UNIVERSITATIS IAGELLONICAE ACTA MATHEMATICA, FASCICULUS XLV
2007

# COMPUTING HILBERT–KUNZ FUNCTIONS OF 1-DIMENSIONAL GRADED RINGS

BY MARTIN KREUZER

**Abstract.** According to a theorem of Monsky, the Hilbert–Kunz function of a 1-dimensional standard graded algebra $R$ over a finite field $K$ has, for $i \gg 0$, the shape $\mathrm{HK}_R(i) = c(R) \cdot p^{\,i} + \varphi(i)$, where $c(R)$ is the multiplicity of $R$ and $\varphi$ is a periodic function. Here we study explicit computer algebra algorithms for computing such Hilbert–Kunz functions: the period length and the values of $\varphi$, as well as a concrete number $N \geq 0$ such that the description above holds for $i \geq N$.

**1. Introduction.** In his papers [**7**] and [**8**] E. Kunz introduced and studied the function $i \mapsto \ell(R/\mathfrak{m}^{[p^i]})$ for a noetherian local ring $(R, \mathfrak{m})$ of characteristic $p$, where $\mathfrak{m}^{[p^i]}$ denotes the $i^{\text{th}}$ *Frobenius power* of $\mathfrak{m}$. He called it the *length of the Frobenius fibers*. Later, in [**6**], P. Monsky called it the *Hilbert–Kunz function* of $R$ and used results about linear recurrence relations to show that this function grows like $c(R) \cdot p^{di}$, where $c(R) \in \mathbb{R}$ is the *Hilbert–Kunz multiplicity* of $R$ and $d = \dim(R)$.

Here we want to examine the task of determining Hilbert–Kunz functions completely using the methods and tools of computer algebra. Since general noetherian local rings are not amenable to exact computation, we work in the following setting. Let $K$ be an algebraic extension field of $\mathbb{F}_p$, let $R = K[x_0, \ldots, x_n]/I$ be a standard graded $K$-algebra, and let $\mathrm{HK}_R(i) = \dim_K R/\langle \bar{x}_0^{p^i}, \ldots, \bar{x}_n^{p^i} \rangle$ be its Hilbert–Kunz function. For 1-dimensional rings $R$, an easy adjustment of the proof of Monsky's theorem (cf. [**6**], Theorem 3.10) yields the following result.

2000 *Mathematics Subject Classification.* Primary 13P10; Secondary 13D40, 13A35.
*Key words and phrases.* Hilbert–Kunz function, Frobenius morphism.

THEOREM 1.1. *If* $\dim(R) = 1$, *there are a number* $c(R) \in \mathbb{R}$ *and a periodic function* $\varphi : \mathbb{N} \to \mathbb{N}$ *such that* $\mathrm{HK}_R(i) = c(R) \cdot p^i + \varphi(i)$ *for all* $i \gg 0$.

It is known that, in the case at hand, the number $c(R)$ is the usual multiplicity of $R$ (see [**6**], Section 1) which can be computed from a system of generators of $I$ by the method described in [**5**], Section 5.4. It is also clear that individual values of $\mathrm{HK}_R(i)$ can be found effectively via Macaulay's Basis Theorem (cf. [**4**], Theorem 1.5.7 and [**5**], 5.1.19). Hence we shall consider here the following questions.

(1) How can one compute $\varphi$? Is there a bound for the length of the period of $\varphi$?
(2) How can one find $N \geq 0$ such that $\mathrm{HK}_R(i) = c(R) \cdot p^i + \varphi(i)$ holds for $i \geq N$?

In Sections 2, 3, and 4 we shall reduce our task of computing the Hilbert–Kunz function of a 1-dimensional graded ring to a problem for 0-dimensional subschemes of projective spaces with $K$-rational support. Then we shall answer the above questions in Section 5 by giving a description of $\mathrm{HK}_R(i)$ which is slightly more precise than Theorem 1.1. (Notice that our proof differs from Monsky's proof since it does not use linear recurrence relations.) In the final section we provide some examples and applications. In particular, we shall see that the homogeneous coordinate ring $R$ of a set of $s$ $\mathbb{F}_p$-rational points in $\mathbb{P}^n$ has Hilbert–Kunz function $\mathrm{HK}_R(i) = s\,p^i - s + 1$, independent of the geometric constellation of the points.

All reduction steps and also the final answer are spelled out in explicit algorithms, ready for implementation in computer algebra systems. A prototype was implemented by the author's former student V. Augustin using the system CoCoA (see [**2**]), was described in [**1**], and is available via the author's web page.

It is natural to ask whether similar algorithms can be constructed also for higher-dimensional graded rings. In general, this is not yet possible since the precise shape of the Hilbert–Kunz function is unknown. The author plans to consider the case $\dim(R) = 2$, for which some additional results are available, in a future paper.

Unless explicitly stated otherwise, we use the definitions and notations introduced in [**4**] and [**5**].

**2. Basic definitions and reductions.** Throughout this paper, we let $p$ be a prime number and $\mathbb{F}_p$ the field with $p$ elements. For reasons which will become clear soon, we work over a field $K$ which is algebraic over $\mathbb{F}_p$. Moreover, we assume that we are given a standard graded $K$-algebra $R = \bigoplus_{i \geq 0} R_i$ via a presentation $R = K[x_0, \ldots, x_n]/I$, where the polynomial ring $K[x_0, \ldots, x_n]$

is graded by $\deg(x_i) = 1$ for $i = 0, \ldots, n$ and $I$ is a homogeneous ideal. The homogeneous maximal ideal of $R$ is $\mathfrak{m} = \bigoplus_{i>0} R_i$. It is generated by the residue classes $\bar{x}_i = x_i + I$ of the indeterminates. In this setting, the Hilbert–Kunz function of $R$ is defined as follows.

DEFINITION 2.1. For every $i \geq 0$, the ideal

$$\mathfrak{m}^{[p^i]} = \langle r^{p^i} \mid r \in \mathfrak{m} \rangle = \langle x_0^{p^i}, \ldots, x_n^{p^i} \rangle$$

is called the $i^{\text{th}}$ *Frobenius power* of $\mathfrak{m}$.

The function $\mathrm{HK}_R : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $i \longmapsto \dim_K(R/\mathfrak{m}^{[p^i]})$ is called the *Hilbert–Kunz function* of $R$.

