

Length Approximations for Independently Generated Ideals

Douglas Hanes

Department of Mathematics, University of Minnesota, Minneapolis, Minnesota 55455

E-mail: hanes@math.umn.edu

Communicated by Craig Huneke

Received March 28, 2000

We study ideals primary to the maximal ideal of a commutative Noetherian local ring. When such an ideal is generated by elements which are independent in the sense of C. Lech, we prove a lower bound on the length of the quotient ring in terms of the orders of the generators. As a corollary we obtain a substantial partial result on Lech's conjecture on the multiplicities of a flat couple of local rings.

© 2001 Academic Press

Key Words: commutative algebra; matrix factorization.

1. INTRODUCTION

In this paper all rings are assumed to be commutative, Noetherian, and to possess a multiplicative unit element. All ring homomorphisms are assumed to be unital.

Let (R, m) be a local ring, and let I be an m -primary ideal, so that the homomorphic image R/I has finite length. Our primary object is to show that if the ideal I is generated by elements which are *independent* (as defined by Lech in [6]), then one may give a lower estimate for the length of R/I in terms of the orders of the generators of I (where by the “order” of an element x we mean the largest t such that $x \in m^t$).

Because of possible confusion caused by the much-used term “independent,” we will call the elements $x_1, \dots, x_r$ of a commutative ring R *Lech-independent*, or independent in the sense of Lech, if for every relation of the form

$$x_1 u_1 + x_2 u_2 + \cdots + x_r u_r = 0$$



in R , one may conclude that $u_i \in (x_1, \dots, x_r)R$ for $1 \leq i \leq r$ (see [6]). As (important) examples, we note that the maximal ideal of any local ring is generated by Lech-independent elements, and that any regular sequence $x_1, \dots, x_n$ is Lech-independent. Moreover, note that if $I \subseteq R$ is generated by Lech-independent elements, and if S is any flat ring extension of R , then the extended ideal IS is still generated by Lech-independent elements.

Lech's main result [6, Theorem 2] on independent sequences is the following theorem. Note that if $I = (x_1, \dots, x_m)$ is an ideal of R , then the sequence of elements $x_1, \dots, x_m$ is Lech-independent if and only if I/I^2 is a free module (of rank m) over R/I . In Lech's presentation the latter of the equivalent hypotheses is used.

THEOREM 1.1 (Lech). *Let $x_1, \dots, x_r$ be a sequence of independent elements in a local ring S of embedding dimension t , and assume that $S/(\underline{x})S$ is equicharacteristic and has finite length. Then $r \leq t$.*

The theorem may be directly applied to flat couples of local rings, which are defined as follows:

DEFINITION 1.1. A *flat couple* or *flat local extension* of local rings is an extension $(R, m) \subseteq (S, n)$ of local rings with the properties that S is a flat R -module and that $mS \subseteq n$.

By the *embedding dimension* $\text{edim}(R)$ of a local ring (R, m) we mean the minimal number of generators $\nu(m)$ of its maximal ideal m . It follows from Theorem 1.1 that if $(R, m) \subseteq (S, n)$ is a flat local extension of local rings of dimension d , then the embedding dimension $\text{edim}(R)$ of R is less than or equal to that of S , since the minimal generators of m map to an independent set of elements of S . In fact, by employing a similar result with regard to localization, Lech shows in [6] that

$$\text{edim}(R) \leq \text{edim}(S)$$

for any flat local extension $(R, m) \subseteq (S, n)$.

Our main result is the following theorem, which gives a lower bound on the length of S/I when I is an n -primary ideal of the local ring (S, n) generated by independent elements.

THEOREM 1.2. *Let $x_1, \dots, x_r$ be a set of Lech-independent elements of a commutative local ring (T, m_T) which generate an ideal primary to the maximal ideal. Suppose that for $1 \leq i \leq r$, $x_i \in m_T^{t_i}$. Then*

$$l(T/(x_1, \dots, x_r)T) \geq \prod_{i=1}^r t_i.$$

Such an inequality is well known for any system of parameters $x_1, \dots, x_d$, and the theorem represents a generalization of this fact in the case that $x_1, \dots, x_d$ is a regular sequence. We note that the statement of the theorem is implied by the results of [6] in the case that each x_i is actually a t th power of some element of m_T . Of course nothing like this can be assumed about a general element $x_i \in m_T^t$, but we will employ the following theorem of [1] in order to realize each x_i as the t th power of some square matrix with entries in m_T .

