Алгебра и анализ
Том 26 (2014), № 5

St. Petersburg Math. J.
Vol. 26 (2015), No. 5, Pages 797–811
http://dx.doi.org/10.1090/spmj/1359
Article electronically published on July 27, 2015

TROPICAL NOETHERITY AND GRÖBNER BASES

YA. KAZARNOVSKIĬ AND A. G. KHOVANSKIĬ

Abstract. A set that is a Gröbner basis for an ideal with respect to every Gröbner ordering is called a universal Gröbner basis for that ideal. In the paper, it is proved that there exists a universal Gröbner basis in which the polynomials have controlled degrees. The main result is the theorem on the *tropical Noetherity* of a ring of Laurent polynomials. This theorem is close to the existence theorem for a universal basis and is needed for the *tropical intersection theory* in $(\mathbb{C}^*)^n$, which will be presented in a forthcoming paper.

Introduction

In this paper, we prove that the ring $\mathcal{R}$ of Laurent polynomials in n variables over an arbitrary field $\mathbf{k}$ is tropically Noetherian (see below). This commutative algebra theorem is involved in various descriptions of a specific version of the Chow ring, the so-called ring of conditions (see below and [1, 2]), for the group $(\mathbb{C}^*)^n$; we prepare such descriptions for publication. The present paper is independent of that material and is comparatively elementary. It employs neither the intersection theory and toric geometry, nor the theory of mixed volumes, nor the constructions of tropical geometry required for the description of the ring of conditions. We believe that this paper is of independent interest.

In the Introduction, we define the notion of tropical Noetherity, outline the content of the paper, and briefly discuss the ring of conditions for the group $(\mathbb{C}^*)^n$.

A Laurent polynomial $P = \sum c_m z^m \in \mathcal{R}$ is a linear combination of monomials $z^m = z_1^{m_1} \dots z_n^{m_n}$, where $m = (m_1, \dots, m_n) \in \mathbb{Z}^n$ and $c_m \in \mathbf{k}$. The support $S(P)$ of a Laurent polynomial P is the set of points $m \in \mathbb{Z}^n$ for which $c_m \neq 0$. With every linear function $f\colon \mathbb{R}^n \to \mathbb{R}$ on the space $\mathbb{R}^n$ containing the lattice $\mathbb{Z}^n$, we associate the *truncation* $P^{(f)}$ *of* $P = \sum c_m z^m$ with respect to the order f. By definition, $P^{(f)} = \sum_{m \in B} c_m z^m$, where B is the subset of the support $S(P)$ of P on which the linear function f attains its maximal value. With every ideal $I \subset \mathcal{R}$ and every order f, we associate the ideal $I^{(f)}$ generated by the truncations of all Laurent polynomials in I with respect to the order f (if $f \equiv 0$, the ideals I and $I^{(f)}$ coincide).

A finite set $\{Q_j\} \subset I$ is called a *system of tropical generators* of an ideal I if, for every order f, the ideal $I^{(f)}$ is generated by the Laurent polynomials $\{Q_j^{(f)}\}$.

Remark 1. The notion of tropical generators of an ideal is close to that of an H-basis (see, e.g., [18, 19]). We thank the referee for this remark.

We prove that the ring $\mathcal{R}$ is *tropically Noetherian*: every ideal I of the ring $\mathcal{R}$ has a system of tropical generators. We prove the existence of tropical generators, and also

2010 *Mathematics Subject Classification.* Primary 16S34.

Key words and phrases. Laurent polynomial, ideal, tropical basis, universal Gröbner basis, Seidenberg theorem.

The first author was partially supported by the grant SS-4850.2012.1; the second author was partially supported by the Canadian grant 0GP0156833.

obtain a fairly explicit description of them. We remark that somewhat weaker similar results were known earlier (cf. [3, 4]).

Theorem. *For each finite set $A \subset \mathbb{Z}^n$, there exists a finite set $\Phi(A) \subset \mathbb{Z}^n$ with the following property: for every ideal I of the ring $\mathcal{R}$ and a system of generators of I with supports in A, one can choose a system of tropical generators $\{Q_j\}$ with supports $S(Q_j)$ lying in $\Phi(A)$.*

In a somewhat sharper form, this theorem is stated and proved in §7. The proof involves the Seidenberg theorem (see §1 and [5, 6]), which refines the Noetherity property of polynomial rings and the Gröbner bases technique. This machinery is partially based on simple results on linear spaces with completely ordered bases (see §2). A slightly bulkier part of this technique is related to the definitions of a Gröbner ordering (see Subsection 2.4) and a Gröbner basis, and also to Buchberger's theorem and Buchberger's algorithm (see §3).

In Subsection 5.1, we estimate the degrees of the polynomials arising in the application of the Buchberger algorithm. It is very important that the estimates obtained depend only on the degrees of the polynomials to which the procedure is applied and do not depend on a Gröbner ordering. The estimates are based on the description of all possible linear orderings on finite subsets of the lattice $\mathbb{Z}^n$ and involve simple considerations from convex geometry (see §4).

In Subsection 5.2, we estimate the degrees of the polynomials in a Gröbner basis in terms of the degrees of the generators of the ideal in question. The resulting estimates do not depend on a Gröbner ordering. They are based on Seidenberg's theorem and on the estimates obtained in Subsection 5.1.

In §6, we give a sufficiently explicit (however, practically not implementable) construction of a *universal Gröbner basis* of an ideal and estimate the degrees of the polynomials in this basis in terms of the degrees of the generators of the ideal. This result, which is not used in this paper, follows directly from the estimates in Subsection 5.2 and demonstrates the strength of these estimates.

§7 contains the main theorem (on the tropical Noetherity of the ring of Laurent polynomials). This theorem also follows easily from the estimates proved in Subsection 5.2.

In the remaining part of the Introduction, we very briefly discuss the ring of conditions for the group $(\mathbb{C}^*)^n$. The reader can skip this part without detriment to the understanding of the paper (the ring of conditions does not appear in the present paper, but the study of it was the main motivation for our results).

The following version of the Chow ring is well known for an n-dimensional reductive group G (see [1, 2]). Two k-dimensional subvarieties X_1 and X_2 of G are *equivalent*, $X_1 \sim X_2$, if $\#(X_1 \cap g_1 Y g_2) = \#(X_2 \cap g_1 Y g_2)$ for every $(n-k)$-dimensional subvariety $Y \subset G$ and almost all $g_1, g_2 \in G$. If $X_1 \sim X_2$ and $Y_1 \sim Y_2$, then the varieties $X_1 \cap g_1 Y_1 g_2$ and $X_2 \cap g_3 Y_2 g_4$ are equivalent for almost all $g_1, g_2, g_3, g_4 \in G$. Thus, on the equivalence classes of subvarieties we have a product that, to every two classes, assigns the intersection of their representatives (put, if necessary, in the general position by the left-right action of the group). The *ring of conditions* $R(G)$ of a group G is the ring of formal linear combinations of equivalence classes with the multiplication described above and extended by linearity to the linear combinations.

The following description of the ring $R((\mathbb{C}^*)^n)$ was given in [8]. For each k-dimensional subvariety $X \subset (\mathbb{C}^*)^n$, we have a certain k-dimensional tropical fan C_X in $\mathbb{R}^n$ (a specific k-dimensional real cycle, which is a linear combination of k-dimensional rational cones) such that $(C_X = C_Y) \Leftrightarrow (X \sim Y)$. A geometric description of all fans of the form C_X and a geometric construction of the tropical fan $C_{X \cap Y}$ by two tropical fans C_X and C_Y are given. Thus, the paper [8] contains a description of the *ring of tropical fans* C_X

isomorphic to the ring $R((\mathbb{C}^*)^n)$. Some close results are contained in [3]. Several nice and strong results in tropical geometry can be found in [9, 10, 11].