It is easy to see that the Hilbert–Kunz function of $R$ does not change if we enlarge the base field $K$ (see [**4**], 2.4.16 and [**5**], 5.1.20). More precisely, for any extension field $L \supseteq K$, the standard graded $L$-algebra $S = L \otimes_K R = L[x_0, \ldots, x_n]/I\,L[x_0, \ldots, x_n]$ satisfies $\mathrm{HK}_S(i) = \mathrm{HK}_R(i)$ for all $i \geq 0$. In particular, we may always extend $K$ to any subfield $L$ of the algebraic closure $\overline{\mathbb{F}}_p$ such that $K \subseteq L \subseteq \overline{\mathbb{F}}_p$.

The first and most basic reduction of our task is to show that it suffices to work over a base field $K$ which is a finitely generated algebraic extension of $\mathbb{F}_p$. In other words, we may assume that $K = \mathbb{F}_q$ is a finite field having $q = p^e$ elements for some $e > 0$. In fact, we may use the field of definition of $I$ which is defined as follows.

DEFINITION 2.2. Let $k \subseteq K$ be a subfield and let $I$ be an ideal in $K[x_0, \ldots, x_n]$.

(a) We say that $I$ is *defined over* $k$ if there exist polynomials in $k[x_0, \ldots, x_n]$ which generate $I$ as an ideal in $K[x_0, \ldots, x_n]$.
(b) The field $k$ is called a *field of definition* of $I$ if $I$ is defined over $k$ and there is no proper subfield $k' \subset k$ such that $I$ is defined over $k'$.

The field of definition of a polynomial ideal can be computed using the following result (see [**4**], Theorem 2.4.17).

THEOREM 2.3. *Every polynomial ideal $I \subseteq K[x_0, \ldots, x_n]$ has a unique field of definition $k$. We may compute $k$ by choosing a term ordering $\sigma$, computing the reduced $\sigma$-Gröbner basis $G$ of $I$, and adjoining the coefficients of the polynomials in $G$ to the prime field $\mathbb{F}_p$.*

In our setting the field of definition of $I$ is a finite field $K_0 = \mathbb{F}_{q_0}$ with $q_0 = p^{e_0}$ for some $e_0 > 0$. We let $I_0 = I \cap K_0[x_0, \ldots, x_n]$ and $R_0 = K_0[x_0, \ldots, x_n]$. Then we have $R = K \otimes_{K_0} R_0$, and therefore $\mathrm{HK}_R(i) = \mathrm{HK}_{R_0}(i)$ for all $i \geq 0$. Let us summarize the discussion so far.

COROLLARY 2.4. *For the purpose of computing the Hilbert–Kunz function of the ring $R = K[x_0, \ldots, x_n]/I$, we may choose any field $\widetilde{K}$ such that $K_0 \subseteq \widetilde{K} \subseteq \overline{\mathbb{F}}_p$ and compute the Hilbert–Kunz function of $\widetilde{R} = \widetilde{K} \otimes_{K_0} R_0$.*

In the sequel we shall always use rings $R = K[x_0, \ldots, x_n]/I$ for which $K = \mathbb{F}_q$ satisfies $q = p^e$ and $e \geq e_0$. By the corollary, we may repeatedly replace $K$ by finite extension fields.

**3. Reduction to the Cohen–Macaulay case.** From here on we shall assume that $\dim(R) = 1$. Next we want to reduce our problem to the case in which $R$ is a Cohen–Macaulay ring and $\bar{x}_0 \in R_1$ is a homogeneous non-zerodivisor of degree one. The failure of $R$ to be a Cohen–Macaulay ring is measured by its local cohomology module

$$J = H^0_{\mathfrak{m}}(R) = \{r \in R \mid \mathfrak{m}^i \cdot r = 0 \text{ for some } i \geq 0\}.$$

Since $J$ is a homogeneous ideal in $R$, we may form the residue class ring $\overline{R} = R/J$. Letting $\overline{\mathfrak{m}}$ be the residue class ideal of $\mathfrak{m}$, it follows that $H^0_{\overline{\mathfrak{m}}}(\overline{R}) = 0$. Thus the ring $\overline{R}$ contains a homogeneous non-zerodivisor, i.e., it is a 1-dimensional Cohen–Macaulay ring.

The ideal $J$ is finitely generated. Hence it is annihilated by a sufficiently high power of $\mathfrak{m} = \langle \bar{x}_0, \ldots, \bar{x}_n \rangle$. Consequently, the ideal $J$ is a finite-dimensional $K$-vector space and the Hilbert functions of $R$ and $\overline{R}$ agree except for finitely many degrees.

Based on this discussion we can now formulate the algorithm for the reduction to the Cohen–Macaulay case. Recall that the *Hilbert series* of a 1-dimensional standard graded $K$-algebra $R$ is of the form $\mathrm{HS}_R(z) = \frac{\mathrm{hn}_R(z)}{1-z}$, where $\mathrm{hn}_R(z) \in \mathbb{Z}[z]$ is the *simplified Hilbert numerator* of $R$ (see [**5**], 5.4.1).

ALGORITHM 3.1. *Let $R = K[x_0, \ldots, x_n]/I$ be a 1-dimensional standard graded ring. Assume that there exists an algorithm for computing the Hilbert–Kunz function of an 1-dimensional standard graded Cohen–Macaulay ring. Consider the following instructions.*

*(1) Compute the ideal $I^{\mathrm{sat}} = I : \mathfrak{M}^\infty$, where $\mathfrak{M} = \langle x_0, \ldots, x_n \rangle$, and let $\overline{R} = K[x_0, \ldots, x_n]/I^{\mathrm{sat}}$.*

*(2) Compute the Hilbert series $\mathrm{HS}_R(z)$ and $\mathrm{HS}_{\overline{R}}(z)$ and set $p(z) = \mathrm{HS}_R(z) - \mathrm{HS}_{\overline{R}}(z)$. Let $r = \deg(p(z))$ and $c = p(1)$.*

*(3) Determine a number $N' \geq 0$ and a tuple $(\varphi'_0, \ldots, \varphi'_{m-1})$ such that we have $\mathrm{HK}_{\overline{R}}(i) = \mathrm{mult}(\overline{R}) \cdot p^i + \varphi'_{i \bmod m}$ for all $i \geq N'$.*

*(4) Return $N = \max\{N', \lceil \log_p(r+1) \rceil\}$ and the tuple $(\varphi_0, \ldots, \varphi_{m-1})$, where $\varphi_i = \varphi'_i + c$ for $i = 0, \ldots, m-1$.*

