HAL
open science

Monomial ideals with tiny squares

Shalom Eliahou, Jürgen Herzog, Maryam Mohammadi Saem

To cite this version:

Shalom Eliahou, Jürgen Herzog, Maryam Mohammadi Saem. Monomial ideals with tiny squares. 2018. hal-01691312

HAL Id: hal-01691312

https://hal.science/hal-01691312v1

Preprint submitted on 23 Jan 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MONOMIAL IDEALS WITH TINY SQUARES

SHALOM ELIAHOU, JÜRGEN HERZOG AND MARYAM MOHAMMADI SAEM

Abstract. Let $I \subset K[x,y]$ be a monomial ideal. How small can $\mu(I^2)$ be in terms of $\mu(I)$? It has been expected that the inequality $\mu(I^2) > \mu(I)$ should hold whenever $\mu(I) \geq 2$. Here we disprove this expectation and provide a somewhat surprising answer to the above question.

1. Introduction

For an ideal I in a Noetherian ring R, let $\mu(I)$ denote as usual the least number of generators of I. If $\mu(I) = m$, how small can $\mu(I^2)$ be in terms of m? Obviously, in suitable rings with zero-divisors, we may have $\mu(I^2) = 0$. There even exist one-dimensional local domains $(R, \mathfrak{m})$ with the property that the square of their maximal ideal $\mathfrak{m}$ requires less generators than $\mathfrak{m}$ itself, see [1, 2]. However, if R is a regular local ring, or if R is a polynomial ring over a field K and I is a homogeneous ideal of R, it has been expected in [3] that the inequality $\mu(I^2) > \mu(I)$ should hold whenever $\mu(I) \geq 2$. This is indeed the case for any integrally closed ideal I in a 2-dimensional regular local ring. On the other hand, it is not too difficult to construct examples of monomial ideals I in a polynomial ring S with at least 4 variables such that $\mu(I^2) < \mu(I)$. However, these examples satisfy $\operatorname{height} I < \dim S$. So far no ideals I with $\mu(I^2) < \mu(I)$ were known for 2-dimensional regular rings. In this paper, we shall prove the following statements.

Theorem 1.1. *For every integer $m \geq 5$, there exists a monomial ideal $I \subset K[x,y]$ such that $\mu(I) = m$ and $\mu(I^2) = 9$.*

Moreover, this result is best possible for $m \geq 6$.

Theorem 1.2. *Let $I \subset K[x,y]$ be a monomial ideal. If $\mu(I) \geq 6$ then $\mu(I^2) \geq 9$.*

Here are some notation to be used throughout. We denote by $\mathcal{M}$ the set of monomials in $K[x,y]$, i.e.

$$\mathcal{M} = \{x^i y^j \mid i, j \in \mathbb{N}\}.$$

As usual, we view $\mathcal{M}$ as partially ordered by divisibility.

For a monomial ideal $J \subset K[x,y]$, we denote by $\mathcal{G}(J)$ its unique minimal system of monomial generators. It is well known that $\mathcal{G}(J)$ is of cardinality $\mu(J)$ and consists of all monomials in J which are minimal under divisibility, i.e.

$$\mathcal{G}(J) = \big(\mathcal{M} \cap J\big) \setminus \big(\mathcal{M} \cap J\big)\mathcal{M}^*$$

where $\mathcal{M}^* = \mathcal{M} \setminus \{1\}$.

Finally, given integers $a \leq b$, we denote by $[a, b]$ the *integer interval* they span, i.e.

$$[a, b] = \{c \in \mathbb{Z} \mid a \leq c \leq b\}.$$

2. Preliminaries

Let $m \geq 2$ be an integer and let $I \subset K[x, y]$ be a monomial ideal such that $\mu(I) = m$. Then $\mathcal{G}(I) = \{u_1, \ldots, u_m\}$, where $u_i = x^{a_i} y^{b_i}$ for all i and where the exponents $a_i, b_i \in \mathbb{N}$ satisfy

$$\begin{aligned} a_1 > a_2 > \cdots > a_m, \\ b_1 < b_2 < \cdots < b_m. \end{aligned} \tag{1}$$

Removing any common factor among the u_i, we may assume $a_m = b_1 = 0$ if desired.

Let $V = \{(i, j) \in \mathbb{N}^2 \mid 1 \leq i \leq j \leq m\}$, and consider the map

$$\begin{array}{rccc} f\colon & V & \to & I^2 \\ & (i, j) & \mapsto & u_i u_j. \end{array}$$

Then $f(V)$ generates I^2, but not minimally so in general. Thus $\mathcal{G}(I^2) \subseteq f(V)$, with equality only occurring in special circumstances. How small can $\mathcal{G}(I^2)$ be? So far this was not well understood. We provide a complete answer in this note.

We partially order $\mathbb{N}^2$ as follows:

$$(i, j) \leq (k, l) \Longleftrightarrow i \leq k \text{ and } j \leq l.$$

Since $V \subset \mathbb{N}^2$, we also view V as partially ordered by $\leq$. Recall that $\mathcal{M}$ is partially ordered by divisibility. These orderings interact in a simple yet useful way, as shown by the lemma below. Recall that an *antichain* in a poset is a subset whose elements are pairwise noncomparable.

