Computing the linear hull: Deciding Deterministic? and Unambiguous? for weighted automata over fields

Jason P. Bell
Department of Pure Mathematics
University of Waterloo
Waterloo, Canada
jpbell@uwaterloo.ca

Daniel Smertnig
Institute for Mathematics and Scientific Computing
NAWI Graz, University of Graz
Graz, Austria
daniel.smertnig@uni-graz.at

***Abstract*—The (*left*) *linear hull* of a weighted automaton over a field is a topological invariant. If the automaton is minimal, the linear hull can be used to determine whether or not the automaton is equivalent to a deterministic one. Furthermore, the linear hull can also be used to determine whether the minimal automaton is equivalent to an unambiguous one. We show how to compute the linear hull, and thus prove that it is decidable whether or not a given automaton over a number field is equivalent to a deterministic one. In this case we are also able to compute an equivalent deterministic automaton. We also show the analogous decidability and computability result for the unambiguous case. Our results resolve a problem posed in a 2006 survey by Lombardy and Sakarovitch.**

***Index Terms*—weighted automata, determinization, sequential, deterministic, unambiguous, linear hull**

I. Introduction

Every unweighted (finite) automaton is equivalent to a *deterministic* automaton[1], and there is a determinization procedure to find such an automaton. For automata with weights in a semiring K (in short, K-automata), this is no longer true. More generally, a K-automaton is *unambiguous* if (i) between each two states p and q and for every word w there is at most one path from p to q labeled by w, and (ii) every word has at most one accepting path [40, Definition I.1.11]. For trim automata (i) and (ii) are equivalent and one may be omitted. Deterministic K-automata are unambiguous, but not every unambiguous K-automaton is equivalent to a deterministic one; furthermore not every K-automaton is equivalent to an unambiguous one. Here, two K-automata are equivalent if they recognize the same K-rational series.

This leads to the following decidability problems for a K-automaton $\mathcal{A}$.

- *Deterministic?* Is there a deterministic K-automaton $\mathcal{A}'$ that is equivalent to $\mathcal{A}$?
- *Unambiguous?* Is there an unambiguous K-automaton $\mathcal{A}'$ that is equivalent to $\mathcal{A}$?

If these questions have a positive answer, it is furthermore desirable to actually produce a corresponding K-automaton. These questions have received particular attention when K is a tropical semiring [11], [30], [1], [25], [24], [23], [17], [32]; the surveys [29], [31] are a good starting point. Similar question have been studied for weighted tree automata [10], [14], [19], [37]. When K is a field, even when $K = \mathbb{Q}$, the question was still essentially completely open until recently. It appears as an open problem in the 2006 survey by Lombardy and Sakarovitch [29, Problem 1]. For unary alphabets and $K = \mathbb{Q}$, the problem *Deterministic?* is decidable by a recent result of Kostolányi [26]. In the same setting *Unambiguous?* is decidable by a result of Berstel and Mignotte [6, Théorème 3] together with a classical theorem of Pólya [7, Chapter 6.3].

In [3] a new invariant for an automaton with weights in a field, the *linear hull*, was introduced, and it was used to prove a multivariate version of Pólya's theorem [3, Theorem 1.2]. This led to a characterization of K-rational series recognized by deterministic, respectively unambiguous, automata in terms of the linear hull of a minimal automaton for the series. Unfortunately, the linear hull is defined as a topological closure (in the *linear Zariski topology*) of the reachability set of an automaton, making its computability a non-trivial problem.

We show that the problems *Deterministic?* and *Unambiguous?* are decidable over number fields[2] (Theorem 1). Furthermore, our work yields an algorithm to compute an equivalent unambiguous, respectively, deterministic weighted automaton if it exists. This uses the main theorems of [3] and a computability result for the linear hull (Theorem 3).

The key point is the computation of the linear Zariski closure of a matrix semigroup (a subsemigroup of the semigroup of all $d \times d$-matrices $M_d(K)$) generated by a closed set. Our approach is inspired by the computation of the Zariski closure of such semigroups by Hrushovski, Ouaknine, Pouly, and Worrell [22], which builds on the case for groups by Derksen, Jeandel, and Koiran [13]; see also [33]. However, our approach stays almost entirely within the linear realm (see Remark 40).

Our approach does not yield any bounds on the runtime. The output size (the size of the linear hull) can be super-exponential in the input size. Namely, if $K = \mathbb{Q}$ and $\mathcal{A}$ has d states, then the linear hull can be of size $2^{d-1}d!$ over a two-letter alphabet

J. P. Bell was supported by NSERC grant RGPIN-2022-02951.

[1] deterministic automata also called *sequential* or *subsequential* [40, Remark V.1.2] automata in the weighted case

[2] The restriction to number fields is not essential, and only made for simplicity of the presentation.

979-8-3503-3587-3/23/$31.00 ©2023 IEEE

(Remarks 7 and 41); by comparison, in the unary case, the algorithm of Kostolányi needs at most $O(d^3)$ operations.

In the group case (section IV), the Burnside–Schur theorem yields an upper bound on the size of a transversal modulo the component containing the identity, giving a bound on the output size that is double-exponential in d (independent of the number of generators; Remark 41). In the semigroup case (section V), this can be combined with a recursion lemma (Lemma 37), to get a similar double-exponential upper bound (now dependent on the number of generators). Further, our results hold for all fields over which it is possible to do linear algebra exactly, and they can be extended to integers as well. For reasons of space and simplicity we relegate details of this and the bounds on the output size to the arXiv version [4].

Notation. Throughout, let K be a number field (a finite-dimensional field extension of $\mathbb{Q}$), and let $d \geq 0$. Let $M_d(K)$ be the semigroup of $d \times d$-matrices. Further, $I \in M_d(K)$ denotes the identity matrix, and $E_{ij} \in M_d(K)$ denotes the ij-th elementary matrix. If X is a subset of a semigroup $\mathcal{S}$, then $\langle X \rangle$ is the subsemigroup generated by X. If $a, b \in \mathbb{Z}$, then $[a, b] \coloneqq \{ x \in \mathbb{Z} : a \leq x \leq b \}$ is the discrete interval. Background on automata can be found in [7], [15], [40].

Acknowledgements. We thank the reviewers for innumerable valuable comments on improving the presentation of the paper for the LICS community. We have tried to implement them as far as possible; any remaining shortcomings are our own.

II. Main results: Decidability of Deterministic? and Unambiguous?

In this section we state the main results of the present paper (Theorems 1 and 3) and show how Theorem 1 follows from Theorem 3 and the results in [3]. The proof of Theorem 3 will then take up the rest of the paper.

We work with row vectors and apply matrices on the right. A d-dimensional *linear representation* over the alphabet Σ consists of a row vector $u \in K^{1 \times d}$, a monoid homomorphism $\mu\colon \Sigma^* \to M_d(K)$, and a column vector $v \in K^d$.

To interpret (u, μ, v) as a K-automaton $\mathcal{A}$, we associate to it a directed graph with edge labels and set of vertices $[1, d]$ as follows: $u = (u_1, \dots, u_d)$ is the vector of initial weights, with an incoming edge to state i with weight u_i. Analogously v is interpreted as vector of terminal weights. For each $a \in \Sigma$, the matrix $\mu(a)$ is an incidence matrix encoding the transition weights of the letter a: the ij-entry of $\mu(a)$ corresponds to the weight of the transition from state i to the state j labeled by a, and it is recorded by putting an edge with label $\mu(a)a$ (omitting the edge if $\mu(a) = 0$). In this way, there is a one-to-one correspondence between linear representations and weighted automata (see [7, Chapter 1.6] for a more complete treatment).

An *accepting path* for a word w is a path in the graph that is labeled by w and leads from an input state (a state with nonzero input weight) to a terminal state (a state with nonzero terminal weight). We always assume that our automata are *trim* (every state lies on some accepting path).

Given any word $w \in \Sigma^*$ one can compute the output $\mathcal{A}(w) \coloneqq u\mu(w)v$ of the K-automaton by

1) for each accepting path labeled by w, taking the product of the weights along each path;
2) summing up these values over all accepting paths for w.

The task of finding all accepting paths for w becomes computationally easier if the automaton is

1) *deterministic*, that is, there exists at most input state and for every state i and every letter $a \in \Sigma$, there is at most one outgoing edge from i that is labeled by a (i.e., every row of $\mu(a)$ has at most one nonzero entry); or
2) *unambiguous*, that is, for every word w there exists at most one accepting path.

Every deterministic automaton is unambiguous.

To an automaton we associate its *behavior*, the K-rational series $\sum_{w \in \Sigma^*} \mathcal{A}(w)w$. Two automata are equivalent if they have the same behavior. Our main theorem is the following.

Theorem 1. *Let $\mathcal{A}$ be a K-automaton. Then it is decidable if $\mathcal{A}$ is equivalent to*

1) a deterministic K-automaton;
2) an unambiguous K-automaton.

In both cases the corresponding deterministic (or unambiguous) K-automaton is computable.

To prove Theorem 1, we will make use of the following linear version of the Zariski topology introduced in [3, Section 3]. The same topology previously appeared in work of Colcombet and Petrisan [12] under the name of "glued spaces" — their minimal cover [12, p.6] of a set of vectors is the closure of that set in the linear Zariski topology.

Definition 2. *On a finite-dimensional vector space V over K, the* linear Zariski topology *is the topology in which a set is closed if and only if it is a finite union of vector subspaces.*

The empty set is represented by the empty union. By definition, a (not necessarily closed) nonempty subset $X \subseteq V$ is *irreducible*, if whenever $X \subseteq Y_1 \cup Y_2$ with closed sets Y_1 and Y_2, then already $X \subseteq Y_1$ or $X \subseteq Y_2$. Since a vector space cannot be covered by finitely many proper subspaces (due to K being infinite), one sees easily that the irreducible closed sets are precisely the vector subspaces of V, and every closed set can be expressed uniquely as the finite union of its irreducible components (i.e., the maximal irreducible subsets).[3]

Most of the paper is devoted to the following.

Theorem 3. *Let $X \subseteq M_d(K)$ be a closed subset (given by a list of basis vectors) and let $\mathcal{S} = \langle X \rangle$ be the semigroup generated by X. Then the linear Zariski closure $\overline{\mathcal{S}}$ is computable (as a list of basis vectors).*

Theorem 3 immediately yields the following corollary, by taking X to be the union of the n one-dimensional spaces generated by $A_1, \dots, A_n$.

Corollary 4. *Let $A_1, \dots, A_n \in M_d(K)$. Then the linear Zariski closure of the semigroup $\langle A_1, \dots, A_n \rangle$ is computable.*

[3] In fact, V is a noetherian topological space, background on which can be found in [9, §II.4.1 and §II.4.2] or [41, Sections 004U and 0050].

We are now able to define the following crucial invariant of a weighted automaton over a field.

Definition 5. *Let $\mathcal{A}$ be a K-automaton on the alphabet Σ with linear representation (u, μ, v). The* (left) linear hull *of $\mathcal{A}$ is the set*

$$\overline{u\mu(\Sigma^*)} = \overline{\{\, u\mu(w) : w \in \Sigma^* \,\}},$$

that is, it is the closure in the linear Zariski topology of the reachability set $\{\, u\mu(w) : w \in \Sigma^* \,\}$.

The linear hulls of two equivalent K-automata need not coincide. However, since K is a field, there always exist minimal linear representations, and these are unique up to conjugation by an invertible matrix (corresponding to a change of basis of the vector space). Correspondingly, the linear hulls of minimal linear representations only differ by a linear isomorphism on the ambient space. In particular, the number of irreducible components and their dimensions are independent of the choice of minimal linear representation. To a K-rational series we associate the linear hull of a minimal linear representation of the series.

The linear hull is *not* left/right symmetric. In fact the number of its irreducible components, on the left/right need not coincide, and neither need the dimensions [3, Example 3.8].

Corollary 6. *Let $\mathcal{A}$ be a K-automaton. Then the linear hull of $\mathcal{A}$ is computable.*

Proof. By Corollary 4 we can compute the linear Zariski closure of the finitely generated matrix semigroup $\mu(\Sigma^*)$. Since $\varphi\colon M_d(K) \to K^{1\times d}$, $A \mapsto uA$ is K-linear, it is continuous in the linear Zariski topology and also closed (i.e., it maps closed sets to closed sets). Therefore $\overline{u\mu(\Sigma^*)} = u\overline{\mu(\Sigma^*)}$. □

Constructing the following automaton $\hat{\mathcal{A}}$ is key in the decidability problem.

Construction of $\hat{\mathcal{A}}$. Given a K-automaton $\mathcal{A}$, with minimal linear representation (u, μ, v), and linear hull $X = W_1 \cup \cdots \cup W_k$ (where $W_1, \ldots, W_k$ are irreducible components, with $m_i := \dim W_i$), we can construct an equivalent K-automaton $\hat{\mathcal{A}}$, with linear representation (u', μ', v'), as follows (see [3, Lemma 3.13] for a rigorous treatment): Renumbering the components, without restriction $u \in W_1$. For each $a \in \Sigma$ and $i \in [1, k]$ there exists some $j \in [1, k]$ such that $W_i\mu(a) \subseteq W_j$. Here, j need not be unique, but for each a we can choose a transition function $f_a\colon [1, k] \to [1, k]$ such that $W_i\mu(a) \subseteq W_{f_a(i)}$ for all $a \in \Sigma$ and $i \in [1, k]$.

Set $m = m_1 + \cdots + m_k \geq d$, so that $K^{1\times m} \cong W_1 \oplus \cdots \oplus W_k$ (typically $m > d$). The linear representation (u', μ', v') will be constructed on this space. Viewing $\mu(a)$ as linear endomorphisms on $K^{1\times d}$, we can restrict $\mu(a)$ to W_i to obtain linear maps $\mu(a)|_{W_i}\colon W_i \to W_{f_a(i)}$. Putting these linear endomorphisms all together, we get the endomorphism $\mu'(a)$ on $K^{1\times m}$. For u' one puts u into the W_1-component and zeroes everywhere else; v' is constructed analogously to the $\mu(a)$ by viewing v as linear functional $K^{1\times d} \to K$. By [3, Lemma 3.13] this gives a K-automaton $\hat{\mathcal{A}}$ equivalent to $\mathcal{A}$.

By construction, the matrices $\mu'(a)$ have a $m_1 \times \cdots \times m_k$ block structure, with the property that every row of blocks contains at most one nonzero block. We say that (u', μ', v') is *semi-monomial* if, in addition, in every block of every $\mu'(a)$, each column has at most one nonzero entry and the analogous property holds for v' (thinking of v' as k blocks of size $m_i \times 1$). Clearly, whether (u', μ', v') is semi-monomial is decidable.

Proof of Theorem 1. First, we compute a minimal linear representation (u, μ, v) of $\mathcal{A}$ [7, p.41–42], say of dimension d. Let $\Gamma := \{\, u\mu(w)v : w \in \Sigma^* \,\}$ denote the set of all outputs of the automaton. Using [3, Lemma 3.11] we can pick the minimal linear representation in such a way that $u\mu(\Sigma^*) \subseteq \Gamma^{1\times d}$.

