Smith reduction and sublattices of finite rank with an application to toric varietes

DBW

November 21, 2010

Abstract

In this note I give a proof of the existence of a Smith normal form for matrices with integer entries. The existence of a good basis for a lattice with a finite index sublattice is a consequence of the Smith normal form. I conclude with an easy application to toric varieties.

Theorem 1. *Let A be a matrix with integer entries. Then there exist integer-values invertible matrices C and B such that $A = CDB$, where D is a diagonal integer-valued matrix.*

Proof. We call an elementary operation on a matrix the addition of an integer multiple of one row (or column) to another row (or column). By means of a combination of elementary operations one can exchange two rows or columns, at the cost of a minus sign. An elementary operation on a matrix A corresponds to the multiplication from the left or the right of A with an elementary matrix, which is a matrix that has 1 along the diagonal and vanishing entries off the diagonal, except at one off-diagonal entry, where it is integer-valued. Thus elemetary matrices are invertible and have unit determinant; in particular, a product of a finite number of elementary matrices is an integer-valued invertible matrix.

Let now $A = (a_{ij})_{1\leq i,j\leq n}$ be an integer-valued matrix. By exchanging rows and or columns, we may assume that $a_{11} \neq 0$. The greatest common divisor of the elements in the first row and the first column (i.e. all a_{ij} with i or j equal to 1) is an integer combination of the latter; hence we may arrive at the situation (by using the Euclidean algorithm) where a_{11} divides all elements of the first column and of the first row, by only using elemtary operations on A. Since now a_{11} divides all elements in the first row and first collumn, we can sweep the first row and column clean, and arrive at the following form of the matrix A:

$$A = LA'M\,, \qquad A' = \begin{pmatrix} d & 0 \\ 0 & \tilde{A} \end{pmatrix}\,. \tag{1}$$

But then the proof is finished by induction, as we can now focus on $\tilde{A}$. □

Remark 1. *The previous theorem states that for any integer-valued matrix, there exists a Smith normal form. This normal form is not unique however. The process described in the proof to obtain the Smith normal form is known as Smith reduction.*

Remark 2. *In the literature the above theorem is stated and proved in greater generality: For any integer-valued $n \times n$-matrix A there exist matrices $C, B \in \mathrm{SL}_n(\mathbb{Z})$ and integers $d_1, \dots, d_r$ such that d_i divides d_j for $i \leq j$ and $A = CDB$ with $D = \mathrm{diag}(0, \dots, 0, d_1, d_2, \dots, d_r)$. The proof is similar; if at the step where one obtains the desired form (1) one a_{ij} cannot be divided by a_{11}, one adds the ith column to the first and repeats the Euclidean algorithm to the first column, then after a finite number of steps a_{11} divides a_{ij}.*

Corollary 1 (Existence of a good basis)**.** *Let Λ be a lattice inside $\mathbb{Z}^n$, such that the quotient $\Lambda/\mathbb{Z}^n$ is a finite abelian group; thus Λ is a sublattice of finite index. Then there exists a basis $\{e_1, \dots, e_n\}$ of $\mathbb{Z}^n$ and nonzero integers $k_1, \dots, k_n$ such that the elements $k_1 e_1, \dots k_n e_n$ form a basis of Λ.*

Proof. Take any basis $\{m_1, \dots, m_n\}$ of Λ. Note, that any basis of Λ must have n elements, since there exist at most n linearly independent elements in $\mathbb{Z}^n$ and since $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ must be a real vector space of dimension n. Write A for the matrix whose columns are the basis vectors $m_1, \dots, m_n$. Then we can write $A = BKC$ with B and C invertible integer-valued matrices and K is a diagonal integer-valued matrix $K = \mathrm{diag}(k_1, \dots, k_n)$. The matrix AC^{-1} is a matrix whose columns are a basis for Λ. The matrix B is a matrix whose columns are a basis of $\mathbb{Z}^n$. Let us write $b_1, \dots, b_n$ for the columns of B. Then the columns of BK are the vectors $b_1 k_1, \dots, b_n k_n$. This proves the corollary. □

