

Max-Planck-Institut
für Mathematik
in den Naturwissenschaften
Leipzig

Toric varieties from cyclic matrix
groups

by

Francesco Galuppi and Mima Stanojkovski

Preprint no.: 25

2020



TORIC VARIETIES FROM CYCLIC MATRIX GROUPS

FRANCESCO GALUPPI AND MIMA STANOJKOVSKI

ABSTRACT. We study cyclic groups and semigroups of matrices from an algebraic geometric viewpoint. We prove that the irreducible components of their Zariski closures are toric varieties and study their geometry. In many cases, we are also able to determine their ideal or, in other words, we find all polynomials that vanish on such groups or semigroups. We present an implementation of our results in SageMath.

INTRODUCTION

In mathematics, as well as in many applied sciences, researchers often face the problem of describing a complicated behaviour or a sophisticated model. A common approach is to find properties that are shared by every status of the model or, in other words, to find *invariants*. Roughly speaking, an invariant is a function that attains the same value at every point of the model. Invariants are employed with different flavours in mathematics, physics and computer science in a wide range of contexts, from dynamical systems to control theory, from program verification to programming language semantics, from knot theory to combinatorics. For a rich list of further applications of invariants, we refer the interested reader to [7, Section 1].

From an algebraic viewpoint, the most meaningful invariants are polynomial functions. To compute the polynomials that vanish on a given model or set means to compute the closure of such set in the Zariski topology. A common approach in applied algebraic geometry is to give a model, coming from biology, statistics or computer science, the structure of an algebraic variety, thus allowing the use of powerful geometric techniques. On the other hand, these classes of models provide examples of families of varieties, whose geometry is interesting in their own right.

In this paper we are interested in algebraic subgroups of $\mathrm{GL}_n(\mathbb{C})$, that is, groups of matrices that are also algebraic varieties. The study of algebraic groups has a long story and a rich literature (see for instance the classic references [8, 12, 15]), but it is also motivated by concrete applications. For instance, groups generated by matrices appear naturally in dynamical systems (also referred to as *automata* or *affine programs*). One prominent question is the membership problem: given a finite number of matrices, how to determine whether one of them is in the group generated by the others? Despite partial results, the question is open in its full generality and a complete solution appears to be hard. A synthetic account on the history of the problem can be found in [1, Section 2]. One way invariants play a role here is in the following simplified version of the membership problem: given a finite number of matrices, how to determine whether one of them is in the closure of the group generated by the others? This leads to the computation of the Zariski closure of a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{C})$ and, consequently, to the evaluation of finitely many polynomial functions.

From a computer science viewpoint, the problem becomes to find an algorithm that, given a finite set of matrices, returns the Zariski closure of the group or the semigroup that they generate, see for instance [4, Theorem 9] and [7, Theorem 16]. However, these results focus on computability and do not give precise information on the geometric properties of the closure. It is our aim to better describe the geometry of these algebraic varieties and it is only natural to start with the simplest situation, i.e. the closure of a cyclic group or semigroup. In this case we are able to compute the dimension and the number of irreducible components of the closure. What strikes us as remarkable is that each such irreducible component turns out to be a *toric variety*. Roughly speaking, a variety is toric if it is the image of a monomial map. A toric variety not only has very pleasant properties - to name a few, it is irreducible, rational and its ideal is generated by binomials - but it can also be

1991 *Mathematics Subject Classification*. 14M25, 20G20.

We are very thankful to Bernd Sturmfels for suggesting this project and for his valuable feedback. We also thank Paul Görlach for insightful mathematical discussions. Finally, we thank Stefano Marseglia and Lorenzo Venturello for their useful SageMath tips.

associated to a polytope that completely encodes its geometry. This makes toric varieties accessible from a theoretical, combinatorial, and computational point of view. For instance, there are effective techniques to determine their degrees and their equations. For more information on toric varieties we refer to [3]. When dealing with non-cyclic subgroups, it is unclear whether the ideal of their closure is still binomial. This is however the case when the generating elements are finitely many diagonal matrices. We point out additionally that binomial ideals themselves sit in a very fertile ground between geometry, algebra, and combinatorics. An important reference on this topic is [5].

For the sake of the reader, we state here our main contributions. Throughout the paper, for a subset X of $\text{Mat}_n(\mathbb{C})$, we will denote by \overline{X} the Zariski closure of X in $\text{Mat}_n(\mathbb{C})$, regarded as \mathbb{C}^{n^2} . We will write $\dim(\overline{X})$, $\deg(\overline{X})$, and $\text{irr}(\overline{X})$ respectively for the dimension, degree, and number of irreducible components of \overline{X} . For a finitely generated abelian group G , i.e. a finitely generated \mathbb{Z} -module, we write G_{tor} for the torsion submodule of G and $\text{rk}(G)$ for the rank of a free complement of G_{tor} in G . For a finite group G , we denote by $|G|$ its order.

Theorem 1. *Let $M \in \text{GL}_n(\mathbb{C})$. Let $X = \langle M \rangle$ be the subgroup of $\text{GL}_n(\mathbb{C})$ generated by M and let G be the subgroup of \mathbb{C}^* generated by the eigenvalues of M . Then $\text{irr}(\overline{X}) = |G_{\text{tor}}|$ and each irreducible component of \overline{X} is a toric variety of dimension*

$$\dim \overline{X} = \begin{cases} \text{rk}(G) & \text{if } M \text{ is diagonalizable,} \\ \text{rk}(G) + 1 & \text{otherwise.} \end{cases}$$

Example 2. Let

$$M = \begin{pmatrix} 10 & -8 \\ 6 & -4 \end{pmatrix} \in \text{GL}_2(\mathbb{C})$$

and let X be the subgroup of $\text{GL}_2(\mathbb{C})$ generated by M . If we set

$$D = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} \text{ and } P = \begin{pmatrix} 1 & 4 \\ 1 & 3 \end{pmatrix},$$

then $M = PDP^{-1}$ and so M is diagonalizable with eigenvalues 2 and 4. The subgroup G of \mathbb{C}^* generated by the eigenvalues of M is $G = \langle 2, 4 \rangle = \langle 2 \rangle \cong \mathbb{Z}$ and so Theorem 1 yields that \overline{X} is an irreducible toric curve in \mathbb{C}^4 . This example was presented in [7, Section 2] in the setting of dynamical systems. Here we determine explicit equations describing the closure of X . Denoting the coordinates of \mathbb{C}^4 by

$$\begin{pmatrix} x & w \\ z & y \end{pmatrix},$$

we see that the three polynomials $f = z$, $g = w$, and $h = x^2 - y$ generate the ideal of $\overline{\langle D \rangle}$. Let $\phi: \mathbb{C}^4 \rightarrow \mathbb{C}^4$ be the linear automorphism defined by

$$\begin{aligned} \begin{pmatrix} x & w \\ z & y \end{pmatrix} &\mapsto P^{-1} \begin{pmatrix} x & w \\ z & y \end{pmatrix} P \\ &= \begin{pmatrix} -3x + 4y + 4z - 3w & -12x + 12y + 16z - 9w \\ x - y - z + w & 4x - 3y - 4z + 3w \end{pmatrix}. \end{aligned}$$

