorff metric. It then follows from Theorem 17 that we can compute in polynomial time an equivalent $\Sigma_{2,\leq}$-sentence. By an inspection of the proof of Theorem 17, the degree of the atoms is at most doubled in this new sentence.

We use the following proposition, which is easily established using elementary calculus:

▶ **Proposition 25.** *Let X and Y be metric spaces.*

1. *Let $F\colon X \to \mathcal{F}(Y)$ and $G\colon X \to \mathcal{F}(Z)$ be continuous with respect to the Hausdorff metric. Then the map*

$$H\colon X \to \mathcal{F}(Y) \times \mathcal{F}(Z),\ H(x) = F(x) \times G(x)$$

is continuous with respect to the Hausdorff metric as well.
2. *Let $F\colon X \to \mathcal{F}(Y)$ be continuous with respect to the Hausdorff metric. Let $f\colon Y \to Z$ be a continuous function. Then the function*

$$H\colon X \to \mathcal{F}(Y \times Z),\ H(x) = F(x) \times f(F(x))$$

is continuous with respect to the Hausdorff metric.

Now, The formula η is a conjunction of atoms of the form $z_j = x_k$, $z_j = y_k$, $z_j = c$, $z_j = z_k + z_\ell$, or $z_j = z_k \times z_\ell$.

We prove the result by structural induction. For a formula $\eta(X, Y, Z)$ with $n + m + s$ free variables (X, Y, Z) write $F_\eta\colon I^n \to \mathcal{F}(I^{m+s})$ for the map that sends $X \in I^n$ to the set $\{(Y, Z) \in I^m \times I^s \mid \eta(X, Y, Z)\}$.

If $\eta(X, Y, z)$ is of the form $z = x_k$, $z = y_k$, or $z = c$ then the function F_η is easily seen to be continuous.

If $\eta(X, Y, z_1, \ldots, z_s) = \nu(X, Y, z_1, \ldots, z_{s-1}) \wedge \mu(X, Y, z_s)$ where $\mu(X, Y, z_s)$ is of the form $z_s = x_k$, $z_s = y_k$, or $z_s = c$ then

$$F_\eta(X) = F_\nu(X) \times \{z_s \in \mathbb{R} \mid \mu(X, Y, z_s)\}\,.$$

Continuity of F_η follows from the first part of Proposition 25.

If $\eta(X, Y, z_1, \ldots, z_s) = \nu(X, Y, z_1, \ldots, z_{s-1}) \wedge \mu(X, Y, z_j, z_k, z_s)$ where $\mu(X, Y, z_j, z_k, z_s)$ is of the form $z_s = z_j \square z_s$ with $\square \in \{+, \times\}$, then

$$F_\eta(X) = F_\nu(X) \times f(F_\nu(X)),$$

where $f(Y, z_1, \ldots, z_{s-1}) = z_j \square z_k$. Continuity of F_η follows from the second part of Proposition 25.

G Proof of Lemma 19

Recall the following facts about the ring $\mathbb{Z}[i]$ of Gaussian integers, see e.g. [11, Kapitel 1, §1] for details:

1. $\mathbb{Z}[i]$ is a unique factorisation domain.
2. The units of $\mathbb{Z}[i]$ are $1, -1, i, -i$.
3. Every prime number $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$ is a prime number in $\mathbb{Z}[i]$.
4. Every prime number $p \in \mathbb{Z}$ with $p \equiv 1 \pmod 4$ admits a factorisation $p = (a + ib)(a - ib)$ into non-associate prime elements $a + ib, a - ib \in \mathbb{Z}[i]$.

Let $p_1, \ldots, p_n$ denote the n first prime numbers with $p_j \equiv 1 \pmod 4$. By the prime number theorem and a quantitative version of Dirichlet's theorem on primes in arithmetic progressions (see *e.g.* [4, Chapter 5, Section 3] or [11, Kapitel VII, §13]) there are $\sim \frac{N}{2 \log N}$ numbers of this type below a given $N \in \mathbb{N}$. It follows that the numbers $p_1, \ldots, p_n$ can be computed in polynomial time from n.