Now compute the linear hull $X = \overline{u\mu(\Sigma^*)}$ (Corollary 6). Let $W_1, \ldots, W_k$ denote the irreducible components of X, with $\dim(W_i) = m_i$ and $m := m_1 + \cdots + m_k$. We now construct the linear representation (u', μ', v'), of dimension $m \geq d$ and with associated automaton $\hat{\mathcal{A}}$, that recognizes the same series. Once we have $\hat{\mathcal{A}}$, we are able to resolve the decidability problem:

- $\mathcal{A}$ is equivalent to a deterministic automaton if and only if X has dimension ≤ 1 (that is, $m_i = 1$ for all i) [3, Theorem 1.3]. In this case $\hat{\mathcal{A}}$ is deterministic [3, Proof of Proposition 3.14].
- The proof of [3, Proposition 5.3] implies that $\mathcal{A}$ is equivalent to an unambiguous automaton if and only if the specific automaton $\hat{\mathcal{A}}$ is semi-monomial, and this can easily be checked. □

Taking $K = \mathbb{Q}$, this solves Problem 1 in [29]. It remains to establish Theorem 3. One way to do so, is to first compute the Zariski closure using [22], from which the linear Zariski closure can then be obtained (see [28, Theorem 1]).

However, it seems unnecessarily complex to first compute the closure in the finer topology, both in principle as well as in terms of computational complexity. We present an alternate approach that stays almost entirely within the realm of linear algebra. In particular, it avoids the need of using Gröbner bases and of computing in extension fields. We proceed in three steps, that successively build on each other: first we consider the problem for a single invertible matrix (section III), then for a closed set X in which the invertible matrices are dense (essentially, the group case; section IV), and finally the case for general closed sets X (the semigroup case; section V).

The linear algebraic approach can be expected to allow a more practical implementation (avoiding inefficient Gröbner bases). Unfortunately, at one point we need to leave to linear realm in an essential way (line 22 of Algorithm 2; see Remark 40). This appears to be the main obstacle to a more efficient implementation.

If one wishes to avoid computations in extension fields, while still using Gröbner bases, it would also be possible to use our computation for the single matrix case (section III) as "subroutine" in [13], [22]. The output then lies between the Zariski closure and the linear Zariski closure, and [28, Theorem 1] can be used to find the latter.

Remark 7. The linear hull can have super-exponentially many components in the dimension d, already in the case where the matrices form a group. The group of signed permutation matrices is a finite subgroup of $\mathrm{GL}_d(\mathbb{Q})$ of order $2^d d!$. By a result of Feit ([16]; see also the introduction of [5] or [27, §6]), for large d, this order is maximal among all finite subgroups of $\mathrm{GL}_d(\mathbb{Q})$. Its linear Zariski closure consists of a union of $2^{d-1}d!$ vector spaces of dimension 1 (a signed permutation and its negative always lie in the same vector space). Even worse, the group of signed permutation matrices is 2-generated for all d, so that a better bound in terms of the number of generators of the group and the dimension is also also hopeless. Since the signed permutation matrices act faithfully on $(1, 2, \ldots, d)$, this group also gives a linear hull of size $2^{d-1}d!$ for a two-letter alphabet and d states.

III. A SINGLE INVERTIBLE MATRIX

In this section, given $A \in \mathrm{GL}_d(K)$ we compute $\overline{\langle A \rangle}$. Basic linear algebra, in particular generalized eigenspaces and the Jordan normal form, are sufficient to do so. While computing the Jordan normal form usually involves computations in a finite extension of K (for all the eigenvalues to be present), we get an algorithm that works over the initial field K.

We first need to understand the structure of the closure of a semigroup in the linear Zariski topology. First note the following behavior of the closure with respect to products.

Lemma 8. *Let $X \subseteq M_d(K)$ be a closed set, and let D, $D' \subseteq X$ be arbitrary subsets. If $DD' \subseteq X$, then also $\overline{D}\,\overline{D'} \subseteq X$.*

Proof. Let $d' \in D'$. Then $Dd' \subseteq X$. Since multiplication by d' from the right is linear, hence continuous and closed, also $\overline{D}d' = \overline{Dd'} \subseteq X$. Now we know $\overline{D}D' \subseteq X$, and still have to show $\overline{D}\,\overline{D'} \subseteq X$. Let $d \in \overline{D}$. From $dD' \subseteq X$ we find $d\overline{D'} = \overline{dD'} \subseteq X$. Thus $\overline{D}\,\overline{D'} \subseteq X$. □

Lemma 9. *Let $\mathcal{S} \subseteq M_d(K)$ be a subsemigroup.*

1) *The closure $\overline{\mathcal{S}}$ is a semigroup.*
2) *If $\overline{\mathcal{S}} \cap \mathrm{GL}_d(K) \neq \emptyset$, then $\overline{\mathcal{S}} \cap \mathrm{GL}_d(K)$ is a linear algebraic group.*
3) *If $\mathcal{S} \subseteq M_d(K)$ is a closed monoid (a closed semigroup containing the identity matrix), there exists a unique irreducible component $\mathcal{S}^0$ containing the identity matrix. Then $\mathcal{S}^0$ is a submonoid of $\mathcal{S}$.*

Proof. 1) We have $\mathcal{S}\mathcal{S} \subseteq \mathcal{S} \subseteq \overline{\mathcal{S}}$. Lemma 8 implies $\overline{\mathcal{S}}\,\overline{\mathcal{S}} \subseteq \overline{\mathcal{S}}$.

2) Clearly $\overline{\mathcal{S}} \cap \mathrm{GL}_d(K)$ is a Zariski-closed subsemigroup of $\mathrm{GL}_d(K)$. Therefore it is a group [13, Lemma 10].

3) By [38, Remark 5.2] (the proof is the same as the one for linear algebraic groups). □

Our main theorem in this section is the following.

Theorem 10. *There exists a computable $N = N(d, K)$, such that for every $A \in \mathrm{GL}_d(K)$ we have $\overline{\langle A \rangle}^0 = \operatorname{span}\{\, A^{Ni} : i \geq 0 \,\}$. In particular, $\overline{\langle A \rangle}$ is computable.*

By $\mu(\overline{\mathbb{Q}})$ we denote the group of all roots of unity, where $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$, which is also the algebraic closure of K.

Lemma 11. *Let $A \in \mathrm{GL}_d(K)$. Assume that for any two eigenvalues λ, $\lambda' \in \overline{\mathbb{Q}}$ of A for which $\lambda/\lambda' \in \mu(\overline{\mathbb{Q}})$, it holds that $\lambda = \lambda'$. Let $n \geq 1$. Then a vector space $V \subseteq K^d$ is A-invariant if and only if it is A^n-invariant.*

In the following proof we make use of the identity $a^n - b^n = \prod_{j=0}^{n-1}(a - \zeta^j b)$, if a, b commute and ζ is an n-th root of unity.

Proof of Lemma 11. If V is A-invariant, then it is A^n-invariant. It suffices to show the converse. Without restriction we work over $\overline{\mathbb{Q}}$. For every $\lambda \in \overline{\mathbb{Q}}$, the space V is A-invariant if and only if it is $(A - \lambda I)$-invariant. If λ_1, …, λ_r are the pairwise distinct eigenvalues of A, then every generalized eigenspace $\ker(A - \lambda_i I)^d$ is A-invariant. If V is A-invariant, we can consider the generalized eigenspaces of the restriction $A|_V$ to obtain a decomposition

$$V = \bigoplus_{i=1}^{r} (\ker(A - \lambda_i I)^d \cap V).$$

Let λ be an eigenvalue of A, and let ζ be a primitive n-th root of unity (which exists because $\overline{\mathbb{Q}}$ is algebraically closed). Then

$$\begin{aligned}(A^n - \lambda^n I)^i &= (A - \lambda I)^i \prod_{j=1}^{n-1} (A - \zeta^j \lambda I)^i \\ &= \prod_{j=1}^{n-1} (A - \zeta^j \lambda I)^i \cdot (A - \lambda I)^i.\end{aligned}$$

for $i \geq 0$. By our assumption on the ratios of eigenvalues, none of the $\zeta^j \lambda$ with $j \in [1, n-1]$ are eigenvalue of A. Thus, the matrices $(A - \zeta^j \lambda I)^i$ are invertible for $j \in [1, n-1]$. Consequently $\ker(A^n - \lambda^n I)^i = \ker(A - \lambda I)^i$.

Let λ_1, …, λ_r denote the pairwise distinct eigenvalues of A. Since V is A^n-invariant,

$$V = \bigoplus_{i=1}^{r} (\ker(A^n - \lambda_i^n I)^d \cap V) = \bigoplus_{i=1}^{r} (\ker(A - \lambda_i I)^d \cap V).$$

It therefore suffices to show the claim when A has a single eigenvalue λ.

Since V is A^n-invariant, it is also $(A^n - \lambda^n I)$-invariant. We show that it is $(A - \lambda I)$ invariant, then it is also A-invariant. It suffices to show that for every $0 \neq v \in V$ and all $i \geq 0$ we have $(A - \lambda I)^i v \in V$.

Let $0 \neq v \in V$. For all $i \geq 0$, let $v_i := (A - \lambda I)^i v$ and $v_i' := (A^n - \lambda^n I)^i v$. Let $k \geq 0$ be minimal such that $v \in \ker((A - \lambda I)^{k+1}) = \ker((A^n - \lambda^n I)^{k+1})$. Then v_k is an eigenvector of A with respect to the eigenvalue λ. Thus

$$\begin{aligned}0 \neq v_k' &= \Big(\sum_{j=0}^{n-1} A^j \lambda^{n-1-j} \Big)^k (A - \lambda I)^k v \\ &= \Big(\sum_{j=0}^{n-1} A^j \lambda^{n-1-j} \Big)^k v_k = (n\lambda^{n-1})^k v_k.\end{aligned}$$

Hence $v_k' \in V$ implies $v_k \in V$.

Suppose now that $v_k, \dots, v_{i+1} \in V$; we show $v_i \in V$. Again

$$v_i' = \Big(\sum_{j=0}^{n-1} A^j \lambda^{n-1-j}\Big)^i (A - \lambda I)^i v = \Big(\sum_{j=0}^{n-1} A^j \lambda^{n-1-j}\Big)^i v_i.$$

Now $Av_i = \lambda v_{i+1}$, and so $A^j v_i \in \operatorname{span}\{v_k, \dots, v_{i+1}\} \subseteq V$ for all $j \in [1, n-1]$. Since also $v_i' \in V$, we get $v_i \in V$. □

Lemma 12. *There exists a computable $N_0 = N_0(d, K)$ such that, for every finite field extension L/K with $[L : K] \le d$ and every root of unity $\zeta \in L$, one has $\zeta^{N_0} = 1$.*

Proof. Let $\zeta \in L$ be a root of unity of some order $n \ge 1$. Then

$$[L : \mathbb{Q}] \ge [\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n),$$

with $\phi(n)$ denoting the Euler-ϕ-function. Since

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] \le d[K : \mathbb{Q}],$$

we must have $\phi(n) \le d[K : \mathbb{Q}]$. Since $\phi(n) \to \infty$ as $n \to \infty$, but the right hand side of the inequality is constant, only finitely many values are possible for n. By taking N_0 to be the least common multiple of these values, the claim follows. □

The constant $N_0 = N_0(d, K)$ in the previous lemma is explicit and does not depend on the matrix A.

Lemma 13. *Let $N := N(d, K) := N_0(d^2, K)$. Let $A \in \mathrm{GL}_d(K)$, and let $V \subseteq K^d$ be a vector subspace. If V is A^n-invariant for some $n \ge 1$, then V is A^N-invariant.*

Proof. Let λ, $\lambda' \in \overline{\mathbb{Q}}$ be eigenvalues of A and let $N = N_0(d^2, K)$. Since λ, λ' are both roots of the characteristic polynomial, which has degree d, the extension $K(\lambda, \lambda')/K$ has degree at most d^2. If there exists a root of unity ζ such that $\lambda/\lambda' = \zeta$, then $\zeta \in K(\lambda, \lambda')$ and hence $\zeta^N = 1$. Thus A^N satisfies the assumption of Lemma 11.

Suppose now that V is A^n-invariant ($n \ge 1$). Then V is A^{nN}-invariant. Lemma 11 gives that V is A^N-invariant. □

Let $A \in \mathrm{GL}_d(K)$. We recall (Lemma 9), that $\overline{\langle A \rangle} \cap GL_d(K)$ is a linear algebraic group, and $\overline{\langle A \rangle}$ has a unique irreducible component containing I. This component is denoted by $\overline{\langle A \rangle}^0$.

Proof of Theorem 10. Let $Z_0 := \overline{\langle A \rangle}^0$. Since A acts by permutation on the finitely many irreducible components of $\overline{\langle A \rangle}$, there exists an $N > 0$ such that $A^N Z_0 = Z_0$. Lemma 13 implies that we can take $N = N(d, K)$, which is computable without knowing Z_0.

Now $A^N \in Z_0$ and hence $\langle A^N \rangle \in Z_0$, because Z_0 is a submonoid of $\overline{\langle A \rangle}$ (by 3) of Lemma 9). Since Z_0 is a vector space, even $\operatorname{span}\langle A^N \rangle \subseteq Z_0$. Thus $\langle A \rangle \subseteq \bigcup_{i=0}^{N-1} A^i \operatorname{span}\langle A^N \rangle \subseteq \bigcup_{i=0}^{N-1} A^i Z_0 \subseteq \overline{\langle A \rangle}$. Taking closures, we get equality throughout, so $\overline{\langle A \rangle}^0 = \operatorname{span}\langle A^N \rangle$.

Finally, by the Cayley-Hamilton theorem there exist (computable) $\lambda_0, \dots, \lambda_{d-1} \in K$ such that $(A^N)^d + \lambda_{d-1}(A^N)^{d-1} + \dots + \lambda_0 I = 0$. Multiplying by A^{Nm} for $m \ge 0$, we see inductively that $\operatorname{span}\langle A^N \rangle = \operatorname{span}\{I, A^N, A^{2N}, \dots, A^{(d-1)N}\}$. Thus $\overline{\langle A \rangle}^0$ and $\overline{\langle A \rangle}$ are computable. □

Example 14. Let

$$A = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}.$$

Since $\phi(n) > 6^2 = 36$ for $n > 126$, we can take $N = N(6, \mathbb{Q}) = 126$. But since the only root of unity appearing for the specific A is -1, we can actually take $N = 2$. Setting $B = A^2$ we find $Z_0 = \operatorname{span}\{\, I, B, B^2, B^3, B^4, B^5 \,\}$ to be $Z_0 = \operatorname{span}\{E_{11} + E_{22} + E_{66}, E_{12}, E_{33} + E_{44} + E_{55}, E_{34} + E_{45}, E_{35}\}$. Finally $\overline{\langle A \rangle} = Z_0 \cup -E_{66} Z_0$. Up to base change the same is true for any matrix with Jordan normal form A.

Remark 15. Instead of using the bound $N(d, K)$ one may compute the eigenvalues of A explicitly in a suitable number field. It is then possible to compute the pairwise ratio of the eigenvalues and check which ones are a root of unity. This has the disadvantage of having to perform computations in a field extension of K and that the resulting N depends on A. However, the resulting N could be much smaller than $N(d, K)$.

IV. Invertible Matrices

In this section we consider the computation of $\overline{\langle X \rangle}$ when $X \subseteq M_d(K)$ is a closed set, and each irreducible component of X contains invertible matrices. In this case, $\overline{\langle X \rangle} \cap \mathrm{GL}_d(K)$ is a linear algebraic group (Lemma 9). The algorithm is that of [13], with the Zariski topology replaced by the linear Zariski topology. However, care must be taken in checking the correctness of the algorithm, as the use of the linear Zariski topology introduces some subtle difficulties. We first state the algorithm, Algorithm 1, and illustrate it on a short example.

