A THEOREM OF HOCHSTER AND HUNEKE CONCERNING TIGHT CLOSURE AND HILBERT-KUNZ MULTIPLICITY

LORI MCDONNELL

Abstract. We provide a (mostly) self-contained treatment of Hochster and Huneke's theorem characterizing Hilbert-Kunz multiplicity in terms of tight closure. This is not a new proof, just an elaboration of the one given in [3].

1. Introduction

The purpose of this note is to give a (mostly) self-contained proof of a theorem of Hochster and Huneke ([3, Theorem 8.17]) which characterizes the Hilbert-Kunz multiplicity of two ideals by their tight closures. We follow closely the treatment given in [3], but expand on some of the details. In preparing this we found one implication in line 12 of page 81 of the proof in [3] which we were unable to justify. However, we were able to use an argument suggested by Neil Epstein to work around this implication. This argument can be found toward the end of the proof of Theorem 4.4.

We begin with some notation. Throughout this note all rings are assumed to be of prime characteristic p and (except in obvious exceptional cases) Noetherian as well. For a ring R we let R° denote the elements of R which are not in any minimal prime of R. For an ideal I of R and $q = p^e$ (for some e), we let $I^{[q]}$ denote the ideal of R generated by the set $\{i^q : i \in I\}$. The *tight closure* of I, denoted by I^*, is defined to be the set of all elements $x \in R$ such that there exists $c \in R^{\circ}$ with $cx^q \in I^{[q]}$ for all $q = p^e$ sufficiently large.

Let (R, m) be a local ring of dimension d. Given an m-primary ideal I of R, we let $\lambda(R/I)$ denote the length of R/I as an R-module. Then one defines the *Hilbert - Kunz multiplicity* of I by

$$e_{HK}(I) := \lim_{q \to \infty} \frac{\lambda\left(R/I^{[q]}\right)}{q^d}.$$

That this limit exists and is positive for all such ideals was shown by Monsky [7].

Date: June 2009.

In [3], Hochster and Huneke give a proof of the following result:

Theorem 1.1. *(cf.* [3, Thoerem 8.17]*) Let (R, m) be a local ring and $J \subseteq I$ m-primary ideals of R.*

(1) If $I \subseteq J^*$ then $e_{HK}(I) = e_{HK}(J)$.
(2) The converse to (1) holds if R is equidimensional and either complete or essentially of finite type over a field.

We note that this theorem provides an analogue to the following result of Rees [8] concerning Samuel multiplicity and integral closure. For an ideal of a ring R, let $\overline{I}$ denote the integral closure of I. If R is local of dimension d and I is m-primary, then the Samuel multiplicity of I is defined by

$$e(I) := d! \lim_{n \to \infty} \frac{\lambda(R/I^n)}{n^d}.$$

Theorem 1.2. *Let (R, m) be a local ring (not necessarily of positive characteristic) and $J \subseteq I$ m-primary ideals of R.*

(1) If $I \subseteq \overline{J}$ then $e(I) = e(J)$.
(2) If R is formally equidimensional then the converse to (1) holds.

Note that the converses of part (1) of both Theorem 1.1 and 1.2 hold under essentially the same conditions.

2. Preliminaries

We begin with a discussion of qth roots. Assume R is reduced and let $\operatorname{Ass}_R R = \operatorname{Min}_R R = \{p_1, \ldots, p_n\}$. For each i let $k_i = R_{p_i} = Q(R/p_i)$. By the Chinese Remainder Theorem, the total quotient ring $Q = Q(R)$ is isomorphic to $k_1 \times \cdots \times k_n$. For each i let $\overline{k_i}$ denote a fixed algebraic closure of k_i and let $\overline{Q}$ denote $\overline{k_1} \times \cdots \times \overline{k_n}$. Clearly, R embeds in $\overline{Q}$ in a natural way. For $q = p^e$ let $R^{1/q} = \{u \in \overline{Q} \mid u^q \in R\}$. Then $R^{1/q}$ is an integral extension of R but in general is not finite. For each $r \in R$ there exists a unique $u \in R^{1/q}$, denoted $r^{1/q}$, such that $u^q = r$. For, if $u^q = r = w^q$ for $u, w \in \overline{Q}$, then $0 = u^q - w^q = (u - w)^q$; since $R^{1/q} \subseteq \overline{Q}$ is reduced, we have $u = w$. Note that the map $\varphi : R \longrightarrow R^{1/q}$ given by $\varphi(r) = r^{1/q}$ is a ring isomorphism, so $R^{1/q}$ is a Noetherian ring. If R is local with maximal ideal m then the maximal ideal of $R^{1/q}$ is $m^{1/q} = \{x^{1/q} \mid x \in m\}$.

Note that the inclusion map $R \hookrightarrow R^{1/q}$, where $q = p^e$, is essentially the same as the the e^{th} iteration of the Frobenius map $f^e : R \to R$ defined by $f^e(r) = r^{p^e}$. To be precise, let S be the ring R, but viewed as an R-module via f^e. Then the map $\rho : S \longrightarrow R^{1/q}$ given by $\rho(s) = s^{1/q}$ is easily seen to be an isomorphism of R-algebras (i.e., a ring isomorphism which is R-linear). Hence, for example, by a result of Kunz [4] R is regular if and only if $R^{1/q}$ is a flat R-module for some (equivalently, every) q.

