International Journal of Pure and Applied Mathematics

Volume 17 No. 2 2004, 143-160

ON THE COMPUTATION OF ARITHMETICAL RANKS

Margherita Barile

Department of Mathematics
University of Bari
Via E. Orabona 4, Bari, 70125, ITALY
e-mail: barile@dm.uniba.it

Abstract: We present new techniques for determining the least number of elements generating the product of two ideals up to radical.

AMS Subject Classification: 13A10
Key Words: arithmetical ranks, monomial ideals

1. Introduction

Determining the minimum number of equations defining a given affine or projective variety – the so-called *arithmetical rank* – is an important and difficult question in algebraic geometry. The case where the defining ideal is generated by monomials has been studied by various authors over the years (see [2], [3], [4], [6], [7]). Nevertheless, there are very few general methods for constructing systems of defining equations. Providing good upper bounds for the arithmetical rank is still a mostly unsolved problem. Lower bounds can be given in terms of non vanishing cohomology groups. For Reisner's variety, Schmitt and Vogel [7] could find 4 defining equations, by taking sums of the minimal monomial generators of the ideal. Later Yan [8] proved by étale cohomology that this is, indeed, the minimum number. There are, however, cases where the method in [7] does not yield the arithmetical rank. Examples were proposed by Lyubeznik [5] and in [1]. In [1] it was shown that sometimes the problem can be solved

Received: July 8, 2004

by taking, instead of sums, linear combinations of the minimal generators with suitable coefficients in the ground field: the result presented there is a generalization of the one in [7]. Nagel and Vogel [6] settled a case where the minimal systems of defining equations are of a more general type.

In this paper we present new methods that enable us to determine the arithmetical rank of large classes of ideals, for which the approach from [1] fails. These methods apply to ideals which, up to radical, can be decomposed into the product of two ideals whose generators are linked by certain divisibility conditions. The technique presented in Section 2 extends the idea in [6], and works in any polynomial ring. The main theorem of Section 4, however, requires that the coefficient ring contains a field whose characteristic is big enough. This limit can be a hint that the arithmetical rank of monomial ideals could depend on the characteristic: it could be the same for all but a finite number of characteristics, and greater in the remaining cases. However, no example in this direction has been found so far. Another interesting aspect of the theorem is that it is based on a well-known family of integers sequences, which includes the triangular and the pyramidal numbers. Section 3 is entirely devoted to their arithmetical properties.

2. Preliminaries

Throughout this paper R will denote a commutative ring with non zero identity. Given an ideal I of R, we say that the elements $\sigma_1, \dots, \sigma_s \in R$ generate I up to radical if $\operatorname{Rad} I = \operatorname{Rad}(\sigma_1, \dots, \sigma_s)$.

If R is a polynomial ring in n indeterminates over an algebraically closed field, we know from Hilbert's Nullstellensatz that this equality holds if and only if $V(I) = V(\sigma_1, \dots, \sigma_s)$, i.e., if and only if the system of polynomial equations $\sigma_1 = \cdots = \sigma_s = 0$ defines the variety corresponding to I in the affine space $\mathbf{A}^n_K$. The least number s with this property is called the *arithmetical rank* of I and is denoted $\operatorname{ara} I$. Since, by Hilbert's Basissatz, the ideal I is finitely generated, its arithmetical rank is always defined, and $\operatorname{ara} I \leq \mu(I)$, where $\mu(I)$ is the minimal number of generators of I. Equality holds only in special cases: then I is called a *complete intersection*. In general $\operatorname{ht} I \leq \operatorname{ara} I$: if equality holds, I is called a *set-theoretic complete intersection*. A better lower bound is provided by the so-called *cohomological dimension* of I, which is defined as follows:

$$\operatorname{cd} I = \max\{i \mid H^i_I(R) \neq 0\},$$

where H^i_I denotes the ith local cohomology group with respect to I. If I is a *squarefree monomial* ideal (i.e. it is generated by products of pairwise distinct

indeterminates), then this number can be easily computed by packages such as *CoCoA*, *Macaulay*, *Singular*: as shown by Lyubeznik [5], in this case $\operatorname{cd} I = \operatorname{pd} I$, where the *projective dimension* $\operatorname{pd} I$ is the length of all minimal free resolutions of I over R.

The main endeavour in computing the arithmetical of an ideal I is improving the gross upper bound $\mu(I)$. Under certain conditions, a lower number of elements generating I up to radical can be constructed by taking linear combinations of a set of minimal generators of I with coefficients in a certain subring of R. A general result in this direction is the following proposition.

Proposition 1. (see [1], Proposition 1.1) *Let R be a commutative ring containing a local ring S. Let P be a finite subset of elements of R. Let $P_0, \dots, P_u$ be subsets of P. For $0 \le l \le u$ let k_l be the cardinality of P_l. Suppose that*

(i) $\bigcup_{l=0}^{u} P_l = P$;

(ii) $k_0 = 1$;

(iii) for all l, $1 \le l \le u$, there is an integer h_l, $2 \le h_l \le k_l$ such that whenever $p_1, \dots, p_{h_l}$ are pairwise distinct elements of P_l, there is $p' \in P_{l'}$, for some $l' < l$, such that p' divides some power of $p_1 \cdots p_{h_l}$.