*This is an algorithm which returns a number $N \geq 0$ and a tuple $(\varphi_0, \ldots, \varphi_{m-1})$ such that $\mathrm{HK}_R(i) = \mathrm{mult}(R) \cdot p^i + \varphi_{i \bmod m}$ for all $i \geq N$.*

PROOF. As shown above, the ring $\overline{R} = K[x_0, \ldots, x_n]/(I : \mathfrak{M}^\infty) = R/(0 : \mathfrak{m}^\infty) = R/J$ is a 1-dimensional standard graded Cohen–Macaulay ring. The

Hilbert series $\mathrm{HS}_J(z) = p(z) = \mathrm{HS}_R(z) - \mathrm{HS}_{\overline{R}}(z)$ is a polynomial, since $J$ is a finite-dimensional $K$-vector space. We have $\dim_K(J) = \mathrm{HF}_J(0) + \cdots + \mathrm{HF}_J(r) = p(1) =: c$, and the Hilbert functions of $R$ and $\overline{R}$ agree in degrees $i \geq r+1$. For these degrees we have $\mathrm{HF}_R(i) = \mathrm{HF}_{\overline{R}}(i) + c$. Moreover, it follows that $\mathrm{mult}(R) = \mathrm{mult}(\overline{R})$.

Next we use the homogeneous short exact sequence

$$0 \longrightarrow (\mathfrak{m}^{[p^i]} + J)/\mathfrak{m}^{[p^i]} \longrightarrow R/\mathfrak{m}^{[p^i]} \longrightarrow R/(\mathfrak{m}^{[p^i]} + J) \longrightarrow 0.$$

For $i \geq \lceil \log_p(r+1) \rceil$ we have $p^i > r$, and therefore $J \cap \mathfrak{m}^{[p^i]} = 0$. This implies $(\mathfrak{m}^{[p^i]} + J)/\mathfrak{m}^{[p^i]} \cong J$, and hence $\mathrm{HS}_R(i) = \mathrm{HS}_{\overline{R}}(i) + c$. Altogether, we see that the correct Hilbert–Kunz function is computed by Step 4. □

To be able to translate the desired computation into the language of algebraic geometry, we would like to make sure that the element $\bar{x}_0 \in R_1$ is a non-zerodivisor. At the moment we only know that $R$ contains *some* homogeneous non-zerodivisor, but not necessarily a linear one. After we have performed the desired reduction, the support of the 0-dimensional projective subscheme $\mathbb{X} = \mathrm{Proj}(R)$ of $\mathbb{P}^n$ is contained in the affine set $D_+(x_0) = \mathbb{P}^n \setminus \mathcal{Z}(x_0)$. The key is the following proposition.

PROPOSITION 3.2. *Let $R = K[x_0, \ldots, x_n]/I$ be a 1-dimensional standard graded Cohen–Macaulay algebra over a finite field $K = \mathbb{F}_q$. If $q > \mathrm{mult}(R)$ then there exists a homogeneous non-zerodivisor $\ell \in R_1$ of degree one for $R$.*

PROOF. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the minimal primes of $R$. Since $R$ is a Cohen–Macaulay ring, an element $\ell \in R_1$ is a non-zerodivisor for $R$ if and only if $\ell \notin \mathfrak{p}_i$ for $i = 1, \ldots, s$. Each $\mathfrak{p}_i \cap R_1$ is a proper $K$-vector subspace of $R_1$, since the homogeneous maximal ideal $\mathfrak{m} = \langle R_1 \rangle$ is not associated. The hypothesis $q > \mathrm{mult}(R) \geq s$ implies that the $K$-vector space $R_1$ cannot be covered by $s$ proper vector subspaces. Hence $R_1 \setminus \bigcup_{i=1}^s \mathfrak{p}_i$ is not empty. □

In principle we should compute the primary decomposition of $I$ to find a linear non-zerodivisor $\ell \in R_1$ as in this proposition. However, in practice it is much easier to try random elements $L \in K[x_0, \ldots, x_n]$ and check whether $I : L \subseteq I$ (for instance, using one of the methods in [**4**], Section 3.2.B). The probability of success is $\frac{q-s}{q}$. Since finite base field extensions and homogeneous linear changes of coordinates do not alter the Hilbert–Kunz function of $R$, the desired reduction of the problem can be achieved as follows.

ALGORITHM 3.3. *Let $R = K[x_0, \ldots, x_n]/I$ be a 1-dimensional standard graded Cohen–Macaualy ring. Consider the following instructions.*

*(1) Compute* $\mathrm{mult}(R)$. *If $q \leq \mathrm{mult}(R)$, enlarge the base field $K$ to a field $K' = \mathbb{F}_{q'}$ with $q' > \mathrm{mult}(R)$. Otherwise, use $K' = K$.*

*(2) Let $R' = K' \otimes_K R$. Simplify the presentation of $R'$ such that $I \cap R'_1 = 0$.*
*(3) Try one element $L \in K'[x_0, \ldots, x_n]$ after another until one is found for which $I : L \subseteq I$.*
*(4) Perform a homogeneous linear change of coordinates such that $L$ is $x_0$ in the new coordinates. Return the transformed ideal $I'$.*

*This is an algorithm which computes a 1-dimensional standard graded Cohen–Macaulay ring $R' = K'[x_0, \ldots, x_n]/I'$ which has the same Hilbert–Kunz function as $R$ and for which $\bar{x}_0 \in R'_1$ is a non-zerodivisor.*

**4. Reduction to rational support.** In this section we assume that $R = K[x_0, \ldots, x_n]/I$ is a 1-dimensional standard graded Cohen–Macaulay $K$-algebra such that $\bar{x}_0 \in R_1$ is a non-zerodivisor for $R$. Let $\mathbb{X} = \mathrm{Proj}(R)$ be the subscheme of $\mathbb{P}^n_K$ defined by $I$. The subscheme $\overline{\mathbb{X}} = \mathrm{Proj}(\overline{R})$ of the projective space over the algebraic closure $\overline{K}$ of $K$ whose homogeneous coordinate ring is $\overline{R} = \overline{K} \otimes_K R$ is zero-dimensional and has a finite support $\mathrm{Supp}(\overline{\mathbb{X}}) = \{p_1, \ldots, p_s\}$.

Our goal in this section is to compute a finite extension field $K'$ such that the points $p_i$ have their coordinates in $K'$. If we then replace $R$ by $R' = K' \otimes_K R$, we have reduced the problem to the case in which $\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ with prime ideals $\mathfrak{p}_i$ which are homogeneous vanishing ideals of $K'$-rational points in $\mathbb{P}^n_{K'}$.

