

NEW ESTIMATES OF HILBERT–KUNZ MULTIPLICITIES FOR LOCAL RINGS OF FIXED DIMENSION

IAN M. ABERBACH AND FLORIAN ENESCU

Abstract. We present results on the Watanabe–Yoshida conjecture for the Hilbert–Kunz multiplicity of a local ring of positive characteristic. By improving on a “volume estimate” giving a lower bound for Hilbert–Kunz multiplicity, we obtain the conjecture when the ring has either Hilbert–Samuel multiplicity less than or equal to 5 or dimension less than or equal to 6. For nonregular rings with fixed dimension, a new lower bound for the Hilbert–Kunz multiplicity is obtained.

§1. Introduction

Let (R, \mathfrak{m}, K) be a local ring of positive characteristic p . If I is an ideal in R , then $I^{[q]} = (i^q : i \in I)$, where $q = p^e$ is a power of the characteristic. For an \mathfrak{m} -primary ideal I , one can consider the Hilbert–Samuel multiplicity and the Hilbert–Kunz multiplicity of I with respect to R .

DEFINITION 1.1. Let I be an \mathfrak{m} -primary ideal in (R, \mathfrak{m}) .

1. The *Hilbert–Samuel multiplicity of R at I* is defined by $e(I) = e(I, R) := \lim_{n \rightarrow \infty} d!(\lambda(R/I^n))/n^d$. The limit exists and is positive.
2. The *Hilbert–Kunz multiplicity of R at I* is defined by $e_{HK}(I) = e_{HK}(I, R) := \lim_{q \rightarrow \infty} (\lambda(R/I^{[q]}))/q^d$. Monsky has shown in [10] that this limit exists and is positive.

It is known that for parameter ideals I , one has $e(I) = e_{HK}(I)$. The following sequence of inequalities is also known to hold:

$$\max\left\{1, \frac{1}{d!}e(I)\right\} \leq e_{HK}(I) \leq e(I)$$

for every \mathfrak{m} -primary ideal I .

Received December 31, 2010. Revised April 14, 2012. Accepted August 29, 2012.
First published online August 1, 2013.

2010 Mathematics Subject Classification. Primary 13A35; Secondary 13H15.

Enescu’s work was partially supported by National Security Agency Young Investigator grants H98230-07-1-0034 and H98230-10-1-0166.

We call a local ring R *formally unmixed* if \hat{R} is equidimensional and $\text{Min}(\hat{R}) = \text{Ass}(\hat{R})$ —that is, if $\dim(\hat{R}/P) = \dim(\hat{R})$ for all its minimal primes P —and if all associated primes of \hat{R} are minimal. Nagata [12, p. 82] calls such rings *unmixed*. However, throughout this article a local unmixed ring is a local ring R that is equidimensional, and $\text{Min}(R) = \text{Ass}(R)$. We also examine lower bounds for formally unmixed nonregular local rings R of dimension d and prime characteristic p .

DEFINITION 1.2. For $d \geq 1$, let m_d be the real numbers such that

$$\sec(x) + \tan(x) = 1 + \sum_{d=1}^{\infty} m_d x^d,$$

where $|x| < \pi/2$.

The following conjecture is central to our argument here.

CONJECTURE 1.3 ([20, Conjecture 4.2]). *Let $d \geq 1$, and let $p > 2$. Let $K = \overline{F}_p$, and let*

$$R_{p,d} = \frac{K[[x_0, \dots, x_d]]}{(x_0^2 + \dots + x_d^2)}.$$

Let (R, \mathfrak{m}, K) be a formally unmixed nonregular local ring of dimension d . Then

$$e_{HK}(R) \geq e_{HK}(R_{p,d}) \geq 1 + m_d.$$

REMARK 1.4. The reader should note that the statement $e_{HK}(R_{p,d}) \geq 1 + m_d$ is part of the conjecture.

This is known for $d \leq 6$, due to Yoshida [22, p. 239]. In fact, $e_{HK}(R_{p,5}) = (17p^2 + 12)/(15p^2 + 10) > m_5 = 17/15$, and $e_{HK}(R_{p,6}) = (781p^4 + 656p^2 + 315)/(720p^4 + 570p^2 + 270) > m_6 = 781/720$.

Therefore, the inequality conjectured by Watanabe and Yoshida includes two inequalities: a stronger one,

$$(1.1) \quad e_{HK}(R) \geq e_{HK}(R_{p,d}),$$

and a weaker one,

$$(1.2) \quad e_{HK}(R) \geq 1 + m_d.$$

As far as we know, the inequality $e_{HK}(R_{p,d}) \geq 1 + m_d$ is open for $d \geq 7$.

REMARK 1.5. Monsky and Gessel in [11] (see also [20, Theorem 4.1]) have shown that

$$\lim_{p \rightarrow \infty} e_{HK}(R_{p,d}) = 1 + m_d,$$

for $d \geq 2$.

Watanabe and Yoshida [22, Theorems 3.1, 4.3] have proved this conjecture in dimensions 3 and 4. The cases $d = 1, 2$ are also known.

In higher dimensions, it was not known until recently whether or not for a fixed dimension d there exists a lower bound, say, $C(d) > 1$, such that every local formally unmixed nonregular ring R satisfies $e_{HK}(R) \geq C(d)$. We have shown the existence of such a lower bound in [1, Theorem 4.12].

REMARK 1.6. If R is a complete intersection of dimension $d \geq 1$ and characteristic $p > 2$, then as the second author and Shimomoto proved in [5, Theorem 4.6],

$$e_{HK}(R) \geq e_{HK}(R_{p,d}).$$

In the present paper, we develop techniques which will produce improved estimates for Hilbert–Kunz multiplicities of local rings. In Section 3, we extend an inequality of Watanabe and Yoshida that gives a lower bound for the Hilbert–Kunz multiplicity of a local ring R in terms of a volume function. In Section 4, we apply this inequality to prove the Watanabe–Yoshida conjecture for rings of Hilbert–Samuel multiplicity at most 5. Section 5 provides an asymptotic solution to the above-mentioned conjecture for rings of dimensions 5 and 6. Furthermore, Section 6 sharpens the lower bound for the Hilbert–Kunz multiplicity of a local ring R provided in [1] in all dimensions.

Shortly after this paper was posted to the arXiv (see [arXiv:1101.5078](https://arxiv.org/abs/1101.5078)), Celikbas, Dao, Huneke, and Zhang in [3] posted a manuscript that obtains a lower bound of the Hilbert–Kunz multiplicity of a d -dimensional ring that improves our bound in certain important cases. Their approach starts with an analysis of radical extensions, comparable to Section 6 of the present article; however, it is different from ours and along the way uses new inequalities that are very interesting in their own right.

§2. Notation, terminology, and background

First, we would like to review some definitions and results that will be useful later. Throughout the paper, R will be a Noetherian ring containing

a field of characteristic p , where p is prime. Also, q will denote p^e , a varying power of p .

If I is an ideal in R , then $I^{[q]} = (i^q : i \in I)$, where $q = p^e$ is a power of the characteristic. Let $R^\circ = R \setminus \bigcup P$, where P runs over the set of all minimal primes of R . An element x is said to belong to the *tight closure* of the ideal I if there exists $c \in R^\circ$ such that $cx^q \in I^{[q]}$ for all sufficiently large $q = p^e$. The tight closure of I is denoted by I^* . By a *parameter ideal*, we mean here an ideal generated by a full system of parameters in a local ring R . A tightly closed ideal of R is an ideal I such that $I = I^*$.

Let $F : R \rightarrow R$ be the Frobenius homomorphism $F(r) = r^p$. We denote by F^e the e th iteration of F ; that is, $F^e(r) = r^q$, $F^e : R \rightarrow R$. One can regard R as an R -algebra via the homomorphism F^e . Although as an abelian group it equals R , it has a different scalar multiplication. We will denote this new algebra by $R^{(e)}$.

DEFINITION 2.1. We say that R is *F-finite* if $R^{(1)}$ is module-finite over R or, equivalently (in the case that R is reduced), if $R^{1/p}$ is module-finite over R . Also, R is called *F-pure* if the Frobenius homomorphism is a pure map—that is, if $F \otimes_R M$ is injective for every R -module M .

If R is F-finite, then $R^{1/q}$ is module-finite over R , for every q . Moreover, any quotient and localization of an F-finite ring is F-finite. Any finitely generated algebra over a perfect field is F-finite. An F-finite ring is excellent.

DEFINITION 2.2. A reduced Noetherian F-finite ring R is *strongly F-regular* if for every $c \in R^0$ there exists q such that the R -linear map $R \rightarrow R^{1/q}$ that sends 1 to $c^{1/q}$ splits over R or, equivalently, that $Rc^{1/q} \subset R^{1/q}$ splits over R .

The notion of strong F-regularity localizes well, and all ideals are tightly closed in strongly F-regular rings. Regular rings are strongly F-regular, and strongly F-regular rings are Cohen–Macaulay and normal.

Let $E_R(K)$ denote the injective hull of the residue field of a local ring (R, \mathfrak{m}, K) .

DEFINITION 2.3. A ring R is called *F-rational* if all parameter ideals are tightly closed. A ring R is called *weakly F-regular* if all ideals are tightly closed. The ring R is F-regular if and only if $S^{-1}R$ is weakly F-regular for all multiplicative sets $S \subset R$.

Regular rings are (strongly) F-regular. For Gorenstein rings, the notions of F-rationality and F-regularity coincide (and if, in addition, the ring is excellent, these coincide with strong F-regularity).

Our work here relies on a number of inequalities that involve the Hilbert–Kunz multiplicity obtained in [1] via duality theory, so we will state them all here together.

THEOREM 2.4. *Let (R, \mathfrak{m}, K) be a local ring of dimension d and characteristic p , where p is prime.*

(i) *Assume that R is Cohen–Macaulay of type t . Then*

$$e_{HK}(R) \geq \frac{e(R)}{e(R) - t + 1}.$$

(ii) *Assume that R is Gorenstein of embedding dimension $\nu = \mu(\mathfrak{m})$. If R or \widehat{R} is not F-regular, then*

$$e_{HK}(R) \geq \frac{e(R)}{e(R) - \nu + d}.$$

(iii) *Assume that R is formally unmixed and that $d \geq 2$.*

If

$$e_{HK}(R) < \frac{e(R)}{e(R) - 1},$$

then R is Gorenstein. Also, R and \widehat{R} are F-regular.