For all l, $0 \le l \le u$, let $P_l = \{p_1^{(l)}, \dots, p_{k_l}^{(l)}\}$, and, for $1 \le l \le u$, let A^l be a $(h_l - 1) \times k_l$ matrix with entries in S such that all its $(h_l - 1)$-minors are invertible. Then

$$\operatorname{Rad}(P) = \operatorname{Rad}\left(p_1^{(0)}, A^1 \begin{pmatrix} p_1^{(1)} \\ \vdots \\ p_{k_1}^{(1)} \end{pmatrix}, \dots, A^u \begin{pmatrix} p_1^{(u)} \\ \vdots \\ p_{k_u}^{(u)} \end{pmatrix}\right).$$

Remark 1. Note that every element $p = p_j^{(l)}$ can be replaced by any other element q such that the ideals (p) and (q) have the same radical.

In the special case where $h_l = 2$ for all $1 \le l \le u$, then, for every index l, A^l can be any row vector of length k_l with all non zero entries. In particular one can choose

$$A^l = \underbrace{(1, \dots, 1)}_{k_l \text{times}}.$$

This was the claim previously proven by Schmitt and Vogel, which is of course true in any commutative ring R with non zero identity. We quote it for the sake of completeness.

Proposition 2. (see [7], p. 249) *Let P be a finite subset of elements of R. Let $P_0, \ldots, P_u$ be subsets of P. For $0 \leq l \leq u$ let k_l be the cardinality of P_l. Suppose that*

(i) $\bigcup_{l=0}^{u} P_l = P$;

(ii) $k_0 = 1$;

(iii) for all l, $1 \leq l \leq u$, whenever p_1, p_2 are pairwise distinct elements of P_l, there is $p' \in P_{l'}$, for some $l' < l$, such that p' divides some power of $p_1 p_2$.

For $0 \leq l \leq u$ let $P_l = \{p_1^{(l)}, \ldots, p_{k_l}^{(l)}\}$. Then

$$\operatorname{Rad}(P) = \operatorname{Rad}\left(p_1^{(0)}, \sum_{i=1}^{k_1} p_i^{(1)}, \ldots, \sum_{i=1}^{k_l} p_i^{(l)}\right).$$

As an immediate consequence we have the following corollary.

Corollary 1. *Let $p_0, p_1, \ldots, p_n \in R$ be such that, for all distinct indices i, j, p_0 divides some power of $p_i p_j$. Let I be an ideal of R such that $p_0, \sum_{i=1}^{n} p_i \in I$. Then $p_i \in I$ for all $i = 0, \ldots, n$.*

This argument will be used several times in the proofs of the following sections.

Proposition 2 can be applied to give a constructive proof of the following well-known proposition.

Proposition 3. *Let I_1 and I_2 be ideals of R, where I_1 is generated ν elements, I_2 is generated by n elements. Then $I_1 I_2$ is generated by $\nu + n - 1$ elements up to radical.*

Proof. Let $\mu_0, \ldots, \mu_{\nu-1}$ be a system of generators of I_1, and let $m_0, \ldots, m_{n-1}$ be a system of generators of I_2. Let

$$P = \{\mu_i m_j | i = 0, \ldots, \nu - 1, j = 0, \ldots, n - 1\}.$$

Then $I_1 I_2 = (P)$. The sets

$$P_l = \{\mu_i m_j | i + j = l\} \quad (l = 0, \ldots, \nu + n - 2)$$

fulfil the assumption of Proposition 2. In fact conditions (i) and (ii) are obviously true; we shall prove that also (iii) holds. Fix an index $l > 0$, and take two distinct elements $\mu_i m_j$ and $\mu_p m_q$ of P_l. Then

$$(i+q)+(j+p) = (i+j)+(p+q) = 2l.$$

But $i \neq p = l-q$, so that $i+q \neq l$. Therefore $j+p \neq l$. Among $i+q$ and $j+p$ one is greater, and one is smaller than l. We may assume that $i+q = l' < l$. Then $\mu_i m_q \in P_{l'}$, and $\mu_i m_q$ divides $(\mu_i m_j)(\mu_p m_q)$. This completes the proof. □

Example 1. In the ring $R = S[x_1, \ldots, x_7]$, where S is a commutative ring with non zero identity, let

$$\mu_0 = x_1x_2x_3,\ \mu_1 = x_4,$$

and

$$m_0 = x_1x_2x_5,\ m_1 = x_2x_3x_6,\ m_2 = x_1x_3x_7.$$

Then

$$\begin{aligned} I &= (x_1x_2x_3x_5, x_1x_2x_3x_6, x_1x_2x_3x_7, x_1x_2x_4x_5, x_2x_3x_4x_6, x_1x_3x_4x_7) \\ &= \operatorname{Rad}(x_1^2x_2^2x_3x_5, x_1x_2^2x_3^2x_6, x_1^2x_2x_3^2x_7, x_1x_2x_4x_5, x_2x_3x_4x_6, x_1x_3x_4x_7) \\ &= \operatorname{Rad}((\mu_0,\mu_1)(m_0,m_1,m_2)) \\ &= \operatorname{Rad}(\mu_0m_0, \mu_0m_1+\mu_1m_0, \mu_0m_2+\mu_1m_1, \mu_1m_2) \\ &= \operatorname{Rad}(x_1^2x_2^2x_3x_5, x_1x_2^2x_3^2x_6+x_1x_2x_4x_5, x_1^2x_2x_3^2x_7+x_2x_3x_4x_6, x_1x_3x_4x_7). \end{aligned}$$