The first step towards this goal is to observe that we are really in an affine situation. More precisely, we have the following results (see [**3, 5, 9**]).

Proposition 4.1. *In the above setting, let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ and $\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ be the primary decompositions of $I$ and $\sqrt{I}$, respectively, where $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$.*
*(a) The ideal $J = I^{\mathrm{deh}} := \langle f(1, x_1, \ldots, x_n) \mid f \in I \rangle$ of $K[x_1, \ldots, x_n]$ is the affine vanishing ideal of $\mathbb{X}$, considered as a subscheme of the affine space $\mathbb{A}^n \cong D_+(x_0)$.*
*(b) The primary decomposition of $J$ is $J = \mathfrak{q}_1^{\mathrm{deh}} \cap \cdots \cap \mathfrak{q}_s^{\mathrm{deh}}$.*
*(c) For $i = 1, \ldots, s$, the ideal $\mathfrak{q}_i^{\mathrm{deh}}$ is primary to the prime ideal $\mathfrak{p}_i^{\mathrm{deh}}$.*
*(d) The primary decomposition of $\sqrt{J} = (\sqrt{I})^{\mathrm{deh}}$ is $\sqrt{J} = \mathfrak{p}_1^{\mathrm{deh}} \cap \cdots \cap \mathfrak{p}_s^{\mathrm{deh}}$.*

In view of this proposition, it will be sufficient to enlarge $K$ to $K'$ such that the ideals $(\mathfrak{p}_i^{\mathrm{deh}})'$ appearing in the primary decomposition of the extension of $\sqrt{J}$ are vanishing ideals of reduced $K'$-points. Furthermore, the following algorithm enables us to compute the radical ideal $\sqrt{J}$. (For a proof, see e.g. [**4**], Corollary 3.7.16.)

Algorithm 4.2. *Let $J \subset K[x_1, \ldots, x_n]$ be a 0-dimensional ideal. Then the following instructions compute the radical $\sqrt{J}$.*

*(1) For $i = 1, \ldots, n$, compute a generator $g_i \in K[x_i]$ of the elimination ideal $J \cap K[x_i]$.*
*(2) Compute the squarefree parts* $\mathrm{sqfree}(g_1), \ldots, \mathrm{sqfree}(g_n)$.
*(3) Return the ideal* $\sqrt{J} = J + \langle \mathrm{sqfree}(g_1), \ldots, \mathrm{sqfree}(g_n) \rangle$.

The next step is intended to prepare $\sqrt{J}$ for an application of the Shape Lemma (see [**5**], Theorem 3.7.25). We want to bring $\sqrt{J}$ into *normal $x_n$-position*. This means that we want to perform a linear change of coordinates such that the zeros of $\widetilde{J} = \sqrt{J}$ in $\overline{K}^n$ have pairwise different $x_n$-coordinates.

ALGORITHM 4.3. *Let $\widetilde{J}$ be a 0-dimensional radical ideal in $K[x_1, \ldots, x_n]$. The following instructions define an algorithm which bring $\widetilde{J}$ into normal $x_n$-position.*

*(1) Compute* $t = \dim_K(K[x_1, \ldots, x_n]/\widetilde{J})$.
*(2) If $q \leq \binom{t}{2}$, enlarge $K$ until it has more than $\binom{t}{2}$ elements.*
*(3) Compute the monic generator $g_n$ of the elimination ideal $\widetilde{J} \cap K[x_n]$. If* $\deg(g_n) = t$, *return the tuple $\tau = (x_1, \ldots, x_n)$ and the ideal $\widehat{J} = \widetilde{J}$ and stop.*
*(4) Repeat the following two steps until* $\deg(g_n) = t$. *Then return the tuple $\tau$ and the ideal $\widehat{J}$ and stop.*
*(5) Choose a non-zero tuple $(c_1, \ldots, c_{n-1}) \in K^{n-1}$ which has not been chosen before. Apply the linear change of coordinates $\tau = (x_1, \ldots, x_{n-1}, x_n - c_1x_1 - \cdots - c_{n-1}x_{n-1})$ to $\widetilde{J}$ and get*

$$\widehat{J} = \langle f(x_1, \ldots, x_{n-1}, x_n - c_1x_1 - \cdots - c_{n-1}x_{n-1}) \mid f \in \widetilde{J} \rangle.$$

*(6) Compute the monic generator $g_n$ of the elimination ideal $\widehat{J} \cap K[x_n]$.*

The correctness proof of this algorithm follows by combining Proposition 3.7.22 and Theorem 3.7.23 of [**5**]. Thus we may assume that $\sqrt{J}$ is in normal $x_n$-position. Now the following consequence of the Shape Lemma (see [**5**], Theorem 3.7.25) yields the desired base field extension.

ALGORITHM 4.4. *Let $\widehat{J}$ be a 0-dimensional radical ideal in $K[x_1, \ldots, x_n]$ which is in normal $x_n$-position. The following instructions define an algorithm which computes a finite extension field $K'$ of $K$ such that the primary decomposition of the extension ideal $\widehat{J}^{\mathrm{ext}} = \widehat{J}\,K'[x_1, \ldots, x_n]$ is of the form $\widehat{J}^{\mathrm{ext}} = \mathfrak{p}'_1 \cap \cdots \cap \mathfrak{p}'_t$, where each $\mathfrak{p}'_j$ is the vanishing ideal of a $K'$-rational point. The algorithm also computes the ideals $\mathfrak{p}'_j$.*

*(1) Compute the reduced* `Lex`*-Gröbner basis $G$ of $\widehat{J}$. It has the shape $G = \{x_1 - g_1, \ldots, x_{n-1} - g_{n-1}, g_n\}$, where $g_i \in K[x_i]$.*
*(2) Extend $K$ to a finite field $K'$ such that $g_n$ factors into linear factors in $K'[x_n]$. (E.g. if $[K' : K] \geq \deg(g_n)$ this is guaranteed.)*

*(3) Compute the zeros* $a_{n1}, \ldots, a_{nt} \in K'$ *of* $g_n$*. (E.g. use Berlekamps's Algorithm, cf.* [**4**]*, Tutorial 6.)*

