


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

Jason P. Bell 

Department of Pure Mathematics, University of Waterloo, Canada

Daniel Smertnig 

Institute for Mathematics and Scientific Computing, NAWI Graz, University of Graz, Austria

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 sequential (deterministic) automaton, respectively, an unambiguous automaton. We show how to compute the linear hull, and thus prove that it is decidable whether or not a given automaton over a (finitely generated) field is equivalent to a sequential [unambiguous] one. In these cases we are also able to compute an equivalent sequential [unambiguous] automaton. The results extend to some commutative domains, in particular PIDs. This resolves a problem posed in a 2006 survey by Lombardy and Sakarovitch.

2012 ACM Subject Classification Theory of computation → Formal languages and automata theory → Automata extensions → Quantitative automata

Keywords and phrases weighted automata, determinization, sequential, unambiguous, linear hull

1 Introduction

Every unweighted (finite) automaton is equivalent to a *deterministic* automaton (which are also called *sequential* or *subsequential* [35, Remark V.1.2] automata in the weighted case), and there is a determinization procedure to find such an automaton. For automata with weights in a semiring K , 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 [35, Definition I.1.11]. For trim automata (i) and (ii) are equivalent and one may be omitted. Sequential K -automata are unambiguous, but not every unambiguous K -automaton is equivalent to a sequential 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} .

- **Sequential?** Is there a sequential 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 [10, 25, 1, 21, 20, 19, 15, 27]; the surveys [24, 26] are a good starting point. Similar question have been studied for weighted tree automata [9, 12, 16, 32]. 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 [24, Problem 1]. For unary alphabets and $K = \mathbb{Q}$, the problem **Sequential?** is decidable by a recent result of Kostolányi [22]. In the same setting **Unambiguous?** is decidable by a result of Berstel and Mignotte [5, Théorème 3] together with a classical theorem of Pólya [6, 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 sequential, 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, which makes its computability a non-trivial problem.

We present a method to compute the linear hull of a weighted automaton over (essentially¹) any field (Theorem 32). Together with the main theorems of [3], this shows that the problems **Sequential?** and **Unambiguous?** are decidable over (essentially) any field and any finite alphabet (Theorem 36). Furthermore, our work yields an algorithm to compute an equivalent unambiguous, respectively, sequential weighted automaton if it exists.

The key point is the computation of the linear Zariski closure of a subsemigroup of $M_d(K)$ 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 [18], which builds on the case for groups by Derksen, Jeandel, and Koiran [11]; see also [28]. While it would be possible to first compute the Zariski closure and then compute the linear Zariski closure from it, we present a solution working directly with the linear Zariski topology, relying on linear algebra instead of Gröbner bases as much as possible. This is a more natural approach for the problem at hand, because it is really largely a problem about vector spaces. Furthermore, one can expect a practical implementation to be simpler; in particular, it is unnecessary to compute in extension fields. Unfortunately, it appears impossible to stay completely within the linear realm, as the rank of matrices plays a crucial role in detecting subgroups of the semigroup. However, the need to leave the linear world is restricted to applications of the elementary Lemma 5.

We do not prove 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 (Remark 34); by comparison, in the unary case, the algorithm of Kostolányi needs at most $O(d^3)$ operations. Our results also partially extend to commutative domains R ; in particular, the results hold for $R = \mathbb{Z}$ (Corollaries 37 and 38).

Throughout the paper, let K be a field and $d \geq 0$. 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 $[a, b] := \{x \in \mathbb{Z} : a \leq x \leq b\}$ is the discrete interval. Background on weighted automata and rational series can be found in [6, 13, 35].

2 The linear Zariski topology

Let K be embedded in an algebraic closure K^{alg} . We make use of a linear version of the Zariski topology introduced in [3, Section 3]. Background on irreducible and noetherian topological spaces can be found in [8, §II.4.1 and §II.4.2] and [36, Sections 004U and 0050].

► **Definition 1.** *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. The vector space V together with the linear Zariski topology is a noetherian topological space, behaving quite similar to the (usual) Zariski topology. In particular, every closed set can be expressed uniquely as a finite union of

¹ There is the obvious issue that one may not be able to compute in the ground field in an effective manner. We skirt this issue by always working in finitely generated fields; in principle it is always possible to reduce to this case by passing to the field generated by all the coefficients of the automaton.

its irreducible components. If K is infinite, then the irreducible closed sets of V are precisely the vector subspaces. If K is finite, they are the vector subspaces of dimension at most one.

For a subset $X \subseteq M_d(K)$ we write $\bar{X} \subseteq M_d(K)$ for its closure in the *linear* Zariski topology. The closure in the usual (classical) Zariski topology is denoted by $\tilde{X} \subseteq M_d(K^{\text{alg}})$. We usually consider the Zariski topology over the algebraic closure, whereas for the linear Zariski topology we work over K itself. Whenever we don't specify the topology, we mean the linear Zariski topology.

For vector subspaces $V, W \subseteq M_d(K)$ we distinguish the pairwise product

$$VW := \{vw : v \in V, w \in W\},$$

which in general is not a vector space, and the product of vector spaces

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

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

► **Lemma 2.** *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.*

Proof. The sets $V, W \subseteq M_d(K)$ are also closed and irreducible in the Zariski topology. In the Zariski topology the multiplication map $\mu: M_d(K) \times M_d(K) \rightarrow M_d(K), (A, B) \mapsto AB$ is continuous, and hence $\mu(V, W) = VW$ is irreducible. Then VW is also irreducible in the, coarser, linear Zariski topology. Thus the same is true for the closure \overline{VW} . Therefore \overline{VW} is a vector space. Since $V \cdot W$ is the smallest vector space containing VW , we have $\overline{VW} = V \cdot W$.

If K is infinite, the irreducibility follows from \overline{VW} being a vector space. If K is finite then $\dim V = \dim W \leq 1$. Then $VW = V \cdot W = \overline{VW}$ and therefore also $\dim \overline{VW} \leq 1$. ◀

► **Remark 3.** The multiplication map μ is *not* continuous in the linear Zariski topology. It is also possible to prove the lemma directly, without resorting to the Zariski topology, by showing $\overline{VW} = V \cdot W$ by hand.

► **Lemma 4.** *Let $\mathcal{S} \subseteq M_d(K)$ be a subsemigroup.*

1. *The closure $\bar{\mathcal{S}}$ is a semigroup.*
2. *If $\bar{\mathcal{S}} \cap \text{GL}_d(K) \neq \emptyset$, then $\bar{\mathcal{S}} \cap \text{GL}_d(K)$ is a linear algebraic group.*

Proof. (1) Let $\bar{\mathcal{S}} = Z_1 \cup \dots \cup Z_l$ with Z_j the irreducible components of $\bar{\mathcal{S}}$. For $j \in [1, l]$ let $\mathcal{S}_j := Z_j \cap \mathcal{S}$. Then \mathcal{S}_j is irreducible and dense in Z_j . For every $s \in \mathcal{S}$ also $s\mathcal{S}_j \subseteq \mathcal{S} \subseteq \bar{\mathcal{S}}$. Since $s\mathcal{S}_j$ is irreducible, there exists $k \in [1, l]$ with $s\mathcal{S}_j \subseteq Z_k$. Since multiplication by s is linear, hence continuous, also $sZ_j = \overline{s\mathcal{S}_j} \subseteq Z_k$.