Lemma 2.1. *Let $A \subseteq R$ be rings, with A a Noetherian domain and $A \subseteq R$ a finite integral extension. Then R is torsion-free as an A-module if and only if $\dim R/p = \dim R$ for all $p \in \operatorname{Ass}_R R$. In the case R is torsion-free over A, we have $Q(A) \subseteq R_W = Q(R)$, where $W = A \backslash \{0\}$ and $Q(-)$ denotes the total quotient ring.*

Proof. For the reverse implication, suppose $a \cdot r = 0$,with $a \in A\backslash\{0\}, r \in R\backslash\{0\}$. Then $a \in P$ for some $P \in \operatorname{Ass}_R R$ as $a \in A \subseteq R$ is a zero-divisor. Now $A/(P \cap A) \subseteq R/P$ is a finite integral extension, and $\dim R = \dim R/P = \dim A/(P \cap A) = \dim A$. But A is a domain, so we must have $P \cap A = 0$. We have $a \in P \cap A$, so we must have $a = 0$, giving a contradiction. Thus, R must be a torsion-free A-module.

Conversely, let $P \in \operatorname{Ass}_R R$. Since R is torsion-free, $P \cap A = (0)$. This implies $\dim R/P = \dim A = \dim R$.

In the case R is torsion-free over A, let $W' = \{s \in R \mid s \text{ a non} - \text{zero} - \text{divisor}\}$. As R is torsion-free over A, $W \subseteq W'$, so $Q(A) \subseteq R_W \subseteq R_{W'}$ and $Q(R) = R_{W'} = (R_W)_{W'} = Q(R_W)$. But as $Q(A) \subseteq R_W$ is integral, $\dim R_W = 0$. Hence, $Q(R_W) = R_W$. □

Lemma 2.2. *Let $A \subseteq R$ be rings. Consider the ring homomorphism $\varphi : R \otimes_A A^{1/q} \to R\left[A^{1/q}\right]$ given by $\varphi\left(r \otimes a^{1/q}\right) = ra^{1/q}$. Then φ is onto and $\ker \varphi$ is nilpotent.*

Proof. Clearly φ is onto. Note, if $\Sigma r_i \otimes a_i^{1/q} \in \ker \varphi$, then we have $\Sigma r_i a_i^{1/q} = 0$. Taking q^{th} powers, we get $\Sigma r_i^q a_i = 0$, and so, $\Sigma r_i^q a_i \otimes 1 = 0$. We can move the a_i's to the other side of the tensor product to obtain $0 = \Sigma r_i^q \otimes a_i = \left(\Sigma r_i \otimes a_i^{1/q}\right)^q$. Hence, $\Sigma r_i \otimes a_i^{1/q}$ is nilpotent. □

Example 2.3. *Note that $R \otimes_A A^{1/p}$ need not be reduced, even if R and A are fields. For example, let k be an imperfect field (i.e., $k = \mathbb{F}_p(t)$, where t is an indeterminate) and $A = k$ and $R = k^{1/p}$. Choose $a \in k \backslash k^p$. Then $\beta = a^{1/p} \otimes 1 - 1 \otimes a^{1/p}$ is nonzero as $\{a^{1/p} \otimes 1, 1 \otimes a^{1/p}\}$ is part of a k-basis for $k^{1/p} \otimes_k k^{1/p}$ since $a^{1/p}$ is part of a k-basis for $k^{1/p}$. However, $\beta^p = 0$.*

We want to determine when the map φ of Lemma 2.2 is an isomorphism, or equivalently, assuming R and A are reduced, under what conditions $R \otimes_A A^{1/q}$ is reduced. We begin this exploration with some remarks concerning separability.

Definition 2.4. Let $A \subseteq S$ be a finite ring extension where A is a Noetherian domain and S is reduced and torsion-free over A. Then $Q(A) \subseteq Q(S) \cong k_1 \times \cdots \times k_n$ where each k_i is a finite field extension of $Q(A)$. An element $s \in S$ is *separable* over A if each component of its image in $k_1 \times \cdots \times k_n$ is separable over $Q(A)$. We say S *is separable over* A if each $s \in S$ is separable over A, or equivalently, each k_i is separable over $Q(A)$.

Remark 2.5. *(*[5]*, page 199) If E/F is a finite separable field extension, then for every field extension L of F, $E \otimes_F L$ is reduced.*

Lemma 2.6. *Let $A \subseteq S$ be a finite separable ring extension with A a Noetherian domain and S reduced and torsion-free over A. Let B be a reduced A-algebra. Then*

(1) If B is flat, then $S \otimes_A B$ is reduced.
(2) If S is flat and B is torsion-free, then $S \otimes_A B$ is reduced.

Proof. We first prove part (1). Note that as S, B are reduced, S and B both inject into a product of fields, say, $S \hookrightarrow k_1 \times \cdots \times k_n$ and $B \hookrightarrow l_1 \times \cdots \times l_m$. By hypothesis $Q(A) \subseteq k_i$ is separable for all i. We want to show that $S \otimes_A B$ injects into a reduced ring.

Claim: $S \otimes_A B \hookrightarrow (k_1 \times \cdots \times k_n) \otimes_{Q(A)} (l_1 \times \cdots l_m) \cong \prod_{i,j} \left(k_i \otimes_{Q(A)} l_j\right)$.

Proof of claim: Note $0 \to S \to k_1 \times \cdots \times k_n$ is exact. Applying $- \otimes_A B$, we obtain

$$0 \quad \to \quad S \otimes_A B \to (k_1 \times \cdots \times k_n) \otimes_A B \cong (k_1 \otimes_A B) \times \cdots \times (k_n \otimes_A B) \quad \text{is exact,}$$

with the injection coming from the fact that B is flat. It suffices to show that if a field k is separable over $Q(A)$ and $B \hookrightarrow l_1 \times \cdots \times l_m$, then $k \otimes_A B \hookrightarrow k \otimes_A (l_1 \times \cdots \times l_m)$.