(iv) *If R is Cohen–Macaulay and has minimal multiplicity, that is, $\nu = e(R) + d - 1$, then*

$$e_{HK}(R) \geq \frac{e(R)}{2}.$$

Proof. Part (i) is [1, Corollary 3.3]. Part (ii) is [1, Corollary 3.7]. Part (iv) is [1, Corollary 3.4].

For part (iii), by a result of Blickle and the second author (see, e.g., [2, Remark 1.3]), we obtain that R is Cohen–Macaulay. If the type of R is greater than 1, then part (i) above gives a contradiction. So, R is Gorenstein, and then part (ii) finishes the proof, as $\nu \geq d + 1$. \square

§3. Volume estimates for Hilbert–Kunz multiplicity lower bounds

A geometric formula first articulated by Watanabe and Yoshida in [20, Theorem 2.2] gives a great deal of information, especially in small dimension. We give an improved version of their formula here.

For any real number s , set

$$v_s = \text{vol}\left\{(x_1, \dots, x_d) \in [0, 1]^d \mid \sum_{i=1}^d x_i \leq s\right\}.$$

Here vol denotes the Euclidean volume of a subset of \mathbb{R}^d . In fact, an explicit formula for v_s , which is due to Pólya and can be traced to Laplace (see [4, (16), p. 233]), is

$$v_s = \sum_{n=0}^{\lfloor s \rfloor} (-1)^n \frac{(s-n)^d}{n!(d-n)!}.$$

THEOREM 3.1 ([20, Theorem 2.2]). *Let (R, \mathfrak{m}, K) be a formally unmixed local ring of characteristic $p > 0$ and dimension d . Let J be a minimal reduction of \mathfrak{m} , and let r be an integer with $r \geq \mu_R(\mathfrak{m}/J^*)$. Let $s \geq 1$ be a rational number. Then*

$$(3.1) \quad e_{HK}(R) \geq e(R)\{v_s - rv_{s-1}\}.$$

Theorem 3.1 is an improvement over Watanabe and Yoshida's theorem when the maximum volume occurs for a value of $s > 2$. Theorem 3.1 can be made considerably more general.

Fix an ideal J in an analytically unramified local ring (R, \mathfrak{m}) . For an element $x \in R$, set $v_J(x) = \sup\{k \mid x \in J^k\}$. We can then set $f_J(x) = \lim_{n \rightarrow \infty} (v_J(x^n))/n$. By work of Rees [14], the number $f_J(x)$ is rational and is the same for any ideal with the same integral closure as J .

THEOREM 3.2. *Let (R, \mathfrak{m}, K) be a formally unmixed local ring of characteristic $p > 0$ and dimension $d \geq 1$. Let J be a parameter ideal with $e = e(J)$. Fix $I \supseteq J^*$, and let $r = \mu_R(I/J^*)$. Let z_1, \dots, z_r be minimal generators of I modulo J^* , and let $t_i = f_J(z_i)$. For any rational number $s \geq 0$, we have*

$$(3.1) \quad e_{HK}(I) \geq e\left(v_s - \sum_{i=1}^r v_{s-t_i}\right).$$

In order to prove Theorem 3.2, we need the following result (where, for any nonnegative real number α , we define $I^\alpha = I^{\lfloor \alpha \rfloor}$).

LEMMA 3.3 ([18, Lemma 2.3]). *Let (R, \mathfrak{m}, K) be a formally unmixed local ring of characteristic $p > 0$ with $d = \dim R \geq 1$. Let J be a parameter ideal of R . Then for any rational number s with $0 \leq s \leq d$, we have*

$$\lim_{q \rightarrow \infty} \frac{\lambda(R/J^{sq})}{q^d} = \frac{e(J)s^d}{d!} \quad \text{and} \quad \lim_{q \rightarrow \infty} \frac{\lambda(R/(J^{sq} + J^{[q]}))}{q^d} = e(J)v_s.$$

Theorem 3.1 follows from Theorem 3.2 by taking $I = \mathfrak{m}$, J a minimal reduction of \mathfrak{m} , and noting that for any minimal generator of \mathfrak{m} , the valuation is at least 1.

Proof of Theorem 3.2. We can apply [8, Theorem 8.17(a)] to observe that $\lambda((B^*)^{[q]}/B^{[q]}) = O(q^{d-1})$.

Let us note that $I = (z_1, \dots, z_r) + J^*$.

The proof now follows from an examination of the inequality

$$\begin{aligned} \lambda\left(\frac{R}{I^{[q]}}\right) &\geq \lambda\left(\frac{R}{(z_1, \dots, z_r)^{[q]} + J^{sq} + (J^*)^{[q]}}\right) \\ &= \lambda\left(\frac{R}{(z_1, \dots, z_r)^{[q]} + J^{[q]} + J^{sq}}\right) - \lambda\left(\frac{I^{[q]} + (J^*)^{[q]} + J^{sq}}{I^{[q]} + J^{[q]} + J^{sq}}\right) \\ &= \lambda\left(\frac{R}{(z_1, \dots, z_r)^{[q]} + J^{[q]} + J^{sq}}\right) + O(q^{d-1}) \\ &\geq \lambda\left(\frac{R}{J^{sq} + J^{[q]}}\right) \\ &\quad - \left(\sum_{i=0}^{r-1} \lambda\left(\frac{(z_1, \dots, z_{i+1})^{[q]} + J^{sq} + J^{[q]}}{(z_1, \dots, z_i)^{[q]} + J^{sq} + J^{[q]}}\right)\right) + O(q^{d-1}) \\ &\geq \lambda\left(\frac{R}{J^{sq} + J^{[q]}}\right) - \left(\sum_{i=0}^{r-1} \lambda\left(\frac{R}{(J^{sq} + J^{[q]}) : z_{i+1}^q}\right)\right) + O(q^{d-1}). \end{aligned}$$

For $N = 1, 2, \dots$, let $\epsilon_N = 1/p^N$, and choose $q_0 > p^N$ such that for all $q \geq q_0$, we have

$$\left| \frac{v_J(z_{i+1}^q)}{q} - t_{i+1} \right| < \epsilon_N.$$

Fix N . For $q \geq q_0$, we then have $v_J(z_{i+1}^q) \geq \lceil (t_{i+1} - \epsilon_N)q \rceil$, and so $z_{i+1}^q \in J^{\lceil (t_{i+1} - \epsilon_N)q \rceil} = J^{\lceil t_{i+1}q \rceil - \epsilon_N q}$.

It follows that $z_{i+1}^q J^{(s-t_{i+1})q} \subseteq J^{sq - \epsilon_N q}$, and hence that $z_{i+1}^q J^{sq} \subseteq J^{(s - \epsilon_N + t_{i+1})q}$.

Therefore,

$$\lambda\left(\frac{R}{(J^{sq} + J[q]) : z_i^q}\right) \leq \lambda\left(\frac{R}{(J^{(s-t_{i+1}+\epsilon_N)q} + J[q])}\right).$$

So,

$$\lambda\left(\frac{R}{J[q]}\right) \geq \lambda\left(\frac{R}{J^{sq} + J[q]}\right) - \left(\sum_{i=0}^{r-1} \lambda\left(\frac{R}{(J^{(s-t_{i+1}+\epsilon_N)q} + J[q])}\right)\right) + O(q^{d-1}).$$

Dividing each term in the last inequality obtained by q^d , taking limits as $q \rightarrow \infty$, and applying Lemma 3.3 to each term plus the fact that $\lim_{\epsilon \rightarrow 0} v_{s-\epsilon} = v_s$ yields (3.1). \square

REMARK 3.4. This result also extends [20, Fact 2.4].

§4. Lower bounds for rings with small Hilbert–Samuel multiplicity

In this section, we apply Theorem 3.2 to provide lower bounds for the Hilbert–Kunz multiplicity of formally unmixed local rings of Hilbert–Samuel multiplicity less than or equal to 5.

We note that

$$1 + m_3 = \frac{4}{3}, \quad 1 + m_4 = \frac{29}{24}, \quad 1 + m_5 = \frac{17}{15}, \quad 1 + m_6 = \frac{781}{720} = 1.0847.$$

THEOREM 4.1. *Let (R, \mathfrak{m}, K) be a Cohen–Macaulay local ring such that $e(R) = 3$ and such that R is not a complete intersection. Then $e_{HK}(R) \geq 13/8$.*

Proof. We may immediately complete the ring R . Let $d = \dim R$, and let $k = \text{embdim}(R) - \dim(R)$. It is known that $k \leq e - 1 = 2$. Since R is not a complete intersection, then $k > 1$, so R is a ring of minimal multiplicity. By [16, Theorem 1.1], we can write $R = S/I$, where $S = K[[x_1, \dots, x_{d+2}]]$. The same result implies that I is a 3-generated ideal of R and that the Hilbert–Burch theorem applies, so I is the ideal of minors of a 3×2 matrix, say, $[a_{ij}]$, where $a_{ij} \in (x_1, \dots, x_{d+2})S$.

Consider the ring $R_1 = K[[y_{11}, \dots, y_{32}, x_1, \dots, x_{d+2}]]/I_2([y_{ij}])$. Then $\dim R_1 = 4 + d + 2 = d + 6$.

Clearly, $R_1/(y_{ij} - a_{ij} \mid 1 \leq i \leq 3, 1 \leq j \leq 2) \cong R$. Since $\dim R_1 - \dim R = 6$, the equations form a regular sequence, so $e_{HK}(R) \geq e_{HK}(R_1)$, and

$$e_{HK}(R_1) = e_{HK}(K[[y_{11}, \dots, y_{32}]]/I_2([y_{ij}])) = 13/8.$$

(The ring R_1 is isomorphic to the Segre product $S_{2,3}$, and so [6, Theorem 3.3] gives the value $13/8$.) \square

Case of a local ring of Hilbert–Samuel multiplicity 3

Let (R, \mathfrak{m}) be a formally unmixed local ring of multiplicity $e = 3$ and characteristic $p > 2$. We can assume that R is complete and unmixed.

If $e_{HK}(R) < e/(e - 1) = 1.5$, then we have that R is Gorenstein by Theorem 2.4(iii). In this case, by Theorem 4.1, if R is not a complete intersection, then $e_{HK}(R) \geq 13/8$. Otherwise, $e_{HK}(R) \geq e_{HK}(R_{p,d})$ by the second author and Shimomoto in [5, Theorem 4.6]. This shows that the Watanabe–Yoshida conjecture is settled for local rings of multiplicity 3.