Proposition 1. *Any finitely generated abelian group is of the form $\mathbb{Z}^m \times \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_k}$.*

Proof. If G is a finitely generated group, there is an epimorphism $\mathbb{Z}^n \to G$. The kernel of this morphism is a sublattice Λ in $\mathbb{Z}^n$. Hence $G \cong \mathbb{Z}^n/\Lambda$. Let $e_1, \dots, e_n$ be the standard basis vectors of $\mathbb{Z}^n$ and let $b_1, \dots, b_r$ be any set of generators of Λ, where $r = \dim_{\mathbb{R}} \Lambda \otimes_Z \mathbb{R}$. Then we can adjoin $m = n - r$ elements of the e_i such that these together with the b_j form a basis for $\mathbb{Z}^n \otimes_{\mathbb{Z}} \mathbb{R}$. Thus we can decompose $\mathbb{Z}^n = \mathbb{Z}^m \times \mathbb{Z}^k$, with $k = n - m$ and where Λ lies in the second factor and is of finite index in $\mathbb{Z}^k$. We can find a basis $f_1, \dots, f_k$ of $\mathbb{Z}^k$ and integers $r_1, \dots, r_k$ such that $r_1 f_1, \dots, r_k f_k$ form a basis of Λ. But then $\mathbb{Z}^n/\Lambda = \mathbb{Z}^m \times (\mathbb{Z}^k/\Lambda)$ and in the obtained basis it is obvious to see that $\mathbb{Z}^k/\Lambda = \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_k}$. □

We now discuss a simple application of the Smith normal form to toric varieties; we show the one-to-one correspondences between integral commutative semigroups and affine toric varieties. All our semigroups are commutative and we will work over an algebraically closed field k, with arbitrary characteristic though.

If S is a semigroup, we write $k[S]$ for the k-algebra generated by all elements x^s where s runs over all elements of S. We will restrict to finitely generated semigroups, so that the k-algebras $k[S]$ will always be finitely generated, hence noetherian. Even more, we will assume our semigroups are integral, by which we mean that they can be embedded into $\mathbb{Z}^n$. Then automatically $k[S]$ will always be finitely generated and admits an embedding $k[S] \to k[Z^n] = k[X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}]$. It follows that $k[S]$ is a domain, thus $X_S = \mathrm{Spec}(k[S])$ is an integral scheme over k.

Definition 1. *For any integral semigroup S we define the universal enveloping group of S to be a group $G(S)$ with an injective morphism $i_S : S \to G(S)$ such that for any morphism of semigroups $f : S \to H$, where H is a group, there exists a unique morphism $j : G(S) \to H$ such that $f = j \circ i_S$.*

Theorem 2. *For any integral semigroup S the universal enveloping group exists and is unique up to isomorphism.*

Proof. Uniqueness of $G(S)$ is obvious by the requirement of the uniqueness of the morphism $i_S : S \to G(S)$ announced in the definition, hence existence is all that is required to prove. We first fix some embedding $S \to \mathbb{Z}^n$ and consider then the subgroup $G(S)$ in $\mathbb{Z}^n$ generated by all elements of S. That is, $G(S)$ consists of all elements $s - s'$, where $s, s' \in S$. If $f : S \to H$ is some morphism of semigroups with H a group, then $j(s - s')$ has to be $j(s) - j(s')$, which is unambiguously defined as the image of S necessarily lies in the centre of H. Thus uniqueness is proved. □

Hence for any semigroup S we have a canonical morphism of affine k-schemes $\mathrm{Spec}(k[G(S)]) \to \mathrm{Spec}(k[S]$. The object $\mathrm{Spec}(k[G(S)])$ is a torus.