*(4) For* $i = 1, \ldots, n-1$ *and* $j = 1, \ldots, t$*, calculate* $a_{ij} = g_i(a_{nj}) \in K'$*. Form the prime ideals* $\mathfrak{p}'_j = \langle x_1 - a_{1j}, \ldots, x_n - a_{nj} \rangle$ *in* $K'[x_1, \ldots, x_n]$*. Return* $K'$ *and the ideals* $\mathfrak{p}'_j$ *and stop.*

Notice that the primary decomposition $\widehat{J}^{\text{ext}} = \mathfrak{p}'_1 \cap \cdots \cap \mathfrak{p}'_t$ enables us to compute the primary decomposition of the ideal $\widetilde{J}^{\text{ext}} = \widetilde{J}\,K'[x_1, \ldots, x_n]$ by reverting the (known) linear change of coordinates $\tau$. Thus we obtain the points $(b_{1j}, \ldots, b_{nj}) \in (K')^n$ which are the zeros of $J' = J\,K'[x_1, \ldots, x_n]$, because $\widetilde{J}^{\text{ext}} = \sqrt{J'}$. The corresponding points $(1 : b_{1j} : \ldots : b_{nj}) \in \mathbb{P}^n_{K'}$ are the zeros of $I' = IK'[x_1, \ldots, x_n]$.

Moreover, letting $\tilde{\mathfrak{p}}_j = \langle x_1 - b_{1j}, \ldots, x_n - b_{nj} \rangle \subset K'[x_1, \ldots, x_n]$, we can use the fact that we know the primary decomposition $\widetilde{J}^{\text{ext}} = \tilde{\mathfrak{p}}_1 \cap \cdots \cap \tilde{\mathfrak{p}}_s$ to compute the primary decomposition of $J'$ by *isolation of primary components:* for $\mathfrak{q}'_j = J' : (J' : \tilde{\mathfrak{p}}_j^{\infty})$, we have $J' = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_t$. Finally, we can homogenize this primary decomposition. By [**9**], Chapter 7, we get the primary decomposition $I' = (\mathfrak{q}'_1)^{\text{hom}} \cap \cdots \cap (\mathfrak{q}'_t)^{\text{hom}}$ of $I'$.

By combining all these steps, we have found a finite extension field $K'$ of $K$ such that the extension ideal $I' = I\,K'[x_0, \ldots, x_n]$ has $K'$-rational zeros. Moreover, we have computed these zeros $p_j = (1 : b_{1j} : \cdots : b_{nj})$ and the primary components of $I'$ corresponding to these points. For ease of reference, we formulate an explicit algorithm.

ALGORITHM 4.5. *Let* $R = K[x_0, \ldots, x_n]/I$ *be a 1-dimensional standard graded Cohen–Macaulay K-algebra such that* $\bar{x}_0 \in R_1$ *is a non-zerodivisor for R. Consider the following instructions.*

*(1) By substituting* $x_0 \mapsto 1$ *in the generators of I, compute the dehomogenization* $J = I^{\text{deh}} \subset K[x_1, \ldots, x_n]$*.*

*(2) Using Algorithm 4.2, compute the radical* $\widetilde{J} = \sqrt{J}$*.*

*(3) Using Algorithm 4.3, compute a finite extension field* $\widehat{K}$ *of K and a linear change of coordinates* $\tau$ *such that the transformed ideal* $\widehat{J}$ *of the extension ideal* $\widetilde{J}\,\widehat{K}[x_1, \ldots, x_n]$ *is in normal* $x_n$*-position.*

*(4) Using Algorithm 4.4, compute a finite extension field* $K'$ *of* $\widehat{K}$ *and points* $p'_1, \ldots, p'_s \in (K')^n$ *such that* $\widehat{J}K'[x_1, \ldots, x_n] = \mathfrak{p}'_1 \cap \cdots \cap \mathfrak{p}'_s$*, where* $\mathfrak{p}'_i$ *is the vanishing ideal of* $p'_i$*.*

*(5) By reverting the linear change of coordinates* $\tau$*, compute the preimages* $\bar{p}_i$ *of the points* $p'_i$*. For* $i = 1, \ldots, s$*, let* $\bar{\mathfrak{p}}_i$ *be the vanishing ideal of* $p_i$ *in* $K'[x_1, \ldots, x_n]$*.*

*(6) For* $i = 1, \ldots, s$*, embed* $\bar{p}_i$ *in* $\mathbb{P}^n_{K'}$ *and get a projective point* $p_i$*, homogenize* $\bar{\mathfrak{p}}_i$ *and get* $\mathfrak{p}_i$*, and compute* $\mathfrak{q}_i = I' : (I' : \mathfrak{p}_i^{\infty})$*, where* $I' = I\,K'[x_1, \ldots, x_n]$*.*

*(7) Return $K'$, the points $p_1, \ldots, p_s \in \mathbb{P}^n_{K'}$, and the ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$.*
*This is an algorithm which computes a finite extension field $K'$ of $K$, points $p_1, \ldots, p_s \in \mathbb{P}^n_{K'}$ and ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \in K'[x_0, \ldots, x_n]$ such that the extension ideal $I' = I\,K'[x_0, \ldots, x_n]$ defines a projective scheme supported at $\{p_1, \ldots, p_s\}$, such that $I' = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ is the primary decomposition of $I'$, and such that $\mathfrak{q}_i$ is primary to the vanishing ideal $\mathfrak{p}_i$ of $p_i$ for $i = 1, \ldots, s$.*

**5. The main algorithm.** In this section we are finally ready to compute the Hilbert–Kunz function. We assume that we are given a 1-dimensional standard graded Cohen–Macaulay ring $R = K[x_0, \ldots, x_n]/I$ over a finite field $K = \mathbb{F}_q$ with $q = p^e$ elements such that $\bar{x}_0 = x_0 + I$ is a non-zerodivisor for $R$. Moreover, we assume that the points $p_1, \ldots, p_s$ in the support of the scheme $\mathbb{X} = \mathrm{Proj}(R)$ are $K$-rational, that the coordinates (and thus the homogeneous vanishing ideal $\mathfrak{p}_j$) of each $p_j$ are known, and that we have computed the $\mathfrak{p}_j$-primary component $\mathfrak{q}_j$ of $I$.

