Math 711: Lecture of November 29, 2006

We aim to prove the following result of Paul Monsky, following his paper [P. Monsky, *The Hilbert-Kunz function*, Mathematische Annalen **263** (1983) 43–49].

Theorem (Monsky). *Let $(R,\, m,\, K)$ be local where R has prime characteristic $p > 0$, let $\mathfrak{A}$ be an m-primary ideal, and let M be a finitely generated R-module of Krull dimension d. Then*

$$\lim_{n\to\infty} \frac{\ell(M/\mathfrak{A}^{[p^n]}M)}{p^{nd}}$$

exists, and is a positive real number.

The function whose value on n is $\ell(M/\mathfrak{A}^{[p^n]}M)$ is called the *Hilbert-Kunz function* of M with respect to $\mathfrak{A}$ and we denote its value on n by $\mathcal{F}_{HK}(\mathfrak{A},\, M)(n)$. If $\mathfrak{A} = m$, we may simply write $\mathcal{F}_{HK}(M)(n)$.

The limit, which we have not yet proved exists, is called the *Hilbert-Kunz multiplicity* of M with respect to $\mathfrak{A}$. We denote it by $e_{HK}(\mathfrak{A},\, M)$. If $\mathfrak{A} = m$, we write simply $e_{HK}(M)$.

Example. Let

$$R = K[[X,\, Y,\, Z]]/(XY - Z^d) = K[[x,\, y,\, z]],$$

where K is a field and X, Y, Z are formal indeterminates. Here, $m = (x,\, y,\, z)R$. Note that R is a normal hypersurface, and

$$R \cong S = K[[U^d,\, V^d, UV]] \subseteq K[[U,\, V]],$$

the formal power series ring in two variables. We shall show that $e_{HK}(R) = 2 - \dfrac{1}{d}$.

Every element of R can be written uniquely in the form $x^iy^jz^k$ where $0 \leq k \leq d-1$. The quotient ring $R/(x^q,\, y^q)R$, where $q = p^n$, has a K-basis consisting of the elements $x^iy^jz^k$, $0 \leq i \leq q-1$, $0 \leq j \leq q-1$, and $0 \leq k \leq d-1$. We can write $q = p^n = a_nd + r_n$ where $a_n \in \mathbb{N}$ and $0 \leq r_n \leq d-1$. Then $z^q = z^{a_nd}z^{r_n} = (xy)^{a_n}z^{r_n}$. As we multiply by z, z^2, $\ldots$ we obtain as multiples all the elements $x^{a_n}y^{a_n}z^s$ for $1 \leq s \leq d-1$. Multiplying by z one more time yields $x^{a_n+1}y^{a_n+1}$. Of course, once we see that $x^iy^jz^k$ is 0 mod $(x^q,\, y^q,\, z^q)$, this also follows for $x^{i'}y^{j'}z^{k'}$ whenever $i' \geq i$, $j' \geq j$, and $k' \geq k$. From this we see that a K-basis for the quotient $R/m^{[q]} = R/(x^q,\, y^q,\, z^q)R$ consists of all monomials $x^iy^jz^k$ such that either

(1) $0 \leq i \leq a_n - 1$, $0 \leq j \leq q-1$, and $0 \leq k \leq d-1$ or

(2) $0 \leq i \leq q-1$, $0 \leq j \leq a_n - 1$, and $0 \leq k \leq d-1$ or

(3) $i = j = a_n$ and $0 \leq k < r_n$.

The number monomials satisfying (1) or (2) is $a_nqd + qa_nd$ while the number satisfying both conditions is a_n^2d. The number satisfying condition (3) is r_n. Hence, $\ell(R/m^{[q]}) = 2a_n^d - a_n^2d + r_n$. Note that since a_n is the integer part of q/d, it lies between $(q/d) - 1$ and q/d, and so $a_n/q \to 1/d$ as $n \to \infty$. Moreover, $0 \le r_n < d$ shows that $r_n/q^2 \to 0$ (for that matter, $r_n/q \to 0$) as $n \to \infty$. Hence,

$$\lim_{n \to infty} \frac{\ell(R/m^{[q]})}{q^2} = \frac{2d}{d} - \frac{d}{d^2} + 0 = 2 - \frac{1}{d}.$$

We next make some elementary observations:

Lemma. *Let (R, m, K) be local where R has prime characteristic $p > 0$, let $\mathfrak{A}$ be an m-primary ideal, and let M be a finitely generated R-module of dimension d.*

(a) *The values of the Hilbert Kunz function of M with respect to $\mathfrak{A}$ are independent of whether we regard the base ring as R, or as $R/\mathrm{Ann}_R M$. Hence, the question of whether the Hilbert-Kunz multiplicity exists is independent of which ring is regarded as the base ring.*

(b) *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be flat local such that $\mathfrak{n} = mS$. Then for all n,*

$$\mathcal{F}_{HK}(\mathfrak{A}, M)(n) = \mathcal{F}_{HK}(\mathfrak{A}, S \otimes_R M)(n),$$

and so the question of whether the Hilbert-Kunz multiplicity exists is not affected by base change from R to S. In particular, we may make a base change from R to $\widehat{R}$.