Lemma 2.1. *Let $v, v' \in V$. If $f(v)$ divides $f(v')$, then either $v = v'$ or else $\{v, v'\}$ is an antichain in V.*

Equivalently, *if $v < v'$, then $\{f(v), f(v')\}$ is an antichain in $\mathcal{M}$.*

Proof. Set $v = (i, j)$, $v' = (k, l)$, and assume $v < v'$. Then $i \leq k$ and $j \leq l$, and at least one of these inequalities is strict. We have $f(v) = u_i u_j = x^{a_i + a_j} y^{b_i + b_j}$. Similarly, $f(v') = x^{a_k + a_l} y^{b_k + b_l}$. Since the a_t are decreasing and the b_t are increasing, and since either $i < k$ or $j < l$, we have

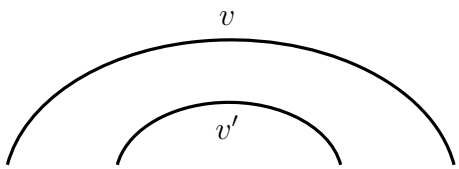
$$\begin{aligned} a_i + a_j &> a_k + b_l, \\ b_i + b_j &< b_k + b_l. \end{aligned}$$

Therefore, neither $u_i u_j$ divides $u_k u_l$, nor conversely. $\square$

Remark 2.2. *If $v, v' \in V$, then v, v' are noncomparable if and only if*

$$\min v < \min v' \leq \max v' < \max v \quad \textit{or} \quad \min v' < \min v \leq \max v < \max v'.$$

Picturing any pair $w = (i, j) \in V$ as an edge joining the vertices $i, j \in \mathbb{N}$, it is useful to keep in mind that graphically, noncomparable pairs $v, v' \in V$ look like this:



For instance, if $v = (1,3)$, the only element of V which is noncomparable to v is $v' = (2,2)$, as is graphically obvious. Therefore by Lemma 2.1, if $u_1u_3 \notin \mathcal{G}(I^2)$, then the only element of $\mathcal{G}(I^2)$ dividing u_1u_3 must be u_2^2.

Of course, noncomparability is not a transitive relation. For instance, the only elements of V which are noncomparable to $v' = (2,2)$ are all $v'' \in V$ of the form $v'' = (1,j)$ with $j \in [3,m]$. Therefore, if $u_2^2 \notin \mathcal{G}(I^2)$, any minimal generator of I^2 dividing it must be of the form u_1u_j for some *a priori* unspecified $j \in [3,m]$.

We shall also need the next lemma.

Lemma 2.3. *Let $v, v_1, v_2 \in V$. Assume that $v_1 \leq v_2$ and that $f(v)$ divides both $f(v_1), f(v_2)$. Then $f(v)$ divides $f(v')$ for all $v' \in V$ such that $v_1 \leq v' \leq v_2$.*

Proof. Set $v = (i,j), v_1 = (i_1,j_1), v_2 = (i_2,j_2), v' = (r,s)$. The hypotheses, together with the respective monotonicity of the a_t and b_t, imply

$$\begin{aligned} a_i + a_j &\leq a_{i_2} + a_{j_2}, \\ b_i + b_j &\leq b_{i_1} + b_{j_1}. \end{aligned}$$

Since $i_1 \leq r \leq i_2$ and $j_1 \leq s \leq j_2$, it follows that

$$\begin{aligned} a_{i_2} + a_{j_2} &\leq a_r + a_s, \\ b_{i_1} + b_{j_1} &\leq b_r + b_s. \end{aligned}$$

Thus $a_i + a_j \leq a_r + a_s$ and $b_i + b_j \leq b_r + b_s$, whence $f(v)$ divides $f(v')$. $\square$

3. Conditions for tiny squares

We now give conditions on a monomial ideal $I = (u_1, \ldots, u_m)$ in $K[x,y]$ which will force $\mu(I^2)$ to be a small constant.

Theorem 3.1. *Let $m \geq 5$. Let $I = (u_1, \ldots, u_m) \subset K[x,y]$ be a monomial ideal with $u_i = x^{a_i}y^{b_i}$ for all i, where $a_1 > \cdots > a_m$ and $b_1 < \cdots < b_m$. Assume that the following divisibility conditions hold:*

$$u_1u_m \mid u_2u_{m-1} \tag{2}$$

$$u_1u_{m-1} \mid u_2u_3,\ u_{m-2}^2 \tag{3}$$

$$u_2^2 \mid u_1u_3,\ u_1u_{m-2} \tag{4}$$

$$u_2u_m \mid u_3u_{m-1},\ u_{m-2}u_{m-1} \tag{5}$$

$$u_{m-1}^2 \mid u_3u_m,\ u_{m-2}u_m. \tag{6}$$

Then $\mu(I^2) = 9$. More precisely, I^2 is minimally generated by the set

$$G = \{u_1^2, u_1u_2, u_2^2\} \cup \{u_1u_{m-1}, u_1u_m, u_2u_m\} \cup \{u_{m-1}^2, u_{m-1}u_m, u_m^2\}.$$

Proof. To see that G generates I^2, we must show that, for all $i, j \in [1, m]$ such that $i \leq j$, the monomial $u_i u_j$ is a multiple of some element in G . We distinguish several cases.

