IDEAL MEMBERSHIP IN SIGNOMIAL RINGS

Žarko Mijajlović, Miloš Milošević, Aleksandar Perović

The paper presents decidability of ideal membership for finitely generated signomial ideals with rational exponents over computable field $K$ of characteristic 0. We also prove the existence of nonrecursive ideals in $K[\bar{x}^\mathbb{Q}]$, where $\bar{x}^\mathbb{Q} = x_1^\mathbb{Q} \cdots x_n^\mathbb{Q}$ is a multiplicative copy of the monoid $\mathbb{Q}^+ = \mathbb{Q} \times \cdots \times \mathbb{Q}$.

1. INTRODUCTION

A signomial in variables $x_1, \ldots, x_n$ is any term of the form

$$r_1 x_1^{s_{11}} \cdots x_n^{s_{1n}} + \cdots + r_k x_1^{s_{k1}} \cdots x_n^{s_{kn}},$$

where the coefficients $r_i$ range over some commutative domain $R$ and the exponents $s_{ij}$ range over some commutative, usually ordered monoid $S$. It turns out that the corresponding signomial ring, denoted by $R[x^S]$, is isomorphic to the semigroup ring of all functions $f : S \to R[x_1^S \cdots x_n^S]$ (if $n = 1$, then $R[x_1^S \cdots x_n^S] = R$) with a finite support, where support of $f$ is the set of all $s \in S$ that are not annihilated by $f$. As a consequence, $R[x^S]$ is not a domain whenever $S$ has a finite cyclic subgroup. There are two main reasons for considering only ordered $S$s:

- the underlying signomial rings are always domains;
- the notion of degree is definable.

A well known and well studied case is the one of the LAURENT polynomials, when $S$ is the set of all integers. By means of localization one can show that LAURENT polynomials greatly, in an algebraical sense, resemble ordinary polynomials: $R[x^\mathbb{Z}]$ is a UFD, Noetherian, there is a nice semantic functional representation, both Nullstellensatz and Real Nullstellensatz hold and so on.

2000 Mathematics Subject Classification: 16S34, 13A99
Keywords and Phrases: Group rings, Laurent polynomial rings, general commutative ring theory.

64
A more interesting and far less explored case is when $S = \mathbb{Q}$ or $\mathbb{R}$. A rather unpleasant feature of those signomial rings is the fact that they are neither Noetherian, nor UFDs. Depending on the particular problem, there are several ways to overcome this difficulty. The paper presents decidability of ideal membership for finitely generated ideals of $K[\bar{x}\mathbb{Q}]$, where $K$ is a computable field of characteristic 0.

2. PRELIMINARIES AND NOTATION

In this section we will make our notation more precise and state some definitions that are required for the main result. Here and after $K$ will denote a computable field of characteristic 0. If $R$ is a certain ring then by $\langle X \rangle_R$ we will denote the ideal of $R$ generated by the set $X$. If the context is clear, $R$ will be omitted. Variables (indeterminates) will be denoted by $x$ and $y$, possibly with indices. A tuple of variables will be denoted by $\bar{x}$ and $\bar{y}$.

For an arbitrary positive integer $m$ let us define a ring monomorphism $\Phi_m : R[\bar{x}\mathbb{Q}] \rightarrow R[\bar{x}\mathbb{Q}]$ by

$$\Phi_m\left(\sum_{i=1}^{k} r_i x_1^{s_{i1}} \cdots x_n^{s_{im}}\right) = \sum_{i=1}^{k} r_i x_1^{ms_{i1}} \cdots x_n^{ms_{im}}.$$ 

If $f_1, \ldots, f_k$ are arbitrary signomials from $R[\bar{x}\mathbb{Q}]$, then let $\pi(f_1, \ldots, f_k)$ be the least positive integer $m$ such that each $\Phi_m(f_i)$ is a Laurent polynomial. It is easy to see that $\Phi_m(f) \in R[\bar{x}\mathbb{Q}]$ if and only if $\pi(f)$ divides $m$. Consequently,

$$\pi(f_1, \ldots, f_k) = \text{LCM}(\pi(f_1), \ldots, \pi(f_k)).$$

3. IDEAL MEMBERSHIP IN $K[\bar{x}\mathbb{Q}]$

Generally, the ideal membership is undecidable in $K[\bar{x}\mathbb{Q}]$. In order to prove this we will need the following technical lemma.

Lemma 3.1. Suppose that $p_0, p_1, \ldots, p_n$ are arbitrary distinct prime numbers and let $f_i = x^{1/p_i} - 1$, where $x$ is a single indeterminate. Then $f_0 \notin \langle f_1, \ldots, f_n \rangle_{K[x]}$.