According to Remark 1 we can set all exponents equal to 1, so that we finally deduce that

$$\begin{aligned} I = \\ \operatorname{Rad}(x_1x_2x_3x_5, x_1x_2x_3x_6+x_1x_2x_4x_5, x_1x_2x_3x_7+x_2x_3x_4x_6, x_1x_3x_4x_7). \end{aligned}$$

Remark 2. Proposition 3 can be used to provide an upper bound for the arithmetical rank of the product of two ideals in the ring of polynomials over an algebraically closed field K. For example, if $R = K[x_1, \ldots, x_\nu, y_1, \ldots, y_n]$, $I_1 = (x_1, \ldots, x_\nu)$, $I_2 = (y_1, \ldots, y_n)$, then

$$\operatorname{ara} I_1I_2 \leq \nu + n - 1.$$

One can show that in this case equality holds (see, e.g., [7], Theorem 2). In particular, the upper bound given in Proposition 3 is sharp. It, however, can be improved for certain classes of ideals.

In the next sections we shall give conditions assuring that, with the notation of Proposition 3, $\operatorname{Rad}(I_1I_2)$ is generated by n elements.

3. An Application of Schmitt-Vogel's Result

We now prove a criterion of the sought type for the case where the ideals are both generated by n elements. An extension will be given at the end of the section.

Proposition 4. *Let $I_1 = (\mu_1, \mu_2, \ldots, \mu_n)$ and $I_2 = (m_1, m_2, \ldots, m_n)$ be ideals of R. Suppose that μ_1 divides some power of $m_i m_j$ for all distinct indices i, j. Set $M = m_1 + \cdots + m_n$. Then*

$$\operatorname{Rad}(I_1 I_2) = \operatorname{Rad}(\mu_1 M,\ \mu_2 M + \mu_1 m_2,\ \mu_3 M + \mu_1 m_3,\ \ldots, \mu_n M + \mu_1 m_n).$$

Proof. The inclusion $\supset$ is trivially true. We shall prove $\subset$. Let I be the radical ideal on the right-hand side of the claim. For all $k = 2, \ldots, n$, $\mu_k M + \mu_1 m_k \in I$ and $\mu_1 M$ divides $(\mu_k M)(\mu_1 m_k)$. By virtue of Corollary 1 this implies that, for all $k = 2, \ldots, n$,

$$\mu_k M,\ \mu_1 m_k \in I. \tag{1}$$

Therefore

$$\mu_1 m_1 = \mu_1 M - \sum_{i=2}^{n} \mu_1 m_i \in I. \tag{2}$$

Moreover, for all $k = 2, \ldots, n$, and for all distinct indices i, j, the elements μ_1 and m_i both divide

$$((\mu_k m_i)(\mu_k m_j))^{\alpha},$$

for some positive integer α, so that $\mu_1 m_i$ divides $((\mu_k m_i)(\mu_k m_j))^{2\alpha}$. According to Corollary 1, this, together with (1) and (2), implies that, for all $k = 2, \ldots, n$ and for all $i = 1, \ldots, n$,

$$\mu_k m_i \in I. \tag{3}$$

The statements (1), (2) and (3) yield the required inclusion. This completes the proof. □

Proposition 4 can be used to compute the arithmetical rank of an ideal, as soon as this is recognized as the radical of a product of two ideals. In the following two examples we show how to proceed.

Example 2. Let $R = K[x_1, \ldots, x_8]$, where K is a field, let I_1 be the ideal generated by

$$\mu_1 = x_1 x_2 x_3,\ \mu_2 = x_7,\ \mu_3 = x_8,$$

and let I_2 be the ideal generated by

$$m_1 = x_1 x_2 x_4 x_5,\ m_2 = x_2 x_3 x_5 x_6,\ m_3 = x_1 x_3 x_4 x_6.$$

These elements fulfil the assumption of Proposition 4. Hence

$$\begin{aligned} I &= (x_1x_2x_3x_4x_5,\ x_1x_2x_3x_5x_6,\ x_1x_2x_3x_4x_6,\\ &\quad x_1x_2x_4x_5x_7,\ x_2x_3x_5x_6x_7,\ x_1x_3x_4x_6x_7,\\ &\quad x_1x_2x_4x_5x_8,\ x_2x_3x_5x_6x_8,\ x_1x_3x_4x_6x_8)\\ &= \operatorname{Rad}(I_1I_2)\\ &= \operatorname{Rad}(x_1x_2x_3(x_1x_2x_4x_5 + x_2x_3x_5x_6 + x_1x_3x_4x_6),\\ &\quad x_7(x_1x_2x_4x_5 + x_2x_3x_5x_6 + x_1x_3x_4x_6) + x_1x_2x_3 \cdot x_2x_3x_5x_6,\\ &\quad x_8(x_1x_2x_4x_5 + x_2x_3x_5x_6 + x_1x_3x_4x_6) + x_1x_2x_3 \cdot x_1x_3x_4x_6)\\ &= \operatorname{Rad}(x_1^2x_2^2x_3x_4x_5 + x_1x_2^2x_3^2x_5x_6 + x_1^2x_2x_3^2x_4x_6,\\ &\quad x_1x_2x_4x_5x_7 + x_2x_3x_5x_6x_7 + x_1x_3x_4x_6x_7 + x_1x_2^2x_3^2x_5x_6,\\ &\quad x_1x_2x_4x_5x_8 + x_2x_3x_5x_6x_8 + x_1x_3x_4x_6x_8 + x_1^2x_2x_3^2x_4x_6). \end{aligned}$$