Then $\phi(\overline{X}) = \overline{\langle D \rangle}$, hence $f \circ \phi$, $g \circ \phi$ and $h \circ \phi$ generate the ideal of \overline{X} . With this choice of coordinates, the map ϕ is represented by the matrix

$$\begin{pmatrix} -3 & 4 & 4 & -3 \\ 4 & -3 & 4 & 3 \\ 1 & -1 & -1 & 1 \\ -12 & 12 & 16 & -9 \end{pmatrix},$$

therefore \overline{X} is described by the equations

$$\begin{cases} x + w = y + z, \\ 12x + 9w = 12y + 16z, \\ (-3x + 4y + 4z - 3w)^2 = 4x - 3y - 4z + 3w. \end{cases}$$

These are the strongest polynomial invariants, so they provide the tightest polynomial conditions that a point has to satisfy in order to belong to $\langle M \rangle$.

The following result generalizes Theorem 1 in the cyclic semigroup case and in the context of not necessarily invertible matrices.

Theorem 3. *Let $M \in \text{Mat}_n(\mathbb{C})$ and let $\nu \in \mathbb{Z}_{>0}$ be the largest size of a Jordan Block of M associated to 0. Write $X = \{M^k \mid k \in \mathbb{Z}_{>0}\}$ for the semigroup of $\text{GL}_n(\mathbb{C})$ generated by M . Let \mathcal{E} denote the collection of invertible eigenvalues of M and, if $\mathcal{E} \neq \emptyset$, let G be the subgroup of \mathbb{C}^* generated by \mathcal{E} . Then \overline{X} can be written as a disjoint union*

$$\overline{X} = X_0 \dot{\cup} X_1$$

of closed sets where

- (1) X_0 is a collection of points with

$$\text{irr}(X_0) = \begin{cases} 0 & \text{if } M \in \text{GL}_n(\mathbb{C}), \\ 1 & \text{if } M = 0, \\ \nu - 1 & \text{otherwise.} \end{cases}$$

- (2) either $X_1 = \mathcal{E} = \emptyset$ or X_1 is a union of $|G_{\text{tor}}|$ toric varieties of dimension

$$\dim X_1 = \begin{cases} \text{rk}(G) & \text{if } M^{\max\{1, \nu\}} \text{ is diagonalizable,} \\ \text{rk}(G) + 1 & \text{otherwise.} \end{cases}$$

The present paper being strongly motivated by results in computer science, in Section 4 we give an overview of existing algorithms and to propose a piece of code that we implemented in SageMath [17] and that relies on the results of this paper.

1. PROBLEM REDUCTION

The present section collects a number of classical result, which we will apply in order to prove Theorems 1 and 3. Recall that, given a subset X of $\text{Mat}_n(\mathbb{C})$, we denote by \overline{X} the Zariski closure of X in $\text{Mat}_n(\mathbb{C}) \cong \mathbb{C}^{n^2}$.

Lemma 4. *Let X be a subgroup of $\text{GL}_n(\mathbb{C})$ and let $g \in \text{GL}_n(\mathbb{C})$. Then $\overline{gXg^{-1}} = g\overline{X}g^{-1}$ and \overline{X} is isomorphic to $\overline{gXg^{-1}}$ as algebraic subvarieties of $\text{Mat}_n(\mathbb{C})$.*

Proof. Let $\phi : \text{Mat}_n(\mathbb{C}) \rightarrow \text{Mat}_n(\mathbb{C})$ denote conjugation under g , which is a homeomorphism restricting to an automorphism of the algebraic group $\text{GL}_n(\mathbb{C})$. As a consequence, \overline{X} and $\phi(\overline{X}) = g\overline{X}g^{-1}$ are isomorphic varieties. The morphism ϕ being a homeomorphism, we get $\phi(\overline{X}) = \overline{\phi(X)}$. \square

The following result is a combination of Lemmas 2.4.2 and 2.4.12 from [15] and is implied by the Jordan-Chevalley decomposition for $\text{GL}_n(\mathbb{C})$.

Lemma 5. *Let X be a subgroup of $\text{GL}_n(\mathbb{C})$. Then the following hold:*

- (1) *If X is commutative, there exists $g \in \text{GL}_n(\mathbb{C})$ such that gXg^{-1} consists of upper triangular matrices.*
- (2) *If X consists of unipotent matrices, then there exists $g \in \text{GL}_n(\mathbb{C})$ such that all elements of gXg^{-1} are upper unitriangular.*

In the present paper, we are concerned with Zariski closures of subsets of $\text{Mat}_n(\mathbb{C})$. However, when the subsets in play consist of invertible matrices, their closure is classically taken in $\text{GL}_n(\mathbb{C})$. The next Lemma shows that, when dealing with commutative subgroups, some important geometric properties do not depend on this choice.

Lemma 6. *Let X be a commutative subgroup of $\text{GL}_n(\mathbb{C})$. Then the Zariski closure $\overline{X} \cap \text{GL}_n(\mathbb{C})$ of X in $\text{GL}_n(\mathbb{C})$ is dense in \overline{X} .*

Proof. Thanks to Lemmas 4 and 5(1), we assume without loss of generality that the matrices in X are upper triangular. It is then clear that $\dim \overline{X} \leq n(n+1)/2$. Let $\Delta = \text{Mat}_n(\mathbb{C}) \setminus \text{GL}_n(\mathbb{C})$ denote the vanishing locus of the determinant. Assume for a contradiction that $\dim(\overline{X} \cap \text{GL}_n(\mathbb{C})) < \dim \overline{X}$. Since $\dim \Delta = n^2 - 1 > \dim \overline{X}$, there exists an irreducible component X_1 of \overline{X} that is contained in Δ . This yields that $X \cap X_1 = \emptyset$, which is a contradiction to \overline{X} being the minimal closed set containing X . \square

Remark 7. Analogously to what is done in the proof of Lemma 6, we may assume in the sequel that any commutative subgroup of $\mathrm{GL}_n(\mathbb{C})$ is given in upper triangular form (see Lemma 4 and Lemma 5(1)). Indeed, thanks to Lemma 6, dimension and number of irreducible components of \overline{X} are the same, independently of whether we look at them in $\mathrm{Mat}_n(\mathbb{C})$ or $\mathrm{GL}_n(\mathbb{C})$. This allows us to make use of the developed theory for linear algebraic groups, e.g. [8, 12, 15].