We have found a new description of the ring $R((\mathbb{C}^*)^n)$ in the terms of mixed volumes of integral polytopes. We completely revised the results of the paper [8] and proved that the ring defined in terms of mixed volumes is isomorphic to the ring of tropical fans. These results are being prepared for publication, see [12]. All of them employ the theorem in commutative algebra to which the present paper is devoted.

§1. Seidenberg's theorem

In this section, we state Seidenberg's theorem for a polynomial ring and its counterpart for the semigroup $\mathbb{Z}^n_{\geq 0}$.

1.1. Polynomial rings. The ring $R = \mathbf{k}[z_1, \ldots, z_n]$ of polynomials in n variables over an arbitrary field $\mathbf{k}$ is *Noetherian*, i.e., every strictly ascending chain

$$I_1 \subset I_2 \subset \cdots \subset I_i \subset \ldots \tag{1}$$

of ideals in R terminates eventually. Abraham Seidenberg proved the theorem (see [5, 6]), that can be stated as follows.

Seidenberg's theorem. *Let f be a strictly monotone increasing function defined on the set of integers. Suppose that, for every i, the ideal I_i in* (1) *is generated by polynomials of degree at most $f(i)$. Then the number of ideals in* (1) *does not exceed a number g_n, which can be calculated explicitly by the function f and the dimension n.*

In the initial papers [5, 6], the phrase "g_n can be calculated explicitly by the function f and the dimension n" has a sharper meaning. The remarkable paper [7] by Guillermo Moreno refines Seidenberg's theorem. In particular, that paper contains examples showing that, even for the simplest increasing function $f(i) = i$, the number g_n as a function of n increases tremendously and is not a *primitive recursive function of* n (see [7]). For our needs, Seidenberg's theorem in the form given above is sufficient. For the details, we refer the reader to the well-written paper [7].

1.2. The semigroup $\mathbb{Z}^n_{\geq 0}$. With every point $m \in \mathbb{Z}^n_{\geq 0}$, we associate the *octant O_m with vertex m* defined by $O_m = \mathbb{Z}^n_{\geq 0} + m$. We recall the following important *finiteness property* of the semigroup $\mathbb{Z}^n_{\geq 0}$ (see, e.g., [13]): the union of an arbitrary set of octants can be represented as a finite union of octants. A subset $J \subset \mathbb{Z}^n_{\geq 0}$ is called an *ideal* in the semigroup $\mathbb{Z}^n_{\geq 0}$ if $m + a \in J$ for all $m \in J$ and $a \in \mathbb{Z}^n_{\geq 0}$. The semigroup $\mathbb{Z}^n_{\geq 0}$ *is Noetherian*, i.e., every strictly ascending chain

$$J_1 \subset J_2 \subset \cdots \subset J_i \subset \ldots \tag{2}$$

of its ideals terminates eventually. This fact is equivalent to the finiteness property of the semigroup $\mathbb{Z}^n_{\geq 0}$. The following statement is also equivalent to the finiteness property of the semigroup $\mathbb{Z}^n_{\geq 0}$: *every ideal $J \subset \mathbb{Z}^n_{\geq 0}$ has a finite number of generators*, i.e., there exists a finite set $G \subset J$ such that every element of J can be represented in the form $m+a$ with $m \in G$ and $a \in \mathbb{Z}^n_{\geq 0}$. By definition, the *degree of a point* $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n_{\geq 0}$ is the number $|m| = m_1 + \cdots + m_n$.

Seidenberg's theorem for $\mathbb{Z}^n_{\geq 0}$. *Let f be a strictly monotone increasing function defined on the set of positive integers. Suppose that the generators of the J_i in* (2) *have degrees at most $f(i)$. Then the number of ideals in* (2) *does not exceed a number g_n, which can be calculated explicitly by the function f and the dimension n.*

With every point $m = (m_1, \dots, m_n) \in \mathbb{Z}^n_{\geq 0}$, we associate the monomial $z^m = z_1^{m_1} \cdot \dots \cdot z_n^{m_n}$. For every ideal $J \subset \mathbb{Z}^n_{\geq 0}$, we consider the ideal $I(J)$ in R consisting of all linear combinations of the monomials z^m for $m \in J$. For the chain (2), Seidenberg's theorem for $\mathbb{Z}^n_{\geq 0}$ follows from Seidenberg's theorem applied to the chain of ideals $I(J_1) \subset I(J_2) \subset \dots \subset I(J_i) \dots$

Remark 2. Using the Gröbner bases technique, it is easy to prove that Seidenberg's theorem is equivalent to its counterpart for the semigroup $\mathbb{Z}^n_{\geq 0}$. The paper [7] contains the proof of the claim for this semigroup, and Seidenberg's theorem is deduced from it.

§2. Linear spaces with ordered bases

A linear space K (in general, infinite-dimensional) over $\mathbf{k}$ with a fixed basis $\{e_m\}$ indexed by the elements of a set $\mathcal{M}$ equipped with a well-ordering $\prec$ is called a *space with a well-ordered basis*.

2.1. Inversion of operators in a space with an ordered basis. We start with a simple statement valid for the vector spaces without an additional structure. An operator $A\colon L \to L$ acting in a (infinite-dimensional) vector space L over $\mathbf{k}$ is said to be *generalized nilpotent* if, for every vector $x \in L$, there is a number k (depending on x) such that $A^k x = 0$.

Proposition 1. *Let E be the identity operator, and let A be a generalized nilpotent operator. Then the operator $E - A$ is invertible, i.e., the operator*

$$B = E + A + A^2 + \dots$$

is well defined and $(E - A)B = E$.

Proof. Indeed, the definition of generalized nilpotency implies that, for every $x \in L$, there is k such that $A^k x = 0$. Therefore, the vector Bx is well defined and is equal to $(E + A + \dots + A^{k-1})x$. Hence, $(E - A)Bx = (E - A^k)x = x$. □

Let K be a space with a well-ordered basis $\{e_m\}$. We say that an operator $A\colon K \to K$ is *upper triangular* in the basis $\{e_m\}$ if, for each index $m \in \mathcal{M}$, in the formula $A(e_m) = \sum \mu_p e_p$ the coefficient μ_p is zero if $m \prec p$ or $m = p$.

Proposition 2. *An upper triangular operator is generalized nilpotent.*

The proof is based on Lemma 3 stated below.

We say that a correspondence C assigning a finite (possibly, empty) subset $C(m)$ of $\mathcal{M}$ to $m \in \mathcal{M}$ is *finitely multivalued decreasing map* if $m \succ g$ for all $m \in \mathcal{M}$ and $g \in C(m) \subset \mathcal{M}$. Let C be a finitely multivalued decreasing map. We say that a sequence $m_1, \dots, m_k \in \mathcal{M}$ is a *C-sequence* if $m_{i+1} \in C(m_i)$ for each $i = 1, \dots, k-1$ (if $C(m_i) = \varnothing$, then the sequence terminates at the term m_i).

Lemma 3. *Every C-sequence $m_1, \dots, m_k$ with a given first term $m_1 = m \in \mathcal{M}$ has length $k \leq N(C, m)$ bounded from above.*

Proof. Assume that there exist arbitrarily long C-sequences starting at $m = m_1$. Since the set $C(m_1)$ is finite, there is a point $m_2 \in C(m_1)$ such that there exist arbitrarily long C-sequences starting at m_1, m_2. Similarly, there is a point $m_3 \in C(m_2)$ such that there exist arbitrarily long C-sequences starting at m_1, m_2, m_3. Continuing this process, we obtain an infinite sequence $m_1 \succ m_2 \succ \dots$. The existence of such a sequence contradicts the fact that the set $\mathcal{M}$ is well-ordered. The lemma is proved. □

Proof of Proposition 2. Let A be an upper triangular operator in a basis $\{e_m\}$. With the operator A, we associate a finitely multivalued decreasing map C defined as follows: the set $C(m)$ coincides with the set of indices m_i for which the coefficients μ_i in the expansion $Ae_m = \sum \mu_i e_{m_i}$ are nonzero (if $Ae_m = 0$, then the set $C(m)$ is empty). By Lemma 3, there is a number $N(m, C)$ such that the length of each C-sequence starting at m is less than $k = N(m, C)$. It is clear that $A^k e_m = 0$. Thus, Proposition 2 follows. □

Theorem 4. *An operator equal to the sum of the identity operator and an upper triangular operator is invertible.*

This follows from Propositions 1 and 2.