Hence $\operatorname{ara} I \leq 3$. Since, for $\operatorname{char} K = 0$, $\operatorname{pd} I = 3$, it follows that $\operatorname{ara} I = 3$. One can check that the same result cannot be obtained by applying Proposition 1 to the set of minimal monomial generators of I.

Example 3. Let

$$I = (x_0x_1x_2,\ x_1x_2x_3,\ x_2x_3x_4,\ x_0x_3x_4).$$

Nagel and Vogel [6] found that

$$I = \operatorname{Rad}(x_1x_2^2x_3 + x_2x_3^2x_4,\ x_0x_1x_2 + x_1x_2x_3 + x_0x_3x_4),$$

and thus proved that $\operatorname{ara} I = 2$, and I is a set-theoretic complete intersection. A similar conclusion can be reached by means of Proposition 4. In fact, if I_1 is the ideal generated by

$$\mu_1 = x_2x_3,\ \mu_2 = x_0,$$

and I_2 is the ideal generated by

$$m_1 = x_1x_2,\ m_2 = x_3x_4,$$

then, according to Proposition 4,

$$I = \operatorname{Rad}(I_1I_2) = (x_1x_2^2x_3 + x_2x_3^2x_4, x_0x_1x_2 + x_0x_3x_4 + x_2x_3^2x_4).$$

If m_1 and m_2 are exchanged, then we get

$$I = \operatorname{Rad}(I_1I_2) = (x_1x_2^2x_3 + x_2x_3^2x_4, x_0x_1x_2 + x_0x_3x_4 + x_1x_2^2x_3).$$

Proposition 4 admits the following easy generalization, which can be proved by the same arguments.

Theorem 1. *Let $I_1 = (\mu_1, \mu_2, \ldots, \mu_\nu)$ and $I_2 = (m_1, m_2, \ldots, m_n)$ be ideals of R. Suppose that μ_1 divides some power of $m_i m_j$ for all distinct indices i, j. Set $M = m_1 + \cdots + m_n$. Then:*

(a) if $\nu \leq n$, $\operatorname{Rad}(I_1 I_2) = \operatorname{Rad}(\mu_1 M,\ \mu_2 M + \mu_1 m_2,\ \mu_3 M + \mu_1 m_3,\ \ldots, \mu_\nu M + \mu_1 m_\nu,\ \mu_1 m_{\nu+1}, \ldots, \mu_1 m_n)$;

(b) if $\nu > n$, $\operatorname{Rad}(I_1 I_2) = \operatorname{Rad}(\mu_1 M,\ \mu_2 M + \mu_1 m_2,\ \mu_3 M + \mu_1 m_3,\ \ldots, \mu_n M + \mu_1 m_n,\ \mu_{n+1} M, \ldots, \mu_\nu M)$.

The claim of Theorem 1 can be summed up as follows.

Corollary 2. *In R consider the ideals*

$$I_1 = (\mu_1, \mu_2, \ldots, \mu_\nu) \qquad \text{and} \qquad I_2 = (m_1, m_2, \ldots, m_n).$$

Suppose that μ_1 divides some power of $m_i m_j$ for all distinct indices i, j. Then $I_1 I_2$ is generated by $\max(\nu, n)$ elements up to radical.

Our next aim is to prove a similar result based on Proposition 1. To this end we need a preliminary study of a special class of integer sequences, which will be presented in the next section.

4. A Recursively Defined Family of Sequences

For all positive integers t we consider the sequence $(c_k^t)_{k \geq 1}$, defined as follows. For all $k \geq 1$,

$$c_k^1 = 1,$$

and, if $t \geq 2$, for all $k \geq 1$,

$$c_k^t = \sum_{i=1}^{k} c_i^{t-1}.$$

For all $k \geq 2$, we thus have, e.g., $c_k^2 = k$,

$c_k^3 = \dfrac{k(k+1)}{2}$ (the k-th triangular number),

$c_k^4 = \dfrac{k(k+1)(k+2)}{6}$ (the k-th pyramidal number).

These sequences are well-known in the history of mathematics. We are going to present some of their arithmetical properties, which will be used in the proofs of the next section, and, first of all, will enable us to derive a closed formula for c_k^t.