Now, we have $0 \to B \to l_1 \times \cdots \times l_m$ is exact. Applying $Q(A) \otimes_A -$ and then $k \otimes_{Q(A)} -$, we obtain

$$0 \to Q(A) \otimes_A B \to Q(A) \otimes_A (l_1 \times \cdots \times l_m) \cong l_1 \times \cdots \times l_m \quad \text{is exact, and}$$
$$0 \to k \otimes_{Q(A)} (Q(A) \otimes_A B) \to k \otimes_{Q(A)} (l_1 \times \cdots \times l_m) \quad \text{is exact,}$$

where the isomorphism in the first line comes from the fact that $l_i \supseteq Q(A)$ for all i. But, $k \otimes_{Q(A)} (Q(A) \otimes_A B) \cong k \otimes_A B$ and $k \otimes_{Q(A)} (l_1 \times \cdots \times l_m) = \prod_i \left(k \otimes_{Q(A)} l_i\right)$ is reduced by separability. Thus, we have $k \otimes_A B \hookrightarrow \prod_i \left(k \otimes_{Q(A)} l_i\right)$, and thus, $k \otimes_A B$ is reduced, implying that $S \otimes_A B$ is reduced.

Now, to prove part (2), suppose S is flat and B is torsion-free. Using the notation above, since S is flat over A, we have

$$0 \to S \otimes_A B \to (S \otimes_A l_1) \times \cdots \times (S \otimes_A l_m)$$

is exact. Therefore, it suffices to show that $S \otimes_A l_i$ is reduced for all i. Since B is torsion-free over A, $Q(A) \subseteq l_i$ for all i, and so $Q(A) \otimes_A l_i \cong l_i$ for all i.

Hence, $k_j \otimes_A l_i \cong k_j \otimes_{Q(A)} l_i$ is reduced for any j, since k_j is separable over $Q(A)$. Since l_i is flat over A,

$$0 \to S \otimes_A l_i \to (k_1 \times \cdots \times k_n) \otimes_A l_i \cong (k_1 \otimes_A l_i) \times \cdots \times (k_n \otimes_A l_i)$$

is exact. Therefore, $S \otimes_A l_i$ is reduced.

□

Remark 2.7. *Suppose we have $A \subseteq R$, a finite extension with A a Noetherian domain and R reduced and torsion-free over A. Then $A^{1/q} \subseteq R\left[A^{1/q}\right]$ is a finite extension and $R\left[A^{1/q}\right]$ is reduced and torsion-free over $A^{1/q}$. Furthermore, the extension $A^{1/q} \subseteq R\left[A^{1/q}\right]$ is separable for $q >> 0$.*

Proof. Using the notation from the beginning of this section, we have $R \subseteq Q(R) \cong k_1 \times \cdots \times k_n$ where k_i is a field for all i. As R is torsion-free over A, $Q(A) \subseteq Q(R)$ by Lemma 2.1 Let $\overline{k_i}$ denote the algebraic closure of k_i. Since R/p_i is a finite extension of A, we have each $\overline{k_i}$ is an algebraic extension of $Q(A)$. Note $R\left[A^{1/q}\right] \subseteq \overline{k_1} \times \cdots \times \overline{k_n}$, a product of fields, so $R\left[A^{1/q}\right]$ is reduced for any q. Now, suppose $a^{1/q}\left(\Sigma r_i a_i^{1/q}\right) = 0$. Then, taking q^{th} powers, we have $a\left(\Sigma r_i^q a_i\right) = 0$. If $a \neq 0$, then $\Sigma r_i^q a_i = 0$ since R is torsion-free over A. Taking q^{th} roots, we have $\Sigma r_i a_i^{1/q} = 0$. Thus, $R\left[A^{1/q}\right]$ is torsion-free over $A^{1/q}$.

To see that $A^{1/q} \subseteq R\left[A^{1/q}\right]$ is a finite extension, note that if $R = A\alpha_1 + \cdots + A\alpha_n$, with $\alpha_i \in R$, then $R[A^{1/q}] = A^{1/q}[R] = A^{1/q}\alpha_1 + \cdots + A^{1/q}\alpha_n$. Thus, $R[A^{1/q}]$ is a finitely generated $A^{1/q}$-module.

Finally, to see that the extension $A^{1/q} \subseteq R\left[A^{1/q}\right]$ is separable for $q >> 0$, write $R = A\alpha_1 + \cdots + A\alpha_n$. Recall that for a field F of characteristic $p > 0$ and an element α in the algebraic closure of F, α^{p^n} is separable over F for all $n >> 0$. So, for each i, there exists a $q_i = p^{e_i}$ such that $\alpha_i^{q_i}$ is separable over A, and therefore α_i is separable over A^{1/q_i}. Now, let $q = \max_i\{q_i\}$. Then we have R, and hence $R[A^{1/q}]$, is separable over $A^{1/q}$. □

Proposition 2.8. *Let $A \subseteq R$ be a finite ring extension where A is a regular local ring and R is reduced and torsion-free over A. Then there exists a power q' of p such that for all $q \geq q'$, $S = R[A^{1/q}]$ is reduced, torsion-free, and separable over $A^{1/q}$. Furthermore, for all $Q \geq q \geq q'$, $S \otimes_{A^{1/q}} A^{1/Q} \cong S[A^{1/Q}]$.*