Case of a local ring of Hilbert–Samuel multiplicity 4

Let (R, \mathfrak{m}) be a formally unmixed local ring of multiplicity $e = 4$ and characteristic $p > 2$. We can complete, and assume that R is complete and unmixed. Let $k = \text{embdim}(R) - \dim(R)$.

If $e_{HK}(R) < 1 + 1/(4 - 1) = 4/3$, then R is Gorenstein by Theorem 2.4(iii). Since $k \leq e - 1 = 3$, then if R has minimal multiplicity ($k = 3$), $e_{HK}(R) \geq 4/2 = 2$ by Theorem 2.4(iv). If $k = 2$, by considering the minimal free resolution of R over S , we see that R is a complete intersection. The case $k = 1$ also leads to R being a complete intersection. In both cases, $e_{HK}(R) \geq e_{HK}(R_{p,d})$ by [5, Theorem 4.6]. This shows that the Watanabe–Yoshida conjecture is settled for local rings of multiplicity 4.

Case of a local ring of Hilbert–Samuel multiplicity 5

Let (R, \mathfrak{m}) be a formally unmixed local ring of multiplicity $e = 5$ and characteristic $p > 2$. We can complete, and we assume that R is complete and unmixed. Let $d = \dim(R)$.

We can assume that R is Gorenstein if $e_{HK} < 1.25$ by Theorem 2.4(iii).

Let us assume that R is Gorenstein, and set $k = \text{embdim}(R) - \dim(R)$. If $k = e - 1$, then R has minimal multiplicity, and then Theorem 2.4(iv) gives $e_{HK}(R) \geq e/2 = 2.5$. So we can assume that $k \leq e - 2 = 3$. In fact, the cases $k = 1, 2$ both imply that R is a complete intersection. (The case $k = 2$ follows from a theorem of Serre as in [15, Theorem 1.2, p. 69].)

If $k = 3$, then write R as S/I , where $S = K[[x_1, \dots, x_{d+3}]]$ is complete local regular and I is a height 3 Gorenstein ideal with $I \subset \mathfrak{n}^2$, where $\mathfrak{n} = (x_1, \dots, x_{d+3})$. By the Buchsbaum–Eisenbud structure theorem (see [15, Theorem 1.5, p. 72]), the ideal I is given by the set of Pfaffians of a 5×5

antisymmetric matrix with entries in S . The upper right corner has at most 10 nonzero entries denoted a_{ij} , $1 \leq i < j \leq 5$. These elements belong to \mathfrak{n} .

Let $A = (y_{ij})$ be an antisymmetric matrix of indeterminates of size 5×5 , and set

$$R_1 = K[[y_{ij}, x_1, \dots, x_{d+3} : 1 \leq i < j \leq 5]] / (Pf(A)),$$

where $(Pf(A))$ is the ideal generated by the Pfaffians of A .

We note that $\dim(R_1) = 7 + d + 3 = 10 + d$. Also, the elements $y_{ij} - a_{ij}$, $1 \leq i < j \leq 5$ form a regular sequence in R_1 since $R_1 / (y_{ij} - a_{ij}, 1 \leq i < j \leq 5) \simeq R$, and the dimension drops exactly by 10.

Therefore,

$$e_{HK}(R) \geq e_{HK}(R_1) = e_{HK}(K[[y_{ij} : 1 \leq i < j \leq 5]]) / (Pf(A)),$$

and the former is a Gorenstein ring of dimension 7 and multiplicity 5.

So, it remains to examine 7-dimensional Gorenstein rings of multiplicity 5.

Let J be an ideal generated by a system of parameters. Since $\mu(\mathfrak{m}) = d + 3$ and $d = \dim(R)$, we get $3 \geq \mu(\mathfrak{m}/J) \geq \mu(\mathfrak{m}/J^*)$.

Using the notation from Theorem 3.2, we note that $e(v_s - \mu(\mathfrak{m}/J^*)v_{s-1}) \geq e(v_s - 3v_{s-1})$.

Now apply Theorem 3.2 with $e = 5$ and $s = 3.32$, and get $e_{HK}(R) \geq 1.112$. (We used Mathematica to compute the volume functions.)

§5. Watanabe–Yoshida conjecture for rings of dimensions 5 and 6

In this section, we show how to use Theorem 3.2 to prove the Watanabe–Yoshida conjecture in dimensions 5 and 6 for large-enough p .

We note that

$$m_5 = \frac{17}{15}, \quad m_6 = \frac{781}{720} = 1.0847.$$

We need results of Goto and Nakamura [7, Theorems 1.1 and 1.2].

THEOREM 5.1. *Let (R, \mathfrak{m}, K) be a homomorphic image of a Cohen–Macaulay ring. Assume that R is equidimensional.*

Then for every parameter ideal I in R , we have

$$e(I) \geq \lambda(R/I^*).$$

In fact, under the assumption that R is a homomorphic image of a Cohen–Macaulay ring and that $\text{Ass}(R) = \text{Assh}(R)$, if

$$e(I) = \lambda(R/I^*),$$

for some parameter ideal I , then R is Cohen–Macaulay and F -rational.

We can prove the following.

THEOREM 5.2. *Let (R, \mathfrak{m}, K) be a formally unmixed local nonregular ring of dimension d and positive prime characteristic $p > 2$. Then*

(i) *if $d = 5$,*

$$e_{HK}(R) \geq e_{HK}(R_{p,d}) \geq \frac{17}{15} = 1 + m_5;$$

(ii) *if $d = 6$,*

$$e_{HK}(R) \geq e_{HK}(R_{p,d}) \geq \frac{781}{720} = 1 + m_6.$$

Proof. We can complete R and enlarge the residue field of R so that it is infinite. The associativity formula for the Hilbert–Kunz multiplicity shows that, for an unmixed ring R , $e_{HK}(R) < 2$ implies that R is a domain (as in [1, Remark 2.6]). Therefore, we can assume that R is a domain.

Let \underline{x} be a minimal reduction for \mathfrak{m} . Set $J = (\underline{x})$. Note that we are in the case where R is both complete and a domain. Set $e = e(R)$.

We claim that either R has minimal multiplicity or $\mu(\mathfrak{m}/J^*) \leq e - 2$.

If R is not F -rational, then $e(J) > \lambda(R/J^*)$. So, $e = e(J) > 1 + \lambda(\mathfrak{m}/J^*) \geq 1 + \mu(\mathfrak{m}/J^*)$. In other words, $e - 1 > \mu(\mathfrak{m}/J^*)$ or $e - 2 \geq \mu(\mathfrak{m}/J^*)$.

Now let us assume that R is Cohen–Macaulay and F -rational. Then $e = e(J) = \lambda(R/J) = \lambda(R/J^*)$. In conclusion, $\lambda(\mathfrak{m}/J^*) = e - 1$. Since $\mu(\mathfrak{m}/J^*) \leq \lambda(\mathfrak{m}/J^*) \leq e - 1$, we see that $\mu(\mathfrak{m}/J^*) > e - 2$ is possible only when $\mu(\mathfrak{m}/J^*) = \lambda(\mathfrak{m}/J^*)$. Recall that $J^* = J$. So we get $\mu(\mathfrak{m}/J) = \lambda(\mathfrak{m}/J)$. But, $\mu(\mathfrak{m}/J) = \dim(\mathfrak{m}/\mathfrak{m}^2 + J) = \lambda(\mathfrak{m}/\mathfrak{m}^2 + J)$. Hence, $\mu(\mathfrak{m}/J) = \lambda(\mathfrak{m}/J)$ leads to $\mathfrak{m}^2 \subseteq J$. But it is well known that $\mathfrak{m}^2 \subseteq J$ implies that $\mathfrak{m}^2 = \mathfrak{m}J$. This proves that R is of minimal multiplicity by [15, Theorem 3.8, p. 45].

Our claim is now proved. In the minimal multiplicity case, Theorem 2.4(iii) implies that $e_{HK}(R) \geq 1.5 \geq e_{HK}(R_{p,d})$, by Remark 1.4, or that $e = 2$, in which case R is a hypersurface and then $e_{HK}(R) \geq e_{HK}(R_{p,d})$ by [5].

Hence, in the minimal multiplicity case, the Watanabe–Yoshida conjecture is true.

So we have reduced our analysis to the case $\mu(\mathfrak{m}/J^*) \leq e - 2$. Let $r = \mu(\mathfrak{m}/J^*)$.

Theorem 3.2 implies that

$$e_{HK}(R) \geq e \cdot (v_s - r v_{s-1}) \geq e \cdot (v_s - (e - 2)v_{s-1}).$$

In fact, if $e \geq e_0$ and $r_0 \geq e - 2$, then also

$$(5.1) \quad e_{HK}(R) \geq e_0 \cdot (v_s - r_0 v_{s-1}).$$

Let us consider the case $d = 5$.

Let $e = e(R)$. If $e \geq 137$, then $e_{HK}(R) \geq e(R)/d!$ implies that $e_{HK}(R) \geq 137/5! = 137/120 = 1.141(6)$.

Let us assume now that $e \leq 136$. We will apply inequality (3.1) repeatedly by giving values to e_0, r_0 , and s .

In the table below, we list these choices together with the corresponding lower bound obtained for $e_{HK}(R)$.

e	e_0	r_0	s	e_{HK}
$35 \leq e \leq 136$	35	134	1.4	≥ 1.153
$18 \leq e \leq 34$	18	32	1.7	≥ 1.197
$11 \leq e \leq 17$	11	15	1.9	≥ 1.187
$7 \leq e \leq 10$	7	8	2.1	≥ 1.161
$5 \leq e \leq 6$	5	4	2.4	≥ 1.313

Now, let us move to the case $d = 6$.

Again, we may assume that $e \geq 5$. For $e \geq 786$, we obtain $e_{HK} \geq 786/6! = 786/720$.

We will now show that

$$G(e) := e(v_s - (e-2)v_{s-1}) \geq \frac{786}{720}$$

for all $5 \leq e \leq 785$.

Since $G(e) = -v_{s-1}e^2 + (v_2 + 2v_{s-1})e$ is a quadratic function in e , we conclude that, for a fixed s , the maximum value of G is attained at $e = m := (v_s + 2v_{s-1})/(2v_{s-1})$.