Example 16. Consider

$$A_1 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -3 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and $X = \mathbb{Q}A_1 \cup \mathbb{Q}A_2$. After initialization, $N = \{I\}$ and $T = \{I, A_1, A_2\}$. Now

$$\overline{\langle A_1 \rangle}^0 = \operatorname{span}\{E_{11}, E_{22} + E_{33}\},$$
$$\overline{\langle A_2 \rangle}^0 = \operatorname{span}\{E_{11} + E_{22} + E_{33}, E_{12}\}.$$

So N becomes $\operatorname{span}\{E_{11}, E_{22} + E_{33}, E_{12}\}$ in the first iteration of the loop at line 7 (Lemma 19 below), and $TN = N \cup A_1 N$ where $A_1 N = \operatorname{span}\{E_{11}, E_{22} - E_{33}, E_{12}\}$, so T remains the same. In the second iteration T and N do not change anymore and the algorithm terminates.

In line 11 we make use of the case of a single invertible matrix to compute $\overline{\langle A \rangle}^0$. Some steps need further elaboration:

A) In line 4, we need to be able to choose $A_i \in Z_i \cap \mathrm{GL}_d(K)$, under the assumption that this intersection is nonempty.
B) In lines 5, 11 and 12, we need to compute the closure of the product of two (or more) irreducible closed sets.

Algorithm 1 Computation of $\overline{\langle X\rangle}$ when the invertible matrices are dense in X. The irreducible components $Z_1, \ldots, Z_r$ are given by their bases. Throughout the algorithm, N is an irreducible closed set, containing the identity matrix, that is monotonically increasing with each iteration. Similarly, T is a finite subset of $\langle I, A_1, \ldots, A_n\rangle$ that is monotonically increasing.

```
function GroupClosure($X$)
    $Z_1, \ldots\ Z_l \leftarrow$ Irreducible components of $X$
Require: $\mathrm{GL}_d(K) \cap Z_i \neq \emptyset$ for all $i \in [1, l]$
    for $i = 1, \ldots, l$ do
        $A_i \leftarrow$ An invertible element of $Z_i$
    $N \leftarrow \overline{(A_1^{-1}Z_1)\cdots(A_l^{-1}Z_l)}$
    $T \leftarrow \{I, A_1, \ldots, A_l\}$
    repeat
        $N' \leftarrow N$
        $T' \leftarrow T$
        for $A \in T$ do
            $N \leftarrow \overline{N\overline{\langle A\rangle}^0}$
            $N \leftarrow \overline{N(ANA^{-1})}$
            for $B \in T$ do
                if $AB \notin TN$ then
                    $T \leftarrow T \cup \{AB\}$
    until $N' = N$ and $T' = T$
    return $TN$
```

We first explain these steps, and then show termination and correctness of the algorithm.

A. Picking elements on which a polynomial does not vanish

The problem of picking an element in $Z_i \cap \mathrm{GL}_d(K)$ is an instance of the more general problem of picking an element in Z_i on which a given polynomial (in this case, the determinant) does not vanish. We give the general result, as we need it later.

Let $V \subseteq M_d(K)$ be a vector subspace and let $R = K[x_{ij} : 1 \leq i, j \leq d]$ be a polynomial ring in d^2 indeterminates. Let $A_0 \in M_d(R)$ be the matrix whose ij-th entry is x_{ij}. The space V is defined by a finite number of homogeneous linear equations in the variables x_{ij}. We can transform this system of equations into a triangular form by Gaussian elimination, and substitute into the entries of A_0 to eliminate a number of variables. This leaves us with a matrix $A \in M_d(R)$ with the following property: Substituting any elements $\alpha_{ij} \in K$ for x_{ij} yields a matrix in V, and conversely, every element of V can be obtained in this way. We call A a *generic matrix* of V. [4]

Lemma 17. *Let $V_1, \ldots, V_n \subseteq M_d(K)$ be irreducible closed subsets. If $X \subseteq M_d(K)$ is a Zariski-closed subset, then it is possible to decide whether $V_1 \cdots V_n \subseteq X$, and if this is not the case, to compute an element of $V_1 \cdots V_n \setminus X$.*

Proof. Let X be defined by nonzero polynomials $f_1, \ldots, f_m \in K[x_{ij} : 1 \leq i, j \leq d]$. We may assume $m \geq 1$ as the claim is trivial otherwise. Represent each V_k by a generic matrix $A_k \in M_d(K(\mathbf{y^{(k)}}))$, where $\mathbf{y^{(k)}} = (y_{ij}^{(k)})$ is a family of d^2 indeterminates. Then

$$V_1 \cdots V_n = \{\, A_1(\alpha_{ij}^{(1)}) \cdots A_n(\alpha_{ij}^{(n)}) : \alpha_{ij}^{(k)} \in K,\\ i, j \in [1, d],\ k \in [1, n] \,\}.$$

Substituting, each of the polynomials $f_l(x_{ij})$ gives rise to a polynomial $g_l(y_{ij}^{(1)}, \ldots y_{ij}^{(n)}) \coloneqq f_l\big(A_1(y_{ij}^{(1)}) \cdots A_n(y_{ij}^{(n)})\big)$ in at most nd^2 indeterminates. Now $V_1 \cdots V_n \subseteq X$ if and only if all of $g_1, \ldots, g_m$ vanish on K^{nd^2}. A polynomial g_l ($l \in [1, m]$) vanishes on all of K^{nd^2} if and only if it is the zero polynomial,[5] and one checks this by simplifying the expression for g_l.

Suppose now that some g_l is nonzero. Let $\prod_{i,j,k} (y_{ij}^{(k)})^{t_{ij}^{(k)}}$ with $t_{ij}^{(k)} \geq 0$ be a monomial of maximal total degree in the support of g_l. Let $P_{ij}^{(k)} \subseteq K$ be a set of cardinality $t_{ij}^{(k)} + 1$. By Alon's Combinatorial Nullstellensatz [2, Theorem 1.2], the finite set

$$\{\, g_l(\alpha_{ij}^{(1)}, \ldots, \alpha_{ij}^{(n)}) = f_l\big(A_1(\alpha_{ij}^{(1)}) \cdots A_n(\alpha_{ij}^{(n)})\big) :\\ (\alpha_{ij}^{(k)}) \in M_d(K) \text{ with } \alpha_{ij}^{(k)} \in P_{ij}^{(k)} \,\}$$

contains a nonzero element. Every such element gives rise to an element of $V_1 \cdots V_k \setminus X$. □

Example 18. Let $V_1 = \operatorname{span}\{E_{11} + E_{12}, E_{21} + E_{22}\}$ and $V_2 = \operatorname{span}\{E_{11} + E_{21}, E_{12} + E_{22}\}$, with generic matrices

$$A_1 = \begin{pmatrix} x & x \\ y & y \end{pmatrix}, \quad A_2 = \begin{pmatrix} z & w \\ z & w \end{pmatrix}.$$

Set $f_1 = x_{11}x_{22} - x_{12}x_{21}$ and $f_2 = (x_{11} - x_{21})(x_{11} - x_{12})$. Evaluating f_1 and f_2 on the product of the generic matrices,

$$A_1A_2 = \begin{pmatrix} 2xz & 2xw \\ 2yz & 2yw \end{pmatrix},$$

we get $g_1 = 4xzyw - 4xwyz = 0$ and $g_2 = 4(xz - yz)(xz - xw)$. So g_1 vanishes on V_1V_2, but g_2 has a leading term $4yzxw$. The Combinatorial Nullstellensatz implies that there is an element in V_1V_2 with w, x, y, $z \in \{0, 1\}$ on which g_2 does not vanish (e.g., $x = z = 1$, $y = w = 0$).

The special case of a single polynomial f follows by setting $m = 1$ and taking X to be the vanishing set of f.

B. Computing the closure of a product

For vector subspaces V, $W \subseteq M_d(K)$ we distinguish the pairwise product $VW \coloneqq \{\, vw : v \in V, w \in W \,\}$ which in general is not a vector space, and the product of vector spaces

$$V \cdot W \coloneqq \operatorname{span} VW = \operatorname{span}\{\, vw : v \in V,\ w \in W \,\},$$

which is the span of the former. We are interested mostly in closed sets, and the next lemma simplifies this issue.

Lemma 19. *Let V, $W \subseteq M_d(K)$ be irreducible closed subsets. Then $\overline{VW} = V \cdot W$. In particular, the set $\overline{VW}$ is irreducible.*

[4] A more conceptual way to think about this is that the coordinate ring of V is again a polynomial ring, and A represents the homomorphism of coordinate rings $K[M_d(K)] \to K[V]$.

[5] We use that K is infinite.

Proof. The sets V, $W \subseteq M_d(K)$ are also closed and irreducible in the Zariski topology.[6] In the Zariski topology the multiplication map $\mu\colon M_d(K) \times M_d(K) \to M_d(K), (A, B) \mapsto AB$ is continuous, and hence $\mu(V, W) = VW$ is irreducible [41, Lemma 0379]. Then VW is also irreducible in the, coarser, linear Zariski topology. Thus the same is true for the closure $\overline{VW}$ [41, Lemma 004W]. So $\overline{VW}$ is a vector space. But $V \cdot W$ is the smallest vector space containing VW, and thus $\overline{VW} = V \cdot W$. □

Now it is easy to compute a generating set for $\overline{VW}$ as the pairwise products of bases of V and W.

Remark 20. The multiplication map μ is *not* continuous in the linear Zariski topology. It is also possible to prove the previous lemma directly, without resorting to the Zariski topology, by showing $\overline{VW} = V \cdot W$ by hand.

C. Termination and Correctness of Algorithm 1

Recall that a group G is a torsion group if every element has finite order. We need the following.

Theorem 21 (Burnside–Schur [21, Theorem 2.3.5])**.** *If $G \leq \mathrm{GL}_d(K)$ is a finitely generated torsion group, then G is finite.*

Theorem 22. *Let $X \subseteq M_d(K)$ be a closed subset* (*given by a list of bases*) *such that $\mathrm{GL}_d(K) \cap X$ is dense in X. Then $\overline{\langle X \rangle}$ is computable.*

Proof. We show that Algorithm 1 terminates and yields $\overline{\langle X \rangle}$. The intersection $\mathrm{GL}_d(K) \cap \overline{\langle X \rangle}$ is a linear algebraic group by 2) of Lemma 9, and we are going to use this structure. To do so, write $\widetilde{X}$ for the closure of a set in the usual Zariski topology (i.e., not the linear one), taken over the algebraic closure $\overline{\mathbb{Q}}$.

Denote by (T_1, N_1), (T_2, N_2), $\ldots$, the subsequent values taken by T and N. Then $N_1 \subseteq N_2 \subseteq \cdots$ is an ascending chain of vector subspaces of the finite-dimensional space $M_d(K)$, and $T_1 \subseteq T_2 \subseteq \cdots$ is an ascending chain of finite subsets of $\langle I, A_1, \cdots, A_l \rangle$. Define $N_\infty := \bigcup_{i \geq 1} N_i$ and $T_\infty := \bigcup_{i \geq 1} T_i$. Set $\mathcal{S} = \bigcup_{i \geq 1} T_i N_\infty = T_\infty N_\infty$.[7] By construction X is dense in $\mathcal{S}$ (this is true in the beginning of the algorithm and is preserved in each step, keeping in mind Lemma 8).

It remains to show that the algorithm terminates and that $\mathcal{S}$ is a closed semigroup. Since each N_i is a vector subspace of $M_d(K)$, the chain of N_i's stabilizes at some $N_\infty = N_m$. For $i \geq 0$ and $A \in T_i$ note $AN_iA^{-1} \subseteq N_{i+1}$ (by line 12) and so $AN_\infty A^{-1} \subseteq N_\infty$. These being vector spaces of the same dimension, even $AN_\infty A^{-1} = N_\infty$. Let $H := N_\infty \cap \mathrm{GL}_d(K)$. For every $i \geq 0$ and A, $B \in T_i$ we have $(AH)(BH) \subseteq ABHH \subseteq T_{i+1}H$ by construction (the first inclusion by $BN_\infty = N_\infty B$; the second one by lines 12 and 15). Therefore $G := \bigcup_{i \geq 1} T_i H \subseteq \mathrm{GL}_d(K)$ is a semigroup. The Zariski closure $\widetilde{G} \subseteq \mathrm{GL}_d(\overline{\mathbb{Q}})$ is a linear algebraic group, and $\widetilde{H}$ is a closed normal subgroup. Indeed, as N_∞ is a vector subspace of $M_d(K)$, the closure $\widetilde{H}$ is simply the vector subspace of $M_d(\overline{\mathbb{Q}})$ defined by the same equations as N_∞, intersected with $\mathrm{GL}_d(\overline{\mathbb{Q}})$. The quotient $\widetilde{G}/\widetilde{H}$ is also a linear algebraic group [8, Theorem II.6.8], so without restriction $\widetilde{G}/\widetilde{H} \subseteq \mathrm{GL}_{d'}$ for some $d' \geq 1$. Let $\pi\colon \widetilde{G} \to \widetilde{G}/\widetilde{H}$ denote the quotient morphism; it is a K-morphism of algebraic K-groups.

By construction of the sets T_i and H, the set $\pi(G)$ is contained in the subsemigroup of $\mathrm{GL}_{d'}(K)$ generated by $\pi(I)$, $\pi(A_1)$, $\ldots$, $\pi(A_l)$. But it also contains all these elements, so $\pi(G) = \langle \pi(I), \pi(A_1), \ldots, \pi(A_l) \rangle$. By line 11, every element of $\pi(G)$ has finite order. Therefore $\pi(G)$ is a torsion group. As we have just argued it is also finitely generated, and thus Burnside–Schur applies to show that $\pi(G)$ is finite.

We now check that finiteness of $\pi(G) = \widetilde{G}/\widetilde{H}$ implies finiteness of T_∞. Note that $\widetilde{H} \cap \mathrm{GL}_d(K) = H$. Thus for A, $B \in \mathrm{GL}_d(K)$ we have $AB^{-1} \in \widetilde{H}$ if and only if $AB^{-1} \in H$ if and only if $AB^{-1} \in N_\infty$. Looking at lines 14–15, once the chain $N_1 \subseteq N_2 \subseteq \cdots$ has stabilized at N_∞, the chain $T_1 \subseteq T_2 \subseteq \ldots$ must also stabilize, say at the finite set $T_\infty = T_n$, because we are at this point only adding elements representing different cosets of $\widetilde{G}$ modulo $\widetilde{H}$. Then $\mathcal{S} = T_n N_m$ is closed.

Finally, $\mathcal{S}$ is a semigroup: if A, $B \in T_\infty$ then $(AN_\infty)(BN_\infty) = ABN_\infty N_\infty \subseteq ABN_\infty \subseteq T_\infty N_\infty$, where the last inclusion is ensured by line 15. □

V. Non-invertible Matrices

Throughout this entire section, let $X \subseteq M_d(K)$ be a closed subset (in the linear Zariski topology) and let $\mathcal{S} := \langle X \rangle$ be the subsemigroup of $M_d(K)$ generated by X. In this section we show how to compute the closure $\overline{\mathcal{S}}$.

Since $\overline{\mathcal{S}}$ is closed in the linear Zariski topology, it is also closed in the Zariski topology. The set $\overline{\mathcal{S}}$ is therefore a linear semigroup (Lemma 9) and in particular strongly π-regular (every element has a power that is contained in a subgroup of $\overline{\mathcal{S}}$). Much is known about the structure of linear semigroups [38], [39], respectively strongly π-regular matrix semigroups [39, Section 2.3.2] [34]. These structural results are reflected in the algorithmic considerations, although they are not directly applicable to $\mathcal{S}$ itself. More general structural results about matrix semigroups, applying also to $\mathcal{S}$, can be found in [35], [36]. However, we will not be making use of them.

Our approach leans heavily on an algorithm for the computation of the Zariski closure, described in [22]. However, we use more semigroup-theoretic language. A key point in [22] is the use of an inductive approach based on the rank: first the closure of the semigroup generated by elements of the maximal rank r is computed, then the closure of all elements of rank $\geq r - 1$, and so on.