THEOREM 1.3 (Backelin, Herzog, and Ulrich). *Let R be a commutative Noetherian ring, and let I be an ideal of R . If $a \in I^t$, then there exists, for some $n > 0$, a matrix $A \in M_n(R)$ such that:*

1. $A^t = a \cdot I_n$, where I_n is the $n \times n$ identity matrix.
2. The ideal generated by the entries of A is equal to I .

The second statement implies—and this will be the key point for our purposes—that the entries of the matrix A are all in I . It turns out that for the considerations of this paper, these “matrix roots” of the elements are just as good as real roots within the ring.

As for Lech, our applications, to be presented in the final section, will be to flat local ring extensions $(R, m) \subseteq (S, n)$. In fact, we are able to prove a very general partial result (Theorem 3.1) on Lech’s conjecture that there should be a general inequality

$$e(R) \leq e(S)$$

on the Hilbert–Samuel multiplicities of the base and flat extension rings with respect to their respective maximal ideals (see [5]).

2. THE MAIN RESULTS ON LENGTHS

In order to prove our results, we need to first extend the definition of independence in order to include the notion of elements of a commutative ring R acting independently on an R -module M .

DEFINITION 2.1. Let T be a commutative ring, and let M be any T -module. Then we say that the elements $x_1, \dots, x_r$ of the ring T act *Lech-independently* on M if, for any relation of the form

$$x_1 u_1 + x_2 u_2 + \cdots + x_r u_r,$$

where each $u_i \in M$, one may conclude that each $u_i \in (x_1, \dots, x_r)M$.

With this definition, one may prove the following lemma and corollary, which generalize similar results of [6], and which are proved in a very similar fashion.

LEMMA 2.1. *Let $x_1, \dots, x_r$ be elements of T which act Lech-independently on M , and suppose that $x_1 = yz$. Then the elements $y, x_2, \dots, x_r$ also act Lech-independently on M , and*

$$(x_1, \dots, x_r)M :_M y = (z, x_2, \dots, x_r)M.$$

Proof. Suppose that one has a relation

$$yu_1 + x_2u_2 + \dots + x_ru_r = 0,$$

where the $u_i \in M$. By multiplying with z , we get a new relation:

$$x_1u_1 + x_2zu_2 + \dots + x_rzu_r = 0.$$

By hypothesis, this implies that $u_1 \in (x_1, \dots, x_r)M$. So if $u_1 = x_1v_1 + x_2v_2 + \dots + x_rv_r$, we may rewrite the first relation as

$$x_1yv_1 + x_2(u_2 + yv_2) + \dots + x_r(u_r + yv_r) = 0.$$

The independence of the x 's now implies that $u_i + yv_i \in (x_1, \dots, x_r)M$ for $i \geq 2$, which shows that $u_i \in (y, x_2, \dots, x_r)M$ for all i .

For the second statement, suppose that for $v \in M$, one has $yv \in (x_1, \dots, x_r)M$. Then there exist elements $w_1, \dots, w_r$ of M such that

$$yv + x_1w_1 + x_2w_2 + \dots + x_rw_r = 0.$$

Multiplying by z then gives

$$x_1(v + zw_1) + x_2zw_2 + \dots + x_rzw_r = 0.$$

The independence of the x 's implies that $v + zw_1 \in (x_1, \dots, x_r)M$, so that $v \in (z, x_2, \dots, x_r)M$, as claimed. ■

COROLLARY 2.1. *Suppose that the elements $x_1, \dots, x_r$ of the ring T act Lech-independently on the module M , and that there exist elements $y_1, \dots, y_r$ of T and positive integers s_i such that $x_i = y_i^{s_i}$ for $1 \leq i \leq r$. If we set $I = (x_1, \dots, x_r)$ and $J = (y_1, \dots, y_r)$, then M/IM has a filtration by $\prod_1^r s_i$ copies of M/JM . In particular, if (T, m) is local and I is primary to m , then*

$$l(M/IM) = \left(\prod_1^r s_i \right) \cdot l(M/JM).$$

Proof. We proceed by induction on $\sum_1^r s_i$; the conclusion is immediate if this sum is equal to r . Thus, we may assume without loss of generality that $s_1 \geq 2$, so that $x_1 = y_1 \cdot y_1^{s_1-1}$. Note that if $\mathcal{A}$ is any ideal of T , and z is an element not in $\mathcal{A}$, then one has an exact sequence:

$$0 \rightarrow M/(\mathcal{A}M :_M z) \rightarrow M/\mathcal{A}M \rightarrow M/(\mathcal{A} + z)M \rightarrow 0.$$