This implies that, for $a \leq m \leq b$,

$$(5.2) \quad G(e) \leq \min(G(a), G(b)).$$

The formula for v_s gives the following: $v_s = s^6/6!$, for $0 \leq s < 1$; $v_s = s^6/6! - (s-1)^6/5!$, for $1 \leq s < 2$; and $v_s = s^6/6! - (s-1)^6/5! - (s-2)^6/(2 \cdot 4!)$, for $2 \leq s < 3$.

For $1 \leq s < 2$, we obtain $m = (s^6 - 4(s-1)^6)/(2(s-1)^6)$. For $2 \leq s < 3$, we obtain $m = (s^6 - 4(s-1)^6 + 3(s-2)^6)/(2(s-1)^6 - 6(s-2)^6)$.

If $296 \leq e \leq 786$, then by letting $s = 1.3$ we obtain $m \geq 3308.57 > 786$. This gives that G is increasing on $[286, 786]$, which shows that on this interval $G(e) \geq G(296) > 1.89$ and so $e_{HK} \geq 1.89$.

For the rest of the analysis, as in the preceding paragraph, we will consider intervals $[a, b]$ containing e , give a specific value to s , and then compute the resulting value for m . In each case, m will happen to land in $[a, b]$, and hence inequality (5.2) will apply.

The numbers including those for specific values for G are computed using Mathematica, and we usually present our numbers while keeping the first decimal point only.

$[a, b]$	s	m	$\min(G(a), G(b))$	$e_{HK} \geq$
[59, 296]	1.6	177.7	$G(59)$	1.133
[26, 58]	1.9	42.2	$G(26)$	1.123
[16, 25]	2.1	22.2	$G(16)$	1.118
[10, 25]	2.2	13.3	$G(10)$	1.118
[5, 9]	2.6	7.3	$G(5)$	1.107

□

§6. Root extensions and comparison of Hilbert–Kunz multiplicities

The next theorem we prove allows us to use Theorem 3.2 to obtain lower bounds for Hilbert–Kunz multiplicities that are not available using Theorem 3.1.

We will need to use a result of Watanabe and Yoshida. Let $\mathfrak{ff}(A)$ denote the total ring of fractions of a ring A .

THEOREM 6.1 ([18, Theorem 2.7]). *Let $(R, \mathfrak{m}) \hookrightarrow (S, \mathfrak{n})$ be a module-finite extension of local domains. Then for every \mathfrak{m} -primary ideal I of R , we have*

$$(6.1) \quad e_{HK}(I) = \frac{e_{HK}(IS)}{[\mathfrak{ff}(S) : \mathfrak{ff}(R)]} \cdot [S/\mathfrak{n} : R/\mathfrak{m}].$$

DEFINITION 6.2. Let (R, \mathfrak{m}) be a domain. Let $z \in \mathfrak{m}$, and let n be a positive integer. Let $v \in R^+$ be any root of $f(X) = X^n - z$. We call $S = R[v]$ a *radical extension* for the pair R, z .

It should be remarked that whenever S is radical for R, z , then $b := [\mathfrak{ff}(S) : \mathfrak{ff}(R)] \leq n$. In what follows, \mathfrak{n} will denote the maximal ideal of S .

LEMMA 6.3. *Let (R, \mathfrak{m}, K) be a domain, let $(S = R[v], \mathfrak{n})$ be a radical extension for R , and let $z \in R$. Assume that K is algebraically closed. Let*

$I \subseteq R$ be such that $z \notin I$ and $\mathfrak{m} = (z) + I$. Suppose that $J = (zr) + I_0 \subseteq R$ is an ideal such that $\lambda_R(J/I_0) = 1$ and in S , $vrIS \subseteq I_0S$. (One such possibility is $J = \mathfrak{m} = (z) + I$.) Let $b = [\mathfrak{f}\mathfrak{f}(S) : \mathfrak{f}\mathfrak{f}(R)]$.

Then

$$e_{HK}(I_0, J) \leq \frac{n}{n-1}e_{HK}(R) - \frac{n}{b(n-1)}e_{HK}(S).$$

Proof. Consider the following sequence of inclusions:

$$\mathfrak{m}S \subset (\mathfrak{m}, v^{n-1})S \subset \cdots \subset (\mathfrak{m}, v^2)S \subset (\mathfrak{m}, v)S = \mathfrak{n}.$$

It is easy to see that

$$(\mathfrak{m}, v^j)^{[q]}S : v^{q(j-1)} \subset (\mathfrak{m}, v^{j+1})^{[q]}S : v^{qj},$$

since, if $cv^{q(j-1)} \in (\mathfrak{m}, v^j)^{[q]}S$, then $cv^{qj} \in (\mathfrak{m}, v^j)^{[q]}v^qS \subset (\mathfrak{m}, v^{j+1})^{[q]}S$.

Thus, $e_{HK}(\mathfrak{m}S, \mathfrak{n}) = \sum_{j=1}^{n-1} e_{HK}((\mathfrak{m}, v^{j+1})S, (\mathfrak{m}, v^j)S) \geq (n-1)e_{HK}(\mathfrak{m}S, (\mathfrak{m}, v^{n-1})S)$.

Consider now the filtration

$$I_0S \subseteq (I_0, zrv^{n-1})S \subseteq \cdots \subseteq (I_0, zrv)S \subseteq (I_0, zr)S = JS.$$

Let $s \in (\mathfrak{m}^{[q]}S :_S v^{(n-1)q}) = (v^n, I)^{[q]}S : v^{(n-1)q} = v^qS + I^{[q]}S :_S v^{(n-1)q}$. Then for any $0 \leq j < n$, we have

$$\begin{aligned} s(zrv^j)^q &\in (v^qS + I^{[q]}S :_S v^{(n-1)q})(zrv^j)^q \\ &\subseteq (zrv^{(j+1)})^qS + (I^{[q]}S :_S v^{(n-1)q})(v^{(n-1)q}r^qv^{(j+1)q}) \\ &\subseteq (zrv^{(j+1)})^qS + I^{[q]}r^qv^{(j+1)q}S \subseteq (zrv^{(j+1)}, I_0)^{[q]}S. \end{aligned}$$

Thus, $e_{HK}((I_0, zrv^{j+1})S, (I_0, zrv^j)S) \leq e_{HK}(\mathfrak{m}S, (\mathfrak{m}, v^{n-1})S)$.

Since in the chain we have at most n inclusions, we get, using Theorem 6.1, that $be_{HK}(I_0, J) = e_{HK}(I_0S, (I_0, zr)S) \leq ne_{HK}(\mathfrak{m}S, (\mathfrak{m}, v^{n-1})S) \leq n/(n-1)e_{HK}(\mathfrak{m}S, \mathfrak{n}) = n/(n-1)(be_{HK}(R) - e_{HK}(S))$, which gives

$$e_{HK}(I_0, J) \leq \frac{n}{n-1}e_{HK}(R) - \frac{n}{b(n-1)}e_{HK}(S). \quad \square$$

In what follows, we consider a Gorenstein local domain (R, \mathfrak{m}, K) with algebraically closed residue field. Let us fix some notation. Let $d = \dim(R)$, and consider a system of parameters $\underline{x} = x_1, \dots, x_d$ that generates a minimal reduction of \mathfrak{m} . Also, $k = \text{embdim}(R) - \dim(R)$. We plan to provide a lower

bound greater than 1 for the Hilbert–Kunz multiplicity of R . We also assume that $p \neq 2$. Note that if $k = 2$ and R is Gorenstein, then R is a complete intersection. This is because, after completing, R is the quotient of a regular ring of dimension $d + 2$ and it has projective dimension 2 over the regular ring. The only possible resolution in this case is of a regular sequence over the regular ring.

The main result in [5, Theorem 4.6] gives the conjectured lower bound for $e_{HK}(R)$ if R is a complete intersection. So we will assume that R is not a complete intersection; hence, $k \geq 3$. Moreover, by a result of Sally [17, Corollary 3.2], no Gorenstein rings except hypersurfaces can have minimal multiplicity (i.e., $e(R) = \mu(\mathfrak{m}) - d + 1$), so $e = e(R) \geq k + 2$. In particular, $e \geq 5$.

LEMMA 6.4. *Let (R, \mathfrak{m}, K) be a local Gorenstein ring, let $k = \text{embdim}(R) - \dim(R)$, and let $e = e(R)$. Let $\underline{x} = x_1, \dots, x_d$ be a system of parameters for R .*

- (i) *The $R/(\underline{x})$ -module $((\underline{x}) : \mathfrak{m}^2)/\underline{x}$ is k -generated with 1-dimensional socle.*
- (ii) *Assume that \underline{x} is a minimal reduction for \mathfrak{m} . Then $k = e - 2$ if and only if $(\underline{x}) : \mathfrak{m}^2 = \mathfrak{m}$.*

Proof. For (i), note that $R/(\underline{x})$ is Gorenstein, and hence we can use Matlis duality. The module $((\underline{x}) : \mathfrak{m}^2)/\underline{x}$ is Matlis dual to $R/((\underline{x}) + \mathfrak{m}^2)$. Here $R/((\underline{x}) + \mathfrak{m}^2)$ is cyclic with k -dimensional socle; therefore, $((\underline{x}) : \mathfrak{m}^2)/\underline{x}$ is k -generated with 1-dimensional socle.

To prove part (ii), we recall [17, Proposition 4.2], which says in our case that $k = e - 2$ if and only if $\mathfrak{m}^3 \subset (\underline{x}) \cdot \mathfrak{m}$ and $\lambda(\mathfrak{m}^2/(\underline{x}) \cdot \mathfrak{m}) = 1$. Hence, one direction of (ii) follows at once. Now assume that $\mathfrak{m}^3 \subset (\underline{x})$. Note that

$$(\underline{x}) \subseteq \mathfrak{m}(\underline{x} : \mathfrak{m}^2) + (\underline{x}) \subseteq (\underline{x}) : \mathfrak{m} \subset (\underline{x} : \mathfrak{m}^2),$$

and since R is Gorenstein, we must have $\mathfrak{m}(\underline{x} : \mathfrak{m}^2) + (\underline{x}) = (\underline{x}) : \mathfrak{m}$.