Let us recall some basic facts about 0-dimensional subschemes of projective spaces (see [**3**] and [**5**], Section 6.3). The Hilbert function $\mathrm{HF}_{\mathbb{X}} : \mathbb{Z} \longrightarrow \mathbb{N}$ of $\mathbb{X}$ is defined by $\mathrm{HF}_{\mathbb{X}}(i) = \dim_K(R_i)$. It satisfies

$$1 = \mathrm{HF}_{\mathbb{X}}(0) < \mathrm{HF}_{\mathbb{X}}(1) < \cdots < \mathrm{HF}_{\mathbb{X}}(a_{\mathbb{X}}) < \mathrm{HF}_{\mathbb{X}}(a_{\mathbb{X}}+1) = \mathrm{HF}_{\mathbb{X}}(a_{\mathbb{X}}+2) = \cdots$$

for some number $a_{\mathbb{X}} \geq -1$ which is called the *a-invariant* of $\mathbb{X}$ (or of $R$). The constant value $\deg(\mathbb{X}) = \mathrm{HF}_{\mathbb{X}}(i)$ for $i \geq a_{\mathbb{X}} + 1$ is called the *degree* of $\mathbb{X}$. The ring $S = R/(\bar{x}_0 - 1)$ is the affine coordinate ring of $\mathbb{X}$ in $\mathbb{A}^n_K \cong D_+(x_0) \subset \mathbb{P}^n_K$. It satisfies $S \cong \Gamma(\mathbb{A}^n_K, \mathcal{O}_{\mathbb{X}}) \cong \mathcal{O}_{\mathbb{X},p_1} \times \cdots \times \mathcal{O}_{\mathbb{X},p_s}$ and $\dim_K(S) = \deg(\mathbb{X})$.

For every $i \geq 0$, there exists an injective $K$-linear map

$$\varrho_i : R_i \longrightarrow \Gamma(\mathbb{A}^n_K, \mathcal{O}_{\mathbb{X}}(i)) \cong \mathcal{O}_{\mathbb{X},p_1} \times \cdots \times \mathcal{O}_{\mathbb{X},p_s}$$

which maps an element $r \in R_i$ to the tuple of its localizations. In particular, we have $\varrho_i(x_0^i) = (1, \ldots, 1)$ for all $i \geq 0$. The map $\varrho = \bigoplus_{i \geq 0} \varrho_i : R \longrightarrow \mathcal{O}_{\mathbb{X},p_1} \times \cdots \times \mathcal{O}_{\mathbb{X},p_s}$ is a homomorphism of $K$-algebras.

For every $i \in \{1, \ldots, s\}$, the local ring $\mathcal{O}_{\mathbb{X},p_i}$ is a 0-dimensional local $K$-algebra and thus a finite dimensional $K$-vector space (and consequently a finite set). Its maximal ideal will be denoted by $\mathfrak{m}_{\mathbb{X},p_i}$. Since $p_i$ is a $K$-rational point, we have $\mathcal{O}_{\mathbb{X},p_i}/\mathfrak{m}_{\mathbb{X},p_i} \cong K$. The following numbers are the last missing ingredients of our main algorithm.

Definition 5.1. For $i = 1, \ldots, s$, the number $\nu_i = \min\{j \geq 0 \mid \mathfrak{m}^j_{\mathbb{X},p_i} = 0\}$ is called the *nilpotency index* of $\mathbb{X}$ at the point $p_i$.

These nilpotency indices are easy to compute in our setting. Let $\bar{\mathfrak{p}}_i$ and $\bar{\mathfrak{q}}_i$ be the dehomogenizations of $\mathfrak{p}_i$ and $\mathfrak{q}_i$, respectively with regard to $x_0 \mapsto 1$.

Then the nilpotency index at $p_i$ satisfies $\nu_i = \min\{j \geq 0 \mid \bar{\mathfrak{p}}_i^j \subseteq \bar{\mathfrak{q}}_i\}$ for $i = 1, \ldots, s$.

Notice that $\mathcal{O}_{\mathbb{X},p_j}/\mathfrak{m}_{\mathbb{X},p_j} \cong K$ for $j = 1, \ldots, s$ implies for every $i \geq 0$ and $r \in R_i$ that the tuple $\varrho_i(r)$ is of the form $\varrho_i(r) = (\kappa_1 + \mu_1, \ldots, \kappa_s + \mu_s)$ with $\kappa_j \in K$ and $\mu_j \in \mathfrak{m}_{\mathbb{X},p_j}$. For all $k \geq 0$ such that $p^k \geq \max\{\nu_1, \ldots, \nu_s\}$, this yields $\varrho(r^{p^k}) = (\kappa_1^{p^k}, \ldots, \kappa_s^{p^k})$, because $(\kappa_j + \mu_j)^{p^k} = \kappa_j^{p^k} + \mu_j^{p^k} = \kappa_j^{p^k}$.

LEMMA 5.2. *Let $k \geq 0$ such that $p^k \geq \max\{\nu_1, \ldots, \nu_s\}$. Then the following formulas hold in $R$.*

*(a)* $\bar{x}_i^{p^{k+e}} = \bar{x}_0^{(q-1)p^k} \cdot \bar{x}_i^{p^k}$ *for* $i = 0, \ldots, n$,
*(b)* $\mathfrak{m}^{[p^{k+e}]} = \bar{x}_0^{(q-1)p^k} \cdot \mathfrak{m}^{[p^k]}$ *where* $\mathfrak{m} = \langle \bar{x}_0, \ldots, \bar{x}_n \rangle$.

PROOF. First we prove (a). For every $\kappa \in K$, the map $\psi_\kappa : \mathbb{N} \longrightarrow K$ defined by $i \mapsto \kappa^{p^i}$ is periodic with a period length dividing $e$, because we have $\kappa^{p^{i+e}} = (\kappa^{p^i})^q = \kappa^{p^i}$. Now we write $\varrho(\bar{x}_i) = (\kappa_{i1} + \mu_{i1}, \ldots, \kappa_{is} + \mu_{is})$ with $\kappa_{ij} \in K$ and $\mu_{ij} \in \mathfrak{m}_{\mathbb{X},p_j}$. Then we obtain

$$\varrho(\bar{x}_i^{p^{k+e}}) = (\kappa_{i1}^{p^{k+e}}, \ldots, \kappa_{is}^{p^{k+e}}) = (\kappa_{i1}^{p^k}, \ldots, \kappa_{is}^{p^k}) = \varrho(\bar{x}_0^{(q-1)p^k} \cdot \bar{x}_i^{p^k}).$$

Since the maps $\varrho_\ell$ are injective, the claim follows. Now (b) is a consequence of $\mathfrak{m}^{[p^{k+e}]} = \langle \bar{x}_0^{p^{k+e}}, \ldots, \bar{x}_n^{p^{k+e}} \rangle = \bar{x}_0^{(q-1)p^k} \cdot \langle \bar{x}_0^{p^k}, \ldots, \bar{x}_n^{p^k} \rangle = \bar{x}_0^{(q-1)p^k} \cdot \mathfrak{m}^{[p^k]}$. □

Our next theorem provides the desired sharpening of [**6**], Theorem 3.10.