By Lemma 2.2, we know that $IM:{}_M y_1 = (y_1^{s_1-1}, x_2, \dots, x_r)M$. Thus, applying the exact sequence given above with $\mathcal{A} = I$ and $z = y_1$ gives the short exact sequence

$$0 \rightarrow \frac{M}{(y_1^{s_1-1}, x_2, \dots, x_r)M} \rightarrow \frac{M}{IM} \rightarrow \frac{M}{(y_1, x_2, \dots, x_r)M} \rightarrow 0.$$

Now, by the induction hypothesis, the modules on the outside of the exact sequence may be filtered by $(s_1 - 1) \cdot \prod_2^r s_i$ and $\prod_2^r s_i$ copies of M/JM , respectively. It follows that M/IM may be filtered by $\prod_1^r s_i$ copies of M/JM , which completes the proof of the corollary. ■

With the corollary as well as the theory of matrix factorization in hand, we are now able to give a proof of the main theorem. The central idea is that, if an element x in the t th power of the maximal ideal of a local ring (S, n) is allowed to act upon a suitable free module $S^{(N)}$, then it follows from Theorem 1.3 that this action can be realized as the t th power of a certain matrix action on $S^{(N)}$, where the matrix in question has entries in the maximal ideal n .

Proof of Theorem 1.2. It follows from Theorem 1.3 that, for each i , there exists n_i and a matrix $A_i \in M_{n_i}(T)$ such that $A_i^{t_i} = x_i \cdot I_{n_i}$, and such that all entries of A_i are contained in the maximal ideal m_T . For each i , denote the free T -module of rank n_i acted upon by A_i by V_i . Now replace each matrix A_i by the matrix

$$V_1 \otimes_T \cdots \otimes_T V_{i-1} \otimes_T A_i \otimes_T V_{i+1} \otimes_T \cdots \otimes_T V_r \in M_N(T),$$

where $N = \prod_1^r n_i$. The new matrices A_i still have entries in m_T , and still satisfy $A_i^{t_i} = x_i \cdot I_N$. But now the A_i all act on the same free module $T^{(N)}$, and also commute.

Thus, the ring $T' = T[A_1, \dots, A_r] \subseteq M_N(T)$ is commutative local (each A_i has a power in m_T) and module-finite over T (T embeds into T' as scalar matrices). Moreover, the free T -module $T^{(N)}$ has a natural T' -module structure which extends the usual T -module structure.

We next note that the elements $x_1, \dots, x_r$ of T' act independently on the module $T^{(N)}$ (since the x_i are in T , this really has nothing to do with the extension ring T'). So by the corollary to the lemma, we see that

$$l(T^{(N)}/(x_1, \dots, x_r)T^{(N)}) = \prod_{i=1}^r t_i \cdot l\left(\frac{T^{(N)}}{\sum_1^r A_i T^{(N)}}\right). \quad (1)$$

(Technically, these lengths are taken over T' , but since T and T' have the same residue field, they are equal to the lengths taken over T .) Since the

matrices A_i all have entries in m_T , it is clear that

$$l\left(\frac{T^{(N)}}{\sum_1^r A_i T^{(N)}}\right) \geq N. \quad (2)$$

Combining the formulas (1) and (2) now implies that

$$l(T/(x_1, \dots, x_r)T) \geq \prod_{i=1}^r t_i,$$

as claimed. ■

Before moving on to the applications, we should make a few remarks about the proof.