Besides the choice of the ambient space for the closure, i.e. $\mathrm{Mat}_n(\mathbb{C})$ or $\mathrm{GL}_n(\mathbb{C})$, other variations of the problem are to be found in the literature. As we pointed out in the introduction, given finitely many matrices, it is of interest to consider both the group and the semigroup they generate. The following result, already proven in [4, Lemma 2] for orthogonal matrices, shows that, for our purposes, it is equivalent whether we deal with groups or semigroups.

Lemma 8. *Let $M \in \mathrm{GL}_n(\mathbb{C})$ and denote by X and Y respectively the subgroup and the semigroup generated by M in $\mathrm{GL}_n(\mathbb{C})$, i.e.*

$$X = \{M^k \mid k \in \mathbb{Z}\} \text{ and } Y = \{M^k \mid k \in \mathbb{Z}_{>0}\}.$$

Then one has $\overline{X} = \overline{Y}$.

Proof. Let $U_X = \overline{X} \cap \mathrm{GL}_n(\mathbb{C})$ and $U_Y = \overline{Y} \cap \mathrm{GL}_n(\mathbb{C})$ denote respectively the closures of X and Y in $\mathrm{GL}_n(\mathbb{C})$. From [2, Lemma 1.1], we know that U_Y is a subgroup of U_X . Since U_X is the smallest closed subgroup of $\mathrm{GL}_n(\mathbb{C})$ containing M , the equality $U_X = U_Y$ holds. We now observe that $X \subseteq U_X \subseteq \overline{X}$ and so $\overline{X} = \overline{U_X}$. An analogous statement holds for U_Y and so we conclude that $\overline{X} = \overline{Y}$. \square

2. ZARISKI CLOSURE OF CYCLIC SUBGROUPS

The aim of Section 2 is to prove Theorem 1. As we will be dealing with cyclic subgroups of the form $X = \langle M \rangle$ with $M \in \mathrm{GL}_n(\mathbb{C})$, we will make implicit use, throughout the present section, of Lemma 4 by assuming that the matrix M is given in Jordan normal form.

2.1. The diagonalizable case. Let $a_1, \dots, a_n \in \mathbb{C}^*$ and let

$$M = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \in \mathrm{GL}_n(\mathbb{C})$$

be a diagonal matrix. Let $X = \{M^k \mid k \in \mathbb{Z}\}$ be the subgroup generated by M and observe that X is contained in a maximal torus. As a consequence, the dimension of \overline{X} is at most n . Define $G = \langle a_1, \dots, a_n \rangle \subseteq \mathbb{C}^*$ to be the group generated by the eigenvalues of M .

For the convenience of the reader, we collect in the following remark the facts about toric varieties that we will be needing in this section.

Remark 9. Given a finite set $\mathcal{A} = \{\alpha_1, \dots, \alpha_n\} \subset \mathbb{Z}^r$, define the map $\Phi_{\mathcal{A}} : (\mathbb{C}^*)^r \rightarrow (\mathbb{C}^*)^n$ by

$$x = (x_1, \dots, x_r) \mapsto (x^{\alpha_i} = x_1^{\alpha_{i1}} \cdots x_r^{\alpha_{ir}} \mid i \in \{1, \dots, n\}).$$

The closure of the image of $\Phi_{\mathcal{A}}$ is the toric variety denoted by $Y_{\mathcal{A}}$. The dimension of $Y_{\mathcal{A}}$ is the rank of the free group generated by \mathcal{A} . In other words, if $A \in \mathrm{Mat}_{r \times n}(\mathbb{Z})$ is the matrix whose columns are $\alpha_1, \dots, \alpha_n$, then $\dim Y_{\mathcal{A}} = \mathrm{rk} A$. Moreover, the ideal of $Y_{\mathcal{A}}$ is generated by the binomials $x^{\beta} - x^{\gamma}$ whenever $\beta, \gamma \in (\mathbb{Z}_{\geq 0})^r$ satisfy $\beta - \gamma \in \ker_{\mathbb{Z}}(A)$. For these facts and more, see [3, Section 1.1].

Example 10. Let us consider $\mathcal{A} = \{(3, -1), (0, 1), (1, 1)\}$. Then $\Phi_{\mathcal{A}} : (\mathbb{C}^*)^2 \rightarrow (\mathbb{C}^*)^3$ is given by

$$(x_1, x_2) \mapsto (x_1^3 x_2^{-1}, x_2, x_1 x_2).$$

In the notation of Remark 9, we have

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

and so $Y_{\mathcal{A}}$ has dimension $\mathrm{rk}(A) = 2$. Since $\ker_{\mathbb{Z}}(A) = \mathbb{Z}(1, 4, -3)$, the toric variety $Y_{\mathcal{A}}$ is defined by the equation $xy^4 = z^3$.

Proposition 11. *If G is torsionfree, then \overline{X} is a toric variety and $\dim \overline{X} = \mathrm{rk}(G)$.*

Proof. Set $r = \text{rk}(G)$. By hypothesis G is a free \mathbb{Z} -module of rank r . Let c_1, \dots, c_r be a \mathbb{Z} -basis of G . For every $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, r\}$ there then exists $\alpha_{ij} \in \mathbb{Z}$ such that

$$\begin{aligned} a_1 &= c_1^{\alpha_{11}} \cdot \dots \cdot c_r^{\alpha_{1r}}, \\ &\vdots \\ a_n &= c_1^{\alpha_{n1}} \cdot \dots \cdot c_r^{\alpha_{nr}}. \end{aligned}$$

We use this data to define the matrix

$$A = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{n1} \\ \vdots & & \vdots \\ \alpha_{1r} & \dots & \alpha_{nr} \end{pmatrix} \in \text{Mat}_{r \times n}(\mathbb{Z}).$$

Let $\mathcal{A} \subset \mathbb{Z}^r$ be the set of lattice points corresponding to the columns of A and let $Y_{\mathcal{A}}$ be the associated toric variety. By Remark 9, a set of generators of its ideal $I_{Y_{\mathcal{A}}}$ is given by binomials derived from a generating set of $\ker_{\mathbb{Z}}(A)$. Observe that every generator of $\ker_{\mathbb{Z}}(A)$ gives a binomial vanishing on X , so $I_{Y_{\mathcal{A}}} \subset I_X$. On the other hand, by [10, Proposition 5], the ideal I_X is generated by binomials with coefficients in $\{0, \pm 1\}$. For this reason, every generator of I_X gives a relation in G and therefore an element of $\ker_{\mathbb{Z}}(A)$. This shows that $I_X = I_{Y_{\mathcal{A}}}$, so $\overline{X} = Y_{\mathcal{A}}$ is a toric variety. Since $\dim \overline{X} = \text{rk } A$, in order to conclude it suffices to show that $\text{rk } A = r$.