Definition 23. *For $\emptyset \neq X \subseteq M_d(K)$ closed, the* generic rank *of X is $\bar{\mathrm{r}}(X) := \max\{\, \mathrm{rank}(A) : A \in X \,\}$.*

[6] To see irreducibility, consider polynomials f, $g \in K[x_{ij}]$ that vanish on proper subsets of V, and such that fg vanishes on all of V. Using the linear homogeneous equations defining V, we can eliminate a number of variables in f and g to obtain nonzero polynomials $\hat{f}$, $\hat{g}$, in a subset of the variables $\{x_{ij}\}$, with the property that $\hat{f}\hat{g}$ vanishes everywhere. However, since K is infinite, this implies $\hat{f}\hat{g} = 0$, a contradiction to $\hat{f}$, $\hat{g} \neq 0$.

[7] The idea will be that $N_\infty \cap \mathrm{GL}_d(K)$ is the irreducible component containing the identity, and T_∞ is in fact a finite set that contains a transversal of the group $\overline{\langle X \rangle} \cap \mathrm{GL}_d(K)$ with respect to $N_\infty \cap \mathrm{GL}_d(K)$.

A disadvantage arising from the coarseness of the linear Zariski topology compared to the Zariski topology is that the generic rank is ill-behaved with respect to products.

Example 24. Consider again Example 18. Then V_1 and V_2 are 2-dimensional vector spaces of generic rank 1. However, V_1V_2 contains all matrices E_{ij}. Thus $\overline{V_1V_2} = M_2(K)$ has generic rank 2. (In the usual Zariski topology, V_1V_2 is not dense in $M_2(K)$: the determinant vanishes on the entire set.)

Example 24 shows that taking a closure of a product of vector spaces may introduce elements of larger rank. Much of the difficulty in the linear Zariski topology setting revolves around ensuring termination in light of this ill-behaved nature of the generic rank (Remark 40).

We call a matrix $A \in M_d(K)$ *completely pseudo-regular* if it is contained in a subgroup of $M_d(K)$.[8] The main issue in computing $\overline{\mathcal{S}}$, is that completely pseudo-regular elements A of $\mathcal{S}$ give rise to subgroups of $\overline{\mathcal{S}}$, i.e., subsemigroups of $M_d(K)$ that are groups with regards to some idempotent matrix as identity. We write $E(A)$ for this idempotent. We will need to deal with these subgroups by reducing to the (already proven) group case.

For a subset $Y \subseteq M_d(K)$ and $n \geq 1$, we define

$$Y^{\leq n} := \bigcup_{k=1}^{n} Y^k = \{\, A_1 \cdots A_k : k \in [1,n], A_1, \ldots, A_k \in Y \,\}$$

and $Y^{\trianglelefteq n} := \{I\} \cup Y^{\leq n}$. For a completely pseudo-regular element $A \in \mathcal{S}$ of rank r and a closed set Y, let $E = E(A)$,

$$\mathcal{T}_0(Y, A) := \left\{ B \in \overline{EY^{\trianglelefteq 2\binom{d}{r}+5}E} : \operatorname{rank}(B) = r \right\}, \quad \text{and}$$

$$\mathcal{T}(Y, A) := \overline{Y^{\trianglelefteq \binom{d}{r}+2}\, \overline{\langle \mathcal{T}_0(Y, A) \rangle}\, Y^{\trianglelefteq \binom{d}{r}+2}}.$$

We now have all the tools to state Algorithm 2.

The main idea in the algorithm is: each set R_s is a (finite) set of completely pseudo-regular elements of rank s. Under the assumption that each R_s is actually a full set of representatives of completely pseudo-regular elements of rank s, we attempt to compute $\overline{\mathcal{S}}$ using a recursive strategy (TryClose). If this fails to yield the entire closure, then in fact some completely pseudo-regular element must be missing and we can find such an element (using FindCPR), add it to R_s, and try again. We give an example illustrating the algorithm; afterwards we deal with the computation of $\mathcal{T}(Y, A)$ (line 15) and termination and correctness of Algorithm 2.

Example 25. Let

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{pmatrix},$$

and $X = A\mathbb{Q} \cup B\mathbb{Q} \cup C\mathbb{Q}$. On the first iteration, in TryClose, all $R_s = T_s = \emptyset$ and $Y_4 = X$, $Y_3 = X^{\leq 5}$ consists of all scalar multiples of nonempty products of at most 5 of the matrices, $Y_2 = (X^{\leq 5})^{\leq 9} = X^{\leq 45}$, and $Y_1 = X^{\leq 405}$. Now $\overline{Y_1^2} \not\subseteq Y_1$ (e.g., A^{406} is not contained in Y_1). So the check on line 4 fails.

Algorithm 2 Computation of $\overline{\langle X \rangle}$ in the general case. FindCPR discovers a new completely pseudo-regular element of rank $> s$. TryClose returns a closed set, that is equal to $\overline{\langle X \rangle}$ if all necessary completely pseudo-regular elements have been discovered.

```
 1: function SemigroupClosure($X$)
Require: $X$ closed set
 2:     $r \leftarrow \bar{\mathrm{r}}(X)$, $R_1, \ldots, R_r \leftarrow \emptyset$
 3:     $Y_i, T_i\ (i \in [1,r]) \leftarrow$ TryClose$(X, R_1, \ldots, R_r)$
 4:     while $\overline{Y_1^2} \not\subseteq Y_1$ do
 5:         $s \leftarrow 0$
 6:         repeat
 7:             $B \leftarrow$ FindCPR$(X, Y_i, T_i, R_i, s)$
 8:             $s \leftarrow \operatorname{rank}(B)$,
 9:             $R_s \leftarrow R_s \cup \{B\}$; $R_1, \ldots, R_{s-1} \leftarrow \emptyset$
10:         until $|R_s| \leq \binom{d}{s}$
11:         $Y_i, T_i\ (i \in [1,r]) \leftarrow$ TryClose$(X, R_1, \ldots, R_r)$
        return $Y_1$

12: function TryClose($X, R_1, \ldots, R_r$)
Require: $X$ closed set; $R_s \subseteq \langle X \rangle$ finite set of completely
    pseudo-regular elements of rank $s$
13:     $r \leftarrow \bar{\mathrm{r}}(X)$, $Y_{r+1} \leftarrow X$
14:     for $s = r, \ldots, 1$ do
15:         $T_s \leftarrow \bigcup_{B \in R_s} \mathcal{T}(Y_{s+1}, B)$
16:         $Y_s \leftarrow \overline{(Y_{s+1} \cup T_s)^{\leq 2\binom{d}{s}+3}}$
        return $Y_1, T_1, \ldots, Y_r, T_r$

17: function FindCPR($X, Y_1, T_1, R_1, \ldots, Y_r, T_r, R_r, s$)
18:     $r \leftarrow \bar{\mathrm{r}}(X)$
19:     for $n \geq 0$ do
20:         for $s' = r, \ldots, s+1$ do
21:             $C_{s'} \leftarrow Y_{s'} \cup \{\, A \in M_d(K) : \operatorname{rank}(A) < s' \,\}$
22:             if $n \geq 2\binom{d}{s'} + 4$ and $X^n \setminus C_{s'} \neq \emptyset$ then
23:                 $A_1 \cdots A_n \leftarrow$ an element of $X^n \setminus C_{s'}$
24:                 $A_k \cdots A_l \leftarrow$ c.p.r. subprod. $\notin Y_{s'+1} \cup T_{s'}$
25:                 return $A_k \cdots A_l$
```

Now FindCPR gets called (with $s = 0$). It discovers $A^6 \in X^6 \setminus Y_3$, which, being invertible, is actually completely pseudo-regular with $E(A) = I$. However, to make the example more illustrative, we deviate here from the actual pseudo-code and presume that FindCPR would instead return the completely pseudo-regular element C.[9] Then $E(C) = E_{33}$ and $R_1 = \{C\}$.

One gets $T_1 = \mathcal{T}(Y_2, C) = \operatorname{span}\{E_{33}\} \cup \operatorname{span}\{E_{23}\} \cup \operatorname{span}\{E_{31} + E_{32}\} \cup \operatorname{span}\{E_{31} - E_{32}\} \cup \operatorname{span}\{E_{21} + E_{22}\} \cup \operatorname{span}\{E_{21} - E_{22}\}$ (note T_1^2, XT_1, $T_1X \subseteq T_1$). So, the second iteration of the loop at line 4 yields $Y_4 = X$, $Y_3 = X^{\leq 5}$, $Y_2 = X^{\leq 45}$, and $Y_1 = (X^{\leq 45} \cup T_1)^{\leq 9} = X^{\leq 405} \cup T_1$. However, again $\overline{Y_1^2} \not\subseteq Y_1$ and FindCPR gets called again. Let us assume that at this point FindCPR returns (correctly) A^6 (with $E(A^6) = I$).

[8] In semigroup theory, an element of $\mathcal{S}$ is *completely regular* if it is contained in a subgroup of $\mathcal{S}$. Completely regular elements of $\mathcal{S}$ are completely pseudo-regular, but the converse may fail if $\mathcal{S}$ is not strongly π-regular: e.g., an inverse to a given matrix $A \in \mathcal{S}$ may exist in $M_d(K)$ but not be contained in $\mathcal{S}$.

[9] Otherwise, the next call to TryClose already returns the entire closure, as we will see below.

Then $R_3 = \{A^6\}$, while now $R_2 = R_1 = \emptyset$ are reset.

On the next call to TryClose, we get $T_3 = \mathcal{T}(A, I) = \operatorname{span}\{E_{11}+E_{22}, E_{33}\} \cup \operatorname{span}\{E_{11}-E_{22}, E_{33}\}$. Then $Y_4 = X$. Multiplying T_3 from the left by B, B^2, C, CB, CB^2, one can find

$$\begin{aligned} Y_3 = {} & \operatorname{span}\{E_{11} + E_{22}, E_{33}\} \cup \operatorname{span}\{E_{11} - E_{22}, E_{33}\} \\ & \cup \operatorname{span}\{E_{21} + E_{22}, E_{33}\} \cup \operatorname{span}\{E_{21} - E_{22}, E_{33}\} \\ & \cup \operatorname{span}\{E_{31} + E_{32}, E_{23}\} \cup \operatorname{span}\{E_{31} - E_{32}, E_{23}\} \\ & \cup \operatorname{span}\{E_{33}\} \cup \operatorname{span}\{E_{23}\} \\ & \cup \operatorname{span}\{E_{31} + E_{32}\} \cup \operatorname{span}\{E_{31} - E_{32}\} \\ & \cup \operatorname{span}\{E_{21} + E_{22}\} \cup \operatorname{span}\{E_{21} - E_{22}\}. \end{aligned}$$

Now one can check $Y_3^2 \subseteq Y_3$, so $Y_1 = Y_2 = Y_3$, and this is the closure of $\langle X \rangle$.

Finally, if we multiply this set with $(1,1,1) = e_1 + e_2 + e_3$ from the left (i.e., summing the rows), we get

$$(1,1,1)Y_3 = \operatorname{span}\{e_1 + e_2, e_3\} \cup \operatorname{span}\{e_1 - e_2, e_3\}.$$

This is the linear hull of the automaton in [3, Example 3.7].

Before we can discuss correctness and termination of the algorithm, we show that the generic rank is computable (Corollary 27), that $\mathcal{T}(Y, A)$ is computable (Lemma 35), and that we need to consider only finitely many completely pseudo-regular elements (Lemma 38), up to a certain equivalence (Definition 31).

A. *Computability of the generic rank*

To compute the generic rank, we relate it to generic matrices (section IV-A).

Lemma 26. *Let $r \in \mathbb{Z}_{\geq 0}$. For an irreducible closed subset $V \subseteq M_d(K)$, the following statements are equivalent.*

a) $\overline{\mathrm{r}}(V) = r$.
b) Every generic matrix of V has rank r.
c) There exists a generic matrix of V with rank r.
d) There exists a Zariski-dense Zariski-open subset $U \subseteq V$ with $\operatorname{rank}(A) = r$ for all $A \in U$.

Proof. The implications b) ⇒ c) and d) ⇒ a) are immediate from the definitions.

c) ⇒ d) Let $R = K[x_{ij} : 1 \leq i, j \leq d]$ and let $A \in M_d(R)$ be a generic matrix of V. Performing Gaussian elimination over the field of fractions $\mathbf{q}(R) = K(x_{ij} : 1 \leq i, j \leq d)$ of R, we find an invertible matrix $T \in M_d(\mathbf{q}(R))$ such that $B = TA$ is in reduced row echelon form. Let $f \in R$ be a nonzero common multiple of the denominators of the entries of T, T^{-1}, and B. Whenever $A(\alpha_{ij}) \in V$ with $f(A(\alpha_{ij})) \neq 0$, we get that $A(\alpha_{ij}) = T^{-1}(\alpha_{ij})B(\alpha_{ij}) \in V$ is well-defined and has rank r (as $B(\alpha_{ij})$ is still in reduced row echelon form and $T(\alpha_{ij})$ is invertible). The set $D(f) = \{\, A(\alpha_{ij}) \in V : f(A(\alpha_{ij})) \neq 0 \,\}$ is nonempty and Zariski-open in V. By Zariski-irreducibility of V it is Zariski-dense in V.

a) ⇒ b) Let A be a generic matrix of V with $\operatorname{rank}(A) = s$. In light of c) ⇒ d) we see that V contains a Zariski-dense subset U of rank s matrices. Thus $\overline{\mathrm{r}}(V) \geq s$. On the other hand, all $(s+1) \times (s+1)$ minors vanish on U. Since these minors are polynomials in the entries of the matrices, also all elements of the Zariski closure of U have rank $\leq s$. Altogether $\overline{\mathrm{r}}(V) = s$. □

The generic rank $r = \overline{\mathrm{r}}(V)$ can therefore be computed using Gauss elimination on a generic matrix of V.

Corollary 27. *Let $V \subseteq M_d(K)$ be an irreducible closed subset. Then $r = \overline{\mathrm{r}}(V)$ is computable.*

B. *A key finiteness result*

The following will be applied in various guises. (This observation has also been used in [22]. Similar considerations are used to derive the bounds in [34].)

Lemma 28. *Let W be a d-dimensional vector space. Let $r \in [0, d]$ and let (U_1, V_1), …, (U_n, V_n) be pairs of vector subspaces of W such that $U_i \cap V_i = 0$ and $\dim V_i = r$ for $i \in [1, n]$. If $n > \binom{d}{r}$, then*

1) there exist $i > j$ such that $U_i \cap V_j = 0$, and
2) there exist $i < j$ such that $U_i \cap V_j = 0$.

Proof. Replacing the U_i by larger spaces if necessary we may suppose $\dim U_i = d - r$ for $i \in [1, n]$. Therefore it suffices to show the first claim, the second one follows by symmetry.

Fixing bases $u_{i,1}$, …, $u_{i,d-r}$ of U_i and $v_{i,1}$, …, $v_{i,r}$ of V_i we can associate to U_i and V_i the elements $\alpha_i := u_{i,1} \wedge \cdots \wedge u_{i,d-r} \in \bigwedge^{d-r} W$ and $\beta_i := v_{i,1} \wedge \cdots \wedge v_{i,r} \in \bigwedge^{r} W$. (A different choice of bases only changes the corresponding α_i, respectively, β_i by a nonzero scalar multiple.) Now $U_i \cap V_j = 0$ if and only if $\alpha_i \wedge \beta_j \neq 0$ in the exterior algebra $\bigwedge W$.