(c) *There exist positive real constants C and C' such that for all n,*

$$Cp^{nd} < \mathcal{F}_{HK}(\mathfrak{A}, M)(n) \le C'p^{nd}.$$

(d) *If $\mathfrak{A}$ is generated by part of a system of parameters for $R/\mathrm{Ann}_R M$, then $e_{HK}(\mathfrak{A}, M) = e_{\mathfrak{A}}(M)$.*

(e) *If $\mathfrak{A} \subseteq \mathfrak{B}$, then $\mathcal{F}_{HK}(\mathfrak{A}, M)(n) \ge \mathcal{F}_{HK}(\mathfrak{B}, M)(n)$ for all n, Hence, $e_{HK}(\mathfrak{A}, M) \ge e_{HK}(\mathfrak{B}, M)$ whenever they exist.*

(f) *Whenever it exists, $e_{HK}(\mathfrak{A}, M) \le e_{\mathfrak{A}}(M)$.*

Proof. Part (a) is obvvious. Part (b) follows from the fact that for any fnite length module N over R, $\ell_S(S \otimes_K N) = \ell_R(N)$ (if N has a finite filtration whose factors are h copies of $K = R/m$, then $S \otimes_K N$ has a filtration whose factors are h copies of $S \otimes_R K = S/mS = S/\mathfrak{n} = L$). One may apply this to each $N = M/\mathfrak{A}^{[q]}M$, noting that

$$S \otimes N \cong (S \otimes_R M)/(\mathfrak{A}S)^{[q]}(S \otimes_R M).$$

For part (c), note that if $\mathfrak{A}$ has k generators then $\mathfrak{A}^{kq} \subseteq \mathfrak{A}^{[q]} \subseteq \mathfrak{A}^q$, since a monomial in k elements of degree kq must have at least one individual exponent that is at least q. Hence,

$$(*) \quad \ell(M/(\mathfrak{A}^k)^q M) \geq \ell(M/\mathfrak{A}^{[q]}M) \geq \ell(M/\mathfrak{A}^q M).$$

The Hilbert polynomial of M with respect to $\mathfrak{A}$ has leading coefficient cn^d for a suitable positive real constant c. It follows that the upper bound in $(*)$ is asymptotic to $c(kq)^d = ck^q(q^d)$, while the lower bound is asymptotic cq^d, and the result follows.

Part (d) is immediate from the definition and Lech's formula for multiplicities with respect to parameter ideals.

Part (e) is obvious from the definition.

For part (f), first note that we can replace R by $R(t)$ as in part (b), and so assume that the residue class field is infinite. Second, we replace R by $R/\mathrm{Ann}_R M$ as in part (a). Let $x_1, \ldots, x_d$ by a system of parameters generating an ideal I that is a reduction of $\mathfrak{A}$. Then

$$e_{\mathfrak{A}}(M) = e_I(M) = e_{HK}(I,\, M) \geq e_{HK}(\mathfrak{A},\, M)$$

by part (e). $\square$

From part (b) of this Lemma, the problem of proving the existence of Hilbert-Kunz multiplicities reduces to the case where the local ring is complete. By the Proposition near the bottom of p. 1 of the Lecture Notes of November 1, we know that there is a flat local map from the complete ring $(R,\, m,\, K)$ to a local ring $(S, \mathfrak{n},\, L)$ such that $\mathfrak{n} = mS$ and L is algebraically closed. Therefore, we may also assume without loss of generality that K is algebraically closed. We shall see that this implies that $F : R \to R$ is module-finite.

Given $e \in \mathbb{N}$ and an R-module M we write ${}^eM$ for M viewed as an R-module via restriction of scalars via the map $F^e : R \to R$. Thus, with $u \in {}^eM$, $r \cdot u = r^{p^e}u$. When $F : R \to R$ is module-finite, so are its iterations F^e, and it follows that if M is finitely generated as an R-module, so is ${}^eM$. Moreover, $M \mapsto {}^eM$ is an exact functor from R-modules to R-modules: neither the underlying abelian groups nor the maps change when we apply this functor.