Further, we can compute in polynomial time representations $p_j = a_j^2 + b_j^2$ with $a_j > 0$ for $j = 1, \ldots, n$. Let $q_j = \frac{a_j^2 - b_j^2}{a_j^2 + b_j^2} + i \frac{2 a_j b_j}{a_j^2 + b_j^2}$. We have $q_j = \frac{a_j + i b_j}{a_j - i b_j}$ where $a_j + i b_j$ and $a_j - i b_j$ are prime elements in $\mathbb{Z}[i]$.

We claim that there are no integer multiplicative relations between the q_j's. Suppose for the sake of contradiction that we have

$$q_1^{e_1} \cdot \cdots \cdot q_n^{e_n} = 1$$

with $e_1, \ldots, e_n \in \mathbb{Z}$ not all zero. Then we obtain the equation

$$(a_1 + ib_1)^{e_1} \cdot \ldots (a_n + ib_n)^{e_n} = (a_1 - ib_1)^{e_1} \cdot \ldots (a_n - ib_n)^{e_n}.$$

Assume without loss of generality that $e_1 \neq 0$. Then $(a_1 - ib_1)$ needs to divide one of the prime factors $(a_j + ib_j)$. Since $(a_j + ib_j)$ is itself prime this implies that $(a_1 - ib_1)$ and $(a_j + ib_j)$ are associates. The units of $\mathbb{Z}[i]$ are the numbers $1, -1, i, -i$. It follows immediately that the numbers $(a_1 - ib_1)$ and $(a_j + ib_j)$ cannot be associates in $\mathbb{Z}[i]$. We conclude that there cannot exist any integer multiplicative relations between the q_j's.

H Proof of Theorem 21

We start with a technical lemma:

▶ **Lemma 26.** *Let $A \in \mathbb{R}^{n\times n}$ be a real matrix. Denote by*

$$\lambda_1, \ldots, \lambda_m, \lambda_{m+1}, \ldots, \lambda_{m+b}, \lambda_{m+b+1}, \ldots, \lambda_{m+b+s}$$

the complex eigenvalues of A, counted with geometric multiplicity. Let $\lambda_1, \ldots, \lambda_m$ have modulus 1. Let $\lambda_{m+1}, \ldots, \lambda_{m+b}$ have modulus strictly greater than 1. Let $\lambda_{m+b+1}, \ldots, \lambda_{m+b+s}$ have modulus strictly smaller than 1. Fix a Jordan basis $v_{j,k}$ of $\mathbb{C}^n$ where $v_{j,1}$ is an eigenvector of λ_j and $(A - \lambda_j I)\, v_{j,k} = v_{j,k-1}$ for all $k > 1$.

Let B denote the span of the vectors $v_{j,k}$ with $m+1 \leq j \leq m+b$ and the vectors $v_{j,k}$ with $1 \leq j \leq m$ and $k > 1$.

Let C denote the span of the vectors $v_{j,k}$ with $m+b+1 \leq j \leq m+b$.

Let Q be the matrix that sends the standard basis of $\mathbb{C}^n$ to the basis

$$v_{1,1}, \ldots, v_{m,1},$$
$$v_{1,2}, \ldots, v_{1,t_1}, \ldots, v_{m,2}, \ldots, v_{m,t_m},$$
$$v_{m+1,1}, \ldots, v_{v_{m+1},t_{m+1}}, \ldots, v_{m+b+s,1}, \ldots, v_{m+b+s,t_{m+b+s}}.$$

Let

$$f\colon \mathbb{R}^n \times \mathbb{T}^m \to \mathbb{C}^n,\ f(x,z) = Q \begin{pmatrix} z_1 & & & & & \\ & \ddots & & & & \\ & & z_m & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} Q^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Let $S \subseteq \mathbb{T}^m$ be the closure of the set $\{(\lambda_1^k, \ldots, \lambda_m^k) \mid k \in \mathbb{N}\}$ in $\mathbb{T}^m$.

Let $K \subseteq \mathbb{R}^n$ be a compact set. Let $x \in K$. Then for all $k \in \mathbb{N}$ we have $A^k x \in K$ if and only if both of the following two conditions are satisfied:

1. *Let $N = m + (t_1 - 1) + \cdots + (t_m - 1) + t_{m+1} + \cdots + t_{m+b}$. For all $m < j \leq N$ we have $(Q^{-1}x)_j = 0$.*

2. $f(x, S) \subseteq K$.