Assume, for the sake of contradiction, $U_i \cap V_j \neq 0$ for all i, $j \in [1, n]$ with $i > j$. Then $\alpha_i \wedge \beta_j = 0$ for $i > j$ but $\alpha_i \wedge \beta_i \neq 0$. Thus β_i cannot be a linear combination of β_1, …, β_{i-1}. Hence the β_1, …, β_n are linearly independent in $\bigwedge^r W$, and therefore $n \leq \dim \bigwedge^r W = \binom{d}{r}$ contradicts the assumption on n. □

C. *Equivalence classes of completely pseudo-regular elements.*

We need an intrinsic characterization of completely pseudo-regular elements.

Lemma 29. *Let $A \in M_d(K)$. The following statements are equivalent.*

a) A is completely pseudo-regular.
b) There exists $A' \in M_d(K)$ such that $A = AA'A$ and $AA' = A'A$.
c) There exist E, $A' \in M_d(K)$ such that $E^2 = E$, $EA = AE = A$, and $AA' = A'A = E$.
d) $\operatorname{rank} A = \operatorname{rank} A^2$.
e) $\operatorname{im}(A) \cap \ker(A) = 0$.

Proof. The equivalence of a), b), and c) holds in all semigroups. For convenience, we recall a proof.

a) ⇒ b) Let $G \subseteq M_d(K)$ be a subgroup containing A, and A' the inverse of A in G.

b) ⇒ c) $E := A'A$ is idempotent as claimed.

c) ⇒ a) The semigroup generated by A, A', and E is a group.

b) ⇒ d) Since $A = A^2 A'$, we have $\mathrm{im}(A) \subseteq \mathrm{im}(A^2)$, and hence $\mathrm{im}(A) = \mathrm{im}(A^2)$.

d) ⇔ e) Clear.

e) ⇒ c) We have $K^d = \mathrm{im}(A) \oplus \ker(A)$, and therefore it is possible to construct a suitable inverse to A on $\mathrm{im}(A)$ and extend it to K^d. □

Suppose that A is completely pseudo-regular and E is an idempotent as in c). Then $\mathrm{rank}\, A = \mathrm{rank}\, E$. From this rank equality and $EA = A$ and $AE = E$, one deduces $\mathrm{im}\, E = \mathrm{im}\, A$ and $\ker E = \ker A$, so that E is uniquely determined by A (an idempotent matrix E is a projection onto the subspace $\mathrm{im}\, E$ along $\ker E$, and it is therefore uniquely determined by its image and its kernel). Then $E = E(A)$ is the identity element of any subgroup containing A.

The element A' with $AA' = A'A = E$ is not uniquely determined, but there is a unique such A' with $A' \in EM_d(K)E$ (because $A'|_{\mathrm{im}\, E}$ is determined by A and $A'|_{\ker E} = 0$). We write A^+ for this element of $EM_d(K)E$ and call it the *pseudo-inverse* of A.

Lemma 30. *If $\mathcal{S} \subseteq M_d(K)$ is a Zariski-closed subsemigroup, then $\mathcal{S}$ is strongly π-regular. For every completely pseudo-regular $A \in \mathcal{S}$, also $E(A)$, $A^+ \in \mathcal{S}$.*

Proof. A Zariski-closed semigroup $\mathcal{S}$ is strongly π-regular by [38, Theorem 3.18] and the remaining claims follow from inspection of the proof of the cited theorem. □

There may be infinitely many completely pseudo-regular elements (and associated subgroups), and we need to reduce the problem to one where we only have to deal with finitely many. To do so, we deal with equivalence classes of completely pseudo-regular elements.

Definition 31. *1) For A, $B \in M_d(K)$ write $A \parallel B$ if $\mathrm{im}(A) = \mathrm{im}(B)$ and $\ker(A) = \ker(B)$.*

2) For A, $B \in \mathcal{S}$ let $A \sim_{\mathcal{S}} B$ if there exist C, D, C', $D' \in \mathcal{S} \cup \{I\}$ such that $B \parallel DAC$ and $A \parallel D'BC'$.

The relation $\sim_{\mathcal{S}}$ is an equivalence relation on $\mathcal{S}$. The rank is constant on each $\sim_{\mathcal{S}}$-equivalence class, and we may therefore speak of the *rank* of an equivalence class. We write $[A]_{\mathcal{S}}$ for the $\sim_{\mathcal{S}}$-equivalence class of $A \in \mathcal{S}$.

The rest of the subsection is dedicated to ultimately proving that, given a completely pseudo-regular element $A \in \mathcal{S}$ of rank r, and under the assumption that we are able to compute a closed set Y containing all elements of $\mathcal{S}$ of rank $> r$, it is possible to compute a closed set that contains the entire equivalence class $[A]_{\mathcal{S}}$ (this is 2) of Lemma 35). This will allow us to compute $\mathcal{T}(Y, A)$.

The following lemma replaces [22, Propositions 9 and 10] in our setting.

Lemma 32. *Let $A = A_1 \cdots A_n$ with $A_1, \ldots, A_n \in M_d(K)$. Suppose there exists $r \geq 0$ such that $\mathrm{rank}(A) = \mathrm{rank}(A_i A_{i+1}) = r$ for all $i \in [1, n-1]$.*

1) There exists a subproduct $A' := A_{i_1} \cdots A_{i_k}$ with $1 = i_1 < i_2 < \cdots < i_{k-1} < i_k = n$ such that $A \parallel A'$ and $k \leq \binom{d}{r} + 3$.

2) If $n \geq 2\binom{d}{r} + 4$, then there are $1 \leq k < l \leq n$ such that $A_k \cdots A_l$ is completely pseudo-regular of rank r.

Proof. 1) For $i \in [3, n-1]$ define $V_i := \mathrm{im}(A_i \cdots A_n)$ and $U_i := \ker(A_1 \cdots A_{i-1})$. Then $V_i \cap U_i = 0$ for all $i \in [3, n-1]$. Suppose $n > \binom{d}{r} + 3$. By Lemma 28, there exist $i, j \in [3, n-1]$ with $j < i$ such that $U_j \cap V_i = 0$. Then

$$A_1 \cdots A_{j-1}(A_j \cdots A_{i-1})A_i \cdots A_n \parallel A_1 \cdots A_{j-1} A_i \cdots A_n,$$

and the second product has fewer factors. The claim follows by repeating this process.

2) For $i \in [1, \lfloor n/2 \rfloor - 1]$, let $U_i = \ker(A_{2i-1} A_{2i})$ and $V_i = \mathrm{im}(A_{2i+1} A_{2i+2})$. Then $U_i \cap V_i = 0$ for all i. By Lemma 28, there are $i < j$ with $U_j \cap V_i = 0$. Then $\mathrm{im}(A_{2i+1} A_{2i+2}) \cap \ker(A_{2j-1} A_{2j}) = 0$ and $2i+1 < 2j$, so $k = 2i+1$ and $l = 2j$ works. □

Lemma 33. *Let $A \in \mathcal{S}$ be completely pseudo-regular and $B \in [A]_{\mathcal{S}}$.*

1) There exist completely pseudo-regular C, $D \in [A]_{\mathcal{S}}$ such that $B = E(D)B$ and $B = BE(C)$.

2) Suppose $B = B_1 B_2$ with B_1, $B_2 \in \mathcal{S}$. Then there exists a completely pseudo-regular element $C \in [A]_{\mathcal{S}}$ such that $B_1 B_2 = B_1 E(C) B_2$.

Proof. Let P, P', Q, $Q' \in \mathcal{S} \cup \{I\}$ such that $A \parallel Q'BP'$ and $B \parallel QAP$. Let $r = \mathrm{rank}(A)$.

1) Since $\mathrm{rank}(B) = r$ as well, we have $\mathrm{im}(QA) = \mathrm{im}(B)$ and $\mathrm{im}(Q'B) = \mathrm{im}(Q'QA) = \mathrm{im}(A)$. Then $\mathrm{rank}(Q'QA) = r$ implies $\ker(Q'QA) = \ker(A)$, so that $Q'QA \parallel A$. In particular, $Q'QA$ is completely pseudo-regular. Now let $D := QAQ'$. Since $\mathrm{rank}(Q'QAQ'QA) = r$, we must have $\mathrm{rank}(D) = r$. Then $\mathrm{im}(D) = \mathrm{im}(QA) = \mathrm{im}(B)$. Since $\mathrm{rank}(AQ'QA) = r$ we must have $\mathrm{im}(QA) \cap \ker(AQ') = 0$, and thus D is completely pseudo-regular. Hence $E(D)B = B$. Finally, $D \parallel QAQ'$ by definition and $A \parallel Q'QAQ'QA = Q'DQA$, so that $A \sim_{\mathcal{S}} D$.

The symmetric claim follows analogously.

2) By 1) there exist completely pseudo-regular elements D, $D' \in [A]_{\mathcal{S}}$ such that $B = E(D)B$ and $B = BE(D')$. Let $C := (B_2 D' P')A(Q' D B_1)$. From $\mathrm{im}(DB_1) \supseteq \mathrm{im}(DB) = \mathrm{im}(B)$ and $\mathrm{rank}(DB_1) \leq \mathrm{rank}(B)$ we get $\mathrm{im}(DB_1) = \mathrm{im}(B)$. Analogously $\ker(B_2 D') = \ker(BD') = \ker(B)$. Also $\mathrm{im}(Q'DB_1) = \mathrm{im}(Q'B) = \mathrm{im}(A)$ and $\ker(B_2 D' P') = \ker(BP') = \ker(A)$. Thus $\mathrm{rank}(C) = r$. Computing $C^2 = (B_2 D' P')A(Q' DBD' P')A(Q' D B_1)$, we see that C is completely pseudo-regular. From $A \parallel (Q'DB_1)C(B_2 D' P')A$ we get $C \sim_{\mathcal{S}} A$.

From $\ker(DB_1) = \ker(C)$ we have $DB_1 = DB_1 E(C)$, and from $\mathrm{im}(B_2 D') = \mathrm{im}(C)$ we have $E(C) B_2 D' = B_2 D'$. Thus $DB_1 E(C) B_2 = DB$ and $B_1 E(C) B_2 D' = BD'$. We deduce $B_1 E(C) B_2|_{\mathrm{im}(D')} = B|_{\mathrm{im}(D')}$. Next $\ker(E(C)B_2) \subseteq \ker(DB) = \ker(B)$ implies $\ker(B_1 E(C) B_2) = \ker(B) = \ker(D')$. So $K^d{=}\mathrm{im}(D') {\oplus} \ker(D')$, so $B_1 E(C) B_2 = B$. □

Proposition 34. *Let $E \in M_d(K)$ be idempotent of rank r and let $H \subseteq E\overline{\mathcal{S}}E$ be a closed subset. Then $\{\, A \in H : \operatorname{rank}(A) = r \,\}$ is contained in a subgroup of $\overline{\mathcal{S}}$ (with neutral element E), and it is possible to compute $\overline{\langle\{\, A \in H : \operatorname{rank}(A) = r \,\}\rangle}$.*

Proof. Let $V = \operatorname{im} E$. By a suitable change of basis, the endomorphisms of V correspond to matrices with arbitrary entries in the upper left $r \times r$-block and zeroes everywhere else. The matrices $A \in H$ with $\operatorname{rank} A = r$ correspond to those matrices where the upper left $r \times r$-block is invertible, and all entries outside this block are zero. We may therefore compute $\overline{\langle\{\, A \in H : \operatorname{rank}(A) = r \,\}\rangle}$ by reducing to the invertible case (see section IV). □

In the following lemma keep in mind that if $A \in \mathcal{S}$ is completely pseudo-regular, then the associated idempotent $E = E(A)$ may not be contained in $\mathcal{S}$ but is always contained in $\overline{\mathcal{S}}$ by Lemma 30.

The, somewhat technical, statement 1) "connects" the idempotent $F = F(B)$ of any completely pseudo-regular to E in way that is needed for proving 2). Statement 1) will not be needed later on.

Lemma 35. *Let $r \geq 0$ and let A be a completely pseudo-regular element of $\mathcal{S}$ of rank r. Suppose $Y \subseteq M_d(K)$ is a closed set with $X \cup \{\, B \in \mathcal{S} : \operatorname{rank}(B) > r \,\} \subseteq Y$. Let $E := E(A)$ and $H := \{\, B \in EY^{\trianglelefteq 2\binom{d}{r}+5}E : \operatorname{rank}(B) = r \,\}$.*

1) *If $F = E(B)$ for some completely pseudo-regular $B \in [A]_{\mathcal{S}}$, then there exist $D \in Y^{\trianglelefteq\binom{d}{r}+2}E$ and $D^+ \in E\overline{\langle H\rangle}Y^{\trianglelefteq\binom{d}{r}+2}$ such that $D^+D = E$ and $DD^+ = F$.*
2) *The set $\overline{\langle H\rangle}$ is computable and $Y^{\trianglelefteq\binom{d}{r}+2}\overline{\langle H\rangle}Y^{\trianglelefteq\binom{d}{r}+2}$ contains $[A]_{\mathcal{S}}$.*

Proof. 1) Recall $A = EA = AE$ and $\operatorname{rank} A = \operatorname{rank} B = \operatorname{rank} E = r$. Let $P, Q \in \mathcal{S} \cup \{I\}$ be such that $B \parallel QAP$. Then $\operatorname{im}(B) = \operatorname{im}(QAP) = \operatorname{im}(QA) = \operatorname{im}(QEA)$, with the middle equality holding because of $\operatorname{rank}(QA) \leq r$. Also because of the ranks, therefore $\operatorname{im}(B) = \operatorname{im}(QE)$ and $\operatorname{rank}(QE) = r$. Analogously one finds $\ker(B) = \ker(EP)$ and $\operatorname{rank}(EP) = r$. Now $(EP)F = EP$ and $F(QE) = QE$. Write $P = P_1 \cdots P_m$ and $Q = Q_1 \cdots Q_n$ with $m, n \geq 0$ and $P_i, Q_i \in X \cup \{\, B \in \mathcal{S} : \operatorname{rank}(B) > r \,\}$. Choosing m, n minimal, we get $\operatorname{rank}(P_iP_{i+1}) = r$ for $i \in [1, m-1]$ and $\operatorname{rank}(Q_iQ_{i+1}) = r$ for $i \in [1, n-1]$. Consider $EP_1 \cdots P_m$ and $Q_1 \cdots Q_nE$. Applying 1) of Lemma 32, we find subproducts $D = Q_{i_1} \cdots Q_{i_k}E$ and $C = EP_{j_1} \cdots P_{j_l}$ with $k, l \leq \binom{d}{r} + 2$ and such that $\operatorname{im}(D) = \operatorname{im}(F)$ and $\ker(C) = \ker(F)$.

Now set $R := CD$. Then $R \in H$. Therefore $\overline{\langle H\rangle}$ contains the pseudo-inverse $R^+ = ER^+ = R^+E$ satisfying $RR^+ = R^+R = E$ by Lemma 30. Define $D^+ := R^+C = R^+EC$. Then $D^+D = R^+CD = R^+R = E$. Furthermore DD^+ is idempotent with $\operatorname{im}(DD^+) = \operatorname{im} F$ and $\ker(DD^+) = \ker F$. Thus $DD^+ = F$.

2) One first computes $\overline{H}$ and then, using Proposition 34, one can compute $\overline{\langle H\rangle} = \overline{\langle\{C \in \overline{H} : \operatorname{rank}(C) = r\}\rangle}$ as a subset of $EM_d(K)E$. Note $E\overline{\langle H\rangle}Y^{\trianglelefteq\binom{d}{r}+2}XY^{\trianglelefteq\binom{d}{r}+2}E \subseteq E\overline{\langle H\rangle}Y^{\trianglelefteq\binom{d}{r}+5}E = E\overline{\langle H\rangle}EY^{\trianglelefteq\binom{d}{r}+5}E$. Every element of this set having rank r is also contained in $E\overline{\langle H\rangle}HE \subseteq \overline{\langle H\rangle}$.