Lemma 1. *For all positive integers k, t it holds:*

$$\sum_{i=1}^{k}(k-i+1)c_i^t = c_k^{t+2}.$$

Proof. First observe that, by definition,

$$\sum_{i=1}^{k-1} c_i^{t+1} = \sum_{i=1}^{k-1}\sum_{j=1}^{i} c_j^t.$$

The index j takes all values from 1 to $k-1$. For any fixed integer j, $1 \le j \le k-1$, the term c_j^t occurs in the internal sum if and only if $j \le i \le k-1$, i.e., for $k-j$ values of i. Hence

$$\sum_{i=1}^{k-1} c_i^{t+1} = \sum_{i=1}^{k-1}(k-i)c_i^t. \tag{4}$$

Now

$$\sum_{i=1}^{k}(k-i+1)c_i^t = \sum_{i=1}^{k}(k-i)c_i^t + \sum_{i=1}^{k} c_i^t = \sum_{i=1}^{k-1}(k-i)c_i^t + c_k^{t+1},$$

which, by (4), is equal to

$$\sum_{i=1}^{k-1} c_i^{t+1} + c_k^{t+1} = \sum_{i=1}^{k} c_i^{t+1} = c_k^{t+2},$$

as was to be proved. □

Lemma 2. *For all positive integers k, t it holds*

$$(k+t-1)c_k^t = tc_k^{t+1}.$$

Proof. We proceed by induction on $t \ge 1$. For $t = 1$ the claim is

$$kc_k^1 = c_k^2,$$

which is true for all positive integers k, because both sides of the equality are equal to k. Now let $t \ge 2$ and assume the claim true for $t-1$ and all positive integers k. We have

$$(k+t-1)c_k^t = (k+t-1)\sum_{i=1}^{k} c_i^{t-1} = \sum_{i=1}^{k}(i+t-2)c_i^{t-1} + \sum_{i=1}^{k}(k-i+1)c_i^{t-1}.$$

If we apply induction to the first sum and Lemma 1 to the second sum we obtain:

$$(t-1)\sum_{i=1}^{k} c_i^t + c_k^{t+1} = (t-1)c_k^{t+1} + c_k^{t+1} = tc_k^{t+1},$$

as desired. □

Lemma 3. *For all positive integers k, t it holds*

$$tc_k^{t+1} = kc_{k+1}^t.$$

Proof. We fix a positive integer k and prove the claim by induction on $t \geq 1$. For $t = 1$ the claim is

$$c_k^2 = kc_{k+1}^1,$$

which is equivalent to $k = k$. Now let $t \geq 2$ and suppose the claim true for $t-1$. Then we have, by Lemma 2:

$$\begin{aligned} tc_k^{t+1} = (k+t-1)c_k^t &= kc_k^t + (t-1)c_k^t \\ &= k\sum_{i=1}^{k} c_i^{t-1} + kc_{k+1}^{t-1} = k\sum_{i=1}^{k+1} c_i^{t-1} \\ &= kc_{k+1}^t, \end{aligned}$$

as required. □

Lemma 2 and Lemma 3 imply the following result.

Corollary 3. *For all positive integers k, t it holds*

$$(k+t-1)c_k^t = kc_{k+1}^t.$$

The preceding results, especially Lemma 3, can be used to derive, by recursion, the closed formula

$$c_k^t = \frac{k(k+1)\cdots(k+t-2)}{(t-1)!} \quad (k \geq 1, t \geq 2)\,.$$

5. Another Generalization

In this section we apply Proposition 1 to produce a new sufficient criterion which assures that, given two ideals I_1 and I_2 generated by 2 and n elements of R respectively, their product $I_1 I_2$ is generated by n elements up to radical.

Our result is based on the $n \times n$ matrices with entries in R that we are going to introduce. Let

$$A_n = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 2 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & n-1 \end{pmatrix}.$$

In other words, $A_n = (a_{ij})$ is the $n \times n$-matrix such that

$$\begin{cases} a_{1j} = 1, & \text{for} \quad j = 1, \ldots, n\,, \\ a_{ii} = i - 1, & \text{for} \quad i = 2, \ldots, n\,, \\ a_{ij} = 0, & \text{otherwise.} \end{cases}$$

Moreover, let

$$B_n = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ n-1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & n-2 & 2 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & n-1 \end{pmatrix}.$$

In other words, $B_n = (b_{ij})$ is the $n \times n$-matrix such that

$$\begin{cases} b_{ii} = i - 1, & \text{for} \quad i = 2, \ldots, n\,, \\ b_{ii-1} = n - i + 1, & \text{for} \quad i = 2, \ldots, n\,, \\ b_{ij} = 0, & \text{otherwise.} \end{cases}$$

In the sequel, for every integer k, the element $k \cdot 1$ of R will be simply denoted by k and called an integer.