Now fix $i, j \in [1, l]$. We have to show $Z_i Z_j \subseteq Z_k$ for some $k \in [1, l]$. For $k \in [1, l]$ define $V_k = \{s \in Z_i : sZ_j \subseteq Z_k\}$. Observe that V_k is a vector subspace of Z_i . By what we just showed $Z_i = V_1 \cup \dots \cup V_l$. By irreducibility, there is a k with $Z_i = V_k$, and hence $Z_i Z_j \subseteq Z_k$.

(2) Clearly $\bar{\mathcal{S}} \cap \text{GL}_d(K)$ is a Zariski-closed subsemigroup of $\text{GL}_d(K)$. Therefore it is a group [11, Lemma 10]. ◀

If $\mathcal{S} \subseteq M_d(K)$ is a closed monoid (a semigroup containing the identity matrix), there is a unique irreducible component \mathcal{S}^0 containing the identity matrix [33, Remark 5.2] (the proof is the same as the one for linear algebraic groups). Furthermore \mathcal{S}^0 is a submonoid of \mathcal{S} .

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 such a way. We call A a generic matrix of V .²

► **Lemma 5.** *Let $V_1, \dots, V_n \subseteq M_d(K)$ 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 $f_1, \dots, f_m \in K[x_{ij} : 1 \leq i, j \leq d]$. We may assume that K is infinite and $m \geq 1$ 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 $g_l(y_{ij}^{(1)}, \dots, y_{ij}^{(n)}) := f_l(A_1(y_{ij}^{(1)}) \cdots A_n(y_{ij}^{(n)}))$ in at most nd^2 indeterminates. Now $V_1 \cdots V_n \subseteq X$ if and only if all of g_1, \dots, g_m vanish on K^{nd^2} . A polynomial g_l , with $l \in [1, m]$, vanishes on all of K^{nd^2} if and only if it is the zero polynomial, 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

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

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

► **Remark 6.** If one is willing to take $P_{ij}^{(k)}$ of size $\deg_{y_{ij}^{(k)}}(g_l) + 1$, then the full strength of the Nullstellensatz is not needed and the easy [2, Lemma 2.1] suffices.

By setting $n = 1$ and taking X to be the vanishing set of a single polynomial f , we get the following important special case.

► **Corollary 7.** *Let $f \in K[x_{ij} : 1 \leq i, j \leq d]$ be a polynomial and $V \subseteq M_d(K)$ an irreducible closed subset. Then it is possible to decide if f vanishes on V , and if it does not, to compute an element $A \in V$ with $f(A) \neq 0$.*

► **Definition 8.** *For $\emptyset \neq X \subseteq M_d(K)$ closed, the generic rank of X is $\bar{r}(X) := \max\{\text{rank}(A) : A \in X\}$.*

► **Lemma 9.** *Let K be infinite and $r \in \mathbb{Z}_{\geq 0}$. For an irreducible closed subset $V \subseteq M_d(K)$, the following statements are equivalent.*

- (a) $\bar{r}(V) = r$.
- (b) Every generic matrix of V has rank r .
- (c) There exists a generic matrix of V with rank r .

² 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 $K[M_d(K)] \rightarrow K[V]$.

(d) *There exists a Zariski-dense Zariski-open subset $U \subseteq V$ with $\text{rank}(A) = r$ for all $A \in U$.*

Proof. The implications (b) \Rightarrow (c) and (d) \Rightarrow (a) are immediate from the definitions.

(c) \Rightarrow (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 $\mathbf{q}(R)$ 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) \Rightarrow (b) Let A be a generic matrix of V with $\text{rank}(A) = s$. In light of (c) \Rightarrow (d) we see that V contains a Zariski-dense subset U of rank s matrices. Thus $\bar{r}(V) \geq s$. On the other hand, since rank can be defined in terms of the vanishing of minors, all elements of the Zariski closure of U have rank $\leq s$. Altogether $\bar{r}(V) = s$. \blacktriangleleft

► **Example 10.** A significant 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. For instance, suppose the characteristic of K is not 2, and consider

$$\begin{pmatrix} x & x \\ y & y \end{pmatrix} \begin{pmatrix} z & w \\ z & w \end{pmatrix} = \begin{pmatrix} 2xz & 2xw \\ 2yz & 2yw \end{pmatrix}.$$

the matrices on the left form two 2-dimensional vector spaces of generic rank 1 as x, y, z, w range through K . We can achieve all matrices of the form E_{ij} having a one in the ij -th coordinate and zeroes everywhere else in the product (right side). Thus the closure of the product of the two spaces is $M_2(K)$, which has generic rank 2.

► **Proposition 11.** *Let $V \subseteq M_d(K)$ be an irreducible closed subset. Then $r = \bar{r}(V)$ is computable and it is possible to compute a basis of V consisting of matrices of rank r .*

Proof. If K is finite, then V is at most 1-dimensional and the claim is trivial. Suppose that K is infinite.

The generic rank $r = \bar{r}(V)$ can be computed using Gauss elimination on a generic matrix of V . The matrices of rank r are dense in V in the Zariski topology, and hence also in the linear Zariski topology, which is coarser. We now use the same notation as in (c) \Rightarrow (d) of the previous lemma. Suppose we have found linearly independent $A_1, \dots, A_k \in V$ each of which has rank r ($k \geq 0$). If $k < \dim V$, there exists a (computable) vector subspace $W \subsetneq V$ containing all of A_1, \dots, A_k . Then there is a linear polynomial g whose vanishing set contains W but not V . Now pick $(A(\alpha_{ij})) \in V$ with $(f \cdot g)(A(\alpha_{ij})) \neq 0$ (using Corollary 7; here f is chosen as in (c) \Rightarrow (d) of Lemma 9). Then $A_{k+1} := A(\alpha_{ij})$ has rank r and the matrices A_1, \dots, A_{k+1} are linearly independent. We may repeat this process to obtain the desired basis. \blacktriangleleft

► **Lemma 12.** *Let $D_1, \dots, D_r \subseteq M_d(K)$ be irreducible subsets. Then $\overline{D_1 \cdots D_r} = \overline{\overline{D_1} \cdots \overline{D_r}}$.*

Proof. It suffices to show the claim for $r = 2$; the general claim follows by induction. The inclusion \subseteq is trivial. For the inclusion \supseteq , first note that $D_1 D_2$ is irreducible in the Zariski topology, and hence also in the linear Zariski topology. Therefore $\overline{D_1 D_2}$ is irreducible, and hence $\overline{D_1 D_2}$ is the vector space spanned by $D_1 D_2$.

Since each D_i is irreducible, the closure $V_i := \overline{D_i}$ is a vector space and $\overline{D_i}$ must contain a basis of V_i . Thus $D_1 D_2$ contains a basis of $\text{span } V_1 V_2$. We conclude $\overline{D_1 D_2} = \overline{V_1 V_2} = \text{span } V_1 V_2 \subseteq \text{span } D_1 D_2 = \overline{D_1 D_2}$. \blacktriangleleft

The linear Zariski closure is well-behaved with respect to scalar extension. More specifically we have the following.