Case $i = 1$. If $j \in \{1, 2, m-1, m\}$, we are done since the corresponding monomial $u_1 u_j$ belongs to G. Assume now $j \in [3, m-2]$. Then $(1, 3) \leq (1, j) \leq (1, m-2)$, and since u_2^2 divides both $u_1 u_3$ and $u_1 u_{m-2}$ by (4), it also divides $u_1 u_j$ by Lemma 2.3.

Case $i, j \in [2, m-2]$. If $(i, j) = (2, 2)$, we are done since $u_2^2 \in G$. If $(i, j) \neq (2, 2)$, then $(2, 3) \leq (i, j) \leq (m-2, m-2)$, and since $u_1 u_{m-1}$ divides both $u_2 u_3$ and u_{m-2}^2 by (3), it follows from Lemma 2.3 that $u_1 u_{m-1}$ also divides $u_i u_j$.

Case $j = m-1$**.** If $i = 2$, then by (2), $u_2 u_{m-1}$ is divisible by $u_1 u_m$ and $u_1 u_m \in G$. If $i \in [3, m-2]$, then $(3, m-1) \leq (i, m-1) \leq (m-2, m-1)$, and since $u_2 u_m$ divides both $u_3 u_{m-1}$ and $u_{m-2} u_{m-1}$ by (5), it also divides $u_i u_{m-1}$ by Lemma 2.3. Finally, if $i = m-1$, we are done since $u_{m-1}^2 \in G$.

Case $j = m$. If $i = 2$, we are done since $u_2 u_m \in G$. If $i \in [3, m-2]$, then $(3, m) \leq (i, m) \leq (m-2, m)$, and since u_{m-1}^2 divides both $u_3 u_m$ and $u_{m-2} u_m$ by (6), it also divides $u_i u_m$ by Lemma 2.3. Finally, if $i \in \{m-1, m\}$, we are done since $u_{m-1} u_m, u_m^2 \in G$.

We conclude that G generates I^2. To establish the equality $G = \mathcal{G}(I^2)$, it remains to see that G is an antichain. Let $A \subset V$ consist of nine pairs (i, j) such that $G = \{u_i u_j \mid (i, j) \in A\}$, for instance

$$A = \{(1,1), (1,2), (2,2), (1,m-1), (1,m), (2,m), (m-1,m-1), (m-1,m), (m,m)\}.$$

Replacing $(2, 2)$ by $(1, 3)$ and $(m-1, m-1)$ by $(m-2, m)$ yields a chain in V, namely

$$\begin{aligned}
&(1,1) < (1,2) < (1,3) < \\
&(1,m-1) < (1,m) < (2,m) < \\
&(m-2,m) < (m-1,m) < (m,m).
\end{aligned}$$

It follows from Lemma 2.1 that the set

$$G' = G \cup \{u_1 u_3, u_{m-2} u_m\} \setminus \{u_2^2, u_{m-1}^2\}$$

is an antichain. In particular, its subset $G \setminus \{u_2^2, u_{m-1}^2\}$ also is. Consider now $u_1 u_3$. Since G generates I^2, then $u_1 u_3$ is a multiple of some element of G. Moreover, since G' is an antichain, the only possible factors of $u_1 u_3$ in G are u_2^2 and u_{m-1}^2. But since $(1, 3) < (m-1, m-1)$, Lemma 2.1 implies that $\{u_1 u_3, u_{m-1}^2\}$ is an antichain. Therefore, the only factor of $u_1 u_3$ in G is u_2^2. Hence, since any monomial in I^2 has at least one factor in $G \cap \mathcal{G}(I^2)$, it follows that $u_2^2 \in \mathcal{G}(I^2)$.

Let us now see that u_2^2 cannot divide another member of G. By Lemma 2.1, the only possible multiples of u_2^2 in G would be $u_1 u_{m-1}$ and $u_1 u_m$. But neither possibility arises, since $u_1 u_{m-1}$ divides $u_2 u_3$ by (3), and $u_1 u_m$ divides $u_2 u_{m-1}$ by (2).

Entirely symmetric arguments apply to u_{m-1}^2. We conclude that $G = \mathcal{G}(I^2)$, as desired. $\square$

4. An explicit construction

We now show that the conditions of Theorem 3.1 ensuring $\mu(I^2) = 9$ are realizable.

Proposition 4.1. *Let $m \geq 5$. Let $I = (u_1, \ldots, u_m)$, where $u_i = x^{a_i}y^{b_i}$ with exponents a_i, b_i defined as follows:*

$$\begin{aligned}(a_1, \ldots, a_m) &= (5m, 4m, 4m-1, \ldots, 3m+4, m, 0),\\ (b_1, \ldots, b_m) &= (a_m, \ldots, a_1).\end{aligned}$$

Then $\mu(I) = m$ and $\mu(I^2) = 9$.