Proof. Note by Remark 2.7, there is a q' such that $A^{1/q} \subseteq S = R[A^{1/q}]$ is a finite separable extension and S is reduced and torsion-free over $A^{1/q}$ for all $q \geq q'$. As A is regular, for $Q \geq q \geq q'$, we have $A^{1/Q}$ is flat over $A^{1/q}$. So by Lemma 2.6, $S \otimes_{A^{1/q}} A^{1/Q}$ is reduced and thus, by Lemma 2.2, we have $S \otimes_{A^{1/q}} A^{1/Q} \cong S[A^{1/Q}]$. □

3. Smoothness

Definition 3.1. Let R be a ring and S an R-algebra. We say that S *is smooth over* R, sometimes denoted as S/R *smooth*, if given an R-algebra T, an ideal N of T satisfying $N^2 = 0$, and an R-algebra homomorphism $u : S \to T/N$, then there exists an R-algebra homomorphism $v : S \to T$ lifting u; i.e., $u = \pi v$ where $\pi : T \to T/N$ is the natural surjection.

We refer the reader to [5] and [6] for a detailed treatment of smoothness. We summarize some of the important properties of smoothness in the following remark:

Remark 3.2. *We list below several properties of smoothness:*

(1) *([5], 28.2) If A is an R algebra, then S/R smooth implies $S \otimes_R A$ is smooth over A. In particular, localization and taking quotients preserve smoothness.*
(2) *([5], 28.1) T/S and S/R smooth imply T/R is smooth.*
(3) *([6], 28.E) If W is a multiplicatively closed subset of R, then R_W/R is smooth.*
(4) *([5], 28.9; [2], 19.7.1) If S/R is smooth and S, R are Noetherian, then S/R is flat.*
(5) *([6], 28.I, 28.L) Let R be a field and S a finite extension field of R. Then S/R is smooth if and only if S/R is separable.*
(6) *([6], 29.E; [5] corollary to theorem 30.5) If S is a finitely generated R-algebra then $\{p \in \operatorname{Spec} R \mid S_p/R_p$ is smooth$\}$ is an open set. In particular, if S_p/R_p is smooth for some $p \in \operatorname{Spec} R$ then there exists an $f \in R\backslash p$ such that S_f/R_f is smooth.*
(7) *([6], 28.K) If k is a field and A is a local ring which is smooth over k, then A is a regular local ring.*
(8) *([6], section 28, example 1) Let A be a ring. Then $A[x]$ is smooth over A.*

Proposition 3.3. *Suppose S is smooth over R, where R and S are Noetherian rings. If R is reduced, so is S.*

Proof. Let $P \in \operatorname{Ass}_S S$. Note that it suffices to show that S_P is a field. Let $Q = P \cap R$ be the contraction of P to R. Since P consists of zero-divisors on S, so does Q. On the other hand, since S is flat over R, any non-zero-divisor on R is a non-zero-divisor on S (i.e., S is torsion-free over R). Hence, Q must consist of zero-divisors on R, so there exists $Q' \in \operatorname{Ass}_R R$ such that $Q \subseteq Q'$. But, as R is reduced, the associated primes are minimal, and so Q must be a minimal prime of R. Furthermore, as R is reduced, R_Q is a field. Now, we have S_Q is smooth over R_Q, and $PS_Q \in \operatorname{Ass}_{S_Q} S_Q$. Thus, we have reduced to the case that R is a field.

Now, S_P is smooth over S, and so by transitivity, S_P is smooth over R. By (7) in the remarks above, S_P is a regular local ring of depth zero, i.e., S_P is a field. □

Proposition 3.4. *Suppose $R \subseteq S$ is a finite extension where R is a Noetherian domain and S is reduced, torsion-free, and separable over R. Then there exists $d \in R\backslash\{0\}$ such that S_d is smooth over R_d.*

Proof. We have $Q(R) \subseteq Q(S) \cong k_1 \times \cdots \times k_n$, where k_i is a finite separable field extension of $Q(R)$ for each i. By part (5) of Remark 3.2, each k_i is smooth over $Q(R)$. Thus, $Q(S)$ is smooth over $Q(R)$. Since $Q(S) \cong S_W$ where $W = R\backslash\{0\}$ (see Lemma 2.1), we have S_W is smooth over R_W. The result now follows by part (6) of Remark 3.2. □

Theorem 3.5. *Suppose S/R is smooth, finite, and R is a Noetherian domain of characteristic p. Then for any $q = p^e$, $S^{1/q} = S\left[R^{1/q}\right]$.*

Proof. Note that since S/R is smooth and R is a domain we have S is reduced (Proposition 3.3) and torsion-free over A (Remark 3.2, part (4)). Also, since $S \cong S^{1/q}$ as rings, and this isomorphism restricts to $R \cong R^{1/q}$, we get that $S^{1/q}/R^{1/q}$ is smooth and finite. Thus, it is enough to prove the theorem for $e = 1$, since $S^{1/p} = S\left[R^{1/p}\right]$ implies $S^{1/p^2} = S^{1/p}\left[R^{1/p}\right] = S\left[R^{1/p^2}\right]$.