Theorem 2. *Let n be a positive integer and suppose that ring R contains a field K such that* $\operatorname{char} K = 0$ *or* $\operatorname{char} K > n-1$. *Consider the ideals $I_1 = (\mu_1, \mu_2)$ and $I_2 = (m_1, \ldots, m_n)$, and suppose that μ_1 divides some power of $m_1 \cdots m_n$. Then*

$$\operatorname{Rad}(I_1 I_2) = \operatorname{Rad}\left((\mu_1 A_n + \mu_2 B_n) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \right). \qquad (*)$$

Proof. The inclusion $\supset$ is obvious. We prove $\subset$. Let I be the radical ideal on the right-hand side of the claim. Let

$$M_0 = \mu_1 \sum_{i=1}^{n} m_i,$$

and, for all $t = 1, \ldots, n-1$,

$$M_t = t\mu_1 \sum_{i=t+1}^{n} c_{i-t}^{t+1} m_i, \qquad N_t = (n-t)\mu_2 \sum_{i=t}^{n} c_{i-t+1}^{t} m_i.$$

Note that $M_0 \in I$, since M_0 is the first element of the vector of generators on the right-hand side of $(*)$. We shall show that for all $t = 1, \ldots, n-1$,

$$M_t + N_t \in I \tag{5}$$

This will imply the claim for the following reason. We have that

$$\begin{aligned} M_1 N_1 &= (n-1)\mu_1\mu_2 \left(\sum_{i=2}^{n} c_{i-1}^{2} m_i \right) \left(\sum_{i=1}^{n} c_i^1 m_i \right) \\ &= (n-1)\mu_1 \left(\sum_{i=1}^{n} m_i \right) \mu_2 \left(\sum_{i=2}^{n} c_{i-1}^{2} m_i \right), \end{aligned}$$

so that M_0 divides $M_1 N_1$. For all $t = 2, \ldots, n-1$ we also have that

$$M_{t-1} = (t-1)\mu_1 \sum_{i=t}^{n} c_{i-t+1}^{t} m_i$$

divides $M_t N_t$. Hence the sets

$$P_0 = \{M_0\}, \qquad P_t = \{M_t, N_t\} \quad (t = 1, \ldots, n-1)$$

fulfil the assumptions of Proposition 2, so that

$$\begin{aligned} &\operatorname{Rad}(M_0, M_1 + N_1, \ldots, M_{n-1} + N_{n-1}) \\ &\qquad = \operatorname{Rad}(M_0, M_1, N_1, \ldots, M_{n-1}, N_{n-1}). \end{aligned}$$

By (5) it follows that

$$\operatorname{Rad}(M_0, M_1, N_1, \ldots, M_{n-1}, N_{n-1}) \subset I \tag{6}$$

Note that

$$\begin{pmatrix} M_0 \\ M_1 \\ 2^{-1}M_2 \\ \vdots \\ (n-1)^{-1}M_{n-1} \end{pmatrix} = \mu_1 \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & c_1^2 & \cdots & \cdots & c_{n-2}^2 & c_{n-1}^2 \\ 0 & 0 & c_1^3 & \cdots & c_{n-3}^3 & c_{n-2}^3 \\ \vdots & \vdots & & & \vdots & \\ 0 & 0 & \cdots & \cdots & 0 & c_1^n \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ \vdots \\ m_n \end{pmatrix},$$

where the $n \times n$-matrix is invertible in R, since its determinant is

$$c_1^2 c_1^3 \cdots c_1^n = 1.$$

This implies that

$$\mu_1 m_1, \ldots, \mu_1 m_n \in (M_0, M_1, \ldots, M_{n-1}),$$

so that, by (6),

$$\mu_1 m_1, \ldots, \mu_1 m_n \in I. \tag{7}$$

Now μ_1 and m_1 both divide $((\mu_2 m_1) \cdots (\mu_2 m_n))^\alpha$ for some positive integer α. Hence

$$\mu_1 m_1 \text{ divides } ((\mu_2 m_1) \cdots (\mu_2 m_n))^{2\alpha}. \tag{8}$$

Let B'_n be the submatrix of B_n formed by the last $n-1$ rows. Then

$$\begin{pmatrix} (n-1)^{-1}N_1 \\ (n-2)^{-1}N_2 \\ \vdots \\ N_{n-1} \end{pmatrix} = \mu_2 B'_n \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}.$$

Moreover, all $(n-1)$-minors of B'_n are lower triangular matrices whose diagonal entries are non zero integers of R not greater than $n-1$: it follows that their determinants are integers not divisible by $\operatorname{char} K$, hence they are invertible elements of K. By virtue of Proposition 1 and (8), we thus have

$$\mu_2 m_1, \ldots, \mu_2 m_n \in I. \tag{9}$$

Relations (7) and (9) imply the inclusion $\subset$, as desired.

We now prove (5). We first introduce some useful notation. Let $\mathbf{e}_i$ be the row vector which is the i-th element of the canonical basis of K^n. Let $\mathbf{r}_i$ be the i-the row vector of A_n, and $\mathbf{s}_i$ be the i-th row vector of B_n. Then

$$\mathbf{r}_1 = \sum_{i=1}^{n} \mathbf{e}_i, \qquad \mathbf{s}_1 = 0,$$

and, for all $i = 2, \ldots, n$,

$$\mathbf{r}_i = (i-1)\mathbf{e}_i \qquad \mathbf{s}_i = (n-i+1)\mathbf{e}_{i-1} + (i-1)\mathbf{e}_i.$$

In order to prove (5) we show that for all $t = 1, \ldots, n-1$, there are $\lambda_{t+1}, \ldots, \lambda_n \in K$ such that

$$\sum_{i=t+1}^{n} \lambda_i(\mu_1\mathbf{r}_i + \mu_2\mathbf{s}_i) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = M_t + N_t.$$