Therefore, $\mathfrak{m} \cdot ((\underline{x}) : \mathfrak{m}^2)/\underline{x} = ((\underline{x}) : \mathfrak{m})/\underline{x}$, and this shows that

$$k = \mu\left(\frac{(\underline{x}) : \mathfrak{m}^2}{(\underline{x})}\right) = \dim_K\left(\frac{(\underline{x}) : \mathfrak{m}^2}{(\underline{x}) : \mathfrak{m}}\right) = \dim_K\left(\frac{\mathfrak{m}}{(\underline{x}) : \mathfrak{m}}\right) = \lambda\left(\frac{\mathfrak{m}}{(\underline{x}) : \mathfrak{m}}\right) = e - 2,$$

because $\lambda(R/\underline{x}) = e$ (\underline{x} forms a minimal reduction for \mathfrak{m}). \square

Let (R, \mathfrak{m}, K) be a local ring with infinite residue field and of dimension d . According to a result due to Northcott and Rees (see [15]) and, independently, to Trung (see [9, Theorem 8.6.6]), there exists a Zariski-open subset

U of $(\mathfrak{m}/\mathfrak{m}^2)^d$ such that any x_1, \dots, x_d with $(x_1 + \mathfrak{m}^2, \dots, x_d + \mathfrak{m}^2) \in U$ forms a minimal reduction for \mathfrak{m} . We will call a set U with this property *reduction-open*.

LEMMA 6.5. *Let (R, \mathfrak{m}, K) be a local Gorenstein ring containing an infinite field of positive prime characteristic $p > 2$. Assume that $k = \text{embdim}(R) - \dim(R) \geq 2$. Let U be a reduction-open subset of $(\mathfrak{m}/\mathfrak{m}^2)^d$. Let \underline{x} be in \mathfrak{m} such that $(x_1 + \mathfrak{m}^2, \dots, x_d + \mathfrak{m}^2) \in U$.*

Then, we may pick minimal generators z_1, \dots, z_k for $((\underline{x}) : \mathfrak{m}^2)/\underline{x}$ and a minimal generator z of \mathfrak{m} such that $zz_i \notin (\underline{x})$ for $1 \leq i \leq k$ and z, x_2, \dots, x_d form a minimal reduction of \mathfrak{m} .

If $k \neq e - 2$, then z can be picked not in $(\underline{x}) : \mathfrak{m}^2$. If $k = e - 2$, one may take $z = z_1$.

Proof. Clearly,

$$(\underline{x}) \subseteq \mathfrak{m}(\underline{x} : \mathfrak{m}^2) + (\underline{x}) \subseteq (\underline{x}) : \mathfrak{m} \subseteq (\underline{x} : \mathfrak{m}^2),$$

and since R is Gorenstein, we must have $\mathfrak{m}(\underline{x} : \mathfrak{m}^2) + (\underline{x}) = (\underline{x}) : \mathfrak{m}$. This is the case because $(\underline{x}) = \mathfrak{m}(\underline{x} : \mathfrak{m}^2) + (\underline{x})$ gives $\mathfrak{m}(\underline{x} : \mathfrak{m}^2) \subseteq (\underline{x})$ or $(\underline{x} : \mathfrak{m}^2) = (\underline{x}) : \mathfrak{m}$, which contradicts the fact that $k \geq 2$.

Choose z_1, \dots, z_k in R such that their images form a minimal set of generators for $((\underline{x}) : \mathfrak{m}^2)/\underline{x}$. We conclude that each $z_i \notin \mathfrak{m}(\underline{x} : \mathfrak{m}^2) + (\underline{x})$, and so $z_i \notin (\underline{x}) : \mathfrak{m}$, $i = 1, \dots, k$. Note that $z_i \in (\underline{x}) : \mathfrak{m}^2$, and hence $\mathfrak{m}^2 \subset (\underline{x}) : z_i$ for all $i = 1, \dots, k$.

Let $U_1 = \{z + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2 : (z + \mathfrak{m}^2, x_2 + \mathfrak{m}^2, \dots, x_d + \mathfrak{m}^2) \in U\}$. Then U_1 is a Zariski-open subset of $\mathfrak{m}/\mathfrak{m}^2$. In what follows, for $a \in R$, \bar{a} will denote the class of the element $a \in R$ modulo \mathfrak{m}^2 ; \hat{a} will denote the class of a in R/\mathfrak{m} ; and \tilde{a} will denote the class of a in $R/(\underline{x})$.

Then

$$U_1 \not\subseteq \bigcup_i ((\underline{x}) : z_i)/\mathfrak{m}^2,$$

since otherwise there exists i such that $U_1 \subseteq ((\underline{x}) : z_i)/\mathfrak{m}^2$, which gives $\mathfrak{m} \subseteq ((\underline{x}) : z_i)$ or $z_i \in (\underline{x}) : \mathfrak{m}$, which is not the case. (Over an infinite field, a dense Zariski-open subset cannot be covered by a finite union of proper vector subspaces because of dimension reasons.)

Note that $(\underline{x} : \mathfrak{m}^2) + \mathfrak{m}^2 = \mathfrak{m}$ implies by Nakayama's lemma that $(\underline{x} : \mathfrak{m}^2) = \mathfrak{m}$. So, a similar argument shows that when $\mathfrak{m} \neq (\underline{x} : \mathfrak{m}^2)$, one has

$$U_1 \not\subseteq \bigcup_i ((\underline{x}) : z_i)/\mathfrak{m}^2 \cup ((\underline{x} : \mathfrak{m}^2) + \mathfrak{m}^2)/\mathfrak{m}^2.$$

This guarantees that, in either case, one can pick z a minimal generator of \mathfrak{m} such that $zz_i \notin (\underline{x})$ for $1 \leq i \leq k$ and that $z \notin (\underline{x}) : \mathfrak{m}^2$, whenever $\mathfrak{m} \neq (\underline{x}) : \mathfrak{m}^2$.

Let us note that $k = e - 2$ is equivalent to $(\underline{x}) : \mathfrak{m}^2 = \mathfrak{m}$ by Lemma 6.4.

Whenever $(\underline{x}) : \mathfrak{m}^2 = \mathfrak{m}$, we know that no z_i can kill all z_j modulo \underline{x} . So for all i, j , there exists $r_{ij} \in R$ such that $\tilde{z}_i \tilde{z}_j = r_{ij} \tilde{u}$, where u gives the socle generator of $R/(\underline{x})$. Here, each r_{ij} is an element in R , and for each i there exists j such that \hat{r}_{ij} in R/\mathfrak{m} is nonzero. After renumbering, we can assume that $\hat{r}_{12} \neq 0$. Since R contains an infinite field we have that K is infinite as well. Let $z'_1 = z_1 + yz_2$, where $y \in R$. Let C be the set $\{\bar{z}_1 + \bar{y} \cdot \bar{z}_2, y \in R\}$ in $\mathfrak{m}/\mathfrak{m}^2$. This is a line in the $(k + d)$ -dimensional space $\mathfrak{m}/\mathfrak{m}^2$.

Let $z'_j = z_j + yz'_1 = z_j + yz_1 + y^2z_2$ for all $j \geq 2$.

We will find $y \in R$ such that $z_1'^2 \notin (\underline{x})$ and for all $j \geq 2$, $z_1'z'_j \notin (\underline{x})$ and $\bar{z}'_1 \in U_1$.

Computing $\tilde{z}'_1{}^2 = (\hat{r}_{11}^2 + 2\hat{r}_{12}\hat{y} + \hat{r}_{22}\hat{y}^2)\tilde{u}$ and $\tilde{z}'_1\tilde{z}'_j = [\hat{r}_{1j} + (\hat{r}_{2j} + \hat{r}_{11})\hat{y} + 2\hat{r}_{12}\hat{y}^2 + \hat{r}_{22}\hat{y}^3]\tilde{u}$, $j = 2, \dots, k$ gives k polynomial functions in $\hat{y} \in K$. Each polynomial is not identically zero because $2\hat{r}_{12} \neq 0$. Let $U = \{\hat{y} \in R/\mathfrak{m} = K : \tilde{z}'_1{}^2 \neq 0, \tilde{z}'_1\tilde{z}'_j \neq 0, \forall j = 2, \dots, k\}$. This is an open nonempty subset of K . For any choice of $y \in R$ such that $\hat{y} \in U$, we have $z_1'^2 \notin (\underline{x})$ and, for all $j \geq 2$, we have $z_1'z'_j \notin (\underline{x})$.

Note that $C \cap U_1$ is an open subset in C . Since C is isomorphic to K , we have a open subset of K , say, U' , such that, for all $y \in R$ such that $\hat{y} \in U'$, $\bar{z}_1 + \bar{y} \cdot \bar{z}_2$ belongs to U_1 . Now, since K is infinite, U' and U must intersect, so we can choose $y \in R$ such that $\hat{y} \in U \cap U'$.

To finish the argument here, it is enough to note that now we can swap z_1 for z'_1 and z'_j for z_j corresponding to our choice for y , and the conditions are now satisfied. \square

From now on, let us fix $z_1, \dots, z_k \in R$ chosen as in Lemma 6.5.

Thus, modulo (\underline{x}) , each zz_i , $i = 1, \dots, k$ generates the socle of $R/(\underline{x})$.

Let us denote $J_i = (z_i, \dots, z_k, \underline{x})$, for all $i = 1, \dots, k$.

Let u in R be an element that generates the socle of $R/(\underline{x})$. Denote $J = (\underline{x}, u)$. Note that according to our remark on the elements zz_i , $J = (I, zz_i)$ for $i = 1, \dots, k$.

Denote $L_i = (\underline{x}, z_i)$, and denote $B_i = (\underline{x}) : L_i$. Note that $L_k = J_k$. Since $z_i \in (\underline{x}) : \mathfrak{m}^2 - (\underline{x}) : \mathfrak{m}$, the chain $(\underline{x}, z_i) \supseteq (\underline{x}, u) \supseteq (\underline{x})$ is saturated; that is,

$\lambda(L_i/(\underline{x})) = 2$. So by duality, $\lambda(R/B_i) = 2$. Since $zz_i \notin (\underline{x})$, the chain $R \supseteq (z, B_i) = \mathfrak{m} \supseteq B_i$ is saturated.

For any $q = p^e$, let $G_q = (\underline{x}^{[q]} : \mathfrak{m}^{[q]})$. Note that $J^{[q]} \subset G_q$.

Consider a radical extension for R and z , $S = R[v]$, such that $v^n = z$. Since R is Henselian and $z \in \mathfrak{m}$, S is local. Set $b = [\text{ff}(S) : \text{ff}(R)] (\leq n)$. Denote $e_{HK}(R) = 1 + \epsilon_R$, $e_{HK}(S) = 1 + \epsilon_S$. In what follows, we will make a sequence of claims that will lead to our main result.