Case 1: R is a field. Then we have $R \hookrightarrow S \cong k_1 \times \cdots \times k_n$ with each k_i/R a finite algebraic separable field extension. Note $S^{1/p} = k_1^{1/p} \times \cdots \times k_n^{1/p}$. It is enough to show that $k_i^{1/p} = k_i\left[R^{1/p}\right]$, because then $S^{1/p} = k_1^{1/p} \times \cdots \times k_n^{1/p} = k_1\left[R^{1/p}\right] \times \cdots \times k_n\left[R^{1/p}\right] = (k_1 \times \cdots \times k_n)\left[R^{1/p}\right] = S\left[R^{1/p}\right]$.

Claim: If L/K is a finite separable algebraic field extension of characteristic p, then $L^{1/p} = L\left[K^{1/p}\right]$.

Proof of claim: Note L/K separable implies $L^{1/p}/K^{1/p}$ is separable. Now, $K^{1/p} \subseteq L\left(K^{1/p}\right) \subseteq L^{1/p}$ and $L^{1/p}/K^{1/p}$ separable imply $L^{1/p}/L\left(K^{1/p}\right)$ is separable. Let $\alpha \in L^{1/p}$. Then $\alpha^p \in L \subseteq L\left(K^{1/p}\right)$. Let $\mathrm{Min}(\alpha, L\left(K^{1/p}\right))$ denote the minimal polynomial of α over the field $L\left(K^{1/p}\right)$. Then we have $\mathrm{Min}\left(\alpha, L\left(K^{1/p}\right)\right) \mid (x^p - \alpha^p)$ implies $\mathrm{Min}\left(\alpha, L\left(K^{1/p}\right)\right) = x - \alpha$ by the separability of $L^{1/p}/L\left(K^{1/p}\right)$. Thus, $\alpha \in L\left(K^{1/p}\right)$. This gives that $L^{1/p} \subseteq L\left(K^{1/p}\right)$. The other containment is clear, giving $L^{1/p} = L\left(K^{1/p}\right) = L\left[K^{1/p}\right]$. $\square_{claim}$

General Case: We want to show that $S^{1/p} = S\left[R^{1/p}\right]$. Since S/R is smooth, $Q(S) = S_{(0)}$ is smooth over $R_{(0)}$; i.e., S is separable over R, by Remark 3.2, part (5). Since S is flat over R and $R^{1/p}$ is torsion-free over R, $S \otimes_R R^{1/p}$ is reduced by part (2) of Lemma 2.6. Hence, by Lemma 2.2, $S \otimes_R R^{1/p} \cong S[R^{1/p}]$.

Define $\varphi : S \otimes_R R^{1/p} \to S^{1/p}$ by $\varphi\left(s \otimes r^{1/p}\right) = sr^{1/p}$. We claim that φ is an isomorphism. Note that it is enough to show that φ is an isomorphism locally at any maximal ideal of

R. Thus, we may assume that (R, m) is local. Now, S/R is finite and flat, which implies $S \otimes_R R^{1/p}/R^{1/p}$ is finite and flat. Recall that if T is a finitely generated flat module over a Noetherian ring then T is free. Therefore, we have $S \otimes_R R^{1/p}$ is a free $R^{1/p}$-module. Similarly, $S^{1/p}$ is a finitely generated free $R^{1/p}$-module.

Over a local ring, a map of finitely generated free modules is an isomorphism if and only if it is an isomorphism after tensoring with the residue field. Now, we have $S \otimes_R R^{1/p} \xrightarrow{\varphi} S^{1/p}$ is a map of free $R^{1/p}$-modules. Tensoring with $R/mR\left(\cong R^{1/p}/m^{1/p}\right)$ gives the map $S/mS \otimes_{R/m} (R/m)^{1/p} \xrightarrow{\bar{\varphi}} (S/mS)^{1/p}$. Since S/mS is smooth over R/m, this is an isomorphism by the first case. Thus, φ is an isomorphism. $\square$

Now, suppose we have $R \subseteq S$ with R a domain and S finite, torsion-free, and separable over R. By Proposition 3.4, there exists a $d \in R/\{0\}$ such that S_d/R_d is smooth. The previous theorem then implies that $\left(S^{1/q}/S\left[R^{1/q}\right]\right)_d = 0$ for any $q = p^e$, so that, given q, there is a power l of d such that $d^l S^{1/q} \subseteq S\left[R^{1/q}\right]$. Using the following lemma, one can find a single power of d that will work for all q.

Proposition 3.6. *(see 6.4 in [3]) Let $A \subseteq R$ be a finite ring extension where A is a regular local ring and R is reduced, torsion-free, and separable over A. Then there exists $c \in A\backslash\{0\}$ such that $cR^{1/q} \subseteq R[A^{1/q}]$ for all q.*

Proof. By Proposition 3.4, there exists $d \in A\backslash\{0\}$ such that R_d is smooth over A_d. In the discussion above, we showed that there exists a power $b = d^l$ of d such that $bR^{1/p} \subseteq R\left[A^{1/p}\right]$. Let $h = 1 + 1/p + \cdots + 1/p^e$.

Claim: $b^h R^{1/pq} \subseteq R\left[A^{1/pq}\right]$ for all $q = p^e$.

Proof: We proceed by induction on e. If $e = 0$, then $h = 1$ and $b^1 R^{1/p} \subseteq R\left[A^{1/p}\right]$. If $e > 0$, take q^{th} roots to obtain $b^{1/q} R^{1/pq} \subseteq R^{1/q}\left[A^{1/pq}\right]$. Now, with $h' = h - 1/q$, we have

$$b^h R^{1/pq} = b^{h'} b^{1/q} R^{1/pq} \subseteq b^{h'} R^{1/q}\left[A^{1/pq}\right] \subseteq \left[R\left[A^{1/q}\right]\right][A^{1/pq}] = R[A^{1/pq}]$$

where the last containment comes from the induction hypothesis. $\square_{claim}$

Now, since b^h divides b^2 (in $A^{1/q}$) for all h, setting $c = b^2$, we have that $cR^{1/q} \subseteq R\left[A^{1/q}\right]$ for all q, as required.