Proof. Since the a_i are decreasing and the b_i are increasing, the u_i constitute an antichain and hence a minimal system of generators of I. In order to show $\mu(I^2) = 9$, it suffices to prove that the divisibility conditions of Theorem 3.1 are met. This is straightforward. For convenience, here are the monomials involved:

$$\begin{array}{lll}
u_1u_m = x^{5m}y^{5m} & u_2u_{m-1} = x^{5m}y^{5m} & \\
u_1u_{m-1} = x^{6m}y^{4m} & u_2u_3 = x^{8m-1}y^{4m+4} & u_{m-2}^2 = x^{6m+8}y^{8m-2}\\
u_2^2 = x^{8m}y^{2m} & u_1u_3 = x^{9m-1}y^{3m+4} & u_1u_{m-2} = x^{8m+4}y^{4m-1}\\
u_2u_m = x^{4m}y^{6m} & u_3u_{m-1} = x^{5m-1}y^{7m+4} & u_{m-2}u_{m-1} = x^{4m+4}y^{8m-1}\\
u_{m-1}^2 = x^{2m}y^{8m} & u_3u_m = x^{4m-1}y^{8m+4} & u_{m-2}u_m = x^{3m+4}y^{9m-1}.
\end{array}$$

□

Let us now look at the degree distribution of $\mathcal{G}(I)$ and of $\mathcal{G}(I^2)$. The generators u_i of I are of degree $a_i + b_i = a_i + a_{m+1-i}$ for all $i \in [1, m]$. For $m \geq 5$, we find

$$\begin{aligned}\deg(u_1) = \deg(u_2) = \deg(u_{m-1}) = \deg(u_m) &= 5m,\\ \deg(u_i) = \deg(u_{m+1-i}) &= 7m+3\end{aligned}$$

for all $3 \leq i \leq m-2$. That is, the ideal I is generated in two degrees only. For I^2 the situation is even simpler. It is generated in the single degree $10m$, the common degree of its nine minimal generators.

Example 4.2. *Here is the case $m = 10$ of Proposition 4.1. We have*

$$I = (x^{50},\, x^{40}y^{10},\, x^{39}y^{34},\, x^{38}y^{35},\, x^{37}y^{36},\, x^{36}y^{37},\, x^{35}y^{38},\, x^{34}y^{39},\, x^{10}y^{40},\, y^{50})$$

and

$$I^2 = (x^{100},\, x^{90}y^{10},\, x^{80}y^{20},\, x^{60}y^{40},\, x^{50}y^{50},\, x^{40}y^{60},\, x^{20}y^{80},\, x^{10}y^{90},\, y^{100}).$$

To conclude this section, let us show that in contrast, if I is generated in a single degree, then $\mu(I^2)$ grows to infinity with $\mu(I)$.

Proposition 4.3. *Let $I \subset K[x, y]$ be a monomial ideal generated in a single degree. If $\mu(I) = m$ then $\mu(I^2) \geq 2m - 1$.*

Proof. Set $\mathcal{G}(I) = \{u_1, \ldots, u_m\}$, and assume $\deg(u_i) = d$ for all i. Since $\deg(u_iu_j) = 2d$ for all i, j, the distinct u_iu_j form an antichain for divisibility. Hence $\mu(I^2)$ equals the number of pairwise distinct u_iu_j. Now that number is at least $2m - 1$, as witnessed by the subset

$$u_1u_1,\, u_1u_2,\, \ldots,\, u_1u_m,\, u_2u_m,\, \ldots,\, u_mu_m.$$

□

5. Computing $\mu(I^k)$

For the ideal I satisfying $\mu(I) = m, \mu(I^2) = 9$ of the preceding section, we now determine $\mu(I^k)$ for all k.

Proposition 5.1. *Given $m \geq 5$, let $I = (u_1, \ldots, u_m)$ be the ideal defined in Proposition 4.1. For all $k \geq 3$, we have $\mu(I^k) = 5k + 1$.*

Proof. It follows from Theorem 3.1 that I^2 is minimally generated by

$$G = \{u_1^2, u_1u_2, u_2^2\} \cup \{u_1u_{m-1}, u_1u_m, u_2u_m\} \cup \{u_{m-1}^2, u_{m-1}u_m, u_m^2\}.$$

Let $J = (u_1, u_2, u_{m-1}, u_m)$ and $H = (u_3, \ldots, u_{m-2})$, so that $I = J + H$. Then $I^2 = J^2$, since $I^2 = (G) \subseteq J^2 \subseteq I^2$. Hence $IJ, IH \subseteq J^2$, from which it follows that $I^k = J^k$ for all $k \geq 3$.

Now, by construction in Proposition 4.1, we have $J = (x^{5m}, x^{4m}y^m, x^my^{4m}, y^{5m})$. Let $J_0 = (x^5, x^4y, xy^4, y^5)$. Then $\mu(J^k) = \mu(J_0^k)$ for all $k \geq 1$. Moreover, we have

$$J_0^3 = (x^{15}, x^{14}y, \ldots, xy^{14}, y^{15})$$

as easily seen. It follows that $J_0^k = (x, y)^{5k}$ for all $k \geq 3$. Therefore

$$\mu(I^k) = \mu(J^k) = \mu(J_0^k) = 5k + 1$$

for all $k \geq 3$, as stated. □

Corollary 5.2. *For any integer $k_0 \geq 2$, there exists a monomial ideal I in $K[x, y]$ such that $\mu(I^k) < \mu(I)$ for all k such that $2 \leq k \leq k_0$.*

Proof. Let $m > 5k_0 + 1$. By Propositions 4.1 and 5.1, there is an ideal I with $\mu(I) = m > 5k_0 + 1$ and satisfying $\mu(I^k) \leq 5k + 1$ for all $k \geq 2$. Therefore $\mu(I^k) < \mu(I)$ for all $2 \leq k \leq k_0$. □