CLAIM 1. *We have*

$$e_{HK}(B_i, \mathfrak{m}) \leq n/(n-1)e_{HK}(R) - 1/(b(n-1))e_{HK}(S).$$

From our observations above about R/B_i , we can apply Lemma 6.3 with $I = B_i$ and $J = \mathfrak{m}$ to get $e_{HK}(B_i, \mathfrak{m}) \leq n/(n-1)e_{HK}(R) - n/(b(n-1))e_{HK}(S)$.

CLAIM 2. *We have*

$$\lim_{q \rightarrow \infty} \frac{1}{q^d} \lambda(G_q/J^{[q]}) = e_{HK}(R) - e_{HK}((\underline{x}), J).$$

We observe that $R/(\underline{x})^{[q]}$ is Gorenstein Artinian.

So, by duality, $\lambda(R/(\underline{x})^{[q]}) = \lambda(\text{Hom}_R(R/L^{[q]}, R/(\underline{x})^{[q]}) = \lambda((\underline{x})^{[q]} : L^{[q]})/(\underline{x})^{[q]}$, for any \mathfrak{m} -primary ideal L in R .

Let $L = \mathfrak{m}$, and we obtain $\lambda(G_q/(\underline{x})^{[q]}) = \lambda(R/\mathfrak{m}^{[q]})$, so $\lambda(R/G_q) = \lambda(R/(\underline{x})^{[q]}) - \lambda(R/\mathfrak{m}^{[q]})$, which is the same as

$$\lambda(G_q/J^{[q]}) = \lambda(R/\mathfrak{m}^{[q]}) - (\lambda(R/(\underline{x})^{[q]}) - \lambda(R/J^{[q]})).$$

Dividing by q^d and taking the limit as $q \rightarrow \infty$ give the claim.

CLAIM 3. *We have*

$$\lambda(G_q/J^{[q]}) \geq \lambda\left(\frac{\sum_{i=1}^k (L_i^{[q]} \cap G_q)}{J^{[q]}}\right).$$

This is immediate since $\sum_{i=1}^k (L_i^{[q]} \cap G_q) \subset G_q$.

Now, we need to introduce further notation. For $i = 1, \dots, k-1$, we let

$$N_{i,q} = \frac{L_i^{[q]} \cap G_q}{J^{[q]}}$$

and put

$$a_i := \limsup \frac{1}{q^d} \lambda \left(\frac{(L_i^{[q]} \cap G_q) \cap \sum_{j=i+1}^k (L_j^{[q]} \cap G_q)}{J^{[q]}} \right),$$

so

$$a_i = \limsup \frac{1}{q^d} \lambda \left(N_{i,q} \cap \sum_{j=i+1}^k N_{j,q} \right).$$

We set $a_k = 0$.

CLAIM 4. *For any $i_0 \in \{1, \dots, k-1\}$,*

$$\lambda \left(\sum_{i=i_0}^k N_{i,q} \right) = \sum_{i=i_0}^k \lambda(N_{i,q}) - \sum_{i=i_0}^{k-1} \lambda \left(N_{i,q} \cap \sum_{j=i+1}^k N_{j,q} \right).$$

Write the following exact sequence

$$0 \rightarrow N_{i,q} \cap \sum_{j=i+1}^k N_{j,q} \rightarrow N_{i,q} \oplus \sum_{j=i+1}^k N_{j,q} \rightarrow \sum_{j=i}^k N_{j,q} \rightarrow 0,$$

and now start with $i = i_0$, and recursively one gets the claim.

CLAIM 5. *We have*

$$\lambda(N_{i,q}) \geq \lambda \left(\frac{L_i^{[q]}}{J^{[q]}} \right) - \lambda \left(\frac{\mathfrak{m}^{[q]}}{B_i^{[q]}} \right).$$

From the short exact sequence

$$0 \rightarrow N_{i,q} \rightarrow \frac{L_i^{[q]}}{J^{[q]}} \rightarrow \frac{L_i^{[q]}}{L_i^{[q]} \cap G_q} \rightarrow 0$$

we see that $\lambda(L_i^{[q]}/J^{[q]}) = \lambda(N_{i,q}) + \lambda(L_i^{[q]}/(L_i^{[q]} \cap G_q))$.

But

$$\lambda \left(\frac{L_i^{[q]}}{L_i^{[q]} \cap G_q} \right) = \lambda \left(\frac{L_i^{[q]} + G_q}{G_q} \right) \leq \lambda \left(\frac{(\underline{x})^{[q]} : B_i^{[q]}}{G_q} \right) = \lambda \left(\frac{\mathfrak{m}^{[q]}}{B_i^{[q]}} \right).$$

Hence,

$$\lambda(N_{i,q}) = \lambda \left(\frac{L_i^{[q]}}{J^{[q]}} \right) - \lambda \left(\frac{L_i^{[q]}}{L_i^{[q]} \cap G_q} \right) \geq \lambda \left(\frac{L_i^{[q]}}{J^{[q]}} \right) - \lambda \left(\frac{\mathfrak{m}^{[q]}}{B_i^{[q]}} \right).$$

CLAIM 6. *We have*

$$\lambda\left(\frac{L_i^{[q]}}{J^{[q]}}\right) = \lambda\left(\frac{J_i^{[q]}}{J_{i+1}^{[q]}}\right) + \lambda\left(\frac{L_i^{[q]} \cap J_{i+1}^{[q]}}{J^{[q]}}\right).$$

For all $i = 1, \dots, k-1$, $L_i^{[q]} + J_{i+1}^{[q]} = J_i^{[q]}$, so

$$\frac{L_i^{[q]}}{J^{[q]}} / \frac{L_i^{[q]} \cap J_{i+1}^{[q]}}{J^{[q]}} \simeq \frac{J_i^{[q]}}{J_{i+1}^{[q]}}$$

and this gives the claim.

CLAIM 7. *We have*

$$\lambda\left(\frac{L_i^{[q]} \cap G_q \cap (\sum_{j=i+1}^k L_j^{[q]} \cap G_q)}{J^{[q]}}\right) \leq \lambda\left(\frac{L_i^{[q]} \cap J_{i+1}^{[q]}}{J^{[q]}}\right).$$

This follows immediately as $L_i^{[q]} \cap G_q \cap (\sum_{j=i+1}^k L_j^{[q]} \cap G_q) \subset L_i^{[q]} \cap J_{i+1}^{[q]}$, since $L_j \subseteq J_{i+1}$ for all $j \geq i+1$.

THEOREM 6.6. *Let (R, \mathfrak{m}) be a local Gorenstein ring. Let \underline{x} be a minimal reduction generated by a system of parameters, and let $z \in \mathfrak{m} \setminus (\underline{x})$ be a minimal generator of \mathfrak{m} picked as described above.*

Let $S = R[v]$ be a radical extension of degree n for R and z , and let z be of degree n . Let $b = [\text{ff}(S) : \text{ff}(R)]$. Then

$$e_{HK}(R) \geq \begin{cases} \frac{e(n-1)}{en-2} + \frac{n(e-2)}{b(en-2)} e_{HK}(S) & \text{if } k = e-2, \\ \frac{e(n-1)}{(n-1)e+k+1} + \frac{n(k+1)}{b((n-1)e+k+1)} e_{HK}(S) & \text{if } k < e-2. \end{cases}$$

For $n = b = 2$, the first case gives

$$e_{HK}(R) \geq \frac{e}{2(e-1)} + \frac{e-2}{2(e-1)} e_{HK}(S),$$

and the second case gives

$$e_{HK}(R) \geq \frac{e}{e+k+1} + \frac{k+1}{e+k+1} e_{HK}(S).$$

Proof. We will keep the notation introduced above and make references to the claims just proved.

We see that $\lambda(G_q/J^{[q]}) \geq \lambda(\sum_{j=1}^k N_{j,q})$, and by Claims 4 and 5, we get

$$\begin{aligned} \lambda\left(\frac{G_q}{J^{[q]}}\right) &\geq \sum_{i=1}^k \lambda(N_{i,q}) - \sum_{i=1}^{k-1} \lambda\left(N_{i,q} \cap \sum_{j=i+1}^k N_{j,q}\right) \\ &\geq \sum_{i=1}^k \left(\lambda\left(\frac{L_i^{[q]}}{J^{[q]}}\right) - \lambda\left(\frac{\mathfrak{m}^{[q]}}{B_i^{[q]}}\right)\right) - \sum_{i=1}^{k-1} \lambda\left(N_{i,q} \cap \sum_{j=i+1}^k N_{j,q}\right), \end{aligned}$$

which by Claim 7 leads to

$$\lambda\left(\frac{G_q}{J^{[q]}}\right) \geq \sum_{i=1}^k \lambda\left(\frac{L_i^{[q]}}{J^{[q]}}\right) - \sum_{i=1}^{k-1} \lambda\left(\frac{L_i^{[q]} \cap J_{i+1}^{[q]}}{J^{[q]}}\right) - \sum_{i=1}^k \lambda\left(\frac{\mathfrak{m}^{[q]}}{B_i^{[q]}}\right).$$

Now using Claim 6 this last term can be bounded below by

$$\sum_{i=1}^{k-1} \lambda\left(\frac{J_i^{[q]}}{J_{i+1}^{[q]}}\right) - \sum_{i=1}^k \lambda\left(\frac{\mathfrak{m}^{[q]}}{B_i^{[q]}}\right) + \lambda\left(\frac{L_k^{[q]}}{J^{[q]}}\right).$$

But $L_k = J_k$, so we get

$$\lambda\left(\frac{G_q}{J^{[q]}}\right) \geq \sum_{i=1}^{k-1} \lambda\left(\frac{J_i^{[q]}}{J_{i+1}^{[q]}}\right) - \sum_{i=1}^k \lambda\left(\frac{\mathfrak{m}^{[q]}}{B_i^{[q]}}\right) + \lambda\left(\frac{J_k^{[q]}}{J^{[q]}}\right).$$

Dividing by q^d and taking the limits lead to

$$\frac{1}{q^d} \lim_{q \rightarrow \infty} \lambda\left(\frac{G_q}{J^{[q]}}\right) \geq \sum_{i=1}^{k-1} e_{HK}(J_{i+1}, J_i) - \sum_{i=1}^k e_{HK}(B_i, \mathfrak{m}) + e_{HK}(J, J_k).$$

Consider the filtration

$$(\underline{x}) \subseteq J \subseteq J_k \subseteq \cdots \subseteq J_2 \subseteq J_1 \subseteq \mathfrak{m}.$$

So, $e_{HK}((\underline{x})) - e_{HK}(R) = e_{HK}((\underline{x}), J) + e_{HK}(J, J_k) + \sum_{i=1}^{k-1} e_{HK}(J_{i+1}, J_i) + e_{HK}(J_1, \mathfrak{m})$.