$\square$

4. The Main Result

We are now ready to prove the main result. First, we recall some definitions and a lemma.

Definition 4.1. Let R be a Noetherian ring of characteristic $p > 0$ and I an ideal of R. We say $x \in I^*$, the *tight closure* of I, if there exists a $c \in R^\circ$ such that $cx^q \in I^{[q]}$ for all $q >> 0$. We say $c \in R^\circ$ is a *q'-weak test element* if there exists q' such that for all $I \subseteq R$ and all $x \in I^*$, we have $cx^q \in I^{[q]}$ for all $q \geq q'$. The element c is a *locally stable q'-weak test element* if its image in every local ring of R is also a q'-weak test element. Finally, c is a *completely stable q'-weak test element* if it is locally stable and its image in the completion of each local ring of R is a q'-weak test element.

Remark 4.2. *(see* [3]*, 6.18 and 6.19) Let R be a reduced, equidimensional local ring of characteristic $p > 0$ and suppose that either R is complete or essentially of finite type over a field. Then R has a completely stable q'-weak test element.*

Lemma 4.3. *(see* [3]*, 8.16) Let J be an ideal in a reduced Noetherian ring R which has a q'-weak test element $c \in R^\circ$. Suppose that $x \in R$ such that $x \notin J^*$. Then for any $d \in R^\circ$, $dx^q \notin J^{[q]*}$ for all $q >> 0$. In particular, for any $d \in R^\circ$, $dx^q \notin J^{[q]}R^{1/q}$ for all $q >> 0$.*

Proof. We will use the contrapositive to prove the lemma. Suppose that there exists $d \in R^\circ$ such that $dx^q \in J^{[q]*}$ for all $q >> 0$. We will show that $x \in J^*$ by showing $c^{q'+1}d^{q'}x^{qq'} \in J^{[qq']}$ for all $q >> 0$. Note if $dx^q \in J^{[q]*}$, then we have $cd^{Qq'}x^{qQq'} \in J^{[qQq']}$ for all Q, as c is a weak q'-test element. So, $(cdx^q)^{Qq'} \in \left(J^{[q]}\right)^{[Qq']}$. Hence, for all Q, we have $1 \cdot (cdx^q)^{Qq'} \in \left(J^{[q]}\right)^{[Qq']}$, which shows that $cdx^q \in J^{[q]*}$ for all $q >> 0$. But since c is a q'-weak test element, we have $c\,(cdx^q)^{q'} \in J^{[q][q']}$ for all $q >> 0$, i.e., $c^{q'+1}d^{q'}x^{qq'} \in J^{[qq']}$ for all $q >> 0$, which shows that $x \in J^*$.

To prove the last statement of the lemma, note that if $v \in J^{[q]}R^{1/Q}$, then $v^Q \in J^{[q][Q]}$ and as above, $1 \cdot v^{Qq''} \in J^{[qQq'']}$ for all q''. Hence, $v \in J^{[q]*}$. In particular, $dx^q \notin J^{[q]*}$ for $q >> 0$ implies $dx^q \notin J^{[q]}R^{1/q}$ for all $q >> 0$.

□

We are now prepared to prove the main result. The proof here follows closely that of Theorem 8.17 in [3], with some details expanded.

Theorem 4.4. *Suppose (R,m) is a local ring and let $J \subseteq I$ be m-primary ideals of R.*

(1) If $I \subseteq J^*$ then $e_{HK}(I) = e_{HK}(J)$.

(2) The converse to (1) holds if R is analytically unramified, formally equidimensional, and has a completely stable q_1-weak test element c.

Proof. (1) Let $I = (x_1, \ldots, x_n)$. Then since $I \subseteq J^*$, for each x_i there exists $a_i \in R^\circ$ such that $a_i x_i^q \in J^{[q]}$ for all $q >> 0$. Let $a = a_1 \cdots a_n \in R^\circ$. Then since $a x_i^q \in J^{[q]}$ for all $q >> 0$, we have $aI^{[q]} \subseteq J^{[q]}$. As J is m-primary, there exists an n such that $m^n I \subset J$. Set $K = m^n$. Let b be a bound on the number of generators for I. Then $I^{[q]}/J^{[q]}$ has at most b generators and is annihilated by $K^{[q]} + aR$, so that $I^{[q]}/J^{[q]}$ is a homomorphic image of $\left(R/(K^{[q]} + aR)\right)^b$. Thus, $\lambda(I^{[q]}/J^{[q]}) \leq b\lambda\left(R/(K^{[q]} + aR)\right)$. Let $S = R/aR$. Since $a \in R^\circ$, $\dim S \leq d-1$. So we have $\lambda\left(I^{[q]}/J^{[q]}\right) \leq b\lambda\left(S/K^{[q]}S\right)$. By a result of Monsky, we have $\lambda(S/K^{[q]}S) \leq e_{HK}(KS)q^{d-1} + Cq^{d-2}$ for some constant C. Therefore,

$$
\begin{aligned}
0 \ \leq \ e_{HK}(J) - e_{HK}(I) &= \lim_{q\to\infty} \left[\lambda\left(R/J^{[q]}\right)/q^d - \lambda\left(R/I^{[q]}\right)/q^d\right] \\
&= \lim_{q\to\infty} \frac{1}{q^d}\lambda\left(I^{[q]}/J^{[q]}\right) \\
&\leq \lim_{q\to\infty} \frac{1}{q^d}\left[e_{HK}(KS)q^{d-1} + Cq^{d-2}\right] \\
&= 0.
\end{aligned}
$$