► **Lemma 13.** *Let $K \subseteq L$ be a field extension and let $X = V_1 \cup \dots \cup V_l \subseteq M_d(K)$ be a closed set. Then $X \subseteq M_d(L)$, and, taking the closure in the larger space, $\overline{X} = (V_1 \otimes_K L) \cup \dots \cup (V_l \otimes_K L)$.*

Let V be a K -vector space. If $X \subseteq V$ is a closed set, it can be specified by finitely many basis elements of its irreducible components. The entries of these matrices generate a subalgebra $R \subseteq K$, finitely generated over the prime field of K . Denoting by X_0 the closed set defined by the same data over the field of fractions $K_0 := \mathbf{q}(R)$, we can compute the closure of X_0 over K_0 , and then extend scalars to K .

In the next section we will be concerned with computing the closure of a subsemigroup $\mathcal{S} \subseteq M_d(K)$ generated by a closed set X . If X has a basis contained in $M_d(K_0)$, then $\mathcal{S} \subseteq M_d(K_0)$. Thus it is sufficient to consider the problem in the case where $K = K_0$ is a finitely generated field, that is, a finitely generated field extension of \mathbb{Q} or of a finite field \mathbb{F}_p .

3 Invertible Matrices

Let K be a finitely generated field. This means that 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 K is given by specifying generators and relations for R , and $R = K_0$ if R is algebraic over K_0 .

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. We first consider the case of a single invertible matrix. By $\mu(K^{\mathrm{alg}})$ we denote the group of all roots of unity. Recall that if $\mathrm{char} K = p > 0$, then p does not divide the order of any root of unity.

► **Lemma 14.** *Let $A \in \mathrm{GL}_d(K)$.*

1. *Assume that for any two eigenvalues $\lambda, \lambda' \in K^{\mathrm{alg}}$ 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 $\mathrm{char} K \nmid n$.*
2. *If $\mathrm{char} K = p > 0$, and $V \subseteq K^d$ is A^{p^n} -invariant for some $n \geq 0$, then V is A^{p^e} -invariant for $e = \mathbf{v}_p((d-1)!)$, the p -adic valuation of $(d-1)!$.*

Proof. Without restriction assume $K = K^{\mathrm{alg}}$. For every $\lambda \in K$, the space V is A -invariant if and only if it is $(A - \lambda)$ -invariant. If $\lambda_1, \dots, \lambda_r$ are the pairwise distinct eigenvalues of A , then every generalized eigenspace $\ker(A - \lambda_i)^d$ is A -invariant. If V is A -invariant, we can consider the generalized eigenspaces of the restriction $A|_V$ to obtain a decomposition

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

(1) If V is A -invariant, then it is A^n -invariant. It suffices to show the converse; let $n \geq 1$. Let λ be an eigenvalue of A , and let ζ be a primitive n -th root of unity (which exists due to $\mathrm{char} K \nmid n$). Then

$$(A^n - \lambda^n)^i = (A - \lambda)^i \prod_{j=1}^{n-1} (A - \zeta^j \lambda)^i = \prod_{j=1}^{n-1} (A - \zeta^j \lambda)^i \cdot (A - \lambda)^i \quad \text{for } i \geq 0.$$

Since $\zeta^j \lambda$ is not an eigenvalue of A , the matrices $(A - \zeta^j \lambda)^i$ are invertible for $j \in [1, n-1]$. Consequently $\ker(A^n - \lambda^n)^i = \ker(A - \lambda)^i$.

Let $\lambda_1, \dots, \lambda_r$ denote the pairwise distinct eigenvalues of A . Since V is A^n -invariant,

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

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

Now V is also $(A^n - \lambda^n)$ -invariant. We show that it is $(A - \lambda)$ 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 $(A - \lambda)^i v \in V$.

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

$$0 \neq v'_k = \left(\sum_{j=0}^{n-1} A^j \lambda^{n-1-j} \right)^k (A - \lambda)^k v = \left(\sum_{j=0}^{n-1} A^j \lambda^{n-1-j} \right)^k v_k = (n\lambda^{n-1})^k v_k.$$

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

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

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

(2) Using the direct-sum decomposition of V along generalized eigenspaces, we can again 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 $k \geq e := \mathbf{v}_p((d-1)!)$, 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. \blacktriangleleft

► **Lemma 15.** *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 $\text{char } K \nmid N_0$.*

Proof. This makes essential use of the fact that K is a finitely generated field. Suppose first that $K = R = K_0$ is a finite field or a number field. The finite field case is trivial. If K is a number field, let $\mu(L)$ be the group of roots of unity of L . Note that

$$\bigcup \{ \mu(L) : L/K \text{ an extension with } [L : K] \leq d \}$$

is finite because $\phi(n) \rightarrow \infty$ as $n \rightarrow \infty$ (here ϕ denotes the Euler- ϕ -function). By taking the least common multiple of $|\mu(L)|$, the claim for number fields follows.

Consider now the general case. By effective Noether normalization, we can compute transcendental x_1, \dots, x_n over K_0 , such that R is a finite module over $K_0[x_1, \dots, x_n]$. Recall that x_1, \dots, x_n is a transcendence basis for K/K_0 . From the generating set of R as a $K_0[x_1, \dots, x_n]$ -algebra, we can compute a bound m for the degree $[K : K_0(x_1, \dots, x_n)]$. 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 $N_0(d, K) = N_0(md, K_0)$. \blacktriangleleft

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

► **Lemma 16.** *Let $N := N(d, K) := p^e N_0(d^2, K)$ with $e = v_p((d-1)!)$. Let $A \in \text{GL}_d(K)$, 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 $\lambda, \lambda' \in K^{\text{alg}}$ 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 14.

Suppose now 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 14 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 14 to deduce that V is $A^{p^e N_0}$ -invariant. ◀

► **Lemma 17.** *Let $A \in \text{GL}_d(K)$ and $N = N(d, K)$. Then the irreducible component of $\overline{\langle A \rangle}$ containing the identity is $\overline{\langle A \rangle}^0 = \text{span}\{A^{N^i} : i \geq 0\}$. In particular, $\overline{\langle A \rangle}$ is computable.*

Proof. Let Z_0 be the unique irreducible component of $\overline{\langle A \rangle}$ containing the identity. 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 16 implies that we can take $n = N(d, K)$, which is computable without knowing Z_0 .

Now $A^n \in Z_0$ and hence $\langle A^n \rangle \in Z_0$. Since Z_0 is a vector space, even $\text{span}\langle A^n \rangle \subseteq Z_0$. Thus $\langle A \rangle \subseteq \bigcup_{i=0}^{n-1} A^i \text{span}\langle A^n \rangle \subseteq \bigcup_{i=0}^{n-1} A^i Z_0 \subseteq \overline{\langle A \rangle}$. Taking closures, we get equality throughout, so $\overline{\langle A \rangle}^0 = \text{span}\langle A^n \rangle$. Finally, $\text{span}\langle A^n \rangle$ is computable using Cayley-Hamilton. ◀

► **Remark 18.** If one can compute with algebraic extensions of K (e.g., if K is a finite field or a number field), one may instead compute the eigenvalues of A explicitly. 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 . The advantage is that the resulting n could be much smaller than $N(d, K)$.

Now that we can compute the closure of a semigroup generated by a single invertible matrix, we can extend this to semigroups generated by closed sets in which the invertible elements are dense. The algorithm is essentially that of [11], 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.

The proof of the termination of the algorithm requires the following.