We have $e_{HK}((\underline{x})) = e$ and $\lim_{q \rightarrow \infty} 1/q^d \lambda(G_q/J^{[q]}) = e_{HK}(R) - e_{HK}((\underline{x}), J)$ as shown in Claim 2, so $e - 2e_{HK}(R) + \lim_{q \rightarrow \infty} 1/q^d \lambda(G_q/J^{[q]}) = e - 2e_{HK}(R) + e_{HK}(R) - e_{HK}((\underline{x}), J) = e_{HK}(J, J_k) + \sum_{i=1}^{k-1} e_{HK}(J_{i+1}, J_i) + e_{HK}(J_1, \mathfrak{m})$.

But,

$$\frac{1}{q^d} \lim_{q \rightarrow \infty} \lambda\left(\frac{G_q}{J[q]}\right) \geq \sum_{i=1}^{k-1} e_{HK}(J_{i+1}, J_i) - \sum_{i=1}^k e_{HK}(B_i, \mathfrak{m}) + e_{HK}(J, J_k),$$

which says that $e - 2e_{HK}(R) + \sum_{i=1}^{k-1} e_{HK}(J_{i+1}, J_i) - \sum_{i=1}^k e_{HK}(B_i, \mathfrak{m}) + e_{HK}(J, J_k) \leq e_{HK}(J, J_k) + \sum_{i=1}^{k-1} e_{HK}(J_{i+1}, J_i) + e_{HK}(J_1, \mathfrak{m})$.

By canceling out the common terms, we see that $e \leq \sum_{i=1}^k e_{HK}(B_i, \mathfrak{m}) + e_{HK}(J_1, \mathfrak{m}) + 2e_{HK}(R)$.

But $e_{HK}(J_1, \mathfrak{m}) = e_{HK}(J_1) - e_{HK}(R)$.

We have also proved earlier that $e_{HK}(B_i, \mathfrak{m}) \leq n/(n-1)e_{HK}(R) - n/(b(n-1))e_{HK}(S)$.

So,

$$e \leq k\left(\frac{n}{n-1}e_{HK}(R) - \frac{n}{b(n-1)}e_{HK}(S)\right) + e_{HK}(J_1) + e_{HK}(R),$$

which can be rearranged as

$$e \leq k\left(\frac{n}{n-1}e_{HK}(R) - \frac{n}{b(n-1)}e_{HK}(S)\right) + e_{HK}(J_1, \mathfrak{m}) + 2e_{HK}(R).$$

If $k = e - 2$, then $J_1 = \mathfrak{m}$, so $e_{HK}(J_1, \mathfrak{m}) = 0$. A small amount of algebra gives the desired conclusion.

Assume that $k < e - 2$. Then according to the setup for this case, we have $J_1 \subsetneq \mathfrak{m}$, $z \notin J_1$, and z is a part of a minimal generating set for \mathfrak{m} . Call this generating set z, y_2, \dots, y_h with $h = k + d$. Then $\mathfrak{m} = (z, y_2, \dots, y_h) + \mathfrak{m}^2$.

So we may pick an ideal $J_0 = (y_2, \dots, y_h) + \mathfrak{m}^2$ such that $J_1 \subseteq J_0 \subseteq J_0 + (z) = \mathfrak{m}$, where $\lambda(\mathfrak{m}/J_0) = 1$. By Lemma 6.3, $e_{HK}(J_0, \mathfrak{m}) \leq n/(n-1)e_{HK}(R) - n/(b(n-1))e_{HK}(S)$. Also, $\lambda(J_0/J_1) = e - k - 3$, so $e_{HK}(J_1, J_0) \leq (e - k - 3)e_{HK}(R)$. Putting this information into our inequality now yields

$$e \leq (k+1)\left(\frac{n}{n-1}e_{HK}(R) - \frac{n}{b(n-1)}e_{HK}(S)\right) + (e - k - 1)e_{HK}(R),$$

and some algebra yields our other case. □

Lower bounds for the Hilbert–Kunz multiplicity of a Gorenstein F-regular ring

We now begin a construction that will yield a lower bound for Gorenstein, F-regular, nonregular local rings. So assume that (R, \mathfrak{m}) is an F-regular local

ring of multiplicity $e = e(R) > 1$ and characteristic $p > 2$. By the results in Section 4, we may actually assume that $e \geq 6$. Note that R must be a normal domain. We may complete and extend the residue field to assume that it is algebraically closed. Let $d = \dim R$, and let $k = \mu(\mathfrak{m}) - d$. Let $\mathbf{x} = x_1, \dots, x_d$ be a minimal reduction of \mathfrak{m} , so that $\lambda(R/(\mathbf{x})) = e$. We now inductively choose $w_1, \dots, w_d \in \mathfrak{m}$ such that, for each $i = 1, \dots, d$,

- (a) the set $w_1, \dots, w_i, x_{i+1}, \dots, x_d$ is a minimal reduction for \mathfrak{m} ;
- (b) there is a set A_i of minimal generators of $(w_1, \dots, w_i, x_{i+1}, \dots, x_d) : \mathfrak{m}^2$ (modulo $(w_1, \dots, w_i, x_{i+1}, \dots, x_d)$) such that $w_{i+1}z \notin (w_1, \dots, w_i, x_{i+1}, \dots, x_d)$ for $z \in A_i$, if $k < e - 2$, $w_{i+1} \notin (w_1, \dots, w_i, x_{i+1}, \dots, x_d) : \mathfrak{m}^2$; and
- (c) if $k = e - 2$, w_{i+1} belongs to A_i ; such a choice is due to Lemma 6.5.

For convenience, we let $\mathbf{w}_i = w_1, \dots, w_i$ and $\mathbf{x}_{i+1} = x_{i+1}, \dots, x_d$.

Now, fix n , and let $v_i = w_i^{1/n}$ be an n th root in R^+ for $1 \leq i \leq n$. As above, let $\mathbf{v}_i = v_1, \dots, v_i$. Set $R_0 = R$, and for $i \geq 1$, set $R_i = R[v_1, \dots, v_i] = R_{i-1}[v_i]$. Each ring is Henselian, so adjoining v_i yields another local ring. Moreover, all the residue fields are the same. If we assume that R_i is normal (e.g., if R_i is F-regular), then $R_{i+1} \cong R_i[X]/(X^n - w_{i+1})$, so R_{i+1} is free of rank n over R_i . (Since R_i is normal, the minimal polynomial of v_{i+1} over $\text{ff}(R_i)$ has coefficients in R_i and hence divides $X^n - w_{i+1}$. If it properly divides, then an interpretation of the product of the constant terms involved will give $w_{i+1} \in (\mathbf{w}_i) + \mathfrak{m}^2 \subseteq R$, meaning that w_{i+1} is not a minimal generator of \mathfrak{m} .) Thus, in the context of Theorem 6.6, applied to $R_i \rightarrow R_{i+1}$, we have $n = b = [\text{ff}(R_{i+1}), \text{ff}(R_i)]$.

Let $t = \max\{i \mid R_i \text{ is normal}\}$. For $1 \leq i \leq t$, let $\phi_i : R_0/(\mathbf{w}_i, \mathbf{x}_{i+1}) \twoheadrightarrow R_i/(\mathbf{v}_i, \mathbf{x}_{i+1})$. We have that each ϕ_i is an isomorphism. In particular, $e(R_i) = e$, for all $i \leq t$; also, for $i \leq t$, R_i is Gorenstein.

If we now write $\mathfrak{m}_{R_0} = (\mathbf{w}_i, \mathbf{x}_{i+1}) + J_i$, where $\mu(J_i) = \mu(\mathfrak{m}_{R_0}) - d$ and where w_{i+1} is a minimal generator of J_i , we have $(\mathbf{w}_i, \mathbf{x}_{i+1}) : \mathfrak{m}_{R_0}^2 = (\mathbf{w}_i, \mathbf{x}_{i+1}) : J_i^2$. Note that $\mathfrak{m}_{R_i} = (\mathbf{v}_i, \mathbf{x}_{i+1}) + J_i$ (minimally). The isomorphism ϕ_i now gives

$$\begin{aligned} \frac{(\mathbf{v}_i, \mathbf{x}_{i+1}) :_{R_i} \mathfrak{m}_{R_i}^2}{(\mathbf{v}_i, \mathbf{x}_{i+1})} &= \frac{((\mathbf{w}_i, \mathbf{x}_{i+1}) :_{R_0} J_i^2)R_i + (\mathbf{v}_i, \mathbf{x}_{i+1})}{(\mathbf{v}_i, \mathbf{x}_{i+1})} \\ &= \frac{((\mathbf{w}_i, \mathbf{x}_{i+1}) :_{R_0} \mathfrak{m}_{R_0}^2)R_i + (\mathbf{v}_i, \mathbf{x}_{i+1})}{(\mathbf{v}_i, \mathbf{x}_{i+1})}. \end{aligned}$$

Since $R'_0 = R_0/(\mathbf{w}_i, \mathbf{x}_{i+1}) \rightarrow R'_i = R_i/(\mathbf{v}_i, \mathbf{x}_{i+1})$ is an isomorphism of R_0 -algebras, we note that, because the images of J_i are minimal generators in the domain, they must be minimal generators in the codomain as well. Moreover, $\text{Ann}_{R'_0}(\mathfrak{m}_0^2)$ maps to $\text{Ann}_{R'_i}(\mathfrak{m}_i^2)$ under the mentioned isomorphism, so the minimal set of generators A_i is a set of generators for

$$\frac{(\mathbf{v}_i, \mathbf{x}_{i+1}) :_{R_i} \mathfrak{m}_{R_i}^2}{(\mathbf{v}_i, \mathbf{x}_{i+1})},$$

and $w_{i+1}z \notin (\mathbf{v}_i, \mathbf{x}_{i+1})$ for $z \in A_i$ because $(\mathbf{v}_i, \mathbf{x}_{i+1}) \cap R_0 = (\mathbf{w}_i, \mathbf{x}_{i+1})$.