Proof. Let $x \in K$.

Assume that $A^k x \in K$ for all $k \in \mathbb{N}$. Let $J = Q^{-1}AQ$. Let us again write $N = m + (t_1 - 1) + \cdots + (t_m - 1) + t_{m+1} + \cdots + t_{m+b}$. If there exists $m < j \leq N$ such that $(Q^{-1}x)_j \neq 0$ then $Q^{-1}x$ has a non-zero component in a generalised eigenspace of A which corresponds to an eigenvalue of modulus strictly greater than 1 or it has a non-zero component in a generalised eigenspace of A corresponding to an eigenvalue of modulus 1 which is not an eigenspace. In both cases the absolute value of $A^k x = QJ^k(Q^{-1}x)$ is unbounded as $k \to \infty$. Since K is assumed to be bounded it follows that $A^k x$ leaves K after finitely many steps.

Now, assume that $(Q^{-1}x)_j = 0$ for all $m < j \leq N$. We claim that $f(x, S)$ is the set of accumulation points of the orbit of x under A. The result then follows immediately.

First, observe that we have by construction

$$A = Q \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_m & & & & \\ & & & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & \\ & & & & & & R \end{pmatrix} Q^{-1}$$

where R is an $(s \times s)$-matrix with $|R^k| \to 0$ as $k \to 0$.

Now, let $z \in S$. We claim that $f(x, z)$ is an accumulation point of the sequence $(A^k x)_{k \in \mathbb{N}}$. Let $\varepsilon > 0$. By Theorem 6 there exist infinitely many $k \in \mathbb{N}$ such that $|\lambda_j^k - z_j| < \varepsilon/2$. For all sufficiently large n we have $|R^k| < \varepsilon/2$. It follows that for each such k we have $|(A^k x) - f(z, x)| < \varepsilon$. Thus, $f(z, x)$ is an accumulation point of the sequence $(A^k x)_k$.

Conversely, let $y \in K$ be an accumulation point of the sequence $(A^k x)_k$. Let $(n_k)_k$ be a sequence of natural numbers such that the sequence $(A^{k_j} x)_j$ converges to y. Since the torus $\mathbb{T}^m$ is compact, the sequence $(\lambda_1^{k_j}, \ldots, \lambda_m^{k_j})_j$ has a convergent subsequence. Thus, let $(k_{j_\ell})_\ell$ denote a subsequence of $(k_j)_j$ such that the sequence $(\lambda_1^{k_{j_\ell}}, \ldots, \lambda_m^{k_{j_\ell}})_\ell$ converges to a limit $z = (z_1, \ldots, z_m) \in \mathbb{T}^m$. Then the sequence $(A^{k_{j_\ell}} x)_\ell$ converges to both $f(x, z)$ and y. It follows that $y = f(x, z)$. ◀

Now, let us prove Theorem 21.

By Theorem 3 the decision problems for $\mathtt{b}\text{-}\Sigma^{++}_{2,\leq}$-sentences is contained in $\exists\forall_{\leq}\mathbb{R}$. We reduce the Compact Escape Problem to this problem.

Suppose we are given a matrix $A \in \mathbb{Q}^{n \times n}$ with rational entries, a family of polynomials $\mathcal{P}$ in n free variables, represented in the standard encoding, and a negation-free propositional formula $\Phi(X)$ over atoms of the form $P \leq 0$, where $P \in \mathcal{P}$. We can convert the standard encodings of the polynomials $P \in \mathcal{P}$ into terms over the signature $\langle \mathbb{Z}, +, \times \rangle$ in polynomial time. We can hence convert the formula $\Phi(X)$ into a $\mathrm{QFF}_{\leq}$-formula in polynomial time. By very slight abuse of notation, let us denote this $\mathrm{QFF}_{\leq}$-formula by $\Phi(X)$ as well. Let $K \subseteq \mathbb{R}^n$ denote the set encoded by $\Phi(X)$.