Let $B = B_1 \cdots B_n \in [A]_{\mathcal{S}}$ with $B_1, \ldots, B_n \in X$. By Lemma 33, there exist completely pseudo-regular elements $C_0, \ldots, C_n \in [A]_{\mathcal{S}}$ such that $B = E_0B_1E_1B_2 \cdots E_{n-1}B_nE_n$ with idempotents $E_i = E(C_i)$. For each E_i, let $A_i \in Y^{\trianglelefteq\binom{d}{r}+2}E$ and $A_i^+ \in E\overline{\langle H\rangle}Y^{\trianglelefteq\binom{d}{r}+2}$ be such that $A_i^+A_i = E$ and $A_iA_i^+ = E_i$ (these exist by 1)). Then

$$B = A_0(A_0^+B_1A_1)(A_1^+B_2A_2) \cdots (A_{n-1}^+B_nA_n)A_n^+.$$

Each $A_i^+B_iA_{i-1}$ is contained in $\overline{\langle H\rangle}$ and $A_n^+ \in E\overline{\langle H\rangle}Y^{\trianglelefteq\binom{d}{r}+2} \subseteq \overline{\langle H\rangle}Y^{\trianglelefteq\binom{d}{r}+2}$, so that we obtain $B \in Y^{\trianglelefteq\binom{d}{r}+2}\overline{\langle H\rangle}Y^{\trianglelefteq\binom{d}{r}+2}$. □

D. Termination and correctness of Algorithm 2

The following lemma forms the basis of the recursive strategy in Algorithm 2. It reduces the problem of computing $\overline{\mathcal{S}}$ to the computation of a suitable set of representatives of the completely pseudo-regular elements.

Lemma 36. *Let $Y \subseteq M_d(K)$ be closed, $r \geq 0$, and suppose Y contains $X \cup \{\, A \in \mathcal{S} : \operatorname{rank}(A) > r \,\}$.*

1) *If B is completely pseudo-regular of rank r, then $[B]_{\mathcal{S}} \subseteq \mathcal{T}(Y, B)$.*
2) *If $T \subseteq M_d(K)$ is closed such that $Y \cup T$ contains every completely pseudo-regular $B \in \mathcal{S}$ with $\operatorname{rank}(B) \geq r$, then*
$$\{\, B \in \mathcal{S} : \operatorname{rank}(B) \geq r \,\} \subseteq \overline{\bigl(Y \cup T\bigr)^{\leq 2\binom{d}{r}+3}}.$$

The claim 1) follows immediately from 2) of Lemma 35. If some element of rank $> r$ is missing from Y, perhaps $[B]_{\mathcal{S}} \not\subseteq \mathcal{T}(Y, B)$, but $\mathcal{T}(Y, B)$ is still computable. We prove 2) of Lemma 36 after Lemma 37.

Several things remain to check; in particular that TRYCLOSE will indeed succeed to compute the closure under certain assumptions on the sets R_s, that FINDCPR will discover new completely pseudo-regular elements, and finally, that loops that increase the size of R_s eventually terminate.

We need two final preparatory lemmas. The first one allows us to find completely pseudo-regular elements. This will be the key ingredient to make FINDCPR work.

Lemma 37. *Let $r \geq 0$ and let $Y, T \subseteq M_d(K)$ be closed such that $X \cup \{\, B \in \mathcal{S} : \operatorname{rank}(B) > r \,\} \subseteq Y$, and set*

$$Y' := \overline{\bigl(Y \cup T\bigr)^{\leq 2\binom{d}{r}+3}}.$$

If there exists $A = A_1 \cdots A_n \in \mathcal{S} \setminus Y'$ with $A_1, \ldots, A_n \in X$ and $\operatorname{rank}(A) \geq r$, then there exist $k < l$ such that the subproduct $A' = A_k \cdots A_l$ is completely pseudo-regular of rank r and not contained in $Y \cup T$.

Proof. Successively grouping together subproducts contained in $Y \cup T$, we find a representation $A_1 \cdots A_n = C_1 \cdots C_t$ with $C_i \in \langle A_1, \ldots, A_n\rangle \cap (Y \cup T)$ and t minimal. By minimality of t, necessarily $C_k \cdots C_l \notin Y \cup T$ for $k < l$. In particular, $\operatorname{rank}(C_k \cdots C_l) = r$. Since $A \notin Y'$, necessarily $t \geq 2\binom{d}{r} + 4$.

Now 2) of Lemma 32 implies that there exist $k < l$ such that $A' := C_k \cdots C_l$ is completely pseudo-regular. □

Proof of Lemma 36, 2). Suppose the claim is false. Then there exists some $A \in \mathcal{S} \setminus Y'$ with $\operatorname{rank}(A) \geq r$. Then Lemma 37 implies that there exists a completely pseudo-regular $B \in \mathcal{S} \setminus (Y \cup T)$ with $\operatorname{rank}(B) \geq r$, contradicting our assumption. □

A second lemma allows us to bound the sizes of the sets R_s, and will ultimately yield termination of the algorithm. Let $R \subseteq M_d(K)$ be a set of completely pseudo-regular matrices. We define a directed graph $G(R)$, whose vertex set is R and having a directed edge $A \to B$ if $\ker(B) \cap \operatorname{im}(A) = 0$. (Loops are permitted, but this shall not make a difference in our considerations.) In the following, 2) should be compared to [22, Proposition 8].

Lemma 38. *1) If A, $B \in G(R)$ are contained in the same strongly connected component (SCC), then $A \sim_{\mathcal{S}} B$.*
2) The graph $G(R)$ has at most $\binom{d}{r}$ SCCs of rank r.

Proof. 1) Observe: if there is an edge $C \to D$ in $G(R)$, then $\ker(DC) = \ker(C)$ and $\operatorname{rank}(D) \geq \operatorname{rank}(DC) = \operatorname{rank}(C)$. So if C, D are two elements of the same SCC, then $\operatorname{rank}(C) = \operatorname{rank}(D)$; if $C \to D$ is an edge, then also $\operatorname{im}(DC) = \operatorname{im}(D)$.

Now let there be paths $A \to C_1 \to \cdots \to C_k \to B$ and $B \to D_1 \to \cdots \to D_l \to A$. Set $Q := BC_k \cdots C_1 A$ and $P := AD_l \cdots D_1 B$. Then $\operatorname{im}(QAP) = \operatorname{im}(B)$ and $\ker(QAP) = \ker(B)$, so that $B \parallel QAP$. Symmetrically, $A \parallel PBQ$.

2) Let $A_1, \ldots, A_k$ be vertices in distinct SCCs of rank r. Define $A_i \geq A_j$ if there is a path from A_i to A_j. This relation is reflexive, transitive, and, since A_i and A_j are in distinct SCCs, anti-symmetric. Thus it is an order relation and we may reindex the matrices in such a way that there is no path from A_j to A_i if $j > i$. In particular, $\ker(A_i) \cap \operatorname{im}(A_j) \neq 0$ for $j > i$ and $\ker A_i \cap \operatorname{im} A_i = 0$. By Lemma 28, $k \leq \binom{d}{r}$. □

Theorem 39. *For a closed set $X \subseteq M_d(K)$ and $\mathcal{S} = \langle X \rangle$, it is possible to compute $\overline{\mathcal{S}}$.*

Proof. We show that Algorithm 2 terminates and outputs $\overline{\mathcal{S}}$.

First note, in TRYCLOSE, the inclusions $X \subseteq Y_s \subseteq \overline{\mathcal{S}}$ and $T_s \subseteq \overline{\mathcal{S}}$ hold for all s. In particular $X \subseteq Y_1 \subseteq \overline{\mathcal{S}}$. If Algorithm 2 terminates, then $Y_1^2 \subseteq Y_1$, and so $Y_1 \subseteq \overline{\mathcal{S}}$ is a closed overmonoid of X contained in $\overline{\mathcal{S}}$, so $\mathcal{S} \subseteq Y_1 \subseteq \overline{\mathcal{S}}$ and thus $Y_1 = \overline{\mathcal{S}}$. Thus only the termination of the algorithm remains to be shown. We start with two observations.

a) In TRYCLOSE, if Y_{s+1} contains $\{\, B \in \mathcal{S} : \operatorname{rank}(B) \geq s + 1 \,\}$ and $Y_{s+1} \cup T_s$ contains all completely pseudo-regular elements of rank s, then Y_s contains $\{\, B \in \mathcal{S} : \operatorname{rank}(B) \geq s \,\}$ by 2) of Lemma 36. Since this condition trivially holds for $s = \overline{\mathrm{r}}(X)$ (as $\{\, B \in \mathcal{S} : \operatorname{rank}(B) \geq r + 1 \,\} = \emptyset$), it suffices to construct the sets T_s so that $Y_{s+1} \cup T_s$ covers the completely pseudo-regular elements of rank $\geq s$, to obtain $\mathcal{S} \subseteq Y_1$ inductively.

b) Throughout the algorithm, R_s is a finite set of completely pseudo-regular elements of rank s. Further, if $\{\, A \in \mathcal{S} : \operatorname{rank}(A) \geq s + 1 \,\} \subseteq Y_{s+1}$, then the elements of R_s are pairwise $\sim_{\mathcal{S}}$-inequivalent. (This follows because any element added to R_s is chosen outside of T_s and 1) of Lemma 36.) Then $|R_s| \leq \binom{d}{s}$ by Lemma 38.
Conversely, if we ever end up with $|R_s| > \binom{d}{s}$ in the algorithm, we must have missed a completely pseudo-regular element of rank $> s$, and we search for such an element (loop at line 6).

To show that the algorithm terminates, we now show:

1) in line 7, the call to FINDCPR always returns a completely pseudo-regular element B of $\mathcal{S}$ of some rank $s' > s$, with B not contained in $Y_{s'+1} \cup T_{s'}$;
2) the loops in lines 4 and 6 terminate.

1) When we call FINDCPR there always exists $s' > s$ and $A \in \mathcal{S} \setminus Y_{s'}$ with $\operatorname{rank}(A) \geq s'$: for the first iteration ($s = 0$), the failed check on line 4 implies $\mathcal{S} \not\subseteq Y_1$. In any other iteration, we have $|R_s| > \binom{d}{s}$, so $\{\, A \in \mathcal{S} : \operatorname{rank}(A) \geq s + 1 \,\} \not\subseteq Y_{s+1}$.

Thus, in FINDCPR, there exists $n \geq 0$ and $s' > s$ such that $X^n \setminus C_{s'} \neq \emptyset$, and the loop will eventually discover such a pair (n, s'). Then $n \geq 2\binom{d}{s'} + 4$, as $X^{\leq 2\binom{d}{s'}+3} \subseteq Y_{s'}$ (lines 13 and 16). We can pick such an element $A = A_1 \cdots A_n \in X \setminus C_{s'}$ (on line 23) using Lemma 17. Lemma 37 gives the existence of a completely pseudo-regular subproduct (chosen on line 24).

2) Consider first the loop on line 6. In each iteration s increases by at least 1 (the rank of B is larger then the value of s passed to FINDCPR). But at latest when $s = r$, we always have $|R_r| \leq \binom{d}{r}$, by observation b), and the loop terminates.

Consider now the outer loop, on line 4. Outside of the loop on line 6, always $|R_s| \leq \binom{d}{s}$ for all s (inside the loop still $|R_s| \leq \binom{d}{s} + 1$). In each iteration we are increasing the size of some R_s by one, while resetting all $R_{s'}$ with $s' < s$ to the empty set. Since $|R_r| \leq \binom{d}{r}$ and R_r is only ever growing, eventually R_r must stabilize. Once this is the case, the algorithm does not modify R_r any more and only touches the sets $R_{r-1}, \ldots, R_1$. At this point R_{r-1} can only ever grow. Thus, eventually, R_{r-1} will also stabilize at $|R_{r-1}| \leq \binom{d}{r-1}$. Inductively we conclude that eventually all the sets $R_{r-1}, \ldots, R_1$ stabilize (there are no more new completely pseudo-regular elements to discover), and the algorithm stops. □

Remark 40 (Efficiency). 1) While the algorithm largely works with linear algebra, and avoids the use of Gröbner bases (which can be computationally inefficient), the function FINDCPR appears to be an obstacle to a reasonably efficient implementation. In particular, in the computation of elements in $X^n \setminus C_{s'}$, the exponent n may become very large (there is no upper bound) and one needs to consider very long products of (generic) matrices. An obvious way of improving the algorithm, is therefore to find a better way of discovering the completely pseudo-regular elements.

2) In FINDCPR, crucially, we choose the elements in $X^n \setminus C_{s'}$ instead of $\overline{X^n} \setminus C_{s'}$ (which would be nicer computationally), to avoid higher rank elements that may potentially appear in the closure (Example 24).

3) We do not get runtime bounds. The problem is a lack of a bound for n in FINDCPR, and the lack of bounds on the number of steps in Algorithm 1.

Remark 41 (Output size)**.** For $X \subseteq M_d(K)$ closed, let $\mathtt{c}(X)$ be the number of irreducible components of X. Let $\mathcal{S} = \overline{\langle X \rangle}$. We sketch a double-exponential upper bound for $\mathtt{c}(\mathcal{S})$ (and therefore also for the linear hull). We only consider $K = \mathbb{Q}$.

First consider the group case (i.e., $\mathrm{GL}_d(\mathbb{Q})$ is dense in X). In this case, we get a double-exponential bound in d that does not depend on X: let $G \coloneqq \mathcal{S} \cap \mathrm{GL}_d(\mathbb{Q})$ and let G^0 be the irreducible component containing I. We need to bound $|G/G^0|$. In Theorem 22, we saw that G/G^0 is a subgroup of $\mathrm{GL}_{d'}(\mathbb{Q})$ for some d'. The embedding arises from applying [8, Theorem II.6.8]. Tracing through [8], in our linear setting, gives

$$d' \le \left(\binom{d^2}{r} + d\right)^2 \le \left(2^{d^2} + d\right)^2 \le 4 \cdot 4^{d^2}$$

(for some r, using that the binomial coefficients sum to 2^{d^2}). Finite subgroups of $\mathrm{GL}_{d'}(\mathbb{Q})$ have cardinality at most $2^{d'} d'!$ if $d' > 10$ and for smaller d' the maximal sizes are also known ([5, Table 1])[10]. So $\mathtt{c}(\mathcal{S}) \le 2^{4 \cdot 4^{d^2}} (4 \cdot 4^{d^2})!$ for all d. In general, one gets a bound that is double-exponential in d, by combining the group case with induction on the recursive strategy Lemma 36 (the bound depends on $\mathtt{c}(X)$).

References

[1] C. Allauzen and M. Mohri, “Efficient algorithms for testing the twins property,” 2003, vol. 8, no. 2, pp. 117–144, weighted automata: theory and applications (Dresden, 2002).

[2] N. Alon, “Combinatorial Nullstellensatz,” 1999, vol. 8, no. 1-2, pp. 7–29, recent trends in combinatorics (Mátraháza, 1995).

[3] J. Bell and D. Smertnig, “Noncommutative rational Pólya series,” *Selecta Math. (N.S.)*, vol. 27, no. 3, pp. Paper No. 34, 34, 2021.

[4] ——, “Computing the linear hull: Deciding sequential? and unambiguous? for weighted automata over fields,” 2023, arXiv version, arXiv:2209.02260.

[5] N. Berry, A. Dubickas, N. D. Elkies, B. Poonen, and C. Smyth, “The conjugate dimension of algebraic numbers,” *Q. J. Math.*, vol. 55, no. 3, pp. 237–252, 2004.

[6] J. Berstel and M. Mignotte, “Deux propriétés décidables des suites récurrentes linéaires,” *Bull. Soc. Math. France*, vol. 104, no. 2, pp. 175–184, 1976.