► **Theorem 19** (Burnside–Schur [17, Theorem 2.3.5]). *If $G \leq \text{GL}_d(K)$ is a finitely generated torsion subgroup, then G is finite.*

► **Proposition 20.** *Let K be a finitely generated field and let $X \subseteq M_d(K)$ be a closed subset such that $\text{GL}_d(K) \cap X$ is dense in X . Then $\overline{\langle X \rangle}$ is computable.*

Proof. We show that Algorithm 1 terminates and computes $\overline{\langle X \rangle}$.

Denote by $(T_1, N_1), (T_2, N_2), \dots$, the subsequent values taken by T and N . Then $N_1 \subseteq N_2 \subseteq \dots$ is an ascending chain of vector subspaces of the finite-dimensional space

■ **Algorithm 1** Computation of $\overline{\langle X \rangle}$ when the invertible matrices are dense in X

```

1: function GROUPCLOSURE( $X$ )
2:    $Z_1, \dots, Z_l \leftarrow$  Irreducible components of  $X$  (given by invertible bases)
Require:  $\mathrm{GL}_d(K) \cap Z_i \neq \emptyset$  for all  $i \in [1, l]$ 
3:   for  $i = 1, \dots, l$  do
4:      $A_i \leftarrow$  An invertible element of  $Z_i$ 
5:    $N \leftarrow \overline{(A_1^{-1}Z_1) \cdots (A_l^{-1}Z_l)}$ 
6:    $T \leftarrow \{I, A_1, \dots, A_l\}$ 
7:   repeat
8:      $N' \leftarrow N$ 
9:      $T' \leftarrow T$ 
10:    for  $A \in T$  do
11:       $N \leftarrow \overline{N \langle A \rangle^0}$ 
12:       $N \leftarrow \overline{N(ANA^{-1})}$ 
13:    for  $B \in T$  do
14:      if  $AB \notin TN$  then
15:         $T \leftarrow T \cup \{AB\}$ 
16:  until  $N' = N$  and  $T' = T$ 
17:  return  $TN$ 

```

$M_d(K)$. Therefore the chain stabilizes at some $N_\infty := N_m$. For $i \geq 0$ and $A \in T_i$ note that $AN_iA^{-1} \subseteq N_{i+1}$ (by line 12 and $I \in N_i$) and thus $AN_\infty A^{-1} = N_\infty$. Let $H := N_\infty \cap \mathrm{GL}_d(K)$. For every $i \geq 0$ and $A \in T_i$ we have $(AH)(AH) \subseteq A^2HH \subseteq T_{i+1}H$ by construction (the first inclusion by $AN_\infty = N_\infty A$; 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. Then the Zariski closure $\tilde{G} \subseteq \mathrm{GL}_d(K^{\mathrm{alg}})$ is a linear algebraic group, and \tilde{H} is a closed normal subgroup. Indeed, as N_∞ is a vector subspace of $M_d(K)$ the closure \tilde{H} is simply the vector subspace of $M_d(K^{\mathrm{alg}})$ defined by the same equations as N_∞ , intersected with $\mathrm{GL}_d(K^{\mathrm{alg}})$. Now the quotient \tilde{G}/\tilde{H} is also a linear algebraic group [7, Theorem II.6.8], so without restriction $\tilde{G}/\tilde{H} \subseteq \mathrm{GL}_{d'}$ for some $d' \geq 1$. Let $\pi: \tilde{G} \rightarrow \tilde{G}/\tilde{H}$ denote the quotient morphism. This 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 $\pi(I), \pi(A_1), \dots, \pi(A_l)$. But it also contains all these elements, so $\pi(G) = \langle \pi(I), \pi(A_1), \dots, \pi(A_l) \rangle$. By line 11, every element of $\pi(G)$ has finite order. Being a cancellative torsion semigroup, therefore $\pi(G)$ is a group. As we have just argued it is also finitely generated, and thus Burnside–Schur applies to show that $\pi(G)$ is finite.

Note that $\tilde{H} \cap \mathrm{GL}_d(K) = H$. Thus for $A, B \in \mathrm{GL}_d(K)$ we have $AB^{-1} \in \tilde{H}$ if and only if $AB^{-1} \in H$ if and only if $AB^{-1} \in N_\infty$. Looking at lines 14–15 of the algorithm, the chain $T_1 \subseteq T_2 \subseteq \dots$ must therefore also stabilize, say at the finite set $T_\infty := T_n$. Thus $\mathcal{S} := \bigcup_{i \geq 0} T_i N_\infty = T_\infty N_\infty$ is closed.

By construction X is dense in \mathcal{S} (this is true in the beginning of the algorithm and is preserved in each step). It remains to show that \mathcal{S} is a semigroup. But 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. ◀

4 Non-invertible matrices

Throughout this 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 . Let $\mathcal{S}_1 := \mathcal{S} \cup \{I\}$ denote the monoid obtained by adjoining the identity matrix (if necessary). 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 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 [33, 34], respectively strongly π -regular matrix semigroups [34, Section 2.3.2] [29]. 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 [30, 31]. 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 [18]. However, we use more semigroup-theoretic language. A key point in [18] 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. In the linear Zariski topology, taking a closure of a product of vector spaces may introduce elements of larger rank (see Example 10) and it is not clear that such an approach can be made to terminate. Much of the additional difficulty in the linear Zariski topology setting revolves around carefully dealing with this ill-behaved nature of the generic rank.

The following key finiteness result will be applied in various guises.

► **Lemma 21.** *Let W be a d -dimensional vector space. Let $r \in [0, d]$ and let $(U_1, V_1), \dots, (U_n, V_n)$ 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 $u_{i,1}, \dots, u_{i,d-r}$ of U_i and $v_{i,1}, \dots, v_{i,r}$ of V_i we can associate to U_i and V_i the elements $\alpha_i := u_{i,1} \wedge \dots \wedge u_{i,d-r} \in \bigwedge^{d-r} W$ and $\beta_i := v_{i,1} \wedge \dots \wedge v_{i,r} \in \bigwedge^r W$. (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 $\beta_1, \dots, \beta_{i-1}$. Hence the β_1, \dots, 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 . ◀

We call a matrix $A \in M_d(K)$ **completely pseudo-regular** if it is contained in a subgroup of $M_d(K)$.³ Such matrices are characterized intrinsically by the following lemma.

► **Lemma 22.** *Let $A \in M_d(K)$. The following statements are equivalent.*

³ 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, as a pseudo-inverse of A may not be contained in \mathcal{S} .

1. A is completely pseudo-regular.
2. There exists $A' \in M_d(K)$ such that $A = AA'A$ and $AA' = A'A$.
3. There exist $E, A' \in M_d(K)$ such that $E^2 = E$, $EA = AE = A$, and $AA' = A'A = E$.
4. $\text{rank } A = \text{rank } A^2$.
5. $\text{im}(A) \cap \ker(A) = 0$.

Proof. The equivalence of (1), (2), and (3) holds in all semigroups. For convenience, we recall a proof.