By [5] we can compute in polynomial time the complex eigenvalues of A

$$\lambda_1, \ldots, \lambda_m, \lambda_{m+1}, \ldots, \lambda_{m+b}, \lambda_{m+b+1}, \ldots, \lambda_{m+b+s}$$

and the matrices Q and Q^{-1} as in Lemma 26. We can further compute the real an imaginary parts of the eigenvalues $\lambda_1, \ldots, \lambda_{m+b+s}$ in polynomial time. More precisely, letting

$\alpha_j = \mathrm{Re}(\lambda_j)$ denote the real part of λ_j, and $\beta_j = \mathrm{Im}(\lambda_j)$ the imaginary part, we can compute in polynomial time:

1. Univariate polynomials with integer coefficients $h_1, \ldots, h_{m+b+s}$, $g_1, \ldots, g_{m+b+s}$, such that $h_j(\alpha_j) = g_j(\beta_j) = 0$ for all $j = 1, \ldots, m+b+s$.
2. Rational numbers $a_1, b_1, c_1, d_1, \ldots, a_{m+b+s}, b_{m+b+s}, c_{m+b+s}, d_{m+b+s}$, such that α_j is the unique root of h_j in the real interval $[a_j, b_j]$ and β_j is the unique root of g_j in the real interval $[c_j, d_j]$.
3. For $j = 1, \ldots, n$ and $k = 1, \ldots, n$ bivariate polynomials $L_{0,j,k} \in \mathbb{Q}[u, v]$, $L_{1,j,k} \in \mathbb{Q}[u, v]$, and indexes $\ell_{j,k} \in \{1, \ldots, m+b+s\}$ such that the matrix Q at row j and column k is given by the complex algebraic number

   $$L_{0,j,k}(\alpha_{\ell_{j,k}}, \beta_{\ell_{j,k}}) + iL_{1,j,k}(\alpha_{\ell_{j,k}}, \beta_{\ell_{j,k}})$$

4. For $j = 1, \ldots, n$ and $k = 1, \ldots, n$ bivariate polynomials $R_{0,j,k} \in \mathbb{Q}[u, v]$, $R_{1,j,k} \in \mathbb{Q}[u, v]$, and indexes $r_{j,k} \in \{1, \ldots, m+b+s\}$ such that the matrix R^{-1} at row j and column k is given by the complex algebraic number

   $$R_{0,j,k}(\alpha_{r_{j,k}}, \beta_{r_{j,k}}) + iR_{1,j,k}(\alpha_{r_{j,k}}, \beta_{r_{j,k}}).$$

By Theorem 7 we can compute in polynomial time a finite set $\gamma_1, \ldots, \gamma_s \in \mathbb{Z}^m$ of generators of the free abelian group of integer multiplicative relations between the complex eigenvalues $\lambda_1, \ldots, \lambda_m$. The size of the integer entries of $\gamma_1, \ldots, \gamma_s$ – and not just their bitsize – is bounded polynomially in the size of the input. It follows that we can compute in polynomial time a $\mathrm{QFF}_{\leq}$-formula $\Psi(C, D)$ with $2m$ free variables that expresses for two given real vectors $C \in \mathbb{R}^n$, $D \in \mathbb{R}^n$ that the complex vector $C + iD$ is contained in the set

$$S = \{(z_1, \ldots, z_m) \in \mathbb{T}^m \mid (z_1, \ldots, z_m)^{\gamma_j} = 1,\ j = 1, \ldots, s\}.$$

By Theorem 6 the set S is equal to the closure of the set $\left\{(\lambda_1^k, \ldots, \lambda_m^k) \mid k \in \mathbb{N}\right\}$.

Let $f \colon \mathbb{R}^n \times \mathbb{T}^m \to \mathbb{C}^n$ be defined as in Lemma 26, *i.e.*,

$$f(x, z) = Q\,\mathrm{diag}(z_1, \ldots, z_m, 0, \ldots, 0)Q^{-1}x.$$

Since we can compute the matrices Q and Q^{-1} in polynomial time as above, we can compute in polynomial time polynomials $F_{k,j} \in \mathbb{Q}[U, V][C, D]$ for $k = 1, \ldots, n$, $j = 1, \ldots, n$, where U and V are vectors of $m+b+s$ variables, such that

$$\mathrm{Re}\, f(X, C + iD) = \left(\sum_{j=1}^{n} F_{1,j}\left(\vec{\alpha}, \vec{\beta}\right)(C, D) \cdot X_j, \ldots, \sum_{j=1}^{n} F_{n,j}\left(\vec{\alpha}, \vec{\beta}\right)(C, D) \cdot X_j\right). \quad (8)$$