2.2. The $\mathcal{M}$-valuation map and direct sum decompositions. Let $v = \sum c_m(v)e_m$ be a nonzero vector in a space K with a well-ordered basis $\{e_m\}$. The coefficients $c_m(v)$ are nonzero on a finite set $S(v) \subset \mathcal{M}$ called the *support* of the vector v.

Definition 1. The map $N_{\mathcal{M}} \colon (K \setminus \{0\}) \to \mathcal{M}$ that, to any vector $v \in K \setminus \{0\}$, assigns the maximal (with respect to the ordering $\prec$) point $N_{\mathcal{M}}(v) \in S(v)$ in the support of v is called the $\mathcal{M}$-*valuation*.

We describe a construction that employs the $\mathcal{M}$-valuation and, with every linear space $L \subset K$, associates a complement $L^\perp \subset K$ (i.e., a space such that $L \oplus L^\perp = K$). For a space $L \subset K$, we consider the following sets:

the image $N_{\mathcal{M}}(L \setminus \{0\}) = \mathcal{J}$ of the set $L \setminus \{0\}$ under the $\mathcal{M}$-valuation;

the complement $\mathcal{M} \setminus \mathcal{J} = \mathcal{J}^\perp$ to the set $\mathcal{J}$ in $\mathcal{M}$.

We define the space $L^\perp$ as the space generated by the vectors e_m for $m \in J^\perp$. The relation $K = L \oplus L^\perp$ is proved below in Theorem 5.

For each point $p \in \mathcal{J}$, we fix a vector $g_p \in L$ such that $N_{\mathcal{M}}(g_p) = e_p$, i.e., $g_p = e_p + \sum \mu_i e_{m_i}$, where $m_i \prec p$. For every index $m \in \mathcal{M}$, we define the following vector $f_m \in K$:

if $m \in \mathcal{J}$, then $f_m = g_m$;

if $m \in \mathcal{J}^\perp$, then $f_m = e_m$.

Theorem 5. 1) $K = L \oplus L^\perp$.

2) *If* $x = x_1 + x_2$, *where* $x_1 \in L$, $x_2 \in L^\perp$, *and* $x_1, x_2 \neq 0$, *then* $N_{\mathcal{M}}(x) = \max(N_{\mathcal{M}}(x_1), N_{\mathcal{M}}(x_2))$.

3) *The vectors* $\{f_m\}$ *form a basis of* K.

4) *The vectors* $\{g_p\}$ *with* $p \in \mathcal{J}$ *form a basis of* L.

5) *The vectors* $\{e_m\}$ *with* $m \in \mathcal{J}^\perp$ *form a basis of* $L^\perp$.

Proof. First, we prove statement 2). Since $J \cap J^\perp = \varnothing$, we have $N_{\mathcal{M}}(x_1) \neq N_{\mathcal{M}}(x_2)$. Therefore, the element $N_{\mathcal{M}}(x_1 + x_2)$ is equal to the largest of the elements $N_{\mathcal{M}}(x_1)$ and $N_{\mathcal{M}}(x_2)$. We consider the linear operator $\Phi \colon K \to K$ defined on the vectors $\{e_m\}$ of the basis by $\Phi(e_m) = f_m$. By the definition of the vectors f_m, the operator Φ is equal to the sum of the identity operator and an operator triangular in the basis $\{e_m\}$. By Theorem 4, the operator Φ is invertible. This immediately implies all the remaining statements of Theorem 5. □

Definition 2. Let $\{g_p\}$, $p \in \mathcal{J}$, be the basis of L occurring in item 4) of Theorem 5. We say that a set $\{v_p = \lambda_p g_p\}$, where the λ_p are arbitrary nonzero elements of the ground field $\mathbf{k}$, is a *Gröbner* $(\mathcal{M})$*-basis of the space* L.

From item 4) of Theorem 5, it follows that every Gröbner $(\mathcal{M})$-basis is a basis and that the dimension of the finite-dimensional space L is equal to the number of points in the set $\mathcal{J}$.

How to use the $\mathcal{M}$-valuation to determine whether two embedded subspaces $L \subset M$ of the space K coincide? Theorem 5 enables us to answer this question.

Corollary 6. *Let $L \subset M \subset K$ be a triple of spaces. We have $M \neq L$ if and only if there is a vector $v \in M \setminus \{0\}$ with support $S(v)$ disjoint from the set $\mathcal{J}$.*

Proof. If $M \neq L$, then there is a vector $x \in M$ representable in the form $x = x_1 + x_2$, where $x_1 \in L$, $x_2 \in L^\perp$, and $x_2 \neq 0$. Since $x_1 \in L \subset M$, the vector $v = x_2 = x - x_1$ lies in M. The support $S(v)$ of v is disjoint from J. □

2.3. A simplest analog of Buchberger's algorithm. Let G be a finite set of nonzero vectors in K. We consider the following two problems. How to find the image $\mathcal{J}$ of $L \setminus \{0\}$ under the $\mathcal{M}$-valuation, where $L \subset K$ is the space generated by the vectors from G? How to find a Gröbner $\mathcal{M}$-basis in L?

We describe an algorithm that solves these two problems. This algorithm is the simplest analog of Buchberger's algorithm, which we need in the sequel.

As a first approximation to the set $\mathcal{J}$, we take the set $\mathcal{J}_G = N_{\mathcal{M}}(G)$. We choose an arbitrary map $\mathcal{F}\colon \mathcal{J}_G \to G$ such that $N_{\mathcal{M}}(g) = p$ for $g = \mathcal{F}(p)$. (In general, the relation $N_{\mathcal{M}}(g) = p$ does not determine the vector g uniquely, and there is a freedom in the choice of $\mathcal{F}$.)

As a first approximation to the $(\mathcal{M})$-basis in L, we take the set $V \subset G$ coinciding with the range of the map $\mathcal{F}$. By construction, we have $N_{\mathcal{M}}(V) = N_{\mathcal{M}}(G)$, and the set V is a Gröbner $\mathcal{M}$-basis of the space $L(\mathcal{J}_G, \mathcal{F}) \subset L$ generated by the vectors in V.

If $G \subset L(\mathcal{J}_G, \mathcal{F})$, then the set $\mathcal{J}$ coincides with its first approximation $\mathcal{J}_G$, the space L coincides with $L(\mathcal{J}_G, \mathcal{F})$, and the set V is a Gröbner $(\mathcal{M})$-basis in L. In this case, the two problems are solved.

If the inclusion $G \subset L(\mathcal{J}_G, \mathcal{F})$ is not fulfilled, then there exist vectors $g_j \in G$ that do not lie in $L(\mathcal{J}_G, \mathcal{F})$. We put $\mathcal{J}_G^\perp = \mathcal{M} \setminus \mathcal{J}_G$ and consider the space $L(\mathcal{J}_G^\perp)$ generated by the vectors e_q, $q \in \mathcal{J}_G^\perp$. By Theorem 5, every vector g_j can be represented in the form $g_j = g_j^1 + g_j^2$, where $g_j^1 \in L(\mathcal{J}_G, \mathcal{F})$ and $g_j^2 \in L(\mathcal{J}_G^\perp,)$. The vectors g_j^2 lie in the space L because g_j and g_j^1 lie in L. We denote by $G_1 \subset L$ the union of V and the set of all nonzero vectors g_j^2. The set G_1 generates the space L. To the set G_1, we apply the procedure that was applied to G. As a result, we construct the set $\mathcal{J}_{G_1} = N_{\mathcal{M}}(G_1)$, the map $\mathcal{F}_1\colon \mathcal{J}_{G_1} \to G_1$, the set $V_1 = \mathcal{F}(G_1)$, and the space $L(\mathcal{J}_{G_1}, \mathcal{F}_1)$ generated by the vectors in V_1. The set $\mathcal{J}_{G_1}$ is a second approximation to the set $\mathcal{J}$. The set $\mathcal{J}_{G_1}$ is strictly larger than $\mathcal{J}_G$ because the supports of the nonzero vectors g_j^2 lie in the complement of $\mathcal{J}_G$. The space $L(\mathcal{J}_{G_1}, \mathcal{F}_1) \subset L$ is strictly larger than $L(\mathcal{J}_G, \mathcal{F})$. If $G_1 \subset L(\mathcal{J}_{G_1}, \mathcal{F}_1)$, then the two problems are solved.