Up to reordering, we assume that the first t columns of A are a basis for the \mathbb{Z} -module spanned by all of its columns. Since A has r rows, we clearly have that $t \leq r$. On the other hand, for every $j > t$, the j -th column $(\alpha_{j1}, \dots, \alpha_{jr})^{\top}$ is a \mathbb{Z} -linear combination of $(\alpha_{11}, \dots, \alpha_{1r})^{\top}, \dots, (\alpha_{t1}, \dots, \alpha_{tr})^{\top}$. Hence there exist $\lambda_{1j}, \dots, \lambda_{tj} \in \mathbb{Z}$ such that

$$\begin{aligned} \alpha_{j1} &= \lambda_{1j}\alpha_{11} + \dots + \lambda_{tj}\alpha_{t1}, \\ &\vdots \\ \alpha_{jr} &= \lambda_{1j}\alpha_{1r} + \dots + \lambda_{tj}\alpha_{tr}. \end{aligned}$$

This means that

$$\begin{aligned} a_j &= c_1^{\alpha_{j1}} \cdot \dots \cdot c_r^{\alpha_{jr}} = c_1^{\lambda_{1j}\alpha_{11} + \dots + \lambda_{tj}\alpha_{t1}} \cdot \dots \cdot c_r^{\lambda_{1j}\alpha_{1r} + \dots + \lambda_{tj}\alpha_{tr}} \\ &= c_1^{\lambda_{1j}\alpha_{11}} \cdot \dots \cdot c_r^{\lambda_{1j}\alpha_{1r}} \cdot \dots \cdot c_1^{\lambda_{tj}\alpha_{t1}} \cdot \dots \cdot c_r^{\lambda_{tj}\alpha_{tr}} \\ &= a_1^{\lambda_{1j}} \cdot \dots \cdot a_t^{\lambda_{tj}}. \end{aligned}$$

Therefore $a_{t+1}, \dots, a_n \in \langle a_1, \dots, a_t \rangle$ and so $t \geq r$. \square

We would like to point out that, in his PhD Thesis (University of Leipzig, 2020), Görlach generalizes Proposition 11 by showing that, if X is a group generated by finitely many diagonal matrices, then the irreducible components of \overline{X} are toric varieties.

The next result implies Theorem 1 for diagonalizable matrices.

Proposition 12. *The variety \overline{X} has $|G_{\text{tor}}|$ irreducible components, each of which is a toric variety of dimension $\text{rk}(G)$.*

Proof. Set $q = |G_{\text{tor}}|$. For every $i \in \{0, \dots, q-1\}$, define $X_i = \{M^{kq+i} \mid k \in \mathbb{Z}\}$. Then X is the disjoint union of the X_i 's and

$$\overline{X} = \overline{X_0 \cup \dots \cup X_{q-1}} = \overline{X_0} \cup \dots \cup \overline{X_{q-1}}.$$

Observe that $X_i = \{M^i \cdot (M^q)^k \mid k \in \mathbb{Z}\}$ equals the image of $\{(M^q)^k \mid k \in \mathbb{Z}\}$ under a linear automorphism of $\text{Mat}_n(\mathbb{C})$, namely multiplication by M^i . Moreover, it clearly holds that

$$M^q = \begin{pmatrix} a_1^q & & 0 \\ & \ddots & \\ 0 & & a_n^q \end{pmatrix}.$$

By construction, the group $\langle a_1^q, \dots, a_n^q \rangle$ is torsionfree of rank equal to $\text{rk}(G)$. Proposition 11 yields that \overline{X}_i has dimension $\text{rk}(G)$ and, being toric, \overline{X}_i is irreducible. \square

Example 13. Define $M \in \mathrm{GL}_2(\mathbb{C})$ to be the matrix

$$M = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 27i & 0 \\ 0 & -\exp(2\pi i/7)/9 \end{pmatrix}$$

and let $X = \langle M \rangle$ be the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by M . It is not difficult to show that $\langle a, b \rangle = \langle \exp(2\pi i/28), 3 \rangle \cong \mathbb{Z}/(28) \oplus \mathbb{Z}$ and so our Proposition 12 yields that \overline{X} is a union of 28 toric plane curves.

In light of Proposition 12, we can cook up cyclic subgroups of $\mathrm{GL}_n(\mathbb{C})$ whose closure has arbitrary dimension and arbitrary number of irreducible components. The next Example shows that we can also build varieties of any degree.

Example 14. Let d be a non-negative integer and define

$$M = \begin{pmatrix} 2 & 0 \\ 0 & 2^d \end{pmatrix} \in \mathbb{C}^2 \text{ and } X = \langle M \rangle.$$

Then \overline{X} is a smooth irreducible affine curve of degree d and equation $y = x^d$. Being toric, the curve \overline{X} is rational and thus, when $d \geq 3$, also singular at infinity.

It is worth to mention that, whenever \overline{X} is toric, there is an effective method for computing the degree of \overline{X} . Indeed, to do so, it suffices to compute the volume of a lattice polytope, as illustrated for example in [3, Theorem 13.4.1].

The next result shows that we can realize every toric variety as the Zariski closure of a cyclic subgroup of $\mathrm{GL}_n(\mathbb{C})$.