Proof. Assume the opposite. Then there are signomials $g_1, \ldots, g_k \in K[\bar{x}\mathbb{Q}]$ such that

$$f_0 = g_1 f_1 + \cdots + g_n f_n.$$ 

Let $m = \pi(f_0, f_1, \ldots, f_n, g_1, \ldots, g_n)$. Then there are unique positive integers $s$ and $d$ such that $m = p_0 d$ and GCD($p_0, d$) = 1. For an arbitrary $i > 0$ we have that

$$\Phi_m(f_i) = x^{p_0^d s} - 1 = (x^{p_0^s} - 1)(x^{p_0^s} - 1)(x^{p_0^s} - 1) + \cdots + 1.$$
and each $\frac{d}{p_i} - j$ is an integer, so $\Phi_m(f_i)$ is divisible by $x^{p_0} - 1$ in $K[x]$. But $\Phi_m(f_0)$ is not divisible by $x^{p_0} - 1$, and we obtain a contradiction. □

An immediate consequence of the preceding lemma is the fact that signomials $x^r - 1$, where $p$ runs through all primes, are independent: a signomial $x^{1/p_0} - 1$ is in the ideal $I$ of $K[x^n]$ generated by $B = \{x^{1/p} - 1 \mid p \in A\}$, where $A$ is some set of primes, if and only if $p_0 \in A$.

**Theorem 3.2.** The ideal membership problem in $K[x^n]$ for the given computable field $K$ is not decidable, i.e. there is a nonrecursive ideal in the ring $K[x^n]$, where $x$ is a single indeterminate.

**Proof.** Let $N$ be a nonrecursive subset of $\mathbb{N}$, and in the discussion preceding the theorem take $A = \{p_n \mid n \in N\}$, where $p_0, p_1, \ldots$ is an increasing enumeration of all primes. Then $x^{1/p_i} - 1 \in I$ if and only if $n \in N$. So, any algorithm which decides the predicate “$x^{1/p_i} - 1 \in I$” will also decide predicate “$n \in N$”, contradicting the fact that $N$ is a nonrecursive set. □

In the rest of this section we will describe one test for the membership to finitely generated ideals in $K[x^n]$.

**Theorem 3.3.** Ideal membership in finitely generated ideals of $K[x^n]$ is decidable.

**Proof.** In order to prove the statement of the theorem it is sufficient to prove the following two facts:

1. there exists an algorithm which decides ideal membership in the ring $K[x^n]$ of Laurent polynomials;

2. the ring extension $K[x^n] \subseteq K[x^n]$ is faithfully flat (in particular, a given Laurent polynomial is contained in a given ideal $I$ of $K[x^n]$ if it is contained in the ideal $IK[x^n]$ generated by $I$ in $K[x^n]$).

Based in (1) and (2), we may decide ideal membership in $K[x^n]$ as follows: suppose $f_0, f_1, \ldots, f_n \in K[x^n]$ are given, and we want to know whether is in the ideal $I$ of $K[x^n]$ generated by $f_1, \ldots, f_n$. Compute a positive integer $m$ such that $f_0, f_1, \ldots, f_n \in K[x^{1/m}]$. Substitution $x_i \mapsto x_i^m$ yields a $K$-algebra automorphism $f(x) \mapsto f(x^m)$ of $K[x^n]$ which restricts to a $K$-algebra isomorphism $K[x^{1/m}] \rightarrow K[x^n]$. Hence we may assume $m = 1$. By (2), it is now enough to test whether $f_0$ is in the ideal of $K[x^n]$ generated by $f_1, \ldots, f_n$; this can be done using the algorithm claimed to exist in (1).

For (1), we note that if $\bar{y} = (y_1, \ldots, y_n)$ is a tuple of distinct indeterminates, each $y_i$ distinct from $x_1, \ldots, x_n$, then the kernel of the surjective $K$-algebra $K[x, \bar{y}] \rightarrow K[x^n]$ with $x_i \mapsto x_i$ and $y_i \mapsto x_i^{-1}$ is generated by the polynomials $x_1 y_1 - 1, \ldots, x_n y_n - 1$.

Thus decidability of ideal membership in $K[x, \bar{y}]$ (using, e.g., Gröbner bases) immediately implies decidability of ideal membership in $K[x^n]$.
For (2), we remark that with $A = K[x^Z]$, the $A$-module $K[x^Q]$ is a directed union of free $A$-modules of the form

$$\bigoplus_{0 \leq i_1, \ldots, i_n \leq m} Ax_1^{i_1} \cdots x_n^{i_n}$$

(internal direct sum of $A$-modules of $K[x^Q]$),

where $m$ ranges over the set of positive integers. Hence $K[x^Q]$ is a flat $A$-module. Moreover, the ring extension $A \subseteq K[x^Q]$ is integral; thus, every maximal ideal of $A$ remains a proper ideal upon extension to $K[x^Q]$ (e.g., by the COHEN–SEIDENBERG theorem). Combining these two facts shows that $K[x^Q]$ is faithfully flat over $A$. □

REFERENCES


Žarko Mijajlović
Matematički fakultet,
Studentski trg 16, 11000 Belgrade,
Serbia
E–mail: zarkom@eunet.yu

Miloš Milošević
Matematički fakultet,
Studentski trg 16, 11000 Belgrade,
Serbia
E–mail: mionamil@eunet.yu

Aleksandar Perović
Saobraćajni fakultet,
Vojvode Stepe 305, 11000 Belgrade,
Serbia
E–mail: pera@sf.bg.ac.yu

(Received September 22, 2006)