- (1) \Rightarrow (2) Let $G \subseteq M_d(K)$ be a subgroup containing A , and A' the inverse of A in G .
- (2) \Rightarrow (3) $E := A'A$ is idempotent and has the claimed properties.
- (3) \Rightarrow (1) The subsemigroup generated by A , A' , and E is a group.
- (2) \Rightarrow (4) Since $A = A^2A'$, we have $\text{im}(A) \subseteq \text{im}(A^2)$, and hence $\text{im}(A) = \text{im}(A^2)$.
- (4) \Leftrightarrow (5) Clear.
- (5) \Rightarrow (3) We have $K^d = \text{im}(A) \oplus \ker(A)$, and therefore it is possible to construct a suitable inverse to A on $\text{im}(A)$ and extend it to K^d . \blacktriangleleft

Suppose that A is completely pseudo-regular and E is an idempotent as in (3). Then $\text{rank } A = \text{rank } E$ and one easily deduces $\text{im } E = \text{im } A$ and $\ker E = \ker A$, so that E is uniquely determined by A . We define $E(A) := E$. The element A' with $AA' = A'A = E$ is not uniquely determined, but one easily sees that there is a unique such A' with $A' \in EM_d(K)E$. We write A^+ for this element of $EM_d(K)E$ and call it the **pseudo-inverse** of A .

► **Lemma 23.** *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 [33, Theorem 3.18] and the remaining claims follow from inspection of the proof of the cited theorem. \blacktriangleleft

- **Definition 24.** 1. For $A, B \in M_d(K)$ write $A \parallel B$ if $\text{im}(A) = \text{im}(B)$ and $\ker(A) = \ker(B)$.
2. For $A, B \in \mathcal{S}$ let $A \sim_{\mathcal{S}} B$ if there exist $C, D, C', D' \in \mathcal{S}_1$ 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 $A \in \mathcal{S}$.

► **Lemma 25.** *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 $B = B_1B_2$ with $B_1, B_2 \in \mathcal{S}$. Then there exists a completely pseudo-regular element $C \in [A]_{\mathcal{S}}$ such that $B_1B_2 = B_1E(C)B_2$.*

Proof. Let $P, P', Q, Q' \in \mathcal{S}_1$ such that $A \parallel Q'BP'$ and $B \parallel QAP$. Let $r = \text{rank}(A)$.

(1) Since $\text{rank}(B) = r$ as well, we have $\text{im}(QA) = \text{im}(B)$ and $\text{im}(Q'B) = \text{im}(Q'QA) = \text{im}(A)$. Then $\text{rank}(Q'QA) = r$ 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 $\text{rank}(Q'QAQ'QA) = r$, we must have $\text{rank}(D) = r$. Then $\text{im}(D) = \text{im}(QA) = \text{im}(B)$. Since $\text{rank}(AQ'QA) = r$ we must have $\text{im}(QA) \cap \ker(AQ') = 0$, 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 $\text{im}(D B_1) \supseteq \text{im}(D B) = \text{im}(B)$ and $\text{rank}(D B_1) \leq \text{rank}(B)$ we get $\text{im}(D B_1) = \text{im}(B)$. Analogously $\ker(B_2 D') = \ker(B D') = \ker(B)$. Also $\text{im}(Q' D B_1) = \text{im}(Q' B) = \text{im}(A)$ and $\ker(B_2 D' P') = \ker(B P') = \ker(A)$. Thus $\text{rank}(C) = r$. Computing $C^2 = (B_2 D' P') A (Q' D B D' P') A (Q' D B_1)$, we see that C is completely pseudo-regular. From $A \parallel (Q' D B_1) C (B_2 D' P') A$ we get $C \sim_{\mathcal{S}} A$.

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

The following lemma replaces [18, Propositions 9 and 10] in our setting.

► **Lemma 26.** *Let $A = A_1 \cdots A_n$ with $A_1, \dots, A_n \in M_d(K)$. Suppose there exists $r \geq 0$ such that $\text{rank}(A) = \text{rank}(A_i A_{i+1}) = r$ 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 exist $k, l \in [1, n]$ with $k < l$ such that $A_k \cdots A_l$ is completely pseudo-regular of rank r .*

Proof. (1) For $i \in [3, n-1]$ define $V_i := \text{im}(A_i \cdots A_n)$ 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 21, 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 $V_i = \text{im}(A_{2i+1} A_{2i+2})$. Then $U_i \cap V_i = 0$ for all i . By Lemma 21, there exist $i < j$ such that $U_j \cap V_i = 0$. Then $\text{im}(A_{2i+1} A_{2i+2}) \cap \ker(A_{2j-1} A_{2j}) = 0$ and $2i+1 < 2j$, so $k = 2i+1$ and $l = 2j$ works. ◀

► **Proposition 27.** *Let $E \in M_d(K)$ be idempotent of rank r and let $H \subseteq E \bar{\mathcal{S}} E$ be a closed subset. Then $\{A \in H : \text{rank}(A) = r\}$ is contained in a subgroup of $\bar{\mathcal{S}}$ (with neutral element E), and it is possible to compute $\overline{\{A \in H : \text{rank}(A) = r\}}$.*

Proof. Let $V = \text{im } E$. 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 $\text{rank } A = r$ 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 $\overline{\{A \in H : \text{rank}(A) = r\}}$ by reducing to the invertible case (see Section 3). ◀

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 $\bar{\mathcal{S}}$ by Lemma 23. For a subset $Y \subseteq M_d(K)$ and $n \geq 1$, we define

$$Y^{\leq n} := \bigcup_{k=1}^n Y^k = \{A_1 \cdots A_k : k \in [1, n] \text{ and } A_1, \dots, A_k \in Y\} \text{ and } Y^{\triangleleft n} := \{I\} \cup Y^{\leq n}.$$

► **Lemma 28.** *Let $r \geq 0$ and let A be a completely pseudo-regular element of \mathcal{S} of rank r . Suppose Y is a closed set with $X \cup \{B \in \mathcal{S} : \text{rank}(B) > r\} \subseteq Y$. Let $E := E(A)$ and $H := \{B \in E Y^{\triangleleft 2\binom{d}{r}+5} E : \text{rank}(B) = r\}$.*

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

Proof. (1) Recall $A = EA = AE$ and $\text{rank } A = \text{rank } B = \text{rank } E = r$. Let $P, Q \in \mathcal{S}_1$ be such that $B \parallel QAP$. Then $\text{im}(B) = \text{im}(QAP) = \text{im}(QA) = \text{im}(QEA)$, with the middle equality holding because of $\text{rank}(QA) \leq r$. Also because of the ranks, therefore $\text{im}(B) = \text{im}(QE)$ and $\text{rank}(QE) = r$. Analogously one finds $\ker(B) = \ker(EP)$ and $\text{rank}(EP) = r$. 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 $P_i, Q_i \in X \cup \{B \in \mathcal{S} : \text{rank}(B) > r\}$. Choosing m, n minimal, we get $\text{rank}(P_i P_{i+1}) = r$ for $i \in [1, m-1]$ and $\text{rank}(Q_i Q_{i+1}) = r$ for $i \in [1, n-1]$. Consider $EP_1 \cdots P_m$ and $Q_1 \cdots Q_n E$. Applying (1) of Lemma 26, 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 $\text{im}(D) = \text{im}(F)$ 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 23. Define $D^+ := R^+C = R^+EC$. Then $D^+D = R^+CD = R^+R = E$. Furthermore DD^+ is idempotent with $\text{im}(DD^+) = \text{im } F$ and $\ker(DD^+) = \ker F$. Thus $DD^+ = F$.

(2) One first computes \overline{H} and then, using Proposition 27, one can compute $\overline{\langle H \rangle} = \overline{\{C \in \overline{H} : \text{rank}(C) = r\}}$ as a subset of $EM_d(K)E$. Note $E\overline{\langle H \rangle}Y^{\triangleleft(\frac{d}{r})+2}XY^{\triangleleft(\frac{d}{r})+2}E \subseteq E\overline{\langle H \rangle}Y^{\triangleleft(\frac{d}{r})+5}E = E\overline{\langle H \rangle}EY^{\triangleleft(\frac{d}{r})+5}E$. Every element of this set having rank r is also contained in $E\overline{\langle H \rangle}HE \subseteq \overline{\langle H \rangle}$.