Proposition 15. *Let $Y \subseteq \mathbb{C}^n$ be an affine toric variety and identify \mathbb{C}^n with the space of diagonal matrices. Then there exists a diagonal $M \in \mathrm{GL}_n(\mathbb{C})$ such that $Y = \overline{\langle M \rangle}$ in \mathbb{C}^n .*

Proof. Let $\{\alpha_1, \dots, \alpha_n\} \subset \mathbb{Z}^r$ be a set of lattice points defining Y as a toric variety. Let

$$A = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{n1} \\ \vdots & & \vdots \\ \alpha_{1r} & \dots & \alpha_{nr} \end{pmatrix} \in \mathrm{Mat}_{r \times n}(\mathbb{Z})$$

be the matrix with columns $\alpha_1, \dots, \alpha_n$. Let c_1, \dots, c_r be r distinct prime numbers and set

$$\begin{aligned} a_1 &= c_1^{\alpha_{11}} \cdot \dots \cdot c_r^{\alpha_{1r}}, \\ &\vdots \\ a_n &= c_1^{\alpha_{n1}} \cdot \dots \cdot c_r^{\alpha_{nr}}. \end{aligned}$$

Finally, define $M = \mathrm{diag}(a_1, \dots, a_n)$. Following the proof of Proposition 11 backwards, we get $Y = \overline{\langle M \rangle}$. \square

When it comes to groups generated by two or more matrices, computing the dimension of their closures can become challenging. However, Proposition 12 helps to get some bounds, as the following examples show.

Example 16. Define $X = \langle A, B \rangle$ where

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}.$$

Then X contains as a subgroup

$$Y = \left\{ \begin{pmatrix} 2^h & 0 \\ 0 & 3^h \end{pmatrix} \mid h \in \mathbb{Z} \right\}.$$

From Proposition 11, it follows that $2 = \dim \overline{Y} \leq \dim \overline{X} \leq 2$ and thus \overline{X} is a surface. With the choice of coordinates from Example 2, we see that \overline{X} is the plane defined by $z = w = 0$ in \mathbb{C}^4 .

Example 17. Define $X = \langle A, B \rangle$ where

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

In contrast to Example 16, the closure of

$$Y = \left\{ \begin{pmatrix} 2^h & 0 \\ 0 & 2^h \end{pmatrix} \mid h \in \mathbb{Z} \right\}$$

does not fill the whole space of diagonal matrices. However, X contains many more cyclic subgroups, namely all

$$Y_d = \langle AB^d \rangle = \left\{ \begin{pmatrix} 2^h & 0 \\ 0 & 2^{h+d} \end{pmatrix} \mid h \in \mathbb{Z} \right\}$$

for $d \in \mathbb{Z}$. Thanks to Proposition 11, the closure of each Y_d is a curve. In particular, \overline{X} contains infinitely many curves and therefore it has dimension 2.

2.2. The general case. In this section we prove Theorem 1. To this end, let $M \in \mathrm{GL}_n(\mathbb{C})$ and let X be the subgroup of $\mathrm{GL}_n(\mathbb{C})$ generated by M . Denote by $\mathcal{E} \subseteq \mathbb{C}^*$ the collection of eigenvalues of M and let G be the subgroup of \mathbb{C}^* generated by \mathcal{E} . Without loss of generality, M is assumed to be given in Jordan normal form. Let M_s and M_u be respectively the semisimple and the unipotent part of M , which satisfy $M_s M_u = M_u M_s$. In particular, $M = M_s M_u$ is upper triangular, M_s is diagonal and M_u is upper unitriangular. We remark that the eigenvalues of M are the same as the eigenvalues of M_s . We define additionally $X_s = \overline{\{M_s^k \mid k \in \mathbb{Z}\}}$ and $X_u = \overline{\{M_u^k \mid k \in \mathbb{Z}\}}$.

Lemma 18. *Let $\lambda \in \mathbb{C}^*$, $k \in \mathbb{Z}_{\geq 0}$, and let $J(m, \lambda) = (b_{ij}) \in \mathrm{GL}_m(\mathbb{C})$ be defined by*

$$b_{ij} = \begin{cases} 1 & \text{if } i = j, \\ \lambda & \text{if } j = i + 1, \\ 0 & \text{otherwise.} \end{cases}$$

Write $J(m, \lambda)^k = (a_{ij})$. Then

$$a_{ij} = \begin{cases} 0 & \text{if } i > j, \\ \binom{k}{j-i} \lambda^{j-i} & \text{otherwise,} \end{cases} \quad (1)$$

and, for each $r \in \{1, \dots, m-1\}$, the following holds:

$$r! a_{1,r+1} = \prod_{i=0}^{r-1} (a_{12} - i\lambda). \quad (2)$$

Proof. Easy computation. □

The following example is meant to illustrate the ideas in the proof of Lemma 20, in which we deal with the unipotent part of our starting matrix.

Example 19. Define

$$M = \begin{pmatrix} -i & 1 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{5} & 1 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{5} & 1 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{5} & 1 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{5} \end{pmatrix} \in \mathrm{GL}_6(\mathbb{C}),$$

which is already in Jordan normal form. In this case

$$M_s = \begin{pmatrix} -i & 0 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{5} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{5} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{5} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{5} \end{pmatrix}, \quad M_u = \begin{pmatrix} 1 & i & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

By Lemma 18(1), for each $k \in \mathbb{Z}$ one has

$$M_u^k = \left(\begin{array}{cc|cccc} 1 & ki & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 5k & 5^2 \cdot \frac{k(k-1)}{2} & 5^3 \cdot \frac{k(k-1)(k-2)}{6} \\ 0 & 0 & 0 & 1 & 5k & 5^2 \cdot \frac{k(k-1)}{2} \\ 0 & 0 & 0 & 0 & 1 & 5k \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right).$$

If we denote by x_{ij} the 36 independent variables corresponding to the entries of a matrix in $\text{Mat}_6(\mathbb{C})$, we see that X_u is contained in the 4-dimensional linear space L defined by the equations

- (1) $x_{ij} = 0$ for $i < j$,
- (2) $x_{1j} = x_{2j} = 0$ for $j \geq 3$,
- (3) $x_{ii} = 1$ for $i \in \{1, \dots, 6\}$,
- (4) $x_{56} = x_{45} = x_{34}$,
- (5) $x_{35} = x_{46}$,
- (6) $5x_{12} = ix_{56}$.

We identify L with the affine space \mathbb{C}^4 , with coordinates x_1, x_2, x_3, x_4 corresponding to the entries $x_{33}, x_{34}, x_{35}, x_{36}$ of the first row of the second (and largest) block of M_u^k . Then X_u is in the image of the map $\mathbb{C} \rightarrow L$ defined by

$$t \mapsto \left(1, 5t, \frac{25t(t-1)}{2}, \frac{125t(t-1)(t-2)}{6} \right).$$

Since the image is a curve and X_u is infinite, the image actually coincides with X_u . After applying the change of coordinates

$$(x_1, x_2, x_3, x_4) \mapsto \left(x_1, \frac{x_2}{5}, \frac{2x_3}{25}, \frac{6x_4}{125} \right),$$

X_u is parametrized by $t \mapsto (1, t, t^2 - t, t^3 - 3t^2 + 2t)$. After the further change of coordinates

$$(x_1, x_2, x_3, x_4) \mapsto (x_1, x_2, x_3 - x_2, x_4 + 3x_3 + x_2),$$

we see that X_u is the image of $t \mapsto (1, t, t^2, t^3)$, so X_u is the twisted cubic curve in the hyperplane defined by $x_1 = 1$ in L .