6. Optimality

We now prove that Theorem 3.1 is best possible, in the sense that $\mu(I^2)$ is bounded below by 9 if $\mu(I) \geq 6$. For that we need some more notation. If $I \subset K[x, y]$ is a monomial ideal with $\mathcal{G}(I) = \{u_1, \ldots, u_m\}$, let us denote

$$\mathcal{G}^2(I) = \{u_iu_j \mid 1 \leq i \leq j \leq m\},$$

i.e. $\mathcal{G}^2(I) = f(V)$ in the notation of the Introduction. Let

$$\gamma\colon \mathcal{G}^2(I) \to \mathcal{G}(I^2)$$

be the map defined, for all $u_iu_j \in \mathcal{G}^2(I)$, by

$$\gamma(u_iu_j) = u_ku_l, \tag{7}$$

where $u_ku_l \in \mathcal{G}(I^2)$ is the *lexicographically first* minimal monomial generator of I^2 dividing u_iu_j. Note that $\gamma \circ \gamma = \gamma$. Finally, given $u_iu_j \in \mathcal{G}^2(I)$, we denote

$$\operatorname{div}(u_iu_j) = \{u_ru_s \in \mathcal{G}^2(I) \mid u_ru_s \text{ divides } u_iu_j\}.$$

Of course $\gamma(u_iu_j) \in \operatorname{div}(u_iu_j)$. We will repeatedly use the following reformulation of Lemma 2.1.

Lemma 6.1. *For all $(i,j) \in V$, we have*

$$\operatorname{div}(u_iu_j) \subseteq \{u_iu_j\} \cup \{u_ru_s \in \mathcal{G}^2(I) \mid (r,s) \text{ is noncomparable to } (i,j) \text{ in } V\}.$$

Proof. As stated in Lemma 2.1, if u_ru_s divides u_iu_j and $(r,s) \neq (i,j)$, then $\{(r,s),(i,j)\}$ is an antichain in V. □

Thus for instance, $\operatorname{div}(u_1u_3) \subseteq \{u_1u_3, u_2^2\}$ as already observed after Remark 2.2. Again, it is useful to keep in mind the picture representing noncomparable pairs following that remark.

Here is the main result of this section.

Theorem 6.2. *Let $I \subset K[x,y]$ be a monomial ideal. If $\mu(I) \geq 6$ then $\mu(I^2) \geq 9$.*

Proof. Let $m = \mu(I)$. As before, we denote $\mathcal{G}(I) = \{u_1, \ldots, u_m\}$, where $u_i = x^{a_i}y^{b_i}$ for all i and where the a_i, b_i are decreasing and increasing, respectively. We start by considering the following six monomials in $\mathcal{G}^2(I)$:

$$u_1^2, u_1u_2, u_1u_3, u_{m-2}u_m, u_{m-1}u_m, u_m^2.$$

By Lemma 6.1, we have $\gamma(u_1^2) = u_1^2$ since $(1,1)$ is comparable to every $(i,j) \in V$, namely $(1,1) \leq (i,j)$. Similarly, each one of the pairs $(1,2), (m-1,m), (m,m)$ is comparable to all elements of V, whence

$$\gamma(u_1u_2) = u_1u_2,\ \gamma(u_{m-1}u_m) = u_{m-1}u_m,\ \gamma(u_m^2) = u_m^2.$$

Consider u_1u_3. Then

$$\gamma(u_1u_3) \in \operatorname{div}(u_1u_3) \subseteq \{u_1u_3, u_2^2\}$$

by Lemma 6.1, since $(1,3)$ is comparable to all elements of V except $(2,2)$. Symmetrically, we have

$$\gamma(u_{m-2}u_m) \in \{u_{m-2}u_m, u_{m-1}^2\}.$$

Thus so far, we have six pairwise distinct minimal monomial generators of I^2, namely

$$A = \{u_1^2, u_1u_2, \gamma(u_1u_3), \gamma(u_{m-2}u_m), u_{m-1}u_m, u_m^2\} \subseteq \mathcal{G}(I^2). \tag{8}$$

Considering u_1u_m, we distinguish two cases.

Case 1: $\gamma(u_1u_m) \neq u_1u_m$**.** Therefore $u_1u_m \notin \mathcal{G}(I^2)$, and $\gamma(u_1u_m) = u_ru_s$ for some $r,s \in [2, m-1]$ such that $r \leq s$. Since $\operatorname{div}(u_2u_3) \cap \operatorname{div}(u_{m-2}u_{m-1}) \subseteq \{u_1u_m\}$ by Lemma 6.1, it follows that $\gamma(u_2u_3) \neq \gamma(u_{m-2}u_{m-1})$. Moreover, it also follows from Lemma 6.1 that $\gamma(u_2u_3), \gamma(u_{m-2}u_{m-1}) \notin A$. So let

$$A' = A \sqcup \{\gamma(u_2u_3), \gamma(u_{m-2}u_{m-1})\}.$$

Then $\operatorname{card}(A') = 8$. There are two subcases.

Case (1.1) If $\gamma(u_1u_m) \notin A'$, then we are done, since joining $\gamma(u_1u_m)$ to A' yields nine minimal generators of I^2.