(2) Suppose $e_{HK}(I) = e_{HK}(J)$ and $I \nsubseteq J^*$, i.e., there exists $x \in I \backslash J^*$, with $x \neq 0$. Then, as above, we have that $\lim_{q\to\infty} \frac{1}{q^d}\lambda(I^{[q]}/J^{[q]}) = 0$. Our goal is to show that there exists a constant $\gamma > 0$ such that $\lambda\left(I^{[q]}/J^{[q]}\right) \geq \gamma q^d$ for $q >> 0$ to obtain a contradiction.

Choose $q \geq q_1$ such that $cx^q \notin J^{[q]}$. Since $J^{[q]}\widehat{R} \cap R = J^{[q]}$, we have $cx^q \notin J^{[q]}\widehat{R}$. As $(J\widehat{R})^{[q]} = J^{[q]}\widehat{R}$ and c is a completely stable q_1-weak test element, we have $x \notin (J\widehat{R})^*$. So we may assume (R,m) is complete, local, reduced and equidimensional. By the Cohen-Structure theorem, R is module finite over a complete regular local domain $A = k\left[[x_1, \ldots, x_d]\right]$ and as R is equidimensional, by Lemma 2.1, we have R is also torsion-free over A.

By Proposition 2.8, we can choose q'' such that $S = R\left[A^{1/q''}\right]$ is separable over $A^{1/q''}$ and by Lemma 3.6 we can choose $d \in A^{\circ}$ such that $dS^{1/q} \subseteq S\left[A^{1/qq''}\right]$ for any q. Since $x \in I$ is not in J^*, by Lemma 4.3 we can choose q' such that $dx^q \notin J^{[q]}R^{1/q}$ for any $q \geq q'$.

Let $K_Q \subseteq A$ be the ideal of elements $a \in A$ such that $ax^Q \in J^{[Q]}$. Note the map $A/K_Q \to I^{[Q]}/J^{[Q]}$ given by $\bar{a} \mapsto \overline{ax^Q}$ is an injection. Since A and R have the same residue class field, $\lambda\left(I^{[Q]}/J^{[Q]}\right) \geq \lambda\left(A/K_Q\right)$, and so it is enough to show there exists $\gamma > 0$ such that $\lambda\left(A/K_Q\right) \geq \gamma Q^d$ for $Q >> 0$.

Now assume $Q \geq q'q''$ and write $Q = qq'q''$. Then $a \in K_Q$ implies that $ax^Q \in J^{[Q]}$. Taking $(1/q)^{th}$ powers, we have $a^{1/q}x^{q'q''} \in J^{[q'q'']}R^{1/q} \subseteq J^{[q'q'']}S^{1/q}$. This implies $da^{1/q}x^{q'q''} \in J^{[q'q'']}\left(dS^{1/q}\right) \subseteq J^{[q'q'']}S\left[A^{1/qq''}\right]$.

Note that as A is regular, $A^{1/qq''}$ is $A^{1/q''}$- flat and so we have $S \otimes_{A^{1/q''}} A^{1/qq''} \cong S\left[A^{1/qq''}\right]$ is S-flat, with the isomorphism coming from Proposition 2.8. Therefore,

$$a^{1/q} \in \left(J^{[q'q'']}S[A^{1/qq''}] :_{S[A^{1/qq''}]} dx^{q'q''}\right) \cong \left(J^{[q'q'']}S :_S dx^{q'q''}\right) S\left[A^{1/qq''}\right].$$

Now, $\left(J^{[q'q'']}S :_S dx^{q'q''}\right) \subseteq \left(J^{[q'q'']}R^{1/q''} :_{R^{1/q''}} dx^{q'q''}\right)$ as $S = R\left[A^{1/q''}\right] \subseteq R^{1/q''}$. By choice of q', $dx^{\tilde{q}} \notin J^{[\tilde{q}]}R^{1/\tilde{q}}$ for any $\tilde{q} \geq q'$. Therefore, $\left(J^{[q'q'']}R^{1/q''} :_{R^{1/q''}} dx^{q'q''}\right) \neq R^{1/q''}$. Thus, $(J^{[q'q'']}S :_S dx^{q'q''}) \subseteq m^{1/q''}$, and so $a^{1/q} \in m^{1/q''}S[A^{1/qq''}] \subseteq m^{1/q''}R^{1/qq''}$. Taking qq'' powers, we get $a^{q''} \in m^{[q]}R$. So if $Q \geq q'q''$ and $a \in K_Q$, then $a^{q''} \in m^{[Q/q'q'']}R \cap A$.