[7] J. Berstel and C. Reutenauer, *Noncommutative rational series with applications*, ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 2011, vol. 137.

[8] A. Borel, *Linear algebraic groups*, 2nd ed., ser. Graduate Texts in Mathematics. Springer-Verlag, New York, 1991, vol. 126.

[9] N. Bourbaki, *Elements of mathematics. Commutative algebra*. Hermann, Paris; Addison-Wesley Publishing Co., Reading, Mass., 1972, translated from the French.

[10] M. Büchse, H. Vogler, and J. May, “Determinization of weighted tree automata using factorizations,” *J. Autom. Lang. Comb.*, vol. 15, no. 3-4, pp. 229–254, 2010.

[11] C. Choffrut, “Une caractérisation des fonctions séquentielles et des fonctions sous-séquentielles en tant que relations rationnelles,” *Theoret. Comput. Sci.*, vol. 5, no. 3, pp. 325–337, 1977.

[12] T. Colcombet and D. Petrişan, “Automata in the category of glued vector spaces,” in *42nd International Symposium on Mathematical Foundations of Computer Science*, ser. LIPIcs. Leibniz Int. Proc. Inform. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2017, vol. 83, pp. Art. No. 52, 14.

[13] H. Derksen, E. Jeandel, and P. Koiran, “Quantum automata and algebraic groups,” *J. Symbolic Comput.*, vol. 39, no. 3-4, pp. 357–371, 2005.

[14] F. Dörband, T. Feller, and K. Stier, “Sequentiality of group-weighted tree automata,” in *Language and automata theory and applications*, ser. Lecture Notes in Comput. Sci. Springer, Cham, [2021] ©2021, vol. 12638, pp. 267–278.

[15] M. Droste, W. Kuich, and H. Vogler, Eds., *Handbook of weighted automata*, ser. Monographs in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin, 2009.

[16] W. Feit, “Orders of finite linear groups,” in *Proceedings of the First Jamaican Conference on Group Theory and its Applications (Kingston, 1996)*. Univ. West Indies, Kingston, [1996], pp. 9–11.

[17] E. Filiot, R. Gentilini, and J.-F. Raskin, “Quantitative languages defined by functional automata,” *Log. Methods Comput. Sci.*, vol. 11, no. 3, pp. 3:14, 32, 2015.

[18] S. Friedland, “The maximal orders of finite subgroups in $\mathrm{GL}_n(\mathbf{Q})$,” *Proc. Amer. Math. Soc.*, vol. 125, no. 12, pp. 3519–3526, 1997.

[19] Z. Fülöp, D. Kószó, and H. Vogler, “Crisp-determinization of weighted tree automata over strong bimonoids,” *Discrete Math. Theor. Comput. Sci.*, vol. 23, no. 1, pp. Paper No. 18, 44, 2021.

[20] G.-M. Greuel and G. Pfister, *A* **Singular** *introduction to commutative algebra*, extended ed. Springer, Berlin, 2008, with contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.

[21] I. N. Herstein, *Noncommutative rings*, ser. Carus Mathematical Monographs. Mathematical Association of America, Washington, DC, 1994, vol. 15, reprint of the 1968 original, With an afterword by Lance W. Small.

[22] E. Hrushovski, J. Ouaknine, A. Pouly, and J. Worrell, “Polynomial invariants for affine programs,” in *LICS ’18—33rd Annual ACM/IEEE Symposium on Logic in Computer Science*. ACM, New York, 2018, p. 10.

[23] D. Kirsten, “Decidability, undecidability, and PSPACE-completeness of the twins property in the tropical semiring,” *Theoret. Comput. Sci.*, vol. 420, pp. 56–63, 2012.

[24] D. Kirsten and S. Lombardy, “Deciding unambiguity and sequentiality of polynomially ambiguous min-plus automata,” in *STACS 2009: 26th International Symposium on Theoretical Aspects of Computer Science*, ser. LIPIcs. Leibniz Int. Proc. Inform. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2009, vol. 3, pp. 589–600.

[25] D. Kirsten and I. Mäurer, “On the determinization of weighted automata,” *J. Autom. Lang. Comb.*, vol. 10, no. 2-3, pp. 287–312, 2005.

[26] P. Kostolányi, “Determinisability of unary weighted automata over the rational numbers,” *Theoret. Comput. Sci.*, vol. 898, pp. 110–131, 2022.

[27] J. Kuzmanovich and A. Pavlichenkov, “Finite groups of matrices whose entries are integers,” *Amer. Math. Monthly*, vol. 109, no. 2, pp. 173–186, 2002.

[28] E. Lefaucheux, J. Ouaknine, D. Purser, and J. Worrell, “Porous invariants,” in *Computer aided verification. Part II*, ser. Lecture Notes in Comput. Sci. Springer, Cham, [2021] ©2021, vol. 12760, pp. 172–194.

[29] S. Lombardy and J. Sakarovitch, “Sequential?” *Theoret. Comput. Sci.*, vol. 356, no. 1-2, pp. 224–244, 2006.

[30] M. Mohri, “Finite-state transducers in language and speech processing,” *Comput. Linguist.*, vol. 23, no. 2, pp. 269–311, 1997.

[31] ——, “Chapter 6: Weighted automata algorithms,” in *Handbook of weighted automata*, ser. Monogr. Theoret. Comput. Sci. EATCS Ser. Springer, Berlin, 2009, pp. 213–254.

[32] M. Mohri and M. D. Riley, “A disambiguation algorithm for weighted automata,” *Theoret. Comput. Sci.*, vol. 679, pp. 53–68, 2017.

[33] K. Nosan, A. Pouly, S. Schmitz, M. Shirmohammadi, and J. Worrell, “On the Computation of the Zariski Closure of Finitely Generated Groups of Matrices,” 2021, preprint.

[34] J. Okniński, “Strongly π-regular matrix semigroups,” *Proc. Amer. Math. Soc.*, vol. 93, no. 2, pp. 215–217, 1985.

[35] ——, “Linear representations of semigroups,” in *Monoids and semigroups with applications (Berkeley, CA, 1989)*. World Sci. Publ., River Edge, NJ, 1991, pp. 257–277.

[36] ——, *Semigroups of matrices*, ser. Series in Algebra. World Scientific Publishing Co., Inc., River Edge, NJ, 1998, vol. 6.

[37] E. Paul, “Finite sequentiality of unambiguous max-plus tree automata,” *Theory Comput. Syst.*, vol. 65, no. 4, pp. 736–776, 2021.

[38] M. S. Putcha, *Linear algebraic monoids*, ser. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1988, vol. 133.

[39] L. E. Renner, *Linear algebraic monoids*, ser. Encyclopaedia of Mathematical Sciences. Springer-Verlag, Berlin, 2005, vol. 134, invariant Theory and Algebraic Transformation Groups, V.

[40] J. Sakarovitch, *Elements of automata theory*. Cambridge University Press, Cambridge, 2009, translated by Reuben Thomas.

[41] T. Stacks project authors, “The stacks project,” https://stacks.math.columbia.edu, 2019.

[10] This theorem of Feit depends on unpublished work. Friedland [18] gives a proof for large d. This yields *some* double-exponential bound.

Appendix

A. Other fields

In the main text we restricted the field K to be a number field (that is, a finite field extension of $\mathbb{Q}$). This restriction was made for simplicity of exposition. In truth our approach does not impose restrictions on the nature of the field, except for the obvious necessity of the field being *computable*, by which we mean (informally) that elements of the field can be represented exactly with finite memory, and equality comparisons between elements as well as the operations $+$, $\cdot$, $-$, $/$ can be computed exactly and in finite time. This allows us to carry out linear algebra (Gaussian elimination) and computations with polynomials over such a field.

The rational numbers and finite fields of prime order (fields of the form $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p a prime number) are computable. Finite-dimensional field extensions of computable fields are again computable when given by, e.g., generators and relations, or by a basis together with structure coefficients explaining the multiplication of basis elements. Fields such as $\mathbb{R}$ or $\mathbb{C}$ are not computable in this sense, however the field of algebraic numbers $\overline{\mathbb{Q}}$ is computable (and implemented, for instance, in the SageMath computer algebra system). The field $\mathbb{Q}(\pi)$ is computable, because π is transcendental and therefore $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$ is a rational function field. The field $\mathbb{Q}(\pi, e)$ is not known to be computable, because it is an open question in transcendence theory whether π and e are algebraically independent over $\mathbb{Q}$.

When considering a weighted automaton, we may always work over fields that are *finitely generated* (but not necessarily finite-dimensional) over their prime field ($\mathbb{Q}$ or $\mathbb{F}_p$, depending on the characteristic). Namely, we can take the field generated by all the entries of the vectors and matrices appearing in a linear representation of the automaton. Let K be a finitely generated field. Then K is a finite field, a number field, or a finitely generated extension of a finite or a number field K_0. In the latter case, K is the field of fractions of an affine K_0-algebra R. We shall assume that R is given by specifying generators and relations for R over K_0. That makes R, and therefore K, computable.

We now outline, section by section, which changes need to be made to deal with finitely generated fields.

1) Section II: If K is a finite field, then every vector space can be covered by a finite number of one-dimensional spaces (lines through the origin). In this case, the irreducible closed sets in the linear Zariski topology are the vector spaces of dimension ≤ 1. It follows that the linear hull always has dimension ≤ 1, and it becomes trivial to compute it. As a consequence, one recovers the well-known result that a weighted automaton over a finite field is always determinizable.

If K is an infinite field, the results in section II remain valid as stated.

2) Section III: The algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ has to be replaced by the algebraic closure K^{alg} of K throughout. While the conclusion of Theorem 10 remains true, several of the lemmas leading up to it, as well as the proof of Theorem 10 itself, have to be adapted for the general case.

Write $\mu(K^{\mathrm{alg}})$ for the group of all roots of unity. If $\operatorname{char} K = p > 0$, then p does not divide the order of any root of unity. For an integer $0 \neq n \in \mathbb{Z}$, let $\mathsf{v}_p(n) \in \mathbb{N}_0$ denote the p-adic valuation, i.e., the number of times that p divides n.

Lemma 42. *Let K be a field. Let $A \in \mathrm{GL}_d(K)$.*

1) *Assume that for any two eigenvalues λ, $\lambda' \in K^{\mathrm{alg}}$ of A for which $\lambda/\lambda' \in \mu(K^{\mathrm{alg}})$, it holds that $\lambda = \lambda'$. Then a vector space $V \subseteq K^d$ is A-invariant if and only if it is A^n-invariant for all $n \geq 1$ with $\operatorname{char} K \nmid n$.*
2) *If $\operatorname{char} K = p > 0$, and $V \subseteq K^d$ is A^{p^n}-invariant for some $n \geq 0$, then V is A^{p^e}-invariant for $e = \mathsf{v}_p((d-1)!)$.*

Proof. Without restriction, assume $K = K^{\mathrm{alg}}$.

1) The proof is the same as the one of Lemma 11. The extra assumption $\operatorname{char} K \nmid n$ (which is automatically satisfied if $\operatorname{char} K = 0$) is necessary and sufficient for a primitive n-th root of unity $\zeta \in K^{\mathrm{alg}}$ to exist.

2) Using the direct-sum decomposition of V along generalized eigenspaces, we can, as in the proof of Lemma 11, restrict to the case where A has a single eigenvalue λ (if $(\lambda/\lambda')^{p^n} = 1$, then $\lambda = \lambda'$). Then $A - \lambda = N$ for some matrix N with $N^d = 0$. Now

$$A^{p^k} = (\lambda + N)^{p^k} = \sum_{i=0}^{\min\{d-1,p^k\}} \binom{p^k}{i} \lambda^{p^k - i} N^i.$$

So, if $k \geq e \coloneqq \mathsf{v}_p((d-1)!)$, then $\binom{p^k}{i} = 0$ for $i \in [1, d-1]$ and $A^{p^k} = \lambda^{p^k}$. Thus, if V is A^{p^k}-invariant for some $k \geq 0$, then it is A^{p^e}-invariant. □

Lemma 43. *Let K be a finitely generated field. There exists a computable $N_0 = N_0(d, K)$ such that, for every finite field extension L/K with $[L : K] \leq d$ and every root of unity $\zeta \in L$, one has $\zeta^{N_0} = 1$ and moreover $\operatorname{char} K \nmid N_0$.*

Proof. This makes essential use of the fact that K is a finitely generated field. Suppose first $K = R = K_0$. Then either K is a finite field, in which case the claim is trivial, or a number field, in which case the claim follows from Lemma 12.

Now consider the general case. By effective Noether normalization [20, Chapter 3.4], we can compute transcendental $x_1, \ldots, x_n$ over K_0, such that R is a finite module over $K_0[x_1, \ldots, x_n]$. Then $x_1, \ldots, x_n$ is a transcendence basis for K/K_0. From the generating set of R as a $K_0[x_1, \ldots, x_n]$-algebra, we can compute a bound m for the degree $[K : K_0(x_1, \ldots, x_n)]$. If L is an extension of degree d of K, then every element of L that is algebraic over K_0 has degree $\leq md$ over K_0. Thus we can take $N_0(d, K) = N_0(md, K_0)$. □

Lemma 44. *Let K be a finitely generated field. Let $p = \operatorname{char} K$. Let $N \coloneqq N(d, K) \coloneqq p^e N_0(d^2, K)$ with $e = \mathsf{v}_p((d-1)!)$. Let $A \in \mathrm{GL}_d(K)$, and let $V \subseteq K^d$ be a vector subspace. If V is A^n-invariant for some $n \geq 1$, then V is A^N-invariant.*

Proof. Let λ, $\lambda' \in K^{\mathrm{alg}}$ be eigenvalues of A and let $N_0 = N_0(d^2, K)$. Since λ, λ' are both roots of the characteristic polynomial, which has degree d, the extension $K(\lambda, \lambda')/K$ has degree at most d^2. If there exists a root of unity ζ such that $\lambda/\lambda' = \zeta$, then $\zeta \in K(\lambda, \lambda')$ and hence $\zeta^{N_0} = 1$. Thus A^{N_0} satisfies the assumption of 1) of Lemma 42.

Now suppose that V is A^n-invariant with $n \geq 1$ and let $n = p^k m$ with $k \geq 0$ and m coprime to p. Replacing n by a multiple of itself if necessary, we may assume $k \geq e$ and $N_0 \mid m$. Applying 2) of Lemma 42 to the matrix A^m raised to the power p^k, the space V is $(A^m)^{p^e}$-invariant. Using $(A^m)^{p^e} = (A^{p^e})^m$ and $N_0 \mid m$, we can now apply 1) of Lemma 42 to deduce that V is $A^{p^e N_0}$-invariant. □

Now the proof of Theorem 10 goes through as in the number field case, with Lemma 13 replaced by Lemma 44.

3) Section IV: The proof of Lemma 17 uses that K is infinite, on the one hand to be able to find arbitrarily large subsets, and on the other to ensure that a nonzero polynomial does not vanish everywhere. However, the conclusion of Lemma 17 remains trivially true for finite fields.

The conclusion of Lemma 19 is true over any field, but the stated proof requires the field to be infinite, to ensure that V, W are also irreducible in the Zariski topology. If K is a finite field, and V and W are closed and irreducible subsets in the linear Zariski topology, then V and W are the zero space or one-dimensional vector spaces. In the latter case, they are not irreducible in the Zariski topology (being a finite union of their finitely many points). However, clearly VW is again the zero space (if one of V and W is zero) or a one-dimensional space (if V and W are one-dimensional), so the conclusion of Lemma 19 holds trivially.

4) Section V: No changes are necessary.