We show that this is the case for $\lambda_i = c_{i-t}^t$, by verifying that

$$\sum_{i=t+1}^{n} c_{i-t}^t \mathbf{r}_i = t \sum_{i=t+1}^{n} c_{i-t}^{t+1}\mathbf{e}_i, \tag{10}$$

and

$$\sum_{i=t+1}^{n} c_{i-t}^t \mathbf{s}_i = (n-t)\sum_{i=t}^{n} c_{i-t+1}^t \mathbf{e}_i. \tag{11}$$

Equality (10) is true because

$$\sum_{i=t+1}^{n} c_{i-t}^t \mathbf{r}_i = \sum_{i=t+1}^{n} c_{i-t}^t (i-1)\mathbf{e}_i,$$

which, by Lemma 2, is equal to

$$t \sum_{i=t+1}^{n} c_{i-t}^{t+1}\mathbf{e}_i.$$

Equality (11) is true because

$$\begin{aligned} \sum_{i=t+1}^{n} c_{i-t}^t \mathbf{s}_i &= \sum_{i=t+1}^{n} c_{i-t}^t ((n-i+1)\mathbf{e}_{i-1} + (i-1)\mathbf{e}_i) \\ &= c_1^t(n-t)\mathbf{e}_t + \sum_{i=t+1}^{n-1} (c_{i-t+1}^t(n-i) + \underline{c_{i-t}^t(i-1)})\mathbf{e}_i \\ &\quad + \underline{c_{n-t}^t(n-1)}\mathbf{e}_n. \end{aligned}$$

If we apply Corollary 3 to the underlined terms we get

$$\begin{aligned} &c_1^t(n-t)\mathbf{e}_t + \sum_{i=t+1}^{n-1} c_{i-t+1}^t(n-i+i-t)\mathbf{e}_i + (n-t)c_{n-t+1}^t\mathbf{e}_n \\ &= (n-t)\sum_{i=t}^{n} c_{i-t+1}^t \mathbf{e}_i, \end{aligned}$$

as desired. This completes the proof of (5) and of the claim. □

Remark 3. According to Proposition 3, the ideal I_1I_2 is generated up to radical by $n+1$ elements. Under the additional condition given in Theorem 1, this number is lowered to n. We are going to present an ideal for which the theorem provides the exact arithmetical rank.

Example 4. Let $R = K[x_1, \ldots, x_7]$, where K is a field such that $\operatorname{char} K \neq 2$. The following elements of R fulfil the assumption of Theorem 2:

$$\mu_1 = x_1x_2x_3, \quad \mu_2 = x_7,$$

$$m_1 = x_1x_4, \quad m_2 = x_2x_5, \quad m_3 = x_3x_6.$$

Let $I_1 = (\mu_1, \mu_2)$ and $I_2 = (m_1, m_2, m_3)$ and consider the ideal

$$I = (x_1x_2x_3x_4, x_1x_2x_3x_5, x_1x_2x_3x_6, x_1x_4x_7, x_2x_5x_7, x_3x_6x_7).$$

Then

$$I = \operatorname{Rad}(I_1I_2),$$

so that, by virtue of Theorem 2, we have:

$$\begin{aligned} I \;=\; & \operatorname{Rad}\,(x_1x_2x_3 \cdot (x_1x_4 + x_2x_5 + x_3x_6)\,, \\ & x_7 \cdot (2x_1x_4 + x_2x_5) + x_1x_2x_3 \cdot x_2x_5, \\ & x_7 \cdot (x_2x_5 + 2x_3x_6) + 2x_1x_2x_3 \cdot x_3x_6)\,. \end{aligned}$$

This means that, if K is algebraically closed, the variety $V(I)$ in $\mathbf{A}^7_K$ is defined by the following system of three equations:

$$\begin{cases} x_1^2x_2x_3x_4 + x_1x_2^2x_3x_5 + x_1x_2x_3^2x_6 &= 0\,, \\ 2x_1x_4x_7 + x_2x_5x_7 + x_1x_2^2x_3x_5 &= 0\,, \\ x_2x_5x_7 + 2x_3x_6x_7 + 2x_1x_2x_3^2x_6 &= 0\,. \end{cases}$$

If, e.g., $\operatorname{char} K = 0$ or $\operatorname{char} K = 3$, computations show that $\operatorname{pd} I = 3$. Hence $\operatorname{ara} I = 3$. The same result is true if $\operatorname{char} K = 2$, even though Theorem 2 does not apply in this case. In fact we still have that $\operatorname{pd} I = 3$, and $V(I)$ is set-theoretically defined by three equations; the latter statement follows from the next general result.