Let m_A denote the maximal ideal of A. Note we can find $D = p^n$ such that $m^D \subseteq m_A R$ and then $a^{q''} \in m^{[Q/q'q'']}R \cap A \subseteq m^{Q/q'q''}R \cap A \subseteq m_A^{Q/q'q''D}R \cap A \subseteq m_A^{(Q/q'q''D)-t}$ for some constant t and $Q >> 0$ (the last inclusion coming from the Artin - Rees Lemma). Now for large Q we'll have

$$m_A^{(Q/q'q''D)-t} \subseteq m_A^{Q/B} \qquad \text{where } B = q'q''Dp.$$

Thus, for $Q >> 0$, $a^{q''} \in m_A^{Q/B}$. Let $d = \dim A$. Then note that $m_A^{dq} \subseteq m_A^{[q]}$ for any $q = p^n$. Let $p^e \geq d$. Then we have for large Q, $a^{q''} \in m_A^{Qp^e/Bp^e} \subseteq m_A^{Qd/Bp^e} \subseteq m_A^{[Q/Bp^e]}$. Now let $H = m_A^{[Q/Bp^eq'']}$. For large Q, $A = \left(H^{[q'']} :_A a^{q''}\right) = (H :_A a)^{[q'']}$ (the last equality coming from the fact that A is regular and so the Frobenius is flat). So, we have $A = (H :_A a)$ and hence $a \in H = m_A^{[Q/Bp^eq'']}$ for large Q. As a was an arbitrary element of K_Q, we have for large Q, $K_Q \subseteq m_A^{[Q/B']} \subseteq m_A^{Q/B'}$ where $B' = Bp^eq''$, and so $\lambda\left(A/K_Q\right) \geq \lambda(A/m_A^{Q/B'})$. Let

$0 < \gamma < \frac{1}{d!(B')^d}$. Then as A is regular we have

$$\begin{aligned}\lambda(A/K_Q) \ \geq \ \lambda(A/m_A^{Q/B'}) \ &= \ \binom{Q/B'+d-1}{d} \\ &= \ \frac{Q^d}{d!(B')^d} + \text{lower terms} \\ &\geq \ \gamma Q^d \quad \text{for } Q >> 0.\end{aligned}$$

□

The argument in the last paragraph of the proof above allowing us to conclude that $K_Q \subseteq \mathfrak{m}_A^{Q/B'}$ was suggested to us by Neil Epstein and allowed us to avoid the implication on page 81, line 12 of the original proof in [3].

Corollary 4.5. *Let (R,m) be a local ring and $J \subseteq I$ m-primary ideals of R.*

(1) If $I \subseteq J^*$ then $e_{HK}(I) = e_{HK}(J)$.

(2) The converse to (1) holds if R is equidimensional and either complete or essentially of finite type over a field.

Proof. Note that part (1) follows from the previous theorem. To prove part (2), suppose that $e_{HK}(I) = e_{HK}(J)$ and R is equidimensional and either complete or essentially of finite type over a field. We first note that that we may reduce to the case R is a domain by going modulo a minimal prime. To see this, recall the associativity formula for Hilbert-Kunz multiplicity says that for any ideal I, $e_{HK}(I) = \sum_{P\in \mathrm{Assh}(R)} e_{HK}(I, R/P)\lambda_{R_P}(R_P)$ where $\mathrm{Assh}(R) = \{P \in \mathrm{Ass}(R) \mid \dim R/P = \dim R\}$. Let $\mathrm{Min}(R) = \{P_1, \ldots, P_n\}$ and I_i and J_i denote the images of I and J respectively in R/P_i. As R is equidimensional, $\mathrm{Assh}(R) = \mathrm{Min}(R)$ and so we have $e_{HK}(I) = \sum_{i=1}^n e_{HK}(I_i)\lambda(R_{P_i}) = \sum_{i=1}^n e_{HK}(J_i)\lambda(R_{P_i}) = e_{HK}(J)$. Since $J \subseteq I$, we have $e_{HK}(I_i) \leq e_{HK}(J_i)$ for all i. The equality of the Hilbert-Kunz multiplicities of I and J forces $e_{HK}(I_i) = e_{HK}(J_i)$ for all i. Furthermore, an element $x \in R$ is in the tight closure of J if and only if its image is in J_i^* for all i. (See [1], Proposition 10.1.2.) Thus, we may reduce to the case R is a domain.

By Remark 4.2, R has a completely stable test element. If R is a complete domain, we are done by Theorem 4.4. If R is a domain which is essentially of finite type over a field, then the completion of R is analytically unramified (see [6], page 251, Lemma 2) and formally equidimensional (see [5], Theorem 31.6 (iii)). The result once again follows from Theorem 4.4.

□

References

1. W. Bruns and J. Herzog, *Cohen-Macaulay Rings.* Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, Cambridge, 1993
2. A. Grothendieck, *Elements de geometrie algebrique*, IV_1. Publ. Math. IHES **20**, 1965.
3. M. Hochster and C. Huneke. Tight closure, invariant theory, and the Briancon-Skoda theorem. *J. Amer. Math. Soc.,* 3:31-116, 1994.
4. E. Kunz, Characterizations of Regular Local Rings of Characteristic p. *Amer. J. of Math.*, Vol. 91 No. 3: 772-784, 1969.
5. H. Matsumura. *Commutative Ring Theory.* Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1986, Translated from the Japanese by M. Reid. MR MR879273 (88h:13001)
6. H. Matsumura. *Commutative Algebra.* W.A. Benjamin, Inc., New York, 1970.
7. P. Monsky. The Hilbert-Kunz function. *Math. Ann.* 263: 43-49, 1983.
8. D. Rees. $\mathfrak{a}$-transforms of local rings and a theorem on multiplicities of ideals. *Proc. Cambridge Phil. Soc* 57: 8-17, 1961.
9. I. Swanson and C. Huneke. *Integral Closure of Ideals, Rings, and Modules.* Cambridge University Press, Cambridge, 2006.

Department of Mathematics, University of Nebraska-Lincoln, Lincoln, NE 68588-0130
E-mail address: s-lmcdonn1@math.unl.edu