Case (1.2) If $\gamma(u_1u_m) \in A'$, then by Lemma 6.1, the only possibilities are as follows:

$$\begin{array}{lclcl}
\gamma(u_1u_m) & = & u_2^2 & = & \gamma(u_1u_3), \\
\gamma(u_1u_m) & = & u_2u_3 & = & \gamma(u_2u_3), \\
\gamma(u_1u_m) & = & u_{m-2}u_{m-1} & = & \gamma(u_{m-2}u_{m-1}), \\
\gamma(u_1u_m) & = & u_{m-1}^2 & = & \gamma(u_{m-1}^2).
\end{array}$$

But then in each case, Lemma 6.1 implies $\gamma(u_2u_{m-2}) \notin A'$, and we are done again.

Case 2: $\gamma(u_1u_m) = u_1u_m$**.** Then $u_1u_m \in \mathcal{G}(I^2)$. Let

$$A' = A \sqcup \{u_1u_m\} = \{u_1^2, u_1u_2, \gamma(u_1u_3), \gamma(u_{m-2}u_m), u_{m-1}u_m, u_m^2, u_1u_m\}.$$

Then $A' \subseteq \mathcal{G}(I^2)$ and $\operatorname{card}(A') = 7$. Comparing $\gamma(u_1u_{m-1})$ to $\gamma(u_1u_3)$, and $\gamma(u_2u_m)$ to $\gamma(u_{m-2}u_m)$, gives rise to four subcases. Let us consider them in turn.

Case (2.1): $\gamma(u_1u_{m-1}) = \gamma(u_1u_3)$**,** $\gamma(u_2u_m) = \gamma(u_{m-2}u_m)$**.**

Since $\operatorname{div}(u_1u_{m-1}) \cap \operatorname{div}(u_1u_3) \subseteq \{u_2^2\}$, we have $\gamma(u_1u_{m-1}) = \gamma(u_1u_3) = u_2^2$. Similarly, we have $\gamma(u_2u_m) = \gamma(u_{m-2}u_m) = u_{m-1}^2$. Therefore

$$\begin{aligned} u_2^2 &\mid u_1u_{m-1}, \\ u_{m-1}^2 &\mid u_2u_m. \end{aligned}$$

Hence $u_2^2u_{m-1}^2 \mid u_1u_{m-1}u_2u_m$, implying $u_2u_{m-1} \mid u_1u_m$. Whence

$$u_2u_{m-1} = u_1u_m \tag{9}$$

since $u_1u_m \in \mathcal{G}(I^2)$. Let

$$A'' = A' \cup \{\gamma(u_2u_3), \gamma(u_{m-2}u_{m-1})\}.$$

Then $A'' \subseteq \mathcal{G}(I^2)$ by construction. We claim that $\operatorname{card}(A'') = 9$. Indeed, Lemma 6.1 implies

$$\{\gamma(u_2u_3), \gamma(u_{m-2}u_{m-1})\} \cap A' \subseteq \{u_1u_m\}.$$

But since $u_1u_m = u_2u_{m-1}$ here, as observed in (9), it follows that

$$u_1u_m \notin \operatorname{div}(u_2u_3) \cup \operatorname{div}(u_{m-2}u_{m-1}), \tag{10}$$

whence the above intersection is empty. Moreover, since $\operatorname{div}(u_2u_3) \cap \operatorname{div}(u_{m-2}u_{m-1}) \subseteq \{u_1u_m\}$, it follows from (10) that $\gamma(u_2u_3) \neq \gamma(u_{m-2}u_{m-1})$. Therefore $\operatorname{card}(A'') = 9$ as claimed, and we are done in this case.

Case (2.2): $\gamma(u_1u_{m-1}) = \gamma(u_1u_3)$**,** $\gamma(u_2u_m) \neq \gamma(u_{m-2}u_m)$**.**

This is by far the most delicate case. As observed in the preceding case, the equality $\gamma(u_1u_{m-1}) = \gamma(u_1u_3)$ implies $\gamma(u_1u_{m-1}) = \gamma(u_1u_3) = u_2^2$. Now $\gamma(u_2u_m) \notin A'$, as follows from Lemma 6.1 and the inequality $\gamma(u_2u_m) \neq \gamma(u_{m-2}u_m)$. Let

$$A'' = A' \cup \{\gamma(u_2u_m)\}.$$

Then $A'' \subseteq \mathcal{G}(I^2)$ and $\operatorname{card}(A'') = 8$. We distinguish four subcases, according to the values of $\gamma(u_2u_m)$ and $\gamma(u_{m-2}u_m)$. Recall that $\gamma(u_{m-2}u_m) \in \{u_{m-2}u_m, u_{m-1}^2\}$.

Case (2.2.1): $\gamma(u_2u_m) = u_2u_m$**,** $\gamma(u_{m-2}u_m) = u_{m-2}u_m$**.**

Then

$$A'' = \{u_1^2, u_1u_2, u_2^2, u_{m-2}u_m, u_{m-1}u_m, u_m^2, u_1u_m, u_2u_m\}.$$

Interestingly here, for $m = 5$, there are explicit cases where $A'' = \mathcal{G}(I^2)$. Now under our hypothesis $m \geq 6$, a ninth element in $\mathcal{G}(I^2) \setminus A''$ is given by $\gamma(u_3u_m)$, as easily follows from the present shape of A'' and Lemma 6.1.