THEOREM 5.3. *In the above setting, let $k \geq 0$ be such that $p^k \geq \max\{\nu_1, \ldots, \nu_s\}$.*

*(a) We have* $\mathrm{HK}_R(k+e) = \mathrm{HK}_R(k) + (\deg \mathbb{X})(q-1)p^k$.
*(b) There is a periodic function $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ whose period length divides $e$ such that* $\mathrm{HK}_R(\ell) = (\deg \mathbb{X})\, p^\ell + \varphi(\ell)$ *for all $\ell \geq 0$ satisfying $p^\ell \geq \max\{\nu_1, \ldots, \nu_s\}$.*

PROOF. First we show (a). By the lemma, we have $\mathrm{HK}_R(k+e) = \dim_K(R/\mathfrak{m}^{[p^{k+e}]}) = \dim_K(R/(\bar{x}_0^{(q-1)p^k} \cdot \mathfrak{m}^{[p^k]}))$. Since $R/\mathfrak{m}^{[p^k]}$ is a finite-dimensional $K$-vector space, we may choose an integer $N > a_{\mathbb{X}}$ such that $(R/\mathfrak{m}^{[p^k]})_N = 0$. Then we have $\dim_K(R_i) = \dim_K(\mathfrak{m}^{[p^k]})_i = \deg \mathbb{X}$ for all $i \geq N$. Moreover, the fact that $\bar{x}_0$ is a non-zerodivisor for $R$ implies $\dim_K(\bar{x}_0^{(q-1)p^k} \cdot \mathfrak{m}^{[p^k]})_i = \deg \mathbb{X}$

for all $i \geq N' = N + (q-1)\,p^k$. Therefore, we may calculate

$$\begin{aligned}
\dim_K(R/(\bar{x}_0^{(q-1)p^k} \cdot \mathfrak{m}^{[p^k]})) &= \sum_{i=1}^{N'} \dim_K(R_i) - \sum_{i=1}^{N'} \dim_K(\bar{x}_0^{(q-1)p^k} \cdot \mathfrak{m}^{[p^k]})_i \\
&= (\deg \mathbb{X})(q-1)p^k + \sum_{i=0}^{N} \dim_K(R_i) - \sum_{i=0}^{N} \dim_K(\mathfrak{m}^{[p^k]})_i \\
&= (\deg \mathbb{X})(q-1)p^k + \dim_K(R/\mathfrak{m}^{[p^k]}) \\
&= (\deg \mathbb{X})(q-1)p^k + \mathrm{HK}_R(k).
\end{aligned}$$

This proves (a). To show (b), we define a function $\psi : \mathbb{N} \longrightarrow \mathbb{N}$ by $\psi(\ell) = \mathrm{HK}_R(\ell) - (\deg \mathbb{X})\,p^\ell$. Then (a) implies $\psi(\ell+e) = \mathrm{HK}_R(\ell+e) - (\deg \mathbb{X})\,p^{\ell+e} = \mathrm{HK}_R(\ell) + (\deg \mathbb{X})(p^{\ell+e} - p^\ell) - (\deg \mathbb{X})\,p^{\ell+e} = \psi(\ell)$ for all $\ell \geq 0$ such that $p^\ell \geq \max\{\nu_1, \ldots, \nu_s\}$. Hence the function $\psi$ is ultimately periodic and its period length divides $e$. By modifying its first values accordingly, we obtain the desired periodic function $\varphi$. □

Based on this theorem and the reductions performed in the preceding sections, we can now state the main algorithm.

Algorithm 5.4. (HK-Algorithm for 1-Dimensional Graded Rings) *Let $p$ be a prime, let $K$ be an algebraic extension field of $\mathbb{F}_p$, let $I \subset K[x_0, \ldots, x_n]$ be a homogeneous ideal, and assume that $R = K[x_0, \ldots, x_n]/I$ is a 1-dimensional ring. Consider the following instructions.*

*(1) Compute $c(R) = \mathrm{mult}(R)$, a finite field $K_1 \subseteq K$ and a homogeneous ideal $I_1 \subset K_1[x_0, \ldots, x_n]$ such that $I = I_1\,K[x_1, \ldots, x_n]$.*

*(2) Using the method described in Algorithm 3.1, compute a number $N' \geq 0$ and an ideal $I_1' \subset K_1[x_0, \ldots, x_n]$ such that the Hilbert–Kunz functions of $R$ and $R' = K_1[x_0, \ldots, x_n]/I_1'$ agree in degree $i \geq N'$ and such that $R'$ is a Cohen–Macaulay ring.*

*(3) Using Algorithm 3.3, compute a finite extension field $K_2$ of $K_1$ and an ideal $I_2 \subset K_2[x_0, \ldots, x_n]$ such that the ring $R'' = K_2[x_0, \ldots, x_n]/I_2$ is a 1-dimensional graded Cohen–Macaulay ring with the same Hilbert–Kunz function as $R'$ and such that $\bar{x}_0$ is a non-zerodivisor for $R''$.*

*(4) Using Algorithm 4.5, compute a finite extension field $K_3$ of $K_2$, points $p_1, \ldots, p_s \in \mathbb{P}^n_{K_3}$, and ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \in K_3[x_0, \ldots, x_n]$ such that the extension ideal $I_3 = I_2\,K_3[x_0, \ldots, x_n]$ defines a projective scheme supported at $\{p_1, \ldots, p_s\}$, such that $I_3 = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ is the primary decomposition of $I_3$, and such that $\mathfrak{q}_i$ is primary to the vanishing ideal of $p_i$ for every $i \in \{1, \ldots, s\}$.*

*(5) For $i = 1, \ldots, s$, compute the nilpotency index $\nu_i$ of the scheme $\mathbb{X} = \mathrm{Proj}(K_3[x_0, \ldots, x_n]/I_3)$ at the point $p_i$.*

*(6) Let* $N = \max\{N', \lceil \log_p(\nu_1) \rceil, \ldots, \lceil \log_p(\nu_s) \rceil\}$ *and* $K_3 = \mathbb{F}_{q'}$ *with* $q' = p^{e'}$. *For* $i = N, \ldots, N + e' - 1$, *compute the numbers* $\psi(i) = \mathrm{HK}_R(i) - c(R)\, p^i$.