If the inclusion in question fails, then we again apply our procedure to the set G_1, etc. This process cannot continue infinitely because the sets $\mathcal{J}_{G_i} \subset \mathcal{J}$ strictly grow with i and the set $\mathcal{J}$ is finite. As a result, both problems will be solved in a finite number of steps.

2.4. Gröbner's ordering, the space $L(J_G, F)$, and truncation of polynomials. In this section, we define Gröbner's ordering and use it to define the space $L(J_G, F)$. We consider truncations of the polynomials belonging to this space with respect to the order f for a linear function f monotone with respect to the Gröbner ordering.

Definition 3. We say that an ordering $\prec$ on the lattice $\mathbb{Z}^n$ is *compatible with the group structure* if $a + c \prec b + c$, whenever a, b, $c \in \mathbb{Z}^n$ and $a \prec b$. The restriction of an ordering on $\mathbb{Z}^n$ compatible with the group structure to $\mathbb{Z}^n_{\geq 0}$ is called a *Gröbner ordering* on $\mathbb{Z}^n_{\geq 0}$ if the semigroup $\mathbb{Z}^n_{\geq 0}$ is a well-ordered set with the minimal element 0 with respect to this ordering.

The function that maps each monomial $z^m = z_1^{m_1} \cdot \ldots \cdot z_n^{m_n}$, where $z = z_1, \ldots, z_n$ and $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n_{\geq 0}$, to its degree m is an isomorphism of the multiplicative semigroup of monomials of nonnegative degree to the semigroup $\mathbb{Z}^n_{\geq 0}$. This function gives rise to an enumeration of the monomials by the elements of the semigroup $\mathbb{Z}^n_{\geq 0}$. The monomials form a basis in the linear space $R = \mathbf{k}[z_1, \ldots, z_n]$. Fixing a Gröbner ordering on the semigroup $\mathbb{Z}^n_{\geq 0}$, we turn the space of polynomials into a linear space with a well-ordered bases to which we can apply the results of Subsections 2.1–2.3.

Definition 4. The $\mathcal{M}$-valuation map from the set of nonzero polynomials $R \setminus \{0\}$ to $\mathbb{Z}^n_{\geq 0}$ that corresponds to a Gröbner ordering on the semigroup $\mathbb{Z}^n$ is called the *Gröbner map* and is denoted by $Gr\colon R \setminus \{0\} \to \mathbb{Z}^n_{\geq 0}$.

We fix a Gröbner ordering on the semigroup $\mathbb{Z}^n_{\geq 0}$. We consider a linear subspace $L(J_G, F)$ (depending on the choice of a map F) for a finite set $G \subset \mathbf{k}[z_1, \ldots, z_n] \setminus \{0\}$. Let J_G be the ideal $\bigcup_{m \in A} O_m$ of $\mathbb{Z}^n_{\geq 0}$, where $A = \mathrm{Gr}(G)$;

let $J_G^{\perp}$ be the coideal in $\mathbb{Z}^n_{\geq 0}$ defined by $J_G^{\perp} = \mathbb{Z}^n_{\geq 0} \setminus J_G$;

let $L(J_G^{\perp})$ be the space of polynomials generated by the monomials z^j with $j \in J_G^{\perp}$;

and let $F\colon J_G \to G$ be a map such that $p \in O_m$ if $g = F(p)$, where $m = \mathrm{Gr}(g)$.

Given a Gröbner ordering, a set G, and a map F, we construct the *linear space* $L(J_G, F) \subset R$ generated by the polynomials $g_p = z^{p-m} g$, where $p \in J_G$, $g = F(p) \in G$, and $m = \mathrm{Gr}(g)$.

Definition 5. Let $f\colon \mathbb{R}^n \to \mathbb{R}$ be a linear function on the space $\mathbb{R}^n$ containing $\mathbb{Z}^n$. For each nonzero polynomial $P = \sum a_m z^m$, we consider its *truncation $P^{(f)}$ with respect to the order f*. By definition, $P^{(f)} = \sum_{m \in B} a_m z^m$, where B is the subset of the support $S(P)$ of P on which the function f attains its maximum value. We denote the maximum value of f on $S(P)$ by $\deg_f(P)$.

It is obvious that

1) $(PQ)^{(f)} = P^{(f)} Q^{(f)}$;

2) if $\deg_f P = \deg_f Q$ and $P^{(f)} + Q^{(f)} \neq 0$, then $(P+Q)^{(f)} = P^{(f)} + Q^{(f)}$.

We say that a linear function f is *monotone with respect to a Gröbner ordering* $\prec$ if $x \prec y$ implies $f(x) \leq f(y)$.

Proposition 7. *Let $L(J_G, F)$ be the space constructed by G, F, and a certain Gröbner ordering, and let f be a function monotone with respect to this ordering. Then, for every polynomial $P \in L(J_G, F)$, its truncation $P^{(f)}$ lies in the ideal generated by the truncations $g_i^{(f)}$ of the polynomials $g_i \in G$.*

Proof. By definition, every polynomial $P \in L(J_G, F)$ can be represented in the form $P = \sum \mu_i g_i z^{a_i - m_i}$, where $g_i = F(a_i)$ and $m_i = \mathrm{Gr}(g_i)$. We denote by $\widetilde{S}(P)$ the set of points a_i for which $\mu_i \neq 0$, and we denote by $\widetilde{B}(P)$ the subset of $\widetilde{S}(P)$ on which the function f is equal to $\deg_f P$. For $a_i \in \widetilde{B}(P)$, we have $\deg_f g_i z^{a_i - m_i} = \deg_f P$. The polynomial

$$Q = \sum_{a_i \in \widetilde{B}} \mu_i g_i^{(f)} z^{a_i - m_i}$$

is nonzero (it is easily seen that, for $a = \mathrm{Gr}(P)$, the monomial z^a occurs in the polynomial Q with a nonzero coefficient). Therefore, $P^{(f)} = Q$. Proposition 7 is proved. □

§3. A Gröbner basis for an ideal

In this section, we discuss Gröbner bases, Buchberger's theorem, and Buchberger's algorithm.

3.1. The space $L(J_G, F)$ and an ideal containing the set G. Let $R = \mathbf{k}[z_1, \dots, z_n]$, and let $\mathrm{Gr}\colon R \setminus \{0\} \to \mathbb{Z}^n_{\geq 0}$ be a Gröbner map for a Gröbner ordering on $\mathbb{Z}^n_{\geq 0}$. The following statement is obvious.

Proposition 8. *For every ideal $I \subset R$, the set $J(I) = \mathrm{Gr}(I \setminus \{0\})$ is an ideal in the semigroup $\mathbb{Z}^n_{\geq 0}$.*

Let $G \subset I \setminus \{0\}$ be a finite set, let J_G be the ideal generated by the elements $\mathrm{Gr}(g)$, $g \in G$, in $\mathbb{Z}^n_{\geq 0}$, and let $L(J_G, F)$ be the subspace corresponding to a map $F\colon J_G \to G$. By definition, the space $L(J_G, F)$ is contained in the ideal I.

Question. Does the space $L(J_G, F)$ coincide with the ideal I, or the ideal I is strictly larger than the space $L(J_G, F)$?