Case (2.2.2): $\gamma(u_2u_m) = u_2u_m$**,** $\gamma(u_{m-2}u_m) = u_{m-1}^2$**.**

Then

$$A'' = \{u_1^2, u_1u_2, u_2^2, u_{m-1}^2, u_{m-1}u_m, u_m^2, u_1u_m, u_2u_m\}.$$

Consider u_2u_{m-1}. If $\gamma(u_2u_{m-1}) \notin A''$, we have our ninth minimal generator and we are done. Assume now for a contradiction that $\gamma(u_2u_{m-1}) \in A''$. Then under the present shape of A'' and Lemma 6.1, the only possibility is $\gamma(u_2u_{m-1}) = u_1u_m$. Therefore

$$\begin{aligned} u_2^2 &\mid u_1u_{m-1}, \\ u_1u_m &\mid u_2u_{m-1}. \end{aligned}$$

Hence $u_1u_2^2u_m \mid u_1u_2u_{m-1}^2$, implying $u_2u_m \mid u_{m-1}^2$. This is a contradiction, since $u_{m-1}^2 = \gamma(u_{m-2}u_m)$, whence u_{m-1}^2 divides $u_{m-2}u_m$ which is not divisible by u_2u_m.

Case (2.2.3): $\gamma(u_2u_m) \neq u_2u_m$**,** $\gamma(u_{m-2}u_m) = u_{m-2}u_m$**.**

By Lemma 6.1, we have $\gamma(u_2u_m) = u_ru_s$ for some $3 \leq r \leq s \leq m-1$. Then

$$A'' = \{u_1^2, u_1u_2, u_2^2, u_{m-2}u_m, u_{m-1}u_m, u_m^2, u_1u_m, u_ru_s\}.$$

Consider $u_{m-3}u_m$. If $\gamma(u_{m-3}u_m) \notin A''$, we have our ninth minimal generator and we are done. If $\gamma(u_{m-3}u_m) \in A''$, then the only possibility allowed by Lemma 6.1 is $\gamma(u_{m-3}u_m) = u_ru_s$. The same lemma then implies $m-2 \leq r \leq s \leq m-1$.

Consider now u_2u_3. If $\gamma(u_2u_3) \notin A''$, we are done. Assume now for a contradiction that $\gamma(u_2u_3) \in A''$. Then the only possibility is $\gamma(u_2u_3) = u_1u_m$. Therefore, since $\gamma(u_1u_3) = u_2^2$ in the present case, we have

$$\begin{aligned} u_2^2 &\mid u_1u_3, \\ u_1u_m &\mid u_2u_3. \end{aligned}$$

Hence $u_1u_2^2u_m \mid u_1u_2u_3^2$, implying $u_2u_m \mid u_3^2$. This is a contradiction, since $\gamma(u_2u_m) = u_ru_s$, whence u_ru_s divides u_2u_m but cannot divide u_3^2 since $r, s \in [m-2, m-1]$.

Case (2.2.4): $\gamma(u_2u_m) \neq u_2u_m$**,** $\gamma(u_{m-2}u_m) = u_{m-1}^2$**.**

As above, we have $\gamma(u_2u_m) = u_ru_s$ for some $3 \leq r \leq s \leq m-1$, and here with $(r, s) \neq (m-1, m-1)$ since $\gamma(u_2u_m) \neq \gamma(u_{m-2}u_m)$ in the present Case (2.2). Then

$$A'' = \{u_1^2, u_1u_2, u_2^2, u_{m-1}^2, u_{m-1}u_m, u_m^2, u_1u_m, u_ru_s\}.$$

To settle this case, it suffices to show that either $\gamma(u_2u_{m-1})$ or $\gamma(u_{m-2}u_{m-1})$ lies outside A''. Assume for a contradiction the contrary, i.e.

$$\{\gamma(u_2u_{m-1}), \gamma(u_{m-2}u_{m-1})\} \subset A''. \tag{11}$$

Lemma 6.1 then implies

$$\{\gamma(u_2u_{m-1}), \gamma(u_{m-2}u_{m-1})\} \subseteq \{u_1u_m, u_ru_s\}. \tag{12}$$

On the other hand, that same lemma implies

$$\operatorname{div}(u_2u_{m-1}) \cap \operatorname{div}(u_{m-2}u_{m-1}) \subseteq \{u_1u_m\}. \tag{13}$$

We cannot have $\gamma(u_{m-2}u_{m-1}) = u_1u_m$. For otherwise, in the present Case (2.2.4), that equality would imply

$$\begin{aligned} u_1u_m &\mid u_{m-2}u_{m-1}, \\ u_{m-1}^2 &\mid u_{m-2}u_m. \end{aligned}$$

Therefore $u_1u_{m-1}^2u_m \mid u_{m-2}^2u_{m-1}u_m$, whence $u_1u_{m-1} \mid u_{m-2}^2$. This is impossible, since u_2^2 divides u_1u_{m-1} in the present Case (2.2), whereas u_2^2 cannot divide u_{m-2}^2 by Lemma 6.1.