Note that the result is a polynomial with real algebraic coefficients. More precisely, the right hand side of the above equation is an element of the ring

$$\mathbb{Q}[\alpha_1, \ldots, \alpha_{m+b+s}, \beta_1, \ldots, \beta_{m+b+s}][X, C, D].$$

Define $N = m + (t_1 - 1) + \cdots + (t_m - 1) + t_{m+1} + \cdots + t_{m+b}$ as in Lemma 26. By Lemma 26 the existence of a point in K that is trapped under A is equivalent to the "informal" sentence

$$\exists X \in I^n . \forall Y \in \mathbb{T}. \quad (9)$$
$$\left(Y \in S \to \left(X \in K \wedge \left((Q^{-1}X)_{m+1} = 0 \wedge \cdots \wedge (Q^{-1}X)_N = 0\right) \wedge f(X, Y) \in K\right)\right).$$

We construct in polynomial time from A and Φ a $\mathtt{b}\text{-}\Sigma^{++}_{\leq}$-sentence

$$\exists U \in I^{m+b+s}.\exists V \in I^{m+b+s}.\exists X \in I^n.\forall C \in I^m.\forall D \in I^m. \tag{10}$$
$$(\Psi(C,D) \to (\chi(U,V) \wedge \Phi(X) \wedge \omega(U,V,X) \wedge \xi(U,V,X,C,D))) .$$

Recall that the formula $\Psi(C,D)$ expresses that the complex number $C+iD$ is contained in the set S. Intuitively speaking, the formula $\chi(U,V)$ will express that the variables U and V represent the real and imaginary parts of the eigenvalues $\lambda_1,\ldots,\lambda_{m+b+s}$. The formula $\omega(U,V,X)$ will express that $(Q^{-1}X)_k = 0$ for $k = m+1,\ldots,m+b+s$. The formula $\xi(U,V,X,C,D)$ will express that $f(X,C+iD) \in K$.

More formally, let

$$\chi(U,V) = \bigwedge_{j=1}^{m+b+s} (h_j(U) = 0 \wedge a_j \leq U \leq b_j \wedge g_j(V) = 0 \wedge c_j \leq V \leq d_j) .$$

Let

$$\omega(U,V,X) = \bigwedge_{k=m+1}^{N} \bigwedge_{s=0}^{1} \left(\sum_{j=1}^{n} R_{s,k,j}(U_{r_{j,k}}, V_{r_{j,k}}) \cdot X_j = 0 \right),$$

Let $\xi(U,V,X,C,D)$ be the formula which is obtained from Φ by replacing each atom $P(X_1,\ldots,X_n) \leq 0$ in Φ by the atom

$$P\left(\sum_{j=1}^{n} F_{1,j}(U,V)(C,D) \cdot X_j, \ldots, \sum_{j=1}^{n} F_{n,j}(U,V)(C,D) \cdot X_j \right) \leq 0,$$

Note that this substitution can be performed in polynomial time. The polynomial P is given by a term t over the signature $\langle \mathbb{Z}, +, \times \rangle$. A term representing the new atom is obtained by substituting in the term t the occurrence of each variable X_k by the polynomial-size term $\sum_{j=1}^{n} F_{k,j}(U,V)(C,D) \cdot X_j$.

Now, observing that the formula $\chi(U,V)$ forces U and V to be equal respectively to the vector of real and imaginary parts of the eigenvalues $\lambda_1,\ldots,\lambda_{m+b+s}$ it follows by construction that the $\mathtt{b}\text{-}\Sigma^{++}_{\leq}$-sentence (10) is equivalent to the informal sentence (9) and hence expresses the existence of a trapped point. There is only one small argument required: By (8) the formula $\xi(\vec{\alpha},\vec{\beta},X,C,D)$ expresses that $\operatorname{Re} f(X,C+iD) \in K$ rather than $f(X,C+iD) \in K$. But if $\Psi(C,D)$ holds true then $C+iD \in S$, so that $f(X,C+iD)$ is real-valued, for instance since it is contained in the closure of the orbit of $A^k x$ by the proof of Lemma 26.

Deciding the truth of the sentence (10) is therefore equivalent to deciding non-termination of the Escape Problem instance (A,K).