Lemma 20. *Assume that $M_u \neq 1$ and let m be the biggest size of a Jordan block of M . Then X_u is a degree $m - 1$ rational normal curve.*

Proof. Let d denote the number of Jordan blocks of M , arbitrarily ordered. For each index $l \in \{1, \dots, d\}$, let λ_l and $m(l)$ denote respectively the eigenvalue and size corresponding to the l -th Jordan block of M . Set $J_l = J(m(l), \lambda_l^{-1})$ so that, for every $k \in \mathbb{Z}$, one has

$$M_u^k = \text{diag}(J_1^k, \dots, J_d^k).$$

Fix now $k \in \mathbb{Z}$ and write $a_{l,ij}$ for the (i, j) -th entry of J_l^k . By Lemma 18(1), all entries of J_l^k are linear functions of entries in the first row of J_l^k and thus, by Lemma 18(2), polynomials in $a_{l,12}$. Furthermore, by Lemma 18(1), two different blocks are compared via

$$a_{l,12} = k\lambda_l^{-1} = \frac{\lambda_s}{\lambda_l} \cdot k\lambda_s^{-1} = \frac{\lambda_s}{\lambda_l} \cdot a_{s,12}.$$

Fix $J \in \{J_1, \dots, J_d\}$ to be an element of maximal size m . Then X_u is contained in a linear space L of dimension m , with coordinates x_1, \dots, x_m corresponding to the entries of the first row of J . More precisely, X_u is contained in the image of the map $\tilde{f} : \mathbb{C} \rightarrow L$ defined by

$$t \mapsto \left(1, t\lambda^{-1}, \frac{t(t-1)}{2}\lambda^{-2}, \dots, \frac{1}{(m-1)!} \prod_{j=0}^{m-2} (t-j)\lambda^{-m+1} \right).$$

The image of \tilde{f} being an irreducible curve and X_u being infinite, $\tilde{f}(\mathbb{C}) = X_u$. After applying the first linear change of coordinates

$$(x_1, x_2, x_3, \dots, x_m) \mapsto (x_1, \lambda x_2, 2\lambda^2 x_3, \dots, (m-1)!\lambda^{m-1} x_m),$$

X_u is parametrized by

$$f(t) = \left(1, t, t(t-1), \dots, \prod_{j=0}^{m-2} (t-j) \right).$$

In order to see that X_u is a degree $m-1$ rational normal curve, we show that there are linear polynomials

$$l_1(x_1), l_2(x_1, x_2), \dots, l_m(x_1, \dots, x_m)$$

such that, for each $r \in \{1, \dots, m\}$, the map $\phi_r : \mathbb{C}^m \rightarrow \mathbb{C}^m$ defined by

$$\phi_r(x_1, \dots, x_m) = (l_1(x_1), \dots, l_r(x_1, \dots, x_r), x_{r+1}, \dots, x_m)$$

has the property that the first r entries of $f \circ \phi_r(x_1, \dots, x_m)$ equal $(1, t, t^2, \dots, t^{r-1})$. We define l_1, \dots, l_m recursively. Set $l_1(x_1) = x_1$ and $l_2(x_1, x_2) = x_2$. Assume now that l_1, \dots, l_r are given and let us define l_{r+1} . By the induction hypothesis, the change of variables

$$(x_1, \dots, x_m) \mapsto (l_1(x_1), \dots, l_r(x_1, \dots, x_r), x_{r+1}, \dots, x_m)$$

turns f into

$$t \mapsto \left(1, t, t^2, \dots, t^{r-1}, \prod_{j=0}^{r-1} (t-j), \dots, \prod_{j=0}^{m-2} (t-j) \right).$$

Now the $(r+1)$ -th entry is of the form $t^r + c_{r-1}t^{r-1} + \dots + c_1t + c_0$ for some $c_0, \dots, c_{r-1} \in \mathbb{C}$. We conclude by defining

$$l_{r+1}(x_1, \dots, x_{r+1}) = x_{r+1} - c_{r-1}x_r - \dots - c_1x_2 - c_0x_1,$$

which is linear in x_1, \dots, x_{r+1} and satisfies by construction the required inductive property. \square

Proposition 21. *The following equalities hold:*

$$\dim \bar{X} = \dim X_s + \dim X_u \text{ and } \text{irr}(\bar{X}) = \text{irr}(X_s).$$

Proof. By Remark 7, the dimension and the number of irreducible components of \bar{X} remain invariant when intersecting \bar{X} with $\text{GL}_n(\mathbb{C})$. For *this proof only*, we will write \bar{X} to mean the Zariski closure of X in $\text{GL}_n(\mathbb{C})$. This applies analogously to X_s and X_u . Recall that \bar{X} , X_s , and X_u are in this case subgroups of $\text{GL}_n(\mathbb{C})$, see for example [15, Lemma 2.2.4].

We start by showing that \bar{X} is abelian. Denote by $D_n(\mathbb{C})$ and $U_n(\mathbb{C})$ respectively the closed subgroups of diagonal and upper unitriangular matrices of $\text{GL}_n(\mathbb{C})$. Since $X_s \subseteq D_n(\mathbb{C})$ and $X_u \subseteq U_n(\mathbb{C})$, we have $X_u \cap X_s = \{1\}$. Since M_s and M_u commute, the commutator map $X_s \times X_u \rightarrow \text{GL}_n(\mathbb{C})$ is trivial on a dense subset of $X_s \times X_u$ and so, being continuous, it is trivial. In particular, X_s and X_u commute and, being \bar{X} contained in the internal direct product $X_s X_u$, the group \bar{X} is abelian.