Remark 2.1. If we just let T^* be the free T -algebra

$$T^* = \frac{T[z_1, \dots, z_r]}{(z_i^{t_i} - x_i)},$$

then the existence of commuting matrix roots for the x_i allow us to give some free T -module $T^{(N)}$ a T^* -module structure in such a way that

$$m_{T^*} \cdot T^{(N)} = m_T \cdot T^{(N)}.$$

The proof could now be carried out by thinking of $T^{(N)}$ as a module over T^* with this module structure, thus removing from view the more strange-looking ring T' .

Remark 2.2. Of course, T^* is itself a free T -module of rank $\prod_{i=1}^r t_i$, and the elements x_i act on T^* as the powers of the z_i . However, if one writes down the matrix for the action of z_i on the free T -module T^* , one sees that the matrix involves many unit entries. This prevents us from drawing the conclusion that

$$l(T^*/(z_1, \dots, z_r)T^*) \geq \text{rank}_T(T^*).$$

This is why we cannot use the much more familiar matrix action of the free extension T^* on *itself* in the proof.

Remark 2.3. What the proof of the theorem really shows is that

$$l(T/(x_1, \dots, x_r)T) = (1/N) \left(\prod_{i=1}^r t_i \right) \cdot l\left(\frac{T^{(N)}}{\sum_1^r A_i T^{(N)}}\right).$$

It was shown above that

$$l\left(\frac{T^{(N)}}{\sum_1^r A_i T^{(N)}}\right) \geq N,$$

but in fact, if s represents the embedding dimension of T , then we know by Lech's result (Theorem 1.1) that $r \leq s$, and it is easy to see that we must have

$$l\left(\frac{T^{(N)}}{\sum_1^r A_i T^{(N)}}\right) \geq N \cdot (1 + s - r).$$

This provides the improved estimate:

$$l(T/(x_1, \dots, x_r)T) \geq \left(\prod_{i=1}^r t_i\right) \cdot (1 + \text{edim}(T) - r).$$

3. APPLICATIONS TO FLAT LOCAL EXTENSIONS

We believe that Theorem 1.2 will have many interesting applications to the theory of Hilbert functions and multiplicities. In this section, we will consider two applications to flat couples of local (or graded) rings. First we apply the results on length to Lech's conjecture that if $(R, m) \subseteq (S, n)$ is a flat local extension of local rings, then $e(R) \leq e(S)$. This conjecture, which first appeared in the 1960 paper [5], naturally arises out of Nagata's work on multiplicities in [7]. The conjecture remains open in most cases, as long as the base ring R has dimension at least 3. For the best partial results, the reader is referred to Lech's original papers [5, 6], as well as to [2] by Herzog.

The result to be presented here is most satisfying in the case that $(R, m) \subseteq (S, n)$ is obtained by localization from a flat extension of graded rings, but we begin with the most general conclusion, which only requires reference to the associated graded ring of the extension ring S . Recall that an extension $(R, m) \subseteq (S, n)$ of local rings is called *flat local* if S is a flat R -module and m embeds into n . Also note that if x is an element of R , then by the initial form of x in $G = \text{gr}_n(S)$ we mean the initial form $\text{in}(x)$ of the image of x in S (not the image in G of the initial form of x in $\text{gr}_m(R)$).

COROLLARY 3.1. *Let $(R, m) \subseteq (S, n)$ be a flat local extension of d -dimensional local rings. Assume that there exists a minimal reduction $I = (x_1, \dots, x_d)$ of m with the property that the initial forms $\text{in}(x_1), \dots, \text{in}(x_d)$ in the associated graded ring $G = \text{gr}_n(S)$ of S form a system of parameters for G . Then $e(S) \geq e(R)$. In fact, if $mS \subseteq n^t$, then*

$$e(S) \geq (1 + \nu(n) - \nu(m))(t^{\nu(m)-d})e(R).$$

Proof. First, we may extend the system of parameters $x_1, \dots, x_d$ to a minimal generating set $x_1, \dots, x_r$ of m . For each i , we fix t_i such that x_i maps into $n^{t_i} \setminus n^{t_i+1}$.

We conclude from the flatness condition and Theorem 1.2 (or Remark 2.3) that

$$e(m; S) = e(R) \cdot l(S/mS) \geq (1 + \nu(n) - \nu(m)) \left(\prod_1^r t_i \right) \cdot e(R). \quad (3)$$

On the other hand, we may note that for any n -primary ideal J of S , if $\text{in}(J)$ represents the ideal of initial forms of J in G , then one has

$$e(J; S) \leq e(\text{in}(J); G).$$

This follows from the fact that, for any $t > 0$, $(\text{in}(J))^t \subseteq \text{in}(J^t)$.