When K is perfect and N is a finite length R-module, ${}^eN$ is also a finite length R-module and, in fact, $\ell({}^eN) = \ell(N)$. To see this, suppose that N has a filtration by h copies of K. Then ${}^eN$ has a filtration by h copies of ${}^eK$, by the exactness of restriction of scalars. The action of m on ${}^eK$ is 0, and, although the action of K on ${}^eK$ is via the iterated Frobenius endomorphism F^e, $F^e : K \to K$ is an isomorphism, and so ${}^eK$ is a one-dimensional vector space over K, i.e., it is isomorphic with K. Note also that if $\mathfrak{B}$ is any ideal of R, then $\mathfrak{B}({}^eM)$, under the abelian group identification of ${}^eM$ with M, becomes $\mathfrak{B}^{[p^e]}M$. Thus,

$${}^eM/(\mathfrak{B}\,{}^eM) = {}^e(M/\mathfrak{B}^{[p^e]}M).$$

From these remarks we obtain:

Proposition. *Let $(R,\, m,\, K)$ be local of prime characteristic $p > 0$ such that $F : R \to R$ is module-finite. Suppose also that K is pefect. Let $\mathfrak{A} \subseteq m$ be any m-primary ideal. Let M be a finitely generated R-module of dimension d. Then for every nonnegative integer n, $\mathcal{F}_{HK}(\mathfrak{A},\, {}^eM)(n) = \mathcal{F}_{HK}(\mathfrak{A},\, M)(n+e)$, and so if $e_{HK}(\mathfrak{A},\, {}^eM)$ exists, so does $e_{HK}(\mathfrak{A},\, M)$, and $e_{HK}(\mathfrak{A},\, {}^eM) = p^{ed}e_{HK}(\mathfrak{A},\, M)$.*

Proof. We have that

$$\mathcal{F}_{HK}(\mathfrak{A},\, {}^eM)(n) = \ell\big({}^eM/(\mathfrak{A}^{[p^n]})^e M\big) = \ell(M/(\mathfrak{A}^{[p^n]})^{[p^e]}M)$$

$$= \ell(M/\mathfrak{A}^{[p^{n+e}]}M) = \mathcal{F}_{HK}(\mathfrak{A},\, M)(n+e)$$

for all n, and so

$$e_{HK}(\mathfrak{A},\, M) = \lim_{n\to\infty} \frac{\mathcal{F}_{HK}(\mathfrak{A},\, M)(n+e)}{p^{(n+e)d}} = \frac{1}{p^{ed}} \lim_{n\to\infty} \frac{\mathcal{F}_{HK}(\mathfrak{A},\, {}^eM)(n)}{p^{nd}} = \frac{1}{p^{ed}} e_{HK}(\mathfrak{A},\, {}^eM),$$

as required. □

We also have:

Lemma. *Let $(R,\, m,\, K)$ be local of prime characteristic $p > 0$, let M be a finitely generated R-module of dimension d, and let $\mathfrak{A} \subseteq M$ be m-primary.*

(a) *If $N \subseteq M$ is such that $\dim(N) < \dim(M)$, then for all $n \geq 0$*

$$\mathcal{F}_{HK}(\mathfrak{A},\, M/N)(n) \leq \mathcal{F}_{HK}(\mathfrak{A},\, M)(n) \leq \mathcal{F}_{HK}(\mathfrak{A},\, M/N)(n) + Cp^{(d-1)n}.$$

Hence,

$$|\mathcal{F}_{HK}(\mathfrak{A},\, M)(n) - \mathcal{F}_{HK}(\mathfrak{A},\, M/N)(n)| \leq Cp^{(d-1)n},$$

and so $e_{HK}(\mathfrak{A},\, M/N)$ and $e_{HK}(\mathfrak{A},\, M)$ exist or not alike, and, if they exist, are equal.

(b) *Let M' be another finitely generated R-module of dimension d, and let W be a multiplicative system in R consisting of nonzerodivisors on M and on M'. If $W^{-1}M = W^{-1}M'$, then there exists a positivive constant C such that for all $n \geq 0$,*

$$|\mathcal{F}_{HK}(\mathfrak{A},\, M)(n) - \mathcal{F}_{HK}(\mathfrak{A},\, M')(n)| \leq Cp^{(d-1)n}.$$

Hence, $e_{HK}(\mathfrak{A},\, M')$ and $e_{HK}(\mathfrak{A},\, M)$ exist or not alike, and, if they exist, are equal.