Let $B = B_1 \cdots B_n \in [A]_S$ with $B_1, \dots, B_n \in X$. By Lemma 25, there exist completely pseudo-regular elements $C_0, \dots, C_n \in [A]_S$ such that $B = E_0 B_1 E_1 B_2 \cdots E_{n-1} B_n E_n$ with idempotents $E_i = E(C_i)$. For each E_i , let $A_i \in Y^{\triangleleft(\frac{d}{r})+2}E$ and $A_i^+ \in E\overline{\langle H \rangle}Y^{\triangleleft(\frac{d}{r})+2}$ be such that $A_i^+ A_i = E$ and $A_i A_i^+ = E_i$ (these exist by (1)). Then

$$B = A_0(A_0^+ B_1 A_1)(A_1^+ B_2 A_2) \cdots (A_{n-1}^+ B_n A_n)A_n^+.$$

Each $A_i^+ B_i A_{i-1}$ is contained in $\overline{\langle H \rangle}$ and $A_n^+ \in E\overline{\langle H \rangle}Y^{\triangleleft(\frac{d}{r})+2} \subseteq \overline{\langle H \rangle}Y^{\triangleleft(\frac{d}{r})+2}$, so $B \in Y^{\triangleleft(\frac{d}{r})+2}\overline{\langle H \rangle}Y^{\triangleleft(\frac{d}{r})+2}$. \blacktriangleleft

At this point we have the tools to deal with one completely pseudo-regular element. The following lemmas will be helpful in finding such elements, and to establish that it is enough to consider finitely many of them. For $r \geq r' \geq 0$, we define

$$N(r', r) := \prod_{s=r'}^r \left(2\binom{d}{s} + 4 \right).$$

► **Lemma 29.** Let $A_1, \dots, A_n \in M_d(K)$. Suppose $r \geq r' \geq 0$ are such that $\text{rank}(A_i) \leq r$ for all $i \in [1, n]$ and $\text{rank}(A_1 \cdots A_n) = r'$. If $n \geq N(r', r)$, then there exist $k, l \in [1, n]$ with $k < l$ such that $A_k \cdots A_l$ is completely pseudo-regular.

Proof. We fix r' and proceed by induction on $r \geq r'$. Suppose $r = r'$. Then $\text{rank}(A_i A_{i+1}) = r$ for all $i \in [1, n-1]$ and the claim holds by (2) of Lemma 26. Let now $r > r'$ and assume the claim holds for $r-1$. By the base case, $r = r'$, any product of at least $2\binom{d}{r} + 4$ consecutive matrices must either contain a completely pseudo-regular subproduct of rank r , or have rank strictly less than r . In the first case, we are done. So, without restriction, we may group the matrices into subproducts of at most $2\binom{d}{r} + 4$ matrices each, to rewrite $A_1 \cdots A_n = A'_1 \cdots A'_m$ with $m \geq N(r', r-1)$ and $\text{rank}(A'_i) \leq r-1$ for each $i \in [1, m]$. The inductive hypothesis implies the claim. \blacktriangleleft

For a completely pseudo-regular element $B \in \mathcal{S}$ of rank r and a closed set Y , let $E = E(B)$,

$$\begin{aligned}\mathcal{T}_0(Y, B) &:= \left\{ A \in \overline{EY^{\leq 2\binom{d}{r}+5}E} : \text{rank}(A) = r \right\}, \text{ and} \\ \mathcal{T}(Y, B) &:= \overline{Y^{\leq \binom{d}{r}+2} \langle \mathcal{T}_0(Y, B) \rangle Y^{\leq \binom{d}{r}+2}}.\end{aligned}$$

If Y contains $X \cup \{A \in \mathcal{S} : \text{rank}(A) > r\}$, then (2) of Lemma 28 implies $[B]_{\mathcal{S}} \subseteq \mathcal{T}(Y, B)$. Otherwise this may not be the case; in any case $\mathcal{T}(Y, B)$ is computable using Proposition 27.

► **Lemma 30.** *Let $r = \bar{r}(X)$ and $r' \in [0, r]$. For $s \in [r', r]$, let R_s be a set of completely pseudo-regular elements of rank s . Let $Y_{r+1} = X$ and Y_s, Y'_s for $s \in [r', r]$ be recursively defined by $Y'_s := Y_{s+1} \cup \bigcup_{B \in R_s} \mathcal{T}(Y_{s+1}, B)$ and $Y_s := \overline{(Y'_s)^{\leq N(r', r)}}$.*

If $A = A_1 \cdots A_n$ with $A_1, \dots, A_n \in X$, $n > N(r', r)$, $\text{rank}(A) \geq r'$, and $A \notin Y_{r'}$, then there exist $k, l \in [1, n]$ with $k < l$ such that $A_k \cdots A_l$ is completely pseudo-regular and not contained in $T(r', r) := \bigcup_{s \in [r', r]} \bigcup_{B \in R_s} \mathcal{T}(Y_{s+1}, B)$.

Proof. It suffices to show that same claim under the assumption $A_1, \dots, A_n \in X \cup T(r', r)$ instead of $A_1, \dots, A_n \in X$. Taking a representation of A with n minimal, we may then assume: for all $k < l$ the subproduct $A_k \cdots A_l$ is not contained in $T(r', r)$. Since $A \notin Y_{r'}$ but $(X \cup T(r', r))^{\leq N(r', r)} \subseteq Y_{r'}$, this minimal n must still satisfy $n > N(r', r)$. Lemma 29 implies that there exist $k, l \in [1, n]$ with $k < l$ such that $A_k \cdots A_l$ is completely pseudo-regular. ◀

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 $A \rightarrow B$ if $\ker(B) \cap \text{im}(A) = 0$. (Loops are permitted, but this shall not make a difference in our considerations.) In the following, (2) should be compared to [18, Proposition 8].

► **Proposition 31.** 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 $C \rightarrow D$ in $G(R)$, then $\ker(DC) = \ker(C)$ and $\text{rank}(D) \geq \text{rank}(DC) = \text{rank}(C)$. So if C, D are two elements of the same SCC, then $\text{rank}(C) = \text{rank}(D)$; if $C \rightarrow D$ is an edge, then also $\text{im}(DC) = \text{im}(D)$.

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

(2) Let A_1, \dots, 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, $\ker(A_i) \cap \text{im}(A_j) \neq 0$ for $j > i$ and $\ker A_i \cap \text{im} A_i = 0$. By Lemma 21 we must have $k \leq \binom{d}{r}$. ◀

► **Theorem 32.** *Let K be a finitely generated field. For a closed set $X \subseteq M_d(K)$ and $\mathcal{S} = \langle X \rangle$, it is possible to compute $\overline{\mathcal{S}}$.*

Proof. Let $r = \bar{r}(X)$. Suppose we have, for each $s \in [0, r]$, a finite set $R_s = \{B_1, \dots, B_{k_s}\}$ of completely pseudo-regular elements of \mathcal{S} of rank s (at the beginning $R_s = \emptyset$ for all $s \in [0, r]$). Recursively compute closed sets $Y'_s, Y_s, T(0, r)$ as in Lemma 30 with $r' = 0$ and set $Y := Y_0$. By construction $X^{\leq N(s, r)} \subseteq Y_s$ and $X \subseteq Y_s \subseteq \overline{\mathcal{S}}$.