It turns out that the answer to this question depends only on the restriction of the Gröbner map to the set G (i.e., it depends neither on the restriction of Gr to the set $I \setminus G$ nor on the choice of a map F).

Theorem 9. *The identity $I = L(J_G, F)$ is valid if and only if the intersection of the support of each polynomial $P \in I$ with the ideal J_G is not empty.*

Theorem 9 follows from Corollary 6.

Definition 6. A *Gröbner basis of an ideal I* with respect to a Gröbner ordering is a finite set G of nonzero polynomials in I such that for the image $A = \mathrm{Gr}(G)$ of G under the Gröbner map we have $\bigcup_{m \in A} O_m = \mathrm{Gr}(I \setminus \{0\})$.

By Theorem 9, a Gröbner basis for an ideal is a basis of that ideal in the usual sense.

Corollary 10. *Let f be a monotone function with respect to a Gröbner ordering, and let $G = \{g_i\}$ be a Gröbner basis of I with respect to this ordering. Then the truncation $P^{(f)}$ of every polynomial $P \in I$ lies in the ideal generated by the truncations $g_i^{(f)}$ of the polynomials $g_i \in G$.*

Corollary 10 follows from Theorem 9 and Proposition 7.

3.2. Buchberger's theorem. Is it true that a given finite set G of polynomials contains a Gröbner basis of the ideal I generated by G? Buchberger's theorem gives an answer to this question. This theorem is a part of Buchberger's algorithm (see Subsection 3.3) and contains its first step (step $1_{(G,F)}$).

For every polynomial $g_i \in G$, we denote by m_i its image under the Gröbner map. Multiplying each polynomial g_i by an appropriate constant, we may assume that the coefficient at the leading monomial z^{m_i} of g_i is equal to 1.

Step $1_{(G,F)}$. In the semigroup $\mathbb{Z}^n_{\geq 0}$, we consider the ideal $J_G = \bigcup O_{m_i}$, where $m_i = \mathrm{Gr}(g_i)$ and $g_i \in G$. For every pair $g_i, g_j \in G$, we denote by $m_{i,j}$ the vertex of the octant $O_{m_i} \cap O_{m_j}$ (obviously, $m_{i,j} - m_i \in \mathbb{Z}^n_{\geq 0}$ and $m_{i,j} - m_j \in \mathbb{Z}^n_{\geq 0}$) and consider the polynomial $g_{i,j} = z^{m_{i,j}-m_i} g_i - z^{m_{i,j}-m_j} g_j$. We fix an arbitrary map $F\colon J_G \to G$ for which $a \in O_m$, where $m = \mathrm{Gr}(F(a))$, and consider the related space $L(J_G, F)$.

Theorem 11 (Buchberger)**.** *A set G contains a Gröbner basis of I if and only if all polynomials $g_{i,j}$ lie in $L(J_G, F)$.*

Proof. The ideal generated by the polynomials g_i consists of all linear combinations of the polynomials of the form $z^b g_i$. It suffices to prove that if all polynomials $g_{i,j}$ lie in $L(J_G, F)$, then $L(J_G, F)$ contains all polynomials of the form $z^b g_i$. We assume that there exist polynomials $z^b g_i \notin L(J_G, F)$ and among them we choose a polynomial for

which the point $a = \mathrm{Gr}(z^b g_i) = b + m_i$ is the smallest with respect to the Gröbner ordering. The space $L(J_G, F)$ contains a polynomial $z^{a-m_j} g_j$ with $g_j = F(a)$. We have $z^{a-m_i} g_i - z^{a-m_j} g_j = z^{a-m_{i,j}} g_{i,j}$. Since $g_{i,j} \in L(J_G, F)$, we obtain $g_{i,j} = \sum \lambda(p) z^{p-m_l} g_l$, where $l = F(p)$. Hence,

$$z^b g_i = z^{a-m_j} g_j - \sum \lambda(p) z^{c(p)} g_l, \quad \text{where} \quad c(p) = a - m_{i,j} + p - m_l.$$

The order of a point p in the support of a polynomial $g_{i,j}$ is strictly smaller than the order of the point $m_{i,j}$. Therefore, $c(p) - m_l < a$. Consequently, the polynomials $z^{c(p)} g_l$ lie in the space $L(J_G, F)$. Therefore, $z^b g_i \in L(J_G, F)$. Theorem 11 is proved. □

3.3. Buchberger's algorithm. This algorithm solves the following problem.

Problem. Given a finite set G of polynomials generating an ideal I, construct a finite set of polynomials containing a Gröbner basis of the ideal.

Buchberger's theorem allows us to check whether or not the set G contain a Gröbner basis of the ideal I. If G contains a Gröbner basis of I, then the problem is solved. If not, then Buchberger's algorithm allows us to successively construct a chain of finite subsets $G = G_0 \subset G_1 \subset \dots$ of I with the following properties:

1) there is a number i such that $G_{i+1} = G_i$;

2) if $G_{i+1} = G_i$, then the set G_i contains a Gröbner basis of I.

Thus, Buchberger's algorithm solves the problem mentioned above.

To pass from one finite set of polynomials to the next one, Buchberger's algorithm employs a two-step procedure. We describe this procedure (for definiteness, we apply it to the initial set G).

Step $1_{(G,F)}$. This step was described in Subsection 3.2.

Step $2_{(G,F)}$. For the space $L(J_G, F)$, we consider the space $L(J_G^{\perp})$ and the decomposition $R = L(J_G, F) \oplus L(J_G^{\perp})$. For every pair of polynomials $g_i, g_j \in G$, we consider the polynomial $g_{i,j}$ and find its decomposition $g_{i,j} = g_{i,j}^1 + g_{i,j}^2$, where $g_{i,j}^1 \in L(J_G, F)$ and $g_{i,j}^2 \in L(J_G^{\perp})$. We consider the set H consisting of all nonzero polynomials $g_{i,j}^2$ and put $G_1 = G \cup H$.

Now, we perform steps $1_{(G,F)}$ and $2_{(G,F)}$. If the resulting set G_1 coincides with G, then G contains a Gröbner basis, and the algorithm stops. If $G \neq G_1$, then we proceed from G to a larger set G_1. The two-step procedure is described.

If $G \neq G_1$, then the ideal J_1 generated by $\mathrm{Gr}(G_1)$ in the semigroup $\mathbb{Z}^n_{\geq 0}$ is strictly larger than the ideal J, because the supports of the nonzero polynomials $g_{i,j}^2$ are disjoint from J. To the set G_1, we apply the same procedure as to G, i.e., we perform steps $1_{(G_1,F_1)}$ and $2_{(G_1,F_1)}$ and construct a larger set G_2. If $G_2 = G_1$, then G_2 contains a Gröbner basis, and the algorithm stops. If $G_1 \neq G_2$, then the ideal J_2 generated by the set $\mathrm{Gr}(G_2)$ in the semigroup $\mathbb{Z}^n_{\geq 0}$ is strictly larger than J_1. We apply to G_2 the same procedure as to G, etc. Since every strictly increasing chain of ideals in the semigroup $\mathbb{Z}^n_{\geq 0}$ eventually terminates, the theorem is proved.

Theorem 12. *Buchberger's algorithm stops after a finite number of steps and gives a solution to the problem in question.*

Remark 3. If two distinct Gröbner orderings give rise to the same Gröbner map of G, then steps $1_{(G,F)}$ and $2_{(G,F)}$ for these orderings are also the same. This remark plays a crucial role in the sequel (see §5) for obtaining estimates of the degrees of the polynomials arising in Buchberger's algorithm.

§4. Orderings on finite subsets of the lattice $\mathbb{Z}^n$

For a finite set $A \subset \mathbb{Z}^n$, we consider the finite set $B \subset \mathbb{Z}^n$ consisting of all points $b = a_i - a_j$ with $a_i, a_j \in A$, $a_i \neq a_j$. In particular, $0 \notin B$, and if $b \in B$, then $-b \in B$. On the lattice $\mathbb{Z}^n$, we fix an arbitrary ordering $\succ$ compatible with the group structure. Let $B_+ \subset B$ be the set of elements greater than zero (in particular, if $b \in B_+$, then $-b \notin B_+$).