The group \bar{X} being abelian, [8, Theorem 15.5] yields that $\bar{X} \cong X_s \times X_u$ (see also [12, Chapter 3.2, Problem 15]). In particular, we get $\dim \bar{X} = \dim X_s + \dim X_u$. Lemma 20 ensures that X_u is irreducible and thus we also have that $\text{irr}(\bar{X}) = \text{irr}(X_s)$. \square

We are finally ready to prove Theorem 1. From Proposition 21 we know that the equalities $\dim \bar{X} = \dim X_s + \dim X_u$ and $\text{irr}(\bar{X}) = \text{irr}(X_s)$ are satisfied. By Proposition 12, we have $\text{irr}(\bar{X}) = |G_{\text{tor}}|$, while its combination with Lemma 20 yields

$$\dim \bar{X} = \text{rk}(G) + \dim X_u = \begin{cases} \text{rk}(G) & \text{if } M_u = 1, \\ \text{rk}(G) + 1 & \text{otherwise.} \end{cases}$$

Corollary 22. *Let $q \in \mathbb{Z}$. If G is torsionfree, then $\bar{X} = \overline{\langle M^q \rangle}$.*

Proof. Let a_1, \dots, a_n be the eigenvalues of M and assume that G is torsionfree. Then the eigenvalues of M^q are a_1^q, \dots, a_n^q and $\langle a_1^q, \dots, a_n^q \rangle$ is a free \mathbb{Z} -submodule of G of the same rank as G . By Theorem 1, the varieties $\overline{\langle M \rangle}$ and $\overline{\langle M^q \rangle}$ are both irreducible of the same dimension. Since $\overline{\langle M \rangle} \supseteq \overline{\langle M^q \rangle}$, they are the same. \square

3. ZARISKI CLOSURE OF CYCLIC SEMIGROUPS

The purpose of this section is to prove Theorem 3. We start by an example, meant once again as an exemplification of the more general proof.

Example 23. Let $M \in \text{Mat}_n(\mathbb{C})$ be defined by

$$M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

and write $X = \{M^k \mid k \in \mathbb{Z}_{>0}\}$ for the semigroup of $\text{GL}_n(\mathbb{C})$ generated by M . Then $M^2 = \text{diag}(0, 0, 4)$ and thus we have

$$X = \{M\} \dot{\cup} \{\text{diag}(0, 0, 2^k) \mid k \geq 2\}.$$

We observe that the set $\{\text{diag}(0, 0, 2^k) \mid k \geq 2\}$ is clearly embeddable in \mathbb{C} and, consisting of infinitely many points, its closure has dimension 1. In particular, we get that

$$\overline{X} = \{M\} \dot{\cup} \{\text{diag}(0, 0, z) \mid z \in \mathbb{C}\}.$$

and so X is the disjoint union of a point and a line.

Until the end of this section, we will work under the hypotheses of Theorem 3. We proceed by considering disjoint cases.

Assume first that $\mathcal{E} = \emptyset$. In this case the only eigenvalue of M is 0, which implies that M is nilpotent and so $X = \overline{X}$ consists of finitely many points. If $M = 0$ then $\overline{X} = \{M\}$, so we assume that $M \neq 0$. It is not difficult to show that, in this case, M^ν is the smallest power of M that is equal to 0 and so \overline{X} consists of $\nu \geq 0$ points. To conclude define $X_0 = \overline{X}$ and $X_1 = \emptyset$. Assume now that M is invertible, equivalently $\nu = 0$ and $\mathcal{E} \neq \emptyset$. Define $X_0 = \emptyset$ and $X_1 = \overline{X}$. We are now done thanks to Theorem 1.

To conclude, assume that M is not invertible and $\mathcal{E} \neq \emptyset$. In this case, $\nu \geq 1$ and there exist m and p positive integers and matrices $N \in \text{Mat}_m(\mathbb{C})$ strictly upper triangular and $M_1 \in \text{GL}_p(\mathbb{C})$ upper triangular such that M has the following block shape:

$$M = \begin{pmatrix} N & 0 \\ 0 & M_1 \end{pmatrix}.$$

Fix such matrices N and M_1 . Then N is nilpotent and ν is the smallest exponent annihilating N . It follows then that

$$X = \{M^k \mid k \in \{1, \dots, \nu - 1\}\} \dot{\cup} \left\{ \begin{pmatrix} 0 & 0 \\ 0 & M_1^k \end{pmatrix} \mid k \geq \nu \right\}.$$

Write $X_0 = \{M^k \mid k \in \{1, \dots, \nu - 1\}\}$ and

$$Y_1 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & M_1^k \end{pmatrix} \mid k \geq \nu \right\}.$$

Then X_0 is a closed variety consisting of $\nu - 1$ points. Set $X_1 = \overline{Y_1}$. We observe that the semigroup generated by M_1 in $\text{GL}_p(\mathbb{C})$ is the image of Y_1 under a linear automorphism of $\text{Mat}_n(\mathbb{C})$. It follows from Lemma 8 that X_1 is isomorphic to the Zariski closure of $\langle M_1 \rangle$ in $\text{Mat}_p(\mathbb{C})$. We conclude this case thanks to Theorem 1 and the proof of Theorem 3 is now complete.

Corollary 24. *The dimension of $\overline{X} \subset \text{Mat}_n(\mathbb{C})$ is at most n .*

Proof. The dimension of \overline{X} is computed by Theorem 3. If M has n distinct eigenvalues, then it is diagonalizable. In this case $M^{\max\{1, \nu\}}$ is diagonalizable as well, so $\dim(\overline{X}) = \text{rk}(G) = n$. If M has a repeated eigenvalue, then $\dim(\overline{X}) \leq \text{rk}(G) + 1 \leq n$. \square

4. EFFECTIVE COMPUTATION OF CLOSURES OF MATRIX GROUPS

The present section is devoted to the question of effectively computing the Zariski closure of matrix groups. Ideally, we seek an algorithm that takes as input a list of matrices $M_1, \dots, M_t \in \text{Mat}_n(\mathbb{Q})$ and returns as output the ideal of the Zariski closure of the group or semigroup generated by M_1, \dots, M_t . If this were the case, we would have an algorithm computing the strongest polynomial invariants of $\langle M_1, \dots, M_t \rangle$.

A diverse literature on the subject is available and already several authors have produced algorithms in this direction. We discuss here briefly some of these results.

When all the matrices are invertible, it makes sense to consider the group they generate: an algorithm computing the closure of such group in $\mathrm{GL}_n(\mathbb{C})$ is presented in [4]. The computation of the closure in $\mathrm{Mat}_n(\mathbb{C})$ or $\mathrm{Mat}_n(\mathbb{R})$ of the generated semigroup is worked out in [7]. In [4] and [10] one can find ways to determine the equations of the group generated by one diagonal matrix. A large group of mathematicians and computer scientists have worked on related problems; see for example [1, 9, 13, 16].