To test whether $Y = \overline{\mathcal{S}}$, it suffices to check $\overline{Y^2} \subseteq Y$. If this is the case, we are done. If not, then $\mathcal{S} \not\subseteq Y$, and so there exists some $n > N(0, r)$ such that $X^n \not\subseteq Y$. We can find such

an n and $A_1, \dots, A_n \in X$ with $A := A_1 \cdots A_n \notin Y$ using Lemma 5. By Lemma 30 (with $r' = 0$), we can find $k < l$ such that $B := A_k \cdots A_l$ is completely pseudo-regular of some rank s and not contained in $T(0, r)$.

Add B to R_s . If $|R_s| \leq \binom{d}{s}$, set $R_{s-1} = \dots = R_0 = \emptyset$, and repeat from the start. Otherwise, $|R_s| > \binom{d}{s}$, so there must exist $B_i, B_j \in R_s$ with $i < j$ and $B_i \sim_S B_j$ by Proposition 31. By construction of B_j , this implies $[B_i]_S \not\subseteq \mathcal{T}(Y_{s+1}, B_i)$.⁴ But then $\mathcal{S} \setminus Y_{s+1}$ contains an element of rank $> s$. We can use Lemma 5 to find $n > N(s+1, r)$ and $A_1 \cdots A_n \in X^n \setminus (Y_{s+1} \cup \{A \in M_d(K) : \text{rank}(A) \leq s\})$. Applying Lemma 30, we obtain a completely pseudo-regular $B' = A_k \cdots A_l$ with $k < l$ of some rank $s' > s$ that is not contained in $T(s+1, r)$. In this case, we add B' to $R_{s'}$, set $R_{s'-1} = \dots = R_0 = \emptyset$, and restart the algorithm.

To see that the algorithm terminates, first note $|R_s| \leq \binom{d}{s}$ for all s . 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 will only modify the sets R_{r-1}, \dots, R_0 and at this point R_{r-1} can only ever grow. Thus, eventually, R_{r-1} will also stabilize. Inductively we conclude that eventually all the sets R_{r-1}, \dots, R_0 stabilize, and the algorithm stops. Then we must have $Y = \bar{\mathcal{S}}$. ◀

5 Decidability of Sequential? and Unambiguous?

Let K be a finitely generated field. We work with row vectors and apply matrices on the right. A linear representation of a K -automaton on d states over the alphabet Σ consists of a row vector $u \in K^{1 \times d}$, a monoid homomorphism $\mu: \Sigma^* \rightarrow M_d(K)$, and a column vector $v \in K^d$.

► **Definition 33.** 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 $\{u\mu(w) : w \in \Sigma^*\}$.

If two K -automata recognize the same K -rational series, their linear hulls need not coincide. However, since K is a field, there always exist minimal linear representations that are unique up to conjugation by an invertible matrix. Correspondingly, the linear hulls of minimal linear representations are conjugates of each other. To a K -rational series we may therefore associate the linear hull of a minimal linear representation, and this is unique up to conjugation (i.e., up to a change of basis).

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

► **Remark 34.** 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 $\text{GL}_d(\mathbb{Q})$ of order $2^d d!$. By a result of Feit ([14]; see also the introduction of [4] or [23, §6]), for large d , this order is maximal among all finite subgroups of $\text{GL}_d(\mathbb{Q})$. Its linear Zariski closure consists of a union of $2^{d-1} d!$ vector spaces of dimension

⁴ B_j was chosen to not be in $\mathcal{T}(Y_{s+1}, B_i)$. An important detail is that Y_{s+1} at this point is the same set as in the step in which B_j was chosen. However, if at any point Y_{s+1} changes, then we must have changed some $R_{s'}$ for $s' > s$. In this case we are always resetting $R_{s'-1} = \dots = R_0 = \emptyset$.

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 $(1, 2, \dots, d)$, this group also gives a linear hull of size $2^{d-1}d!$ for a two-letter alphabet and d states.

► **Corollary 35.** *Let \mathcal{A} be a K -automaton. Then the linear hull of \mathcal{A} is computable.*

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

► **Theorem 36.** *Let K be a finitely generated field and \mathcal{A} a K -automaton. Then it is decidable if \mathcal{A} is equivalent to a sequential [unambiguous] K -automaton. In these cases the corresponding sequential [unambiguous] K -automaton is computable.*

Proof. First we may replace \mathcal{A} by a minimal linear representation. Let X be the linear hull of \mathcal{A} . Once we have that, we can explicitly construct $\hat{\mathcal{A}}$ as in [3, Lemma 3.13]. If $\hat{\mathcal{A}}$ is unambiguous [sequential], then we are done. If $\hat{\mathcal{A}}$ is ambiguous, then [3] implies that there is no unambiguous [sequential] weighted automaton equivalent to \mathcal{A} . ◀

This solves Problem 1 in [24] for finitely generated fields. Given an automaton over any field, the problem can be reduced to the finitely generated field generated by all the weights. So, under the assumption that one can always get a suitable representation of this field, the problem has a positive answer for every field.

Finally, suppose that R is not a field but only a (commutative) domain and consider the same problem for R -automata. One can then carry out the procedure over the quotient field $K = \mathbf{q}(R)$ of R . However the existence of a sequential [unambiguous] K -automaton equivalent to the initial one, may not imply the existence of a sequential [unambiguous] R -automaton. Luckily, if R is completely integrally closed we obtain the following.

► **Corollary 37.** *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 36.

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 sequentiality. However, if R is a principal ideal domain (PID) there is a way to pass to R .

► **Corollary 38.** *Let R be a finitely generated PID and \mathcal{A} a R -automaton. Then it is decidable if \mathcal{A} is equivalent to a sequential R -automaton. In this case a corresponding sequential 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 sequential R -automaton, it is equivalent to a sequential K -automaton. Suppose conversely that \mathcal{A} is equivalent to a sequential 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 [6, 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 $a_1, \dots, a_n \in K^{1 \times d}$ such that $\Omega \subseteq (Ka_1 \cup \dots \cup Ka_n) \cap R^{1 \times d}$. We may take the coordinates of each a_i to be in R and to be coprime. Then $\Omega \subseteq Ra_1 \cup \dots \cup Ra_n$. This yields an R -sequential automaton equivalent to \mathcal{A} (on n states) [24, Proposition 5]. ◀

Corollaries 37 and 38 apply to the ring of integers \mathbb{Z} , and so Problem 1 of [24] 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 38) can indeed be carried out.