Moreover, $\mathbf{w}_i, \mathbf{x}_{i+1}$ form a minimal reduction for \mathfrak{m}_{R_0} ; hence, $\mathbf{v}_i, \mathbf{x}_{i+1}$ form a minimal reduction for \mathfrak{m}_{R_i} . We also need that $v_1, \dots, v_i, w_{i+1}, x_{i+2}, \dots, x_d$ form a minimal reduction of \mathfrak{m}_{R_i} .

When $k < e - 2$, $w_{i+1} \notin (\mathbf{w}_i, \mathbf{x}_{i+1}) : \mathfrak{m}_{R_0}^2$. Since $\text{Ann}_{R'_0}(\mathfrak{m}_0^2)$ maps to $\text{Ann}_{R'_i}(\mathfrak{m}_i^2)$ under the isomorphism $R'_0 \rightarrow R'_i$, we get $w_{i+1} \notin (\mathbf{v}_i, \mathbf{x}_{i+1}) : \mathfrak{m}_{R_i}^2$. Finally, if $k = e - 2$, then $w_{i+1} \in A_i$ by our initial choice.

This shows that Theorem 6.6 may be applied to the extension $R_i \rightarrow R_{i+1}$ if R_i is F-regular; that is, that w_{i+1} satisfies the necessary conditions to be chosen as the z in Theorem 6.6.

We make several observations about the case that we may obtain an R_d in the above manner. If we write $\mathfrak{m}_{R_0} = (w_1, \dots, w_d) + J$ with $\mu(J) = \mu(\mathfrak{m}_{R_0}) - d$, then $\mathfrak{m}_{R_d} = (v_1, \dots, v_d) + J$. Thus, every generator of J is in $\overline{(w_1, \dots, w_d)R_d} = \overline{(v_1^n, \dots, v_d^n)R_d} = \overline{\mathfrak{m}_{R_d}^n}$. In addition, we note that via the isomorphism ϕ_d we may filter $R_d/(v_1, \dots, v_d)$ by essentially the same filtration as we take of $R_0/(w_1, \dots, w_d)$. Let $r = \max\{j \mid (\mathfrak{m}_{R_0}^j + (w_1, \dots, w_d))/(w_1, \dots, w_d) \neq 0\}$. We may then take a socle generator $u \in \mathfrak{m}_{R_0}^r$, modulo (\mathbf{w}_d) . The same element will now represent a socle element in $R_d/(\mathbf{v}_d)$ and will have valuation at least rn . Hence, if $rn \geq d$, then by the Briançon–Skoda theorem, $u \in (\mathbf{v}_d)^*$, and R_d is not F-regular.

In particular, if $n \geq \lceil d/2 \rceil$ (if $k = e - 2$) or if $n \geq \lceil d/3 \rceil$ (if $k < e - 2$, by Lemma 6.4), the ring R_d cannot be F-regular.

Choose such n , and let $s = \max\{i : R_i \text{ is F-regular}\}$. Note that $s < d$, and hence R_{s+1} is not F-regular.

In each application of Theorem 6.6, $b = n$, so from the theorem, for each $i \leq t$ (or $i < d$ if $t = d$), we have

$$e_{HK}(R_i) \geq \begin{cases} 1 + \frac{e-2}{en-2}(e_{HK}(R_{i+1}) - 1) & \text{if } k = e - 2, \\ 1 + \frac{k+1}{(n-1)e+k+1}(e_{HK}(R_{i+1}) - 1) & \text{if } k < e - 2. \end{cases}$$

By [1, Corollary 3.10], $e_{HK}(R_{s+1}) \geq 1 + 1/d$.

Hence,

$$e_{HK}(R_0) \geq \begin{cases} 1 + \left(\frac{e-2}{en-2}\right)^{s+1} \left(\frac{e}{2} - 1\right) & \text{if } k = e - 2, \\ 1 + \left(\frac{k+1}{(n-1)e+k+1}\right)^{s+1} \left(\frac{1}{d}\right) & \text{if } k < e - 2. \end{cases}$$

We then get the following lower bounds for nonregular rings, using that we may assume that $6 \leq e \leq d!$, $k \geq 3$:

$$e_{HK}(R_0) \geq \begin{cases} 1 + \left(\frac{4}{6^{\lfloor d/2 \rfloor - 2}}\right)^d \cdot 2 & \text{if } k = e - 2, \\ 1 + \left(\frac{4}{(\lfloor d/3 \rfloor)^{d+4}}\right)^d \left(\frac{1}{d}\right) & \text{if } k < e - 2. \end{cases}$$

Therefore, we can state the final result.

THEOREM 6.7. *Let R be a local Gorenstein F -regular ring of dimension $d \geq 2$, Hilbert–Samuel multiplicity $e \geq 6$, and positive characteristic $p > 2$. Let $k = \text{embdim}(R) - \dim(R)$. Assume further that R is not a complete intersection.*

Thus if $e \geq d! + 1$, then $e_{HK}(R) \geq 1 + 1/d!$. Otherwise,

$$e_{HK}(R) \geq \begin{cases} 1 + \left(\frac{4}{6^{\lfloor d/2 \rfloor - 2}}\right)^d \cdot 2 & \text{if } k = e - 2, \\ 1 + \left(\frac{4}{(\lfloor d/3 \rfloor)^{d+4}}\right)^d \left(\frac{1}{d}\right) & \text{if } k < e - 2. \end{cases}$$

Proof. It suffices to remind the reader that the first claim is well known (see [2, p. 2507]). The last inequality is what we have proved in Section 6. \square

Acknowledgments. The authors are indebted to one of the referees for several important suggestions and corrections that improved the manuscript. Notably, the referee observed that Yoshida’s results in [22] can be used to improve our Theorem 5.2. Some of the computations in the paper were performed with Wolfram Mathematica [21]. We also thank Alexander Koldobskiy for providing insight into the explicit formula for v_s in Section 3.

REFERENCES

- [1] I. M. Aberbach and F. Enescu, *Lower bounds for Hilbert–Kunz multiplicities in local rings of fixed dimension*, Michigan Math. J. **57** (2008), 1–16. MR 2492437. DOI 10.1307/mmj/1220879393.
- [2] M. Blickle and F. Enescu, *On rings with small Hilbert–Kunz multiplicity*, Proc. Amer. Math. Soc. **132** (2004), 2505–2509. MR 2054773. DOI 10.1090/S0002-9939-04-07469-6.

- [3] O. Celikbas, H. Dao, C. Huneke, and Y. Zhang, *Bounds on the Hilbert-Kunz multiplicity*, Nagoya Math. J. **205** (2012), 149–165. MR 2891167.
- [4] D. Chakerian and D. Logothetti, *Cube slices, pictorial triangles, and probability*, Math. Mag. **64** (1991), 219–241. MR 1131009. DOI 10.2307/2690829.
- [5] F. Enescu and K. Shimomoto, *On the upper semi-continuity of the Hilbert-Kunz multiplicity*, J. Algebra **285** (2005), 222–237. MR 2119113. DOI 10.1016/j.jalgebra.2004.11.014.
- [6] K. Eto and K.-i. Yoshida, *Notes on Hilbert-Kunz multiplicity of Rees Algebra*, Comm. Algebra **31** (2003), 5943–5976. MR 2014910. DOI 10.1081/AGB-120024861.
- [7] S. Goto and Y. Nakamura, *Multiplicity and tight closures of parameters*, J. Algebra **244** (2001), 302–311. MR 1856539. DOI 10.1006/jabr.2001.8907.
- [8] M. Hochster and C. Huneke, *Tight closure, invariant theory, and the Briançon-Skoda theorem*, J. Amer. Math. Soc. **3** (1990), 31–116. MR 1017784. DOI 10.2307/1990984.
- [9] C. Huneke and I. Swanson, *Integral closure of ideals, rings, and modules*, London Math. Soc. Lecture Note Ser. **336**, Cambridge University Press, Cambridge, 2006. MR 2266432.
- [10] P. Monsky, *The Hilbert-Kunz function*, Math. Ann. **263** (1983), 43–49. MR 0697329. DOI 10.1007/BF01457082.
- [11] P. Monsky and I. Gessel, *The limit as $p \rightarrow \infty$ of the Hilbert-Kunz multiplicity of $\sum x_i^{d_i}$* , preprint, 2010, [arXiv:1007.2004](https://arxiv.org/abs/1007.2004) [math.AC].
- [12] M. Nagata, *Local Rings*, Pure Appl. Math. (Hoboken) **13**, Wiley, New York, 1962. MR 0155856.
- [13] D. G. Northcott and D. Rees, *Reductions of ideals in local rings*, Math. Proc. Cambridge Philos. Soc. **50** (1954), 145–158. MR 0059889.
- [14] D. Rees, *Valuations associated with ideals, II*, J. London Math. Soc. **31** (1956), 221–228. MR 0078971.
- [15] J. D. Sally, *Numbers of Generators of Ideals in Local Rings*, Marcel Dekker, New York, 1978. MR 0485852.
- [16] ———, *Cohen-Macaulay local rings of maximal embedding dimension*, J. Algebra **56** (1979), 168–183. MR 0527163. DOI 10.1016/0021-8693(79)90331-4.
- [17] ———, *Tangent cones at Gorenstein singularities*, Compos. Math. **40** (1980), 167–175. MR 0563540.
- [18] K.-i. Watanabe and K.-i. Yoshida, *Hilbert-Kunz multiplicity and an inequality between multiplicity and colength*, J. Algebra **230** (2000), 295–317. MR 1774769. DOI 10.1006/jabr.1999.7956.
- [19] ———, *Hilbert-Kunz multiplicity of two-dimensional local rings*, Nagoya Math. J. **162** (2001), 87–110. MR 1836134.
- [20] ———, *Hilbert-Kunz multiplicity of three-dimensional local rings*, Nagoya Math. J. **177** (2005), 47–75. MR 2124547.
- [21] Wolfram Research, *Mathematica*, Version 7.0, Champaign, IL, 2008.
- [22] K.-i. Yoshida, “Small Hilbert-Kunz multiplicity and (A_1) -type singularity” in *Proceedings of the 4th Japan-Vietnam Joint Seminar on Commutative Algebra by and for Young Mathematicians*, Meiji University, Japan, 2009.

Ian M. Aberbach
Department of Mathematics
University of Missouri
Columbia, Missouri 65211
USA
aberbachi@missouri.edu

Florian Enescu
Department of Mathematics and Statistics
Georgia State University
Atlanta, Georgia 30303
USA
fenescu@gsu.edu