Lemma 13. *The convex hull $\Delta(B_+)$ of the set B_+ does not contain the point 0.*

Proof. If $0 \in \Delta(B_+)$, then 0 is contained in the interior of one of the simplexes with vertices $\{b_0, \dots, b_k\} \subset B_+$, i.e., there exist $\lambda_i > 0$ such that $\sum \lambda_i = 1$ and $\sum \lambda_i b_i = 0$. The points $b_0, \dots, b_k$ have integral coordinates and are affinely independent (i.e., the smallest affine space containing these points is k-dimensional). Consequently, the numbers λ_i are rational and become integral after multiplying by an appropriate positive integer N. However, the relation $\sum (N\lambda_i) b_i = 0$ is impossible because $b_i \succ 0$ and, respectively, $(N\lambda_i) b_i \succ 0$ and $\sum (N\lambda_i) b_i \succ 0$. This contradiction proves the lemma. □

Let $\Delta^c(B_+)$ be the minimal cone having 0 as the vertex and containing the polytope $\Delta(B_+)$. Let $J = \{b_1, \dots, b_{n-1}\}$ be an arbitrary sequence of points in B_+ containing $n-1$ elements. We denote by f_J the linear function on R^n the value $f_J(x)$ of which at a point $x \in \mathbb{R}^n$ is equal to the determinant of the $(n \times n)$-matrix with the columns $\{b_1, \dots, b_{n-1}, x\}$.

Lemma 14. *If the dimension of the cone $\Delta^c(B_+)$ is n, then this cone can be determined by a system $f_{J_i} \geq 0$ of lineal inequalities, where J_i is a sequence of elements in B_+ of length $n-1$.*

Proof. Each $(n-1)$-dimensional face Γ_i of the cone $\Delta^c(B_+)$ contain $n-1$ linearly independent vectors belonging to the set B_+. We order these vectors so that, for the resulting sequence J_i, the function f_{J_i} be nonnegative on the cone $\Delta^c(B_+)$. For each face Γ_i, we consider the inequality $f_{J_i} \geq 0$. The system of inequalities obtained determines the multiface cone $\Delta^c(B_+)$. □

The function $f\colon \mathbb{R}^n \to \mathbb{R}$ is *monotone* (*strictly monotone*) on $A \subset \mathbb{Z}^n$ with respect to an ordering $\succ$ if, for all $a, b \in A$ such that $a \succ b$, we have $f(a) \geq f(b)$ ($f(a) > f(b)$). A strictly monotone function gives rise to the same ordering on A as $\succ$ does, i.e., for $a, b \in A$, the inequalities $f(a) > f(b)$ and $a \succ b$ are equivalent.

Example 1. The functions f_{J_i} occurring in Lemma 14 are nonnegative on B_+ and, consequently, they are monotone on A.

Let $\mathbb{R}^n$ be the space with coordinates $x_1, \dots, x_n$ and the standard Euclidean metric.

Corollary 15. *If the diameter of A does not exceed ρ, then the cone $\Delta^c(B_+)$ is given by a system of inequalities $a_1^i x_1 + \dots + a_n^i x_n \geq 0$ in which $a_j^i \in \mathbb{Z}$ and $|a_i^j| \leq \rho^{n-1}$.*

Proof. If $J_i = \{b_1^i, \dots, b_{n-1}^i\}$, then the coefficient a_j^i of f_{J_i} is equal to the determinant of the matrix with the columns $b_1^i, \dots, b_{n-1}^i, e_j$, where e_j is the jth basis vector in $\mathbb{R}^n$. This determinant is an integer whose absolute value does not exceed the $(n-1)$-dimensional volume V_{n-1} of the parallelepiped spanned by the vectors $b_1^i, \dots, b_{n-1}^i$. By assumption, the lengths of the vectors in B do not exceed ρ. Therefore, $V_{n-1} \leq \rho^{n-1}$. □

Theorem 16. *Suppose that A contains the point 0 and all basis vectors e_i, and let the ordering on A be such that $e_i \succ 0$ for $i = 1, \dots, n$. If the diameter of A does not exceed ρ, then there is a strictly monotone linear function on A with coefficients that do not exceed ρ^{n-1}.*

Proof. Corollary 15 implies that the coefficients of each function f_{J_i} are integers with absolute values not exceeding ρ^{n-1}. Since $\{e_i\} \in B_+$, the coefficients of all functions f_{J_i} are nonnegative. It suffices to prove that some face Γ_j of the cone $\Delta^c(B_+)$ contains no basis vectors (all coefficients of the function f_{J_j} corresponding to this face are positive). The existence of such a face is proved below in Lemma 18. □

Renumbering the vectors $\{e_j\}$, we may assume that $e_1 \prec \cdots \prec e_n$. The following lemma is valid for each $(n-1)$-dimensional face Γ_i of the cone $\Delta^c(B_+)$.

Lemma 17. *If $e_k \in \Gamma_i$ and $m < k$, then $e_m \in \Gamma_i$.*

Proof. The function f_{J_i} is zero on Γ_i, is monotone on A, and is positive on $\Delta^c(B_+) \setminus \Gamma_i$. Therefore, $f_{J_i}(e_m) \le f_{J_i}(e_k) = 0$. Since $e_m \in B_+$, we have $f_{J_i}(e_m) \ge 0$. Hence, $f_{J_i}(e_m) = 0$ and, consequently, $e_m \in \Gamma_i$. □

Lemma 18. *There exists an $(n-1)$-dimensional face Γ_j in $\Delta^c(B_+)$ that contains no basis vectors.*

Proof. The set $\mathcal{G}$ of all faces of the cone $\Delta^c(B_+)$ (including the cone itself and its vertex 0) is partially ordered by inclusion. We define a map $\Psi\colon \{e_i\} \to \mathcal{G}$ that takes the basis vector e_m to the smallest face $\Psi(e_m)$ containing e_m. Each proper face of the cone $\Delta^c(B_+)$ is the intersection of the $(n-1)$-faces of $\Delta^c(B_+)$. Lemma 17 shows that $\Psi(e_m) \subset \Psi(e_k)$ if $e_m \prec e_k$. Therefore, the face $\Psi(e_1)$ is contained in each face $\Psi(e_i)$. The face $\Psi(e_1)$ is not a vertex. If $\Psi(e_1) = \Delta^c(B_+)$, then there is nothing to prove because each face contains no basis vectors. Otherwise, for the role of Γ_j we can take an arbitrary $(n-1)$-dimensional face not containing $\Psi(e_1)$. Indeed, if $e_m \in \Gamma_j$, then $\Psi(e_m) \subset \Gamma_j$ and $\Psi(e_1) \subset \Psi(e_m) \subset \Gamma_j$. □

§5. Estimation of the degrees of polynomials

We say that $\alpha\colon \mathbb{R}^n \to \mathbb{R}$ is an *admissible function* whenever α is a linear function, $\alpha(x_1, \dots, x_n) = \alpha_1 x_1 + \cdots + \alpha_n x_n$, with positive coefficients $\alpha_1, \dots, \alpha_n$ that are linearly independent over $\mathbb{Q}$. We say that x is less than y with respect to the α-ordering if $\alpha(x) < \alpha(y)$. The following statement can easily be verified.