References

- 1 Cyril Allauzen and Mehryar Mohri. Efficient algorithms for testing the twins property. volume 8, pages 117–144. 2003. *Weighted automata: theory and applications* (Dresden, 2002).
- 2 Noga Alon. Combinatorial Nullstellensatz. volume 8, pages 7–29. 1999. *Recent trends in combinatorics* (Mátraháza, 1995). doi:10.1017/S0963548398003411.
- 3 Jason Bell and Daniel Smertnig. Noncommutative rational Pólya series. *Selecta Math. (N.S.)*, 27(3):Paper No. 34, 34, 2021. doi:10.1007/s00029-021-00629-2.
- 4 Neil Berry, Artūras Dubickas, Noam D. Elkies, Bjorn Poonen, and Chris Smyth. The conjugate dimension of algebraic numbers. *Q. J. Math.*, 55(3):237–252, 2004. doi:10.1093/qjmath/55.3.237.
- 5 Jean Berstel and Maurice Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Bull. Soc. Math. France*, 104(2):175–184, 1976.
- 6 Jean Berstel and Christophe Reutenauer. *Noncommutative rational series with applications*, volume 137 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2011.
- 7 Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991. doi:10.1007/978-1-4612-0941-6.
- 8 Nicolas Bourbaki. *Elements of mathematics. Commutative algebra*. Hermann, Paris; Addison-Wesley Publishing Co., Reading, Mass., 1972. Translated from the French.
- 9 Matthias Büchse, Heiko Vogler, and Jonathan May. Determinization of weighted tree automata using factorizations. *J. Autom. Lang. Comb.*, 15(3-4):229–254, 2010.
- 10 Christian Choffrut. Une caractérisation des fonctions séquentielles et des fonctions sous-séquentielles en tant que relations rationnelles. *Theoret. Comput. Sci.*, 5(3):325–337, 1977. doi:10.1016/0304-3975(77)90049-4.
- 11 Harm Derksen, Emmanuel Jeandel, and Pascal Koiran. Quantum automata and algebraic groups. *J. Symbolic Comput.*, 39(3-4):357–371, 2005. doi:10.1016/j.jsc.2004.11.008.
- 12 Frederic Dörband, Thomas Feller, and Kevin Stier. Sequentiality of group-weighted tree automata. In *Language and automata theory and applications*, volume 12638 of *Lecture Notes in Comput. Sci.*, pages 267–278. Springer, Cham, [2021] ©2021. doi:10.1007/978-3-030-68195-1_21.
- 13 Manfred Droste, Werner Kuich, and Heiko Vogler, editors. *Handbook of weighted automata*. Monographs in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin, 2009. doi:10.1007/978-3-642-01492-5.
- 14 Walter Feit. Orders of finite linear groups. In *Proceedings of the First Jamaican Conference on Group Theory and its Applications (Kingston, 1996)*, pages 9–11. Univ. West Indies, Kingston, [1996].

- 15 Emmanuel Filiot, Raffaella Gentilini, and Jean-François Raskin. Quantitative languages defined by functional automata. *Log. Methods Comput. Sci.*, 11(3):3:14, 32, 2015. doi:[10.2168/LMCS-11\(3:14\)2015](https://doi.org/10.2168/LMCS-11(3:14)2015).
- 16 Zoltán Fülöp, Dávid Kószó, and Heiko Vogler. Crisp-determinization of weighted tree automata over strong bimonoids. *Discrete Math. Theor. Comput. Sci.*, 23(1):Paper No. 18, 44, 2021.
- 17 I. N. Herstein. *Noncommutative rings*, volume 15 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, DC, 1994. Reprint of the 1968 original, With an afterword by Lance W. Small.
- 18 Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, and James Worrell. Polynomial invariants for affine programs. In *LICS '18—33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, page 10. ACM, New York, 2018. doi:[10.1145/3209108.3209142](https://doi.org/10.1145/3209108.3209142).
- 19 Daniel Kirsten. Decidability, undecidability, and PSPACE-completeness of the twins property in the tropical semiring. *Theoret. Comput. Sci.*, 420:56–63, 2012. doi:[10.1016/j.tcs.2011.11.006](https://doi.org/10.1016/j.tcs.2011.11.006).
- 20 Daniel Kirsten and Sylvain Lombardy. Deciding unambiguity and sequentiality of polynomially ambiguous min-plus automata. In *STACS 2009: 26th International Symposium on Theoretical Aspects of Computer Science*, volume 3 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages 589–600. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2009.
- 21 Daniel Kirsten and Ina Mäurer. On the determinization of weighted automata. *J. Autom. Lang. Comb.*, 10(2-3):287–312, 2005.
- 22 Peter Kostolányi. Determinisability of unary weighted automata over the rational numbers. *Theoret. Comput. Sci.*, 898:110–131, 2022. doi:[10.1016/j.tcs.2021.11.002](https://doi.org/10.1016/j.tcs.2021.11.002).
- 23 James Kuzmanovich and Andrey Pavlichenkov. Finite groups of matrices whose entries are integers. *Amer. Math. Monthly*, 109(2):173–186, 2002. doi:[10.2307/2695329](https://doi.org/10.2307/2695329).
- 24 Sylvain Lombardy and Jacques Sakarovitch. Sequential? *Theoret. Comput. Sci.*, 356(1-2):224–244, 2006. doi:[10.1016/j.tcs.2006.01.028](https://doi.org/10.1016/j.tcs.2006.01.028).
- 25 Mehryar Mohri. Finite-state transducers in language and speech processing. *Comput. Linguist.*, 23(2):269–311, 1997.
- 26 Mehryar Mohri. Chapter 6: Weighted automata algorithms. In *Handbook of weighted automata*, Monogr. Theoret. Comput. Sci. EATCS Ser., pages 213–254. Springer, Berlin, 2009. doi:[10.1007/978-3-642-01492-5_6](https://doi.org/10.1007/978-3-642-01492-5_6).
- 27 Mehryar Mohri and Michael D. Riley. A disambiguation algorithm for weighted automata. *Theoret. Comput. Sci.*, 679:53–68, 2017. doi:[10.1016/j.tcs.2016.08.019](https://doi.org/10.1016/j.tcs.2016.08.019).
- 28 Klara Nosan, Amaury Pouly, Sylvain Schmitz, Mahsa Shirmohammadi, and James Worrell. On the Computation of the Zariski Closure of Finitely Generated Groups of Matrices. 2021. Preprint. [arXiv:2106.01853](https://arxiv.org/abs/2106.01853).
- 29 Jan Okniński. Strongly π -regular matrix semigroups. *Proc. Amer. Math. Soc.*, 93(2):215–217, 1985. doi:[10.2307/2044747](https://doi.org/10.2307/2044747).
- 30 Jan Okniński. Linear representations of semigroups. In *Monoids and semigroups with applications (Berkeley, CA, 1989)*, pages 257–277. World Sci. Publ., River Edge, NJ, 1991.
- 31 Jan Okniński. *Semigroups of matrices*, volume 6 of *Series in Algebra*. World Scientific Publishing Co., Inc., River Edge, NJ, 1998. doi:[10.1142/9789812816290](https://doi.org/10.1142/9789812816290).
- 32 Erik Paul. Finite sequentiality of unambiguous max-plus tree automata. *Theory Comput. Syst.*, 65(4):736–776, 2021. doi:[10.1007/s00224-020-10021-w](https://doi.org/10.1007/s00224-020-10021-w).
- 33 Mohan S. Putcha. *Linear algebraic monoids*, volume 133 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1988. doi:[10.1017/CB09780511600661](https://doi.org/10.1017/CB09780511600661).
- 34 Lex E. Renner. *Linear algebraic monoids*, volume 134 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2005. Invariant Theory and Algebraic Transformation Groups, V.

- 35 Jacques Sakarovitch. *Elements of automata theory*. Cambridge University Press, Cambridge, 2009. Translated from the 2003 French original by Reuben Thomas. doi:10.1017/CB09781139195218.
- 36 The Stacks project authors. The stacks project. <https://stacks.math.columbia.edu>, 2019.