As far as we know, no complexity analysis has been run in [4, 7, 10]. It is however worth to mention that all these algorithms rely on a polynomial-time algorithm of Ge [6, Theorem 1.1], dealing with units in number fields. The last author's work is generalized in [11, Theorem 1.11] to any \mathbb{Q} -algebra. To our knowledge, among the discussed algorithms, the only one that has been implemented is [10, Algorithm 3], in the software Mathematica 5 [18]. Its purpose is to find algebraic relations among recurrence sequences. In particular, when the sequences encode the powers of the eigenvalues of a diagonal matrix M , the algorithm outputs the ideal of $\overline{\langle M \rangle}$.

In this section, we present a first step in the direction of implementing these algorithms in favour of the interested community. We propose here a short algorithm based on the results stated in this paper and implemented in the software SageMath [17].

Given a square matrix M defined over \mathbb{Q} , our goal is to compute the Zariski closure of the semigroup generated by M over a suitable number field K . In light of what is discussed in Section 3, it is not restrictive to assume that M is invertible, so we do. Thanks to Lemma 8, moreover, the closure of the group and of the semigroup generated by M are the same. As a further simplification, we also assume that M is diagonalizable over the algebraic closure. Again, this assumption is not too strong, because the set of diagonalizable matrices is dense in $\mathrm{Mat}_n(\mathbb{Q})$ - in other words, the set of non diagonalizable matrices has measure zero.

Algorithm:

Input:: $n \in \mathbb{Z}_{>0}$, $M \in \mathrm{GL}_n(\mathbb{Q})$ diagonalizable
Output:: the ideal of the closure of $\langle M \rangle$ in $\mathrm{Mat}_n(K)$

Algorithm steps:

- (1) Use implemented SageMath commands to compute
 - the characteristic polynomial f of M ,
 - a splitting field K of f over \mathbb{Q} ,
 - a Jordan normal form C of M and $P \in \mathrm{GL}_n(K)$ such that $C = P^{-1}MP$,
 - a vector E of eigenvalues of M in K ;
- (2) Define a (minimal) set S of prime ideals of the ring of integers \mathcal{O}_K such that for $\mathfrak{p} \in S$ and $e \in E$ one has $\mathfrak{p} \nmid \mathcal{O}_K e$;
- (3) Use implemented SageMath command to compute the finitely generated subgroup U_S of S -units of K^* [then the group $G \subseteq \mathbb{C}^*$ generated by E is contained in U_S . A good reference on S -units is [14]];
- (4) Compute an integer q with $|G_{\mathrm{tor}}| \mid q \mid |(U_S)_{\mathrm{tor}}|$;
- (5) Compute the matrix A of the projection of G to the free part of U_S given by SageMath [see Proposition 12];
- (6) Compute the ideal of the toric variety associated to A in $K[x_0, \dots, x_{n-1}]$ [see Proposition 11. Here we refine the `ToricIdeal` command in SageMath to deal with incorrect cases, e.g. when $A = (1 \ 0)$];
- (7) For $i \in \{1, \dots, q\}$, multiply the $n \times n$ coordinate matrix by C^i to get the ideals of M^{i+qk} [see Proposition 12];
- (8) Compute the ideal of $\overline{\langle C \rangle}$ in $K[x_0, \dots, x_{n^2-1}]$;
- (9) Apply the change of variables induced by P to get the ideal of $\overline{\langle M \rangle}$ in $K[x_0, \dots, x_{n^2-1}]$.

We remark that our implemented algorithm is actually broader: it takes as input any invertible matrix M and works with its semisimple part M_s , computing the Zariski closure of the group generated by M_s .

REFERENCES

- [1] L. Babai, R. Beals, J. Cai, G. Ivanyos, and E. Luks. Multiplicative equations over commuting matrices. In *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms (Atlanta, GA, 1996)*, pages 498–507. ACM, New York, 1996.
- [2] J. Bernik. On groups and semigroups of matrices with spectra in a finitely generated field. *Linear Multilinear Algebra*, 53(4):259–267, 2005.
- [3] D. Cox, J. Little, and H. Schenck. *Toric varieties*, volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011.
- [4] H. Derksen, E. Jeandel, and P. Koiran. Quantum automata and algebraic groups. *J. Symbolic Comput.*, 39(3-4):357–371, 2005.
- [5] D. Eisenbud and B. Sturmfels. Binomial ideals. *Duke Math. J.*, 84(1):1–45, 1996.
- [6] G. Ge. *Algorithms related to multiplicative representations of algebraic numbers*. PhD thesis, University of California, Berkeley, 1993.
- [7] 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*, page 10. ACM, New York, 2018.
- [8] J. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York-Heidelberg, 1975. Graduate Texts in Mathematics, No. 21.
- [9] A. Jensen, T. Kahle, and L. Katthän. Finding binomials in polynomial ideals. *Res. Math. Sci.*, 4:Paper No. 16, 10, 2017.
- [10] M. Kauers and B. Zimmermann. Computing the algebraic relations of C -finite sequences and multisequences. *J. Symbolic Comput.*, 43(11):787–803, 2008.
- [11] H. W. Lenstra Jr. and A. Silverberg. Algorithms for commutative algebras over the rational numbers. *Found. Comput. Math.*, 18(1):159–180, 2018.
- [12] A. L. Onishchik and É. B. Vinberg. *Lie groups and algebraic groups*. Springer Series in Soviet Mathematics. Springer-Verlag, Berlin, 1990. Translated from the Russian and with a preface by D. A. Leites.
- [13] J. Ouaknine and J. Worrell. On the positivity problem for simple linear recurrence sequences. In *Automata, languages, and programming. Part II*, volume 8573 of *Lecture Notes in Comput. Sci.*, pages 318–329. Springer, Heidelberg, 2014.
- [14] M. Rosen. S -units and S -class group in algebraic function fields. *J. Algebra*, 26:98–108, 1973.
- [15] T. A. Springer. *Linear algebraic groups*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, second edition, 2009.
- [16] B. Sturmfels, R. Weismantel, and G. Ziegler. Gröbner bases of lattices, corner polyhedra, and integer programming. *Beiträge Algebra Geom.*, 36(2):281–298, 1995.
- [17] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.4)*, 2019. <https://www.sagemath.org>.
- [18] Inc. Wolfram Research. *Mathematica*, version 5.0 edition, 2003.

MAX PLANCK INSTITUTE FOR MATHEMATICS IN THE SCIENCES, INSELSTRASSE 22, 04103 LEIPZIG, GERMANY
E-mail address: galuppi@mis.mpg.de, stanojko@mis.mpg.de