Applying this to the ideal mS , we see that

$$e(m; S) \leq e(\text{in}(mS); G) \leq e(\text{in}(x_1), \dots, \text{in}(x_d); G).$$

Finally, since the elements $\text{in}(x_1), \dots, \text{in}(x_d)$ form a homogeneous system of parameters of G of degrees $t_1, \dots, t_d$, respectively, we have that

$$e(\text{in}(x_1), \dots, \text{in}(x_d); G) = \left(\prod_1^d t_i \right) \cdot e(G) = \left(\prod_1^d t_i \right) \cdot e(S).$$

Thus, we may conclude that

$$e(m, S) \leq \left(\prod_1^d t_i \right) \cdot e(S) \quad (4)$$

(actually, we could prove equality).

Now combining the inequalities (3) and (4) implies that

$$e(S) \geq (1 + \nu(n) - \nu(m)) \left(\prod_{d+1}^r t_i \right) \cdot e(R).$$

This certainly implies all of the conclusions of the corollary. ■

Remark 3.1. We remark that the hypothesis of Corollary 3.1 on the flat couple $(R, m) \subseteq (S, n)$ is considerably weaker than that of *tangential flatness*. The extension is called tangentially flat if the associated homomorphism $\text{gr}_m(R) \rightarrow \text{gr}_n(S)$ which maps m^t/m^{t+1} to n^t/n^{t+1} , for each $t \geq 0$, is flat. This condition implies, among other things, that the initial forms in the graded ring of S of a minimal reduction of m will constitute a system of parameters of 1-forms in the graded ring of S .

The condition of tangential flatness, and its relation to the various Lech–Hironaka conjectures, has been considered by Herzog in, e.g., [2, 3] (for Hironaka's statements see [4]).

The condition on the initial forms of the parameters x_i of R need not hold in general. However, it is clear in the case that S is a standard graded algebra over a field and the elements x_i map to homogeneous elements of S . Notice that one may easily extend the notion of a flat couple of rings to the case of a ring extension $R \subseteq S$ of $\mathbf{N}$ -graded rings with homogeneous maximal ideals m and n , respectively. In this case, one says that $(R, m) \subseteq (S, n)$ is a flat couple of $\mathbf{N}$ -graded rings if the homogeneous maximal ideal m of R is mapped into the homogeneous maximal ideal n of S , and if S is a flat R -module. It is then easy to see that $(R, m) \subseteq (S, n)$ is a flat couple of $\mathbf{N}$ -graded rings if and only if the extension $R_m \subseteq S_n$ of local rings is flat local. In the graded case we obtain the following:

COROLLARY 3.2. *Let $(R, m) \subseteq (S, n)$ be a flat extension of standard graded algebras of dimension d . If m has a minimal reduction $I = (x_1, \dots, x_d)$ with the property that each x_i maps to a homogeneous element of positive degree in S , then $e(m; R) \leq e(n; S)$.*

Finally, in the case of a flat extension of graded rings, we may obtain a similar inequality on the a -invariants of the respective rings. We recall the definition, which may be found in [8].

DEFINITION 3.1. Let R be a finitely generated $\mathbf{N}$ -graded K -algebra of dimension d , where $R_0 = K$ is a field. If m is the homogeneous maximal ideal of R , then the a -invariant $a(R)$ of R is defined to be the greatest integer i for which the i th graded piece of the d th local cohomology module $H_m^d(R)$ is nonzero.

If R is Cohen–Macaulay, and if $x_1, \dots, x_d$ is a homogeneous system of parameters of degrees $t_1, \dots, t_d$, respectively, then the a -invariant may be computed as

$$a(R) = \deg G - \sum_1^d t_i,$$

where G is a form of maximal degree not in $(x_1, \dots, x_d)$. It follows that if R is a standard graded algebra (i.e., generated by 1-forms over a field), then $a(R) + d$ is equal to the *reduction number* of R .