Proposition 19. *If $\alpha\colon \mathbb{R}^n \to \mathbb{R}$ is an admissible function, then the α-ordering is compatible with the group structure on $\mathbb{Z}^n$. On the semigroup $\mathbb{Z}^n_{\ge 0}$, the α-ordering is a Gröbner ordering.*

Proof. Since the function α is linear, we have $\alpha(x+z) < \alpha(y+z)$ if $\alpha(x) < \alpha(y)$. Since the coefficients α_i are linearly independent over $\mathbb{Q}$, the relation $\alpha(x) = \alpha(y)$ for $x, y \in \mathbb{Z}^n$ is valid only if $x = y$. Finally, the α-ordering yields a well-ordering on the semigroup $\mathbb{Z}^n_{\ge 0}$ with the minimal element 0, because the coefficients α_i are positive (for a given point $x \in \mathbb{Z}^n_{\ge 0}$, there is a finite number of points $y \in \mathbb{Z}^n_{\ge 0}$ for which $x \succ y$). □

Below in §7, we shall need the following statement.

Proposition 20. *For every nonzero linear function f that is nonnegative on $\mathbb{Z}^n_{\ge 0}$, there is a Gröbner ordering on $\mathbb{Z}^n_{\ge 0}$ with respect to which the function f is monotone.*

Proof. We give an example of such an ordering. Fixing an arbitrary admissible function α, we define the required ordering as follows: if $f(x) > f(y)$, then, by definition, $x \succ y$; if $f(x) = f(y)$, then, by definition, $x \succ y$ if $\alpha(x) > \alpha(y)$. □

5.1. The degrees of the polynomials in Buchberger's algorithm. Let G be a finite set of polynomials in $\mathbf{k}[z_1, \dots, z_n]$ of degrees at most N. We consider an arbitrary Gröbner ordering on $\mathbb{Z}^n$.

Theorem 21. *There exists an admissible function α such that*

1) *the Gröbner map defined for the given Gröbner ordering and for the α-ordering coincide on the polynomials belonging to G;*

2) *the coefficients α_i of the function α satisfy the inequalities $1 \le \alpha_i \le N^{n-1} n^{\frac{n-1}{2}}$.*

Proof. Let $A \subset \mathbb{Z}^n_{\ge 0}$ be the set of points $m = (m_1, \dots, m_n)$ defined by the inequalities $m_i \ge 0$, $|m| = m_1 + \dots + m_n \le N$. The set A contains the point 0, all points $e_1, \dots, e_n$, and the supports of all polynomials of degree at most N. The diameter of A is $\rho = Nn^{1/2}$. By Theorem 16, there is a linear function $l(x) = a_1 x_1 + \dots + a_n x_n$ that determines the same ordering on A as the given Gröbner basis, and the coefficients a_i of which satisfy $1 \le a_i \le N^{n-1} n^{(n-1)/2}$. To construct the required function α, it suffices to slightly perturb the coefficients of l to obtain a function giving rise to the same ordering on A and having the coefficients α_i linearly independent over $\mathbb{Q}$ and satisfying the same inequalities $1 \le \alpha_i \le \rho^{n-1} = N^{n-1} n^{(n-1)/2}$. Theorem 21 is proved. □

Let G be a set of nonzero polynomials generating the ideal I. Suppose that the degrees of the polynomials in G do not exceed a certain number N.

Theorem 22. *For each Gröbner ordering, the degrees of the polynomials $g^2_{i,j}$ that arise when applying Buchberger's two-step procedure to the polynomials in G do not exceed $C(N, n) = 2N^n n^{\frac{n-1}{2}}$.*

Proof. For different Gröbner orderings determining the same Gröbner map on G, the two steps of the procedure coincide. We use the Gröbner α-ordering, where α is the function as in Theorem 21. Since the degrees of g_i and g_j do not exceed N, the degree of $g_{i,j}$ does not exceed $2N$. Therefore, $\alpha(\mathrm{Gr}(g_{i,j})) \le N^{n-1} n^{\frac{n-1}{2}} 2N$ (because the coefficients α_i do not exceed the number $N^{n-1} n^{n-1/2}$), i.e., $\alpha(\mathrm{Gr}(g_{i,j})) \le C(N, n)$. Since $\mathrm{Gr}(g^2_{i,j}) \prec \mathrm{Gr}(g_{i,j})$, we have $\alpha(\mathrm{Gr}(g^2_{i,j})) \le C(N, n)$. Since the coefficients of the function α are at least 1, the degree of the polynomial $g^2_{i,j}$ does not exceed $C(N, n)$. □

5.2. The degrees of the polynomials in a Gröbner basis.

Theorem 23. *Let I be an ideal in $\mathbf{k}[z_1, \dots, z_n]$ generated by polynomials of degree at most N. Then, for each Gröbner ordering, there is a basis of I in which all polynomials have degrees at most $F_1(N)$. The number $F_1(N)$ can be calculated explicitly by the degree N and the dimension n.*

Proof. For each set G of generators of I and each Gröbner ordering, Buchberger's algorithm allows us to construct a chain of subsets $G \subset G_2 \subset \dots \subset G_k \subset \dots$ for which the chain of ideals $J \subset J_1 \subset J_2 \subset \dots \subset J_k \subset \dots$ in $\mathbb{Z}^n_{\ge 0}$ generated by the images of G_i under the Gröbner map strictly increases. We define the function F_1 of a natural argument by the following relations: $F_1(1) = N$ and $F_1(i) = C(F_1(i), n)$ if $i > 1$, where C is the function occurring in Theorem 22. By Theorem 22, the ideal J_k is generated by elements of degree not exceeding $F_1(k)$. By Seidenberg's theorem applied to the semigroup $\mathbb{Z}^n_{\ge 0}$, the above chain of ideals terminates at some ideal J_M. The elements of G_M have degree at most $F_1(N)$. In the set G_M, we can choose a Gröbner basis for the ideal J. □

§6. The universal Gröbner basis

This section is not used in what follows. We placed it here to illustrate the results proved above.

We say that a finite set G of polynomials in an ideal I contains a *universal Gröbner basis* if, for each Gröbner ordering, the set G contains a Gröbner basis with respect to this ordering. It has long been known (see [14, 15, 16]) that every ideal has a universal Gröbner basis. A simple proof can be found in [17]. Below, we not only prove the existence of such a basis but also present quite an explicit construction of it.

Theorem 24. *Let I be an ideal in $\mathbf{k}[z_1, \dots, z_n]$ generated by polynomials of degree at most N. Then there exists a universal Gröbner basis of I in which the degrees of all polynomials do not exceed $F_1(N)$.*

Proof. Consider a finite subset $T(N)$ of $\mathbb{Z}^n_{\geq 0}$ defined by the following condition: $m \in T(N)$ if and only if $|m| \leq F_1(N)$. We construct a finite subset G of I as follows. For every convex polytope Δ the vertices of which lie in $T(N)$, we choose a polynomial P in I for which the Newton polytope is Δ. If there are no such polynomials in I, then we ignore the polytope Δ. We define G as the set of all polynomials obtained in this way. By construction, the set G has the following property. For every Gröbner ordering and every polynomial $Q \in I$ of degree at most $F_1(N)$, there is a polynomial $P \in G$ such that the images of P and Q under the Gröbner map coincide. To conclude the proof, it remains to use Theorem 23. □

Theorem 24 can be refined. For the refined version of it (Theorem 25), we need some more definitions.

For a point $m = (m_1, \dots, m_n) \in \mathbb{Z}^n_{\geq 0}$, consider the parallelepiped $\prod(m)$ defined by the relations

$$x = (x_1, \dots, x_n) \in \prod(m) \Leftrightarrow 0 \leq x_1 \leq m_1, \dots, 0 \leq x_n \leq m_n.$$

We say that an integral polytope is $\mathbb{Z}^n_{\geq 0}$-*convex* if all its vertices lie in $\mathbb{Z}^n_{\geq 0}$ and, for each vertex m, this polytope contains the parallelepiped $\prod(m)$. For a polynomial P, we consider the smallest $\mathbb{Z}^n_{\geq 0}$-convex polytope $\Delta_{\geq 0}(P)$ containing the support of P and construct a finite subset $\widetilde{G}$ of I as follows. For each $\mathbb{Z}^n_{\geq 0}$-convex polytope Δ the vertices of which lie in $T(N)$, we choose a polynomial P in I for which $\Delta_{\geq 0}(P) = \Delta$. If there are no such elements in I, then we ignore this $\mathbb{Z}^n_{\geq 0}$-convex polytope Δ. We define $\widetilde{G}$ as the set of all polynomials obtained in this way.