Therefore $\gamma(u_{m-2}u_{m-1}) \neq u_1u_m$, whence $\gamma(u_{m-2}u_{m-1}) = u_ru_s$ by (12). Since $r, s \in [3, m-1]$, this and Lemma 6.1 imply $(r, s) = (m-2, m-1)$. That is, we have

$$\gamma(u_{m-2}u_{m-1}) = u_ru_s = u_{m-2}u_{m-1}. \tag{14}$$

Consider now u_2u_{m-1}. It follows from (12), (13) and (14), that $\gamma(u_2u_{m-1}) = u_1u_m$. In the present Case (2.2), this yields

$$\begin{aligned} u_1u_m &\mid u_2u_{m-1}, \\ u_2^2 &\mid u_1u_{m-1}. \end{aligned}$$

Therefore $u_2u_m \mid u_{m-1}^2$. But u_{m-1}^2 divides $u_{m-2}u_m$ in the present Case (2.2.4), yet u_2u_m cannot divide $u_{m-2}u_m$. This contradiction shows that (11) is absurd. Therefore

$$\operatorname{card}\bigl(A'' \cup \{\gamma(u_2u_{m-1}), \gamma(u_{m-2}u_{m-1})\}\bigr) \geq 9.$$

This settles Case (2.2.4) and concludes Case (2.2).

Case (2.3): $\gamma(u_1u_{m-1}) \neq \gamma(u_1u_3)$**,** $\gamma(u_2u_m) = \gamma(u_{m-2}u_m)$**.**

This case is symmetrical to Case (2.2). It follows from it by interchanging the variables x, y and reversing the sequence $u_1, \ldots, u_m$.

Case (2.4): $\gamma(u_1u_{m-1}) \neq \gamma(u_1u_3)$**,** $\gamma(u_2u_m) \neq \gamma(u_{m-2}u_m)$**.**

Being in Case (2), recall that

$$A' = A \sqcup \{u_1u_m\} = \{u_1^2, u_1u_2, \gamma(u_1u_3), \gamma(u_{m-2}u_m), u_{m-1}u_m, u_m^2, u_1u_m\},$$

a subset of cardinality 7 in $\mathcal{G}(I^2)$. It follows from the present hypotheses that

$$A' \cap \{\gamma(u_1u_{m-1}), \gamma(u_2u_m)\} = \emptyset. \tag{15}$$

Thus, it suffices to show $\gamma(u_1u_{m-1}) \neq \gamma(u_2u_m)$, for then this would imply

$$\operatorname{card}\bigl(A' \cup \{\gamma(u_1u_{m-1}), \gamma(u_2u_m)\}\bigr) = 9 \tag{16}$$

and we would be done. Assume for a contradiction the contrary, i.e. that $\gamma(u_1u_{m-1}) = \gamma(u_2u_m)$. Lemma 6.1 then implies

$$\gamma(u_1u_{m-1}) = \gamma(u_2u_m) = u_ru_s \tag{17}$$

for some $r, s \in [3, m-2]$ with $r \leq s$. Thus u_ru_s divides both u_1u_{m-1} and u_2u_m. Since $(1, m-1) < (1, m) < (2, m)$ in V, Lemma 2.3 implies that u_ru_s also divides u_1u_m. But since $u_1u_m \in A' \subseteq \mathcal{G}(I^2)$, it follows that $u_ru_s = u_1u_m$. Thus $u_ru_s \in A'$, contrary to the conjunction of (17) and (15). This contradiction settles (16) and concludes the proof of the present last case, and hence of the theorem. $\square$

For completeness, let us give optimal lower bounds on $\mu(I^2)$ for monomial ideals $I \subset K[x,y]$ such that $\mu(I) = m \leq 5$. The result is as follows.

$$\mu(I^2) \geq \begin{cases} 1 & \text{if } m = 1, \\ 3 & \text{if } m = 2, \\ 5 & \text{if } m = 3, \\ 7 & \text{if } m = 4, \\ 8 & \text{if } m = 5. \end{cases}$$

As stated, these five lower bounds are sharp. The verification is left to the reader.

Let us conclude this paper with two questions. Let $m \geq 6$ be an integer, and let $I \subset K[x,y]$ be a monomial ideal such that $\mu(I) = m$. We have seen in Proposition 4.3 that if I is generated in a single degree, then $\mu(I^2) \geq 2m - 1$. Our ideals in Proposition 4.1 reaching the absolute minimum $\mu(I^2) = 9$ are generated in two degrees depending on m, namely $5m$ and $7m + 3$.

Here is our first question. If I is generated in two degrees $d_1 < d_2$ *such that the difference* $d = d_2 - d_1$ *is fixed and independent of* m, does it follow that $\mu(I^2)$ must grow to infinity with m? This seems to be true for $d = 1$, but it would be nice to have a proof.

Our second question is, what would be the proper generalization of the present results in n variables?

References

[1] J. Herzog and R. Waldi, A note on the Hilbert function of a one-dimensional Cohen-Macaulay ring. Manuscripta Math. **16** (1975), 251-260.

[2] F. Orecchia, One-dimensional local rings with reduced associated graded ring and their Hilbert functions. Manuscripta Math. **32** (1980), 391–405.

[3] J. Herzog, M. Mohammadi Saem and N. Zamani, On the number of generators of powers of an ideal, 2017, arXiv:1707.07302.

Shalom Eliahou, Univ. Littoral Côte d'Opale, EA 2597 - LMPA - Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville, F-62228 Calais, France and CNRS, FR 2956, France

E-mail address: `eliahou@univ-littoral.fr`

Jürgen Herzog, Fachbereich Mathematik, Universität Duisburg-Essen, Campus Essen, 45117 Essen, Germany

E-mail address: `juergen.herzog@uni-essen.de`

Maryam Mohammadi Saem, Faculty of Science, University of Mohaghegh Ardabili, P.O. Box 179, Ardabil, Iran

E-mail address: `m.mohammadisaem@yahoo.com`