DEFINITION 3.2. Let R be a standard graded algebra over a field K . For any system of parameters of 1-forms $x_1, \dots, x_d$, let $r_{\underline{x}}$ denote the maximal degree of a form of R not in the ideal $(x_1, \dots, x_d)$. Then the *reduction number* $r(R)$ of R is defined to be the minimum of all such $r_{\underline{x}}$. If (R, m) is a Noetherian local ring, then we define the reduction number of R to be $r(R) = r(\text{gr}_m R)$.

Since the a -invariant (or reduction number) is yet another measure of the complexity of a graded ring, the following corollary provides added

evidence for the general notion that a flat extension ring must be at least as “complex” as the base ring.

COROLLARY 3.3. *Let $(R, m) \subseteq (S, n)$ be a flat extension of positively graded rings, generated by 1-forms over a field K . Assume that R and S are Cohen–Macaulay, and that R possesses a system of parameters $x_1, \dots, x_d$ such that each x_i maps to a homogeneous element of positive degree in S . Then $a(R) \leq a(S)$.*

Proof. Assume as before that m is generated by $x_1, \dots, x_d$, where each x_i maps into $n^{t_i} \setminus n^{t_i+1}$. The proof of Lemma 2.2 implies that

$$A_1^{t_1-1} A_2^{t_2-1} \dots A_r^{t_r-1} S^{(N)} \not\subseteq mS^{(N)},$$

where the A_i are commuting matrix roots of the generators x_i of I (as in the proof of Theorem 1.2). Since the matrices all have entries in n , this implies that

$$n^{(\sum t_i)-r} \not\subseteq mS.$$

We know that the highest degree form x of R which is not in I has degree $a(R) + d$. The image of x in S may not be homogeneous, but all components have degree at least $a(R) + d$ in S . Moreover, it follows from the flatness that $n^{(\sum t_i)-r} x \notin IS$. Putting all this together shows that there exists a form $y \in S \setminus IS$ of degree at least $(\sum_1^r t_i) - r + a(R) + d$.

Finally, since S is Cohen–Macaulay and $x_1, \dots, x_d$ is a homogeneous system of parameters, this shows that

$$a(S) \geq \left(\sum_1^r t_i \right) - r + a(R) + d - \left(\sum_1^d t_i \right) = \left(\sum_{d+1}^r t_i \right) - (r - d) + a(R),$$

and thus $a(S) \geq a(R)$ simply because the t_i are all positive. ■

As in the case of Lech’s conjecture, this provides a proof in the graded Cohen–Macaulay case about a statement which would more naturally be made of local rings. However, I think the results presented here are persuasive enough in order to venture the general conjecture on reduction numbers.

CONJECTURE 3.1. *Let $(R, m) \subseteq (S, n)$ be a flat local extension of local rings. Then the reduction number of R is less than or equal to that of S .*

A proof of the conjecture would be of interest in its own right, but would also contribute to continuing efforts to prove Lech’s proposed inequality on the Hilbert–Samuel multiplicities, since rough estimates of one invariant can often be made in terms of the other.

REFERENCES

1. J. Backelin, J. Herzog, and B. Ulrich, Linear maximal Cohen-Macaulay modules over strict complete intersections, *J. Pure Appl. Algebra* **71** (1991), 187–202.
2. B. Herzog, Lech–Hironaka inequalities for flat couples of local rings, *Manuscripta Math.* **68** (1990), 351–371.
3. B. Herzog, Local singularities such that all deformations are tangentially flat, *Trans. Amer. Math. Soc.* **324** (1991), 555–601.
4. H. Hironaka, Certain numerical characters of singularities, *J. Math. Kyoto Univ.* **10** (1970), 151–187.
5. C. Lech, Note on multiplicities of ideals, *Ark. Math.* **4** (1960), 63–86.
6. C. Lech, Inequalities related to certain couples of local rings, *Acta Math.* **112** (1964), 69–89.
7. M. Nagata, The theory of multiplicity in general local rings, in “Proceedings of the International Symposium on Algebraic Number Theory. Tokyo-Nikko, 1955,” pp. 191–226, Science Council of Japan, Tokyo, 1956.
8. K. I. Watanabe, Rational singularities with k^* action, in “Commutative Algebra (Proc. of the Trento Conference),” Lecture Notes in Pure and Applied Mathematics, Vol. 84, pp. 339–351, Dekker, New York/Basel, 1983.