Proof. For part (a), note that for every $q = p^n$ we have, with $\overline{M} = M/N$, the exact sequence

$$N/\mathfrak{A}^{[q]}N \to M/\mathfrak{A}^{[q]}M \to \overline{M}/\mathfrak{A}^{[q]}\overline{M} \to 0,$$

and while the first map need not be injective, we still have that the length of the module in the middle is at most the sum of the lengths of the other two modules. The inequality on the right is exactly this statement, while the inequality on the left is immediate from the surjectivity of the map on the right. The bound on the absolute value of the difference follows at once, and so does the final statement once we divide by q^d.

To prove part (b), note that we have a map $M \hookrightarrow W^{-1}M'$ that becomes an isomorphism when we localize at W. Choose $w \in W$ to be the product of the denominators of the images of a finite set of generators for M. Then the injection maps $wM \hookrightarrow M'$, and since $M \cong wM$ we have an injection $M \hookrightarrow M'$ whose cokernel Q is killed by an element of W, which implies that $\dim(Q) \leq \dim(M)$. The short exact sequences

$$M/\mathfrak{A}^{[q]}M \to M/\mathfrak{A}^{[q]}M' \to Q/\mathfrak{A}^{[q]}Q \to 0$$

yield inequalities

$$\mathcal{F}_{HK}(\mathfrak{A},\, M')(n) \leq \mathcal{F}_{HK}(\mathfrak{A},\, M)(n) + C_1 p^{nd}$$

for some real constant C_1 and for all n, using part (a). In an exactly similar way, there is a short exact sequence

$$0 \to M' \to M \to Q' \to 0$$

with $\dim(Q') < d$, and we obtain

$$\mathcal{F}_{HK}(\mathfrak{A},\, M)(n) \leq \mathcal{F}_{HK}(\mathfrak{A},\, M')(n) + C_2 p^{nd}$$

for all n. The inequality we need now follows with $C = \max\{C_1,\, C_2\}$, and the final statement is obvious. □

Discussion: the existence of Hilbert-Kunz multiplicities reduces to the case of complete local domains with perfect residue class field. We have already seen that the existence of Hilbert-Kunz multiplicities reduces to the case where the ring is complete local with algebraically closed residue class field. In particular, the residue class field may be assumed to be perfect. By part (a) of the Lemma above, we may reduce to the case where M has pure dimension. We may replace R by $R/\mathrm{Ann}_R M$ and therefore suppose that M is faithful, and so that M and R have the same minimal primes, which are also the associated primes of M.

Let W be the multiplicative system of elements not in any minimal prime of R, which consists of nonzerodivisors on M. Then $W^{-1}M$ is a module over $W^{-1}R$, which is a semilocal Artin ring, and so is the product of its localizations at the various minimal primes P_i, $1 \leq i \leq h$, of R. Hence,

$$W^{-1}M \cong \prod_{i=1}^{h} M_{P_i} = \bigoplus_{i=1}^{h} M_{P_i}.$$

Choose a power of P_i that kills M_{P_i}, say $P_i^{N_i}$, and let $M_i = \mathrm{Ann}_M P_i^{N_i}$. Every element of M_{P_i} can be multiplied into the image of M by an element of $R - P_i$, and, if we multiply further by an element of $R - P_i$, we obtain a multiple in M_i. Thus, $(M_i)_{P_i} = M_{P_i}$. The M_i

are mutually disjoint, however: a nonzero element of M cannot be killed by both a power of P_i and a power of P_j for $i \neq j$, or else M will have an associated prime containing both P_i and P_j. Thus,

$$M_1 \oplus M_2 \oplus \cdots \oplus M_h \subseteq M$$

and the two become equal when we localize at W. Therefore, to show that the Hilbert-Kunz multiplicity of M exists, it suffices to show this for every M_i.

We can therefore reduce to the case where $\mathrm{Ass}\,(M)$ contains a unique associated prime P. Replacing R by $R/\mathrm{Ann}_R M$, we may also assume that R has a unique minimal prime P. Choose e so large that $P^{[p^e]} = 0$. To show that the Hilbert-Kunz multiplicity of M exists, it suffices to prove this for ${}^eM$ instead. But P kills ${}^eM$, which is consequently a module over R/P. We have therefore reduced to the case where R is a complete local domain with perfect residue class field and $\dim\,(M) = \dim\,(R)$. Moreover, M has no nonzero submodule of smaller dimension, which implies that M is torsion-free over R. Now choose $R^\rho \subseteq M$ such that ρ is the torsion-free rank of M over R. Then M/R^ρ is torsion, and so we have reduced to considering the case where $M = R^\rho$. But then we have reduced to the case where $M = R$, as required. □

It remains to prove the case where $M = R$ is a complete local domain with perfect residue class field. This is the most interesting part of the argument.