B. Integral domains that are not fields

Suppose that R is not a field but only a (commutative) domain (such as $\mathbb{Z}$) and consider the problem of deciding determinizability and ambiguity for R-automata. Of course, one can carry out the procedure over the quotient field $K = \mathbf{q}(R)$ of R. However the existence of a deterministic K-automaton equivalent to the initial one, may not imply the existence of a deterministic R-automaton. Similar considerations apply for unambiguous automata. Luckily, if R is completely integrally closed we obtain the following.

Corollary 45. *Let R be a finitely generated completely integrally closed domain and $\mathcal{A}$ an R-automaton. Then it is decidable if $\mathcal{A}$ is equivalent to an unambiguous R-automaton. In this case a corresponding unambiguous R-automaton is computable.*

Sketch of proof. By [3, Theorem 1.2], the R-automaton $\mathcal{A}$ is equivalent to an unambiguous R-automaton, if and only if $\mathcal{A}$ is equivalent to an unambiguous K-automaton over K. The latter property can be decided by Theorem 1.

Suppose $\mathcal{A}'$ is an unambiguous K-automaton that is equivalent to $\mathcal{A}$ (over K) and let $S \in R\langle\langle X \rangle\rangle$ be the corresponding rational series. Using [3, Proposition 6.1] we get a representation of S as an unambiguous K-rational series, and by [3, Proposition 9.1] we obtain a representation as an unambiguous rational series over R, which yields an R-automaton. □

Unfortunately, passing through an unambiguous rational series as in the previous corollary, and back to an unambiguous automaton, it does not seem to be clear how to preserve the deterministic property. However, if R is a principal ideal domain (PID) there is a way to pass to R.

Corollary 46. *Let R be a finitely generated PID and $\mathcal{A}$ a R-automaton. Then it is decidable if $\mathcal{A}$ is equivalent to a deterministic R-automaton. In this case a corresponding deterministic R-automaton is computable.*

Sketch of Proof. We claim that this again reduces to the same question over K. Clearly, if $\mathcal{A}$ is equivalent to a deterministic R-automaton, it is equivalent to a deterministic K-automaton. Suppose conversely that $\mathcal{A}$ is equivalent to a deterministic K-automaton. Then the linear hull of every minimal K-automaton is at most one-dimensional [3, Theorem 1.3].

Let (u, μ, v) be a minimal linear representation of $\mathcal{A}$ over K. By [7, Theorem 7.1.1] we may assume that in fact $u \in R^{1\times d}$, $\mu(w) \in M_d(R)$, and $v \in R^d$ for all $w \in \Sigma^*$. Let $\Omega := \{\, u\mu(w) : w \in \Sigma^* \,\}$. Now there are $a_1, \ldots, a_n \in K^{1\times d}$ such that $\Omega \subseteq (Ka_1 \cup \cdots \cup Ka_n) \cap R^{1\times d}$. We may take the coordinates of each a_i to be in R and to be coprime. Then $\Omega \subseteq Ra_1 \cup \cdots \cup Ra_n$. This yields an R-deterministic automaton equivalent to $\mathcal{A}$ (on n states) [29, Proposition 5]. □

Corollaries 45 and 46 apply to the ring of integers $\mathbb{Z}$, and so Problem 1 of [29] also has a positive answer in this case. The restriction to finitely generated domains is again so that basic computations (and the linear algebra in Corollary 46) can indeed be carried out.

C. Derivation of bounds

We sketch how to derive the bounds on the output size (Remark 41) in the case $K = \mathbb{Q}$. As a first step, we know that a quotient of a linear algebraic subgroup of GL_d by a normal subgroup is again linear algebraic (so, it can be be embedded in some $\mathrm{GL}_{d'}$). This is a standard result in the theory of algebraic groups [8, Theorem II.6.8], but unfortunately, making d' explicit requires tracing through the proofs. We sketch how to do this, following the proof in Borel's book [8].

We are ultimately interested in the K-rational points $G(K)$ of a linear algebraic group G, but to obtain the desired result, it is necessary to work in the language of algebraic geometry. In a sense, this also means to consider the points $G(K^{\mathrm{alg}})$ over the algebraic closure K^{alg} of K. However, the varieties will be defined over K and morphisms will be K-morphisms (see [8, §11] for the precise definitions), so the results then descend to the group of K-rational points.

Consider the linear algebraic group GL_d. It is defined over our base field K, having the coordinate ring

$$K[\mathrm{GL}_d] = K[x_{ij}, \det(x_{ij})^{-1}] \cong K[x_{ij}, t]/(t\det(x_{ij}) - 1).$$

(here i, j range over $[1, d]$).

The group $\mathrm{GL}_d(K^{\mathrm{alg}})$ acts on $K^{\mathrm{alg}}[\mathrm{GL}_d]$ by left translation, that is, for $g \in \mathrm{GL}_d(K^{\mathrm{alg}})$ and $f \in K^{\mathrm{alg}}[\mathrm{GL}_d]$, the action is defined by $(g, f) \mapsto \lambda_g f$ with $\lambda_g f(x) = f(g^{-1}x)$ for all $x \in \mathrm{GL}_d(K^{\mathrm{alg}})$ [8, §II.1.9]. Here $g^{-1}x$ is just the usual the matrix product.

Let $L \subseteq K^{\mathrm{alg}}[\mathrm{GL}_d]$ be the d^2-dimensional K^{alg}-vector space spanned by $\{ x_{ij} : i, j \in [1, d] \}$. (This vector space is *defined over* K, in the sense of [8, §11.1].) Then L is invariant under the $\mathrm{GL}_d(K^{\mathrm{alg}})$-action: taking $f = x_{ij}$ and g, $y \in \mathrm{GL}_d(K^{\mathrm{alg}})$ with $g^{-1} = (g'_{ij})$, $y = (y_{ij})$, we have

$$\lambda_g x_{ij}(y) = x_{ij}(g^{-1}y) = \sum_{\nu=1}^{d} g'_{i\nu} y_{\nu j} = \sum_{\nu=1}^{d} g'_{i\nu} x_{\nu j}(y),$$

so $\lambda_g x_{ij} \in \mathrm{span}\{ x_{1j}, \dots, x_{dj} \} \subseteq L$. By definition, the space L contains all homogeneous linear polynomials in x_{ij}.

Now consider the case where $G \leq \mathrm{GL}_d$ is a subgroup which is defined as the vanishing set of a set of homogeneous linear polynomials in the x_{ij} and with coefficients in K (this is the situation we are dealing with in section IV). Solving the linear system, we obtain a subset $I \subseteq [1, d]^2$ such that the $\{ x_{ij} : (i, j) \in I \}$ form a set of free variables for the system. The coordinate ring $K[G]$ is he quotient of $K[\mathrm{GL}_d]$ by these equations. We may think of it as

$$K[G] = K[x_{ij}, f(x_{ij})^{-1}] \cong K[x_{ij}, t]/(tf(x_{ij}) - 1),$$

where now $(i, j) \in I$ and $f(x_{ij})$ is a polynomial in x_{ij} with $(i, j) \in I$, obtained from the determinant by substituting the solution of the linear system. As in the case $G = \mathrm{GL}_d$ before, the group $G(K^{\mathrm{alg}})$ acts on $K^{\mathrm{alg}}[G]$ by left translation, and we have a $G(K^{\mathrm{alg}})$-invariant vector subspace L_G spanned by $\{ x_{ij} : (i, j) \in I \}$ and with $\dim(L_G) = |I| \leq d^2$.

The following is a version of [8, Theorem II.6.8], restricted to our setting, that gives an explicit bound on the dimension of a matrix group that G/N can be embedded in.

Proposition 47. *Let $G \leq \mathrm{GL}_d$ be a K-subgroup. Let $N \subseteq G$ be a closed normal K-subgroup, defined as a K-variety in G by homogeneous linear polynomials in the matrix entries $\{ x_{ij} : (i, j) \in I \}$, with coefficients in K. Then there exists $r \in [1, d]$ such that G/N is an affine K-subgroup of $\mathrm{GL}_{d'}$ and*

$$d' \leq \left(\binom{d^2}{r} + d \right)^2 \leq (2^{d^2} + d)^2.$$

Sketch of Proof. The vanishing ideal $J \subseteq K^{\mathrm{alg}}[G]$ of H is generated by the homogeneous linear polynomials defining H. Therefore, the finite-dimensional G-invariant subspace L_G of $K^{\mathrm{alg}}[G]$ contains this generating set of J. Let $W = L_G \cap J$ and $r = \dim(W)$. Put $E = (\bigwedge^r V) \oplus (K^{\mathrm{alg}})^d$. Then

$$\dim_{K^{\mathrm{alg}}}(E) = \binom{|I|}{r} + d \leq \binom{d^2}{r} + d.$$

Following the proof of [8, Theorem II.5.1], this gives an immersive representation $\alpha : G \to \mathrm{GL}(E)$ (defined over K) and a line $D = \bigwedge^r V \subseteq E$ satisfying the conclusions of [8, Theorem II.5.1] with respect to $H = N$. As in [8, Theorem II.5.6], this can be improved to $N = \ker(\alpha)$ (and the analogous condition $\mathfrak{n} = \ker(d\alpha)$ on the associated derivation), by replacing E by a subspace E' of $\mathrm{GL}(E)$ (cf. the third paragraph of the proof of [8, Theorem II.5.6]). Then $\dim(E') \leq \dim(E)^2$.

Finally, the proof of [8, Theorem II.6.8] shows that G/N is an affine K-subgroup of $\mathrm{GL}(E')$. □

Since the morphism in the previous proposition is a K-morphism, it gives rise to an embedding of K-rational points $(G/N)(K) \subseteq \mathrm{GL}_{d'}(K)$. In the output of Algorithm 1, the subgroup N is the irreducible component of G containing the identity, and G/N is finite. The number of irreducible components of the output is $|(G/N)(K)|$. We have now seen that $(G/N)(K)$ is a finite subgroup of $\mathrm{GL}_{d'}(K)$ with explicitly bounded d', so it suffices to bound the size of finite subgroups of $\mathrm{GL}_{d'}(K)$.

To do so, we now restrict to $K = \mathbb{Q}$. By a theorem of Feit [16], finite subgroups of $\mathrm{GL}_{d'}(\mathbb{Q})$ have cardinality at most $2^{d'} d'!$ if $d' > 10$. For $d' \leq 10$, Feit also classified the finite subgroups of maximal cardinality [5, Table 1]. Unfortunately, the theorem of Feit depends on unpublished work of Weisfeiler (see the introduction of [18] or [27, §5, §6] for a discussion). Let $X \subseteq M_d(K)$ be closed such that $X \cap \mathrm{GL}_d(K)$ is dense in X. Set $\mathcal{S} = \langle X \rangle$. Under the assumption that the Feit result holds, one obtains

$$\mathsf{c}(\overline{\mathcal{S}}) \leq 2^{4 \cdot 4^{d^2}} (4 \cdot 4^{d^2})!$$

for all d by bounding $(2^{d^2} + d)^2 \leq 4 \cdot 4^{d^2}$. (This also works for $d \leq 10$ because the bound is sufficiently large compared to the cardinalities of finite subgroups listed in [5, Table 1].) Of course this bound is not sharp, e.g., for $d = 1$ it gives $\approx 1.3 \cdot 10^{18}$, whereas in this case actually $\mathsf{c}(\overline{\mathcal{S}}) = 1$.

Avoiding the use of unpublished work, independently of the theorem of Feit, Friedland [18] uses a different (published) result of Weisfeiler to show that a finite subgroup of $\mathrm{GL}_d(\mathbb{Q})$ has cardinality $\leq 2^d d!$ for all sufficiently large d. From this result one gets the existence of *some* double-exponential bound for $\mathsf{c}(\overline{\mathcal{S}})$, but not an explicit one. In any case, Weisfeiler's results, and hence these bounds, depend on the classification of finite simple groups.

To extend a bound to different fields K, it would be necessary to understand the maximal cardinality of finite subgroup of $\mathrm{GL}_{d'}(K)$.

Semigroup case. In the general (semigroup) case we get a bound on the output size by combining the bound for the group case with the recursive strategy of Lemma 36. Here it is no longer possible to obtain a bound that is independent of the size of the input set (and that only depends on the dimension d). To see this, consider a finite subset $M \subseteq K$ and let

$$X = \bigcup_{m \in M} \mathrm{span} \left\{ \begin{pmatrix} 1 & m \\ 0 & 0 \end{pmatrix} \right\} \subseteq M_2(K),$$

which is a union of $|M|$ pairwise distinct one-dimensional vector spaces, so $\mathsf{c}(X) = |M|$. One checks easily that X is a semigroup.

Let us start with some easy observations: if $X, Y \subseteq M_d(K)$ are closed sets, then $\mathsf{c}(\overline{XY}) \leq \mathsf{c}(X)\,\mathsf{c}(Y)$. Thus

$$\mathsf{c}(\overline{X^{\leq n}}) \leq \sum_{i=1}^{n} \mathsf{c}(X)^i \leq n\,\mathsf{c}(X)^n \leq \mathsf{c}(X)^{n+1},$$

and also $\mathsf{c}(\overline{X^{\trianglelefteq n}}) \leq 1 + n\,\mathsf{c}(X)^n \leq \mathsf{c}(X)^{n+1}$.

Now we can bound the size of the sets $\mathcal{T}(Y, A)$ (page 8): Assume that $C(d)$ is the maximal size of a finite subgroup of $M_d(K)$. Then $\mathsf{c}(\overline{\langle \mathcal{T}_0(Y, A)\rangle}) \leq C(r)$ (with $r = \operatorname{rank}(A)$), and

$$\mathsf{c}(\mathcal{T}(Y, A)) \leq C(r)\,\mathsf{c}(Y)^{2\binom{d}{r}+4}.$$

Looking at TryClose and keeping in mind Lemma 38, we get

$$\mathsf{c}(T_s) \leq \binom{d}{s} C(s)\,\mathsf{c}(Y_s)^{2\binom{d}{r}+4} \leq 2^d C(d)\,\mathsf{c}(Y_s)^{2^d+4},$$

and

$$\begin{aligned} \mathsf{c}(Y_s) &\leq \big(\mathsf{c}(Y_{s+1}) + \mathsf{c}(T_s)\big)^{2\binom{d}{s}+3} \\ &\leq \big(\mathsf{c}(Y_{s+1}) + 2^d C(d)\,\mathsf{c}(Y_s)^{2^d+4}\big)^{2^d+3}. \end{aligned}$$

Suppose $C(d)$ satisfies a double-exponential bound, i.e., $C(d) \leq 2^{2^{Q(d)}}$ for some polynomial $Q(s)$. Then also $\mathsf{c}(Y_s)$ satisfies a double exponential bound, i.e.,

$$\mathsf{c}(Y_s) \leq \mathsf{c}(Y_{s+1})^{2^{P_0(d)}},$$

for a suitable polynomial $P_0(d)$ (which does not depend on Y_{s+1}). Inductively, we get

$$\mathsf{c}(\overline{\mathcal{S}}) = \mathsf{c}(Y_1) \leq \mathsf{c}(X)^{2^{(d-1)P_0(d)}}.$$

So altogether we obtained the following.

Proposition 48. *If $X \subseteq M_d(\mathbb{Q})$ is a closed set and $\mathcal{S} = \langle X\rangle$, then the number of components $\mathsf{c}(\overline{\mathcal{S}})$ of $\overline{\mathcal{S}}$ can be bounded by*

$$\mathsf{c}(\overline{\mathcal{S}}) \leq \mathsf{c}(X)^{2^{P(d)}},$$

with $P(d)$ a suitable polynomial. A similar upper bound holds for the number of components of the linear hull of a $\mathbb{Q}$-automaton.

The conclusion holds over any field K where one has a bound on cardinality of a finite subgroup of $\mathrm{GL}_d(K)$ that is double-exponential in d.