Theorem 25. *The set $\widetilde{G}$ of polynomials described above contains a universal Gröbner basis of I.*

Proof. It suffices to repeat nearly *verbatim* the argument used in the proof of Theorem 24. The crucial fact is that if for polynomials P and Q we have $\Delta_{\geq 0}(P) = \Delta_{\geq 0}(Q)$, then the elements $\mathrm{Gr}(P)$ and $\mathrm{Gr}(Q)$ coincide for every Gröbner ordering. □

§7. The main theorem

For an integral polytope $\Delta \subset \mathbb{R}^n$, we define the *set $M(\Delta)$ of Laurent polynomials* as follows: a Laurent polynomial P belongs to $M(\Delta)$ if its Newton polytope $\Delta(P)$ is obtained by shifting the polytope Δ by an integral vector, $\Delta(P) = \Delta + m$. Let I be an ideal in the ring of Laurent polynomials in n variables, and let $U \subset \mathbb{R}^n$ be a bounded set.

Definition 7. A finite set $G \subset I$ of Laurent polynomials is said to be a U-approximation of I if, for each integral polytope $\Delta \subset U$, either $M(\Delta) \cap I = \varnothing$ or $M(\Delta) \cap G \neq \varnothing$.

For every bounded domain U, there exists a U-approximation G of I. Indeed, there exist only finitely many integral polytopes in U. For every such polytope Δ, we take a

Laurent polynomial $P \in I$ with $\Delta(P) = \Delta$ (if such polynomials exist in the ideal I) and include these polynomials in G.

Main theorem. *Let I be an ideal generated by the Laurent polynomials whose Newton polytopes lie in the cube $-N \le m_i \le N$, $i = 1, \dots, n$. Let G be a U-approximation of the ideal I, where U is the region defined by the inequalities $|m_1| + \cdots + |m_n| \le F_1(2Nn)$. Then the polynomials in G give a system of tropical generators of the ideal I.*

Proof. Let $f(m_1, \dots, m_n) = \alpha_1 m_1 + \cdots + \alpha_n m_n$. We consider the automorphism of the torus $(\mathbb{C}^*)^n$ that sends a point $(z_1, \dots, z_n)$ to the point $(y_1, \dots, y_n)$, where $y_i = z_i$ for $\alpha_i \ge 0$ and $y_i = z_i^{-1}$ for $\alpha_i < 0$. This automorphism maps the cube and the region U in the space of the degrees of the monomials into themselves, and the linear function f becomes a function f^* with nonnegative coefficients. By Proposition 20, the function f^* is monotone with respect to some Gröbner ordering in the ring of polynomials in $y_1, \dots, y_n$. Multiplying Laurent polynomials by appropriate monomials, we obtain polynomials, and the Laurent polynomials in the set of generators of I transform into polynomials of degree at most $2Nn$. To conclude the proof, it remains to use Theorem 23 and Corollary 10. □

References

[1] C. De Concini and C. Procesi, *Complete symmetric varieties.* II, *Intersection theory*, Algebraic Groups and Related Topics (Kyoto/Nagoya, 1983), Adv. Stud. Pure Math., vol. 6, North-Holland, Amsterdam, 1985, pp. 481–513. MR803344 (87a:14038)

[2] C. De Concini, *Equivariant embeddings of homogeneous spaces*, Proc. Intern. Congress of Mathematicians, vol. 1, 2 (Berkeley, Calif., 1986), Amer. Math. Soc., Providence, RI, 1987, pp. 369–377. MR934236 (89e:14045)

[3] W. Fulton and B. Sturmfels, *Intersection theory on toric varieties*, Topology **36** (1997), no. 2, 335–353. MR1415592 (97h:14070)

[4] B. Ya. Kazarnovskiĭ, *Truncations of systems of equations ideals and varietes*, Izv. Ross. Akad. Nauk Ser. Mat. **63** (1999), no. 3, 119–132; English transl., Izv. Math. **63** (1999), no. 3, 535–547. MR1712124 (2000j:13053)

[5] A. Seidenberg, *On the length of a Hilbert ascending chain*, Proc. Amer. Math. Soc. **29** (1971), 443–450. MR0280473 (43:6193)

[6] ———, *Constructive proof of Hilbert's theorem on ascending chains*, Trans. Amer. Math. Soc. **174** (1972), 305–312. MR0314829 (47:3379)

[7] G. Moreno-Socias, *Length of polynomial ascending chains and primitive recursiveness*, Math. Scand. **71** (1992), no. 2, 181–205. MR1212703 (94d:13019)

[8] B. Ya. Kazarnovskiĭ, *c-fans and Newton polyhedra of algebraic varietes*, Izv. Ross. Akad. Nauk Ser. Mat. **67** (2003), no. 3, 23–44; English transl., Izv. Math. **67** (2003), no. 3, 439–460. MR1992192 (2005a:14072)

[9] G. Mikhalkin, *Counting curves via lattice paths in polygons*, C. R. Math. Acad. Sci. Paris **336** (2003), no. 8, 629–634. MR1988122 (2004d:14077)

[10] E. Shustin, *A tropical approach to enumerative geometry*, Algebra i Analiz **17** (2005), no. 2, 170–214; English transl., St. Petersburg Math. J. **17** (2006), no. 2, 343–375. MR2159589 (2006i:14058)

[11] I. Itenberg, G. Mikhalkin, and E. Shustin, *Tropical algebraic geometry*, 2nd ed., Birkhauser, Basel, 2009. MR2508011 (2010d:14086)

[12] B. Ya. Kazarnovskiĭ and A. G. Khovanskiĭ, *Algebra and tropical geometry*, 2011–2013, pp. 1–42. (to appear).

[13] S. P. Chulkov and A. G. Khovanskiĭ, *Geometry of the semigroup $\mathbb{Z}^n_{\ge 0}$. Applications to combinatorics, algebra and differential equations*, MCNMO, M., 2006. (Russian)

[14] F. Mora and L. Robbiano, *The Gröbner fan of an ideal. Computational aspects of commutative algebra*, J. Symbolic Comput. **6** (1988), no. 2-3, 183–208. MR988412 (90d:13004)

[15] V. Weispfenning, *Constructing universal Gröbner bases*, Lecture Notes in Comput. Sci., vol. 356, Springer, Berlin, 1989, pp. 408–417. MR1008554 (91e:13029)

[16] N. Schwartz, *Stability of Gröbner bases*, J. Pure Appl. Algebra **53** (1988), no. 1-2, 171–186. MR955616 (89i:13024)

[17] B. Ya. Kazarnovskiĭ and A. G. Khovanskiĭ, *The universal Gröbner bases*, Proc. Intern. Conf. on Polynomial Computer Algebra, St. Peterburg, 2011, pp. 65–69. (Russian)

[18] F. S. Macaulay, *The algebraic theory of modular systems*, Cambridge Tracts in Math. and Math. Phys., vol. 19, Cambridge Univ. Press, Cambridge, 1916. MR1281612 (95i:13001)
[19] Th. Sauer, *Gröbner bases, H-bases and interpolations*, Trans. Amer. Math. Soc. **353** (2001), no. 6, 2293–2308. (electronic) MR1814071 (2002b:13035)

Institute for Information Transmission Problems (Kharkevich Institute), Russian Academy of Sciences, Bolshoy Karetny per. 19, build. 1, Moscow 127051, Russia
E-mail address: kazbori@gmail.com

Institute for Systems Analysis, Russian Academy of Sciences, 60-letiya Oktyabrya pr. 9, Moscow 117312; Independent University of Moscow, Bolshoy Vlasyevskiĭ Pereulok 11, Moscow 119002, Russia

University Of Toronto, Canada
E-mail address: askold@math.toronto.edu

Received 17/OCT/2013

Translated by B. M. BEKKER