Proposition 5. *Suppose that ring R contains a field K such that* $\operatorname{char} K = 2$, *and $|K| > 2$. Let $\mu_1, \mu_2, m_1, m_2, m_3 \in R$ be such that μ_1 divides some power*

of $m_1m_2m_3$, and let $t \in K \setminus \{0,1\}$. Set

$$\begin{aligned} u_1 &= \mu_1(m_1+m_2+m_3)\,, \\ u_2 &= \mu_2(tm_1+t^2m_2+(1+t+t^2)m_3)+\mu_1t^2m_2\,, \\ u_3 &= \mu_2((1+t)m_1+(1+t^2)m_2+(t+t^2)m_3)+\mu_1(t+t^2)m_3\,. \end{aligned}$$

Let $I_1=(\mu_1,\mu_2)$, $I_2=(m_1,m_2,m_3)$ and let $J=(u_1,u_2,u_3)$. Then

$$\mathrm{Rad}\,(I_1I_2)=\mathrm{Rad}\,(J).$$

Proof. We shall show that $\mu_i m_j \in \mathrm{Rad}\,(J)$ for all $i=1,2$ and all $j=1,2,3$. Note that

$$u_2+u_3=\mu_2(m_1+m_2+m_3)+\mu_1(t^2m_2+(t+t^2)m_3),$$

and that u_1 divides the product of the two summands on the right-hand side. Hence, according to Corollary 1,

$$v_1=\mu_2(m_1+m_2+m_3)\in\mathrm{Rad}\,(J),$$

$$v_2=\mu_1(t^2m_2+(t+t^2)m_3)\in\mathrm{Rad}\,(J). \tag{12}$$

Furthermore,

$$\begin{aligned} w_1 &= (1+t)u_1+(1+\frac{1}{t})v_2 \\ &= \mu_1((1+t)m_1+(1+t+t^2+t)m_2+(1+t+t+t^2+1+t)m_3) \\ &= \mu_1((1+t)m_1+(1+t^2)m_2+(t+t^2)m_3)\in\mathrm{Rad}\,(J), \end{aligned}$$

and

$$w_2=w_1+u_1=\mu_1(tm_1+t^2m_2+(1+t+t^2)m_3)\in\mathrm{Rad}\,(J).$$

Note that w_1 divides the product of the two summands of u_3, so that, by Corollary 1,

$$z_1=\mu_2((1+t)m_1+(1+t^2)m_2+(t+t^2)m_3)\in\mathrm{Rad}\,(J),$$

$$\mu_1(t+t^2)m_3\in\mathrm{Rad}\,(J)\,. \tag{13}$$

As w_2 divides the product of the two summands of u_2, by Corollary 1 we also have

$$z_2=\mu_2(tm_1+t^2m_2+(1+t+t^2)m_3)\in\mathrm{Rad}\,(J).$$

Since t^2 and $t+t^2 = t(1+t)$ are both non zero elements of K, and $u_1 \in \mathrm{Rad}\,(J)$, relations (12) and (13) imply that

$$\mu_1 m_1, \mu_1 m_2, \mu_1 m_3 \in \mathrm{Rad}\,(J). \tag{14}$$

Now μ_1 and m_1 both divide some power of $(\mu_2 m_1)(\mu_2 m_2)(\mu_2 m_3)$. Hence the same holds for $\mu_1 m_1$. Note that

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \mu_2 \begin{pmatrix} 1+t & 1+t^2 & t+t^2 \\ t & t^2 & 1+t+t^2 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}.$$

The 2-minors of the matrix are

$$\begin{aligned} \Delta_{12} &= t+t^2 = t(1+t) \neq 0\,, \\ \Delta_{23} &= 1+t \neq 0\,, \\ \Delta_{13} &= 1+t^2 = (1+t)^2 \neq 0\,. \end{aligned}$$

By virtue of Proposition 1, it follows that

$$\mu_2 m_1, \mu_2 m_2, \mu_2 m_3 \in \mathrm{Rad}\,(J). \tag{15}$$

Relations (14) and (15) yield the claim. □

Remark 4. Note that in the previous Example it is impossible to find three defining equations for $V(I)$ by forming K-linear combinations of the minimal generators of I. More precisely, Proposition 1 only yields the upper bound $\mathrm{ara}\, I \leq 4$.

Acknowledgements

Partially supported by PRIN Algebra Commutativa e Computazionale, Italian Ministry of Education, University and Research.

References

[1] M. Barile, On the number of equations defining certain varieties, *Manuscripta Math.*, **91** (1996), 483-494.

[2] H.-G. Gräbe, Über den arithmetischen Rang quadratfreier Potenzproduktideale, *Math. Nachr.*, **120** (1985), 217-227.

[3] A. Jaballah, Monomiale Ideale und mengentheoretische vollständige Durchschnitte, *Arch. Math.*, **51** (1988), 308-312.

[4] G. Lyubeznik, *Set-Theoretic Intersections and Monomial Ideals*, Ph.D. Thesis, Columbia University (1984).

[5] G. Lyubeznik, On the local cohomology modules $H^i_{\mathcal{A}}(R)$ for ideals $\mathcal{A}$ generated by monomials in an R-sequence, In: *Complete Intersections, LNM*, Springer, New York, **1092** (1984), 214-220.

[6] U. Nagel, W. Vogel, Über mengentheoretische Durchschnitte und Zusammenhang algebraischer Mannigfaltigkeiten im $\mathbf{P}^n$, *Arch. Math.*, **49** (1987), 414-419.

[7] Th. Schmitt, W. Vogel, Note on set-theoretic intersections of subvarieties of projective space, *Math. Ann.*, **245** (1979), 247-253.

[8] Z. Yan, An étale analog of the Goresky-MacPherson formula for subspace arrangements, *J. Pure and Appl. Algebra*, **146** (2000), 305-318.