Lemma 1. *Let S be an integral semigroup. The morphism of k-schemes* $\mathrm{Spec}(k[G(S)]) \to \mathrm{Spec}(k[S]$ *is an open embedding.*

Proof. We have to prove that the image of $\mathrm{Spec}(k[G(S)]) \to \mathrm{Spec}(k[S]$ is an open subset in $X_S = \mathrm{Spec}(k[S]$. If S is generated by elements $s_1, \ldots, s_n$, then $G(S)$ is as a group generated by elements $s_1, \ldots, s_n$ and $y = -(s_1 + \ldots + s_n)$. Hence $k[G(S)] = k[S]_y$, which is a localization at y, and hence $rmSpec(k[G(S)])$ is a principal open subset of X_S. □

Corollary 2. *The dimension of* $\mathrm{Spec}(k[S])$ *is the rank of the group $G(S)$.*

Definition 2. *We define the category of affine toric varieties as the category with objects* $\mathrm{Spec}(k[S])$*, where S is an integral semigroup, and where the morphisms are the morphisms of k-schemes* $\mathrm{Spec}(k[S']) \to \mathrm{Spec}(k[S])$*induced by a morphism of semigroups $S \to S'$.*

It is not hard to paraphrase the above definition in terms of objects $T \to X$, where X is the spectrum of a k-algebra $k[S]$ with S an integral semigroup and with T a torus and with morphisms $(T, X) \to (T', X')$ a commuting diagram

$$\begin{array}{ccc} T & \longrightarrow & T' \\ \downarrow & & \downarrow \\ X & \longrightarrow & X' \end{array}$$

So we have seen that integral semigroups induce a couple (T, X) where X is an affine variety with an open embedding of the torus T in X, such that the action of T on itself extends to an action of T on X; we have a morphism of k-algebras $k[X] \to k[T] \otimes k[X]$ given by $x^s \mapsto x^s \otimes x^s$, for any $s \in S$. Now we proceed to prove that given an affine variety X with an open embedding of a torus T in X, such that the action of T on itself extends to an action of T on X, there is a semigroup such that $X = \mathrm{Spec}(k[S])$ and $T = \mathrm{Spec}(k[G(S)]$. This is where the usage of the Smith normal form will appear.

Theorem 3. *Let X be an affine variety over k and $T \to X$ an open embedding of a torus T in X, such that the action of T on itself can be extended to an action of T on X. Then there is an integral semigroup S such that $T \cong \mathrm{Spec}(k[G(S)])$ and $X = \mathrm{Spec}(k[S])$, and the open embedding $T \to X$ is induced by the morphism of algebras $k[S] \to k[G(S)]$.*

Proof. We can always write $T = \mathrm{Spec}(k[\mathbb{Z}^n])$ for some n. Since X is affine it is the spectrum of some k-algebra A. Since the action of the torus extends, we have a commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & A \otimes_k k[\mathbb{Z}^n] \\ \downarrow & & \downarrow \\ k[\mathbb{Z}^n] & \longrightarrow & k[\mathbb{Z}^n] \otimes_k k[\mathbb{Z}^n] \end{array}$$

where the vertical maps are embeddings. Hence $A \subset k[\mathbb{Z}^n]$ and if $\sum a_\alpha x^\alpha$ is in A, the morphism $A \to A \otimes k[\mathbb{Z}^n]$ is given by $\sum a_\alpha x^\alpha \mapsto \sum a_\alpha x^\alpha \otimes x^\alpha$. But then it follows that $A = \bigoplus kx^\alpha$, where the sum runs over all α, such that x^α is in A. Since A is a ring, it follows that A is of the form $k[S]$ with S some sub-semigroup of $\mathbb{Z}^n$.

The proof is thus finished if we can show that $G(S) = \mathbb{Z}^n$. As the dimensions of T and X must match, we see that S must generate a rank n sublattice Λ. If this is a proper lattice, then by the existence of a good basis we can find a basis $e_1, \ldots, e_n$ of $\mathbb{Z}^n$ such $k_1 e_1, \ldots, k_n e_n$ is a basis of Λ, where $k_i \geq 1$ are not all equal to one. On the level of coordinates inside some affine space, the morphism $k[S] \to k[\mathbb{Z}^n]$ then corresponds to $x_i \mapsto x_i^{k_1}$, which is not an embedding unless all k_i are equal to one. Hence $\mathbb{Z}^n = \Lambda$ and $G(S) = \mathbb{Z}^n$.

□