*(7) Find the period length* $m$ *of* $\psi$ *and set* $\varphi_{i \bmod m} = \psi(i)$ *for* $i = N, \ldots, N + m - 1$. *Return the numbers* $c(R), N, m$ *and the tuple* $(\varphi_0, \ldots, \varphi_{m-1})$.

*This is an algorithm which computes numbers* $c(R) > 0$, $N \geq 0$, $m \geq 1$, *and a tuple* $(\varphi_0, \ldots, \varphi_{m-1})$ *such that* $m$ *is the period length of the map* $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ *defined by* $\varphi(i) = \varphi_{i \bmod m}$ *and such that*

$$\mathrm{HK}_R(i) = c(R) \cdot p^i + \varphi(i) \qquad \textit{for all } i \geq N.$$

**6. Examples and applications.** Let us begin this section by applying the above HK-Algorithm to the examples given in the foundational papers [**7**] and [**6**].

Example 6.1. (See [**7**], Example 4.6.a)
Let $p$ be an odd prime, let $K = \mathbb{F}_p$, let $I = \langle x_1^3 - x_0^2 x_1 \rangle$, and let $R = K[x_0, x_1]/I$. We follow the steps of Algorithm 5.4.

(1) We compute $\mathrm{mult}(R) = 3$ and use $K_1 = K$.
(2) The ring $R$ is already a Cohen–Macaulay ring.
(3) The element $\bar{x}_0 \in R_1$ is already a non-zerodivisor.
(4) The ideal $J = \langle x_1^3 - x_1 \rangle \subset K[x_1]$ is already a radical ideal in $x_1$-position and the polynomial $g_1 = x_1(x_1 - 1)(x_1 + 1)$ splits into linear factors. There are three points $a_1 = 0$, $a_2 = 1$, and $a_3 = -1$ which are zeros of $J$. Thus we have $K_3 = K$, $\mathfrak{q}_1 = \langle x_1 \rangle$, $\mathfrak{q}_2 = \langle x_1 - x_0 \rangle$, $\mathfrak{q}_3 = \langle x_1 + x_0 \rangle$, and $I_3 = I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3$.
(5) We have $\nu_1 = \nu_2 = \nu_3 = 1$, since $\mathfrak{m}_{\mathbb{X},p_i} = 0$.
(6) We obtain $N = 0$, $e' = 1$, and $\psi(0) = 1 - 3 = -2$.
(7) The period length of $\psi$ is $m = 1$.

Hence the Hilbert–Kunz function of $R$ is $\mathrm{HK}_R(i) = 3\, p^i - 2$ for all $i \geq 0$.

Example 6.2. (See [**7**], Example 4.6.b)
Let $p$ be a prime, let $K = \mathbb{F}_p$, let $I = \langle x_1^4 - x_0^3 x_1 \rangle$, and let $R = K[x_0, x_1]/I$. Using Algorithm 5.4, the computation proceeds as in the previous example (with $\mathrm{mult}(R) = 4$) until Step 4. There we find $g_1 = x_1(x_1 - 1)(x_1^2 + x_1 + 1)$ and we have to distinguish two cases.

(a) If $p \equiv 1 \mod 3$ then the equation $x_1^2 + x_1 \equiv -1 \mod p$ has two distinct solutions $a_1$ and $a_2 = -a_1 - 1$ in $K$. Hence $J$ has four distinct zeros $a_1$, $a_2$, $a_3 = 0$, and $a_4 = 1$. The computation continues as in the previous example and yields $\mathrm{HK}_R(i) = 4\, p^i - 3$ for all $i \geq 0$.
(b) If $p \equiv -1 \mod 3$ then the polynomial $x_1^2 + x_1 + 1$ is irreducible over $\mathbb{F}_p$. Hence we have to pass to $K_3 = \mathbb{F}_{p^2}$ in order to get a factorization $x_1^2 + x_1 + 1 = (x_1 - a_1)(x_1 - a_2)$ with $a_1, a_2 \in K_3$. Thus Step 4 results in $K_3 = \mathbb{F}_{p^2}$

and $I_3 = I\,K_3[x_0, x_1] = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3 \cap \mathfrak{q}_4$, where $\mathfrak{q}_i = \langle x_1 - a_i x_0 \rangle$. Let us follow the remaining steps of the algorithm.

(5) We have $\nu_1 = \nu_2 = \nu_3 = \nu_4 = 1$.
(6) We have $N = 0$ and $e' = 2$. We compute the numbers $\psi(0) = 1 - 4 = -3$ and $\psi(1) = (4p - 4) - 4p = -4$.
(7) The period length of $\psi$ is $m = 2$.

Hence the Hilbert function of $R$ is now $\mathrm{HK}_R(i) = \begin{cases} 4\,p^i - 3 & \text{if } i \text{ is even,} \\ 4\,p^i - 4 & \text{if } i \text{ is odd.} \end{cases}$

EXAMPLE 6.3. (See [**6**], Section 1, p. 46)
Let $p \neq 5$ be a prime, let $K = \mathbb{F}_p$, let $I = \langle x_1^5 - x_0^5 \rangle \subset K[x_0, x_1]$, and let $R = K[x_0, x_1]/I$. The first steps of the computation of $\mathrm{HK}_R$ work as above. We find $\mathrm{mult}(R) = 5$ in Step 1 and have to factor $g_1 = x_1^5 - 1$ in Step 4. This task leads to three cases.

(a) If $p \equiv 2 \mod 5$ or $p \equiv 3 \mod 5$ then we have to pass to $K_3 = \mathbb{F}_{p^4}$ in order to split $g_1$ into linear factors. We get $g_1 = (x_1 - a_1) \cdots (x_1 - a_5)$ with $a_1 = 1$ and $a_2, \ldots, a_5 \in K_3$. In Step 6 we find $e' = 4$ and have to compute the four values $\psi(0) = -4$, $\psi(1) = -6$, $\psi(2) = -4$, $\psi(3) = -6$. Hence the period length of $\psi$ is $m = 2$ in Step 7, and the Hilbert–Kunz function of $R$ is
$$\mathrm{HK}_R(i) = \begin{cases} 5\,p^i - 4 & \text{if } i \geq 0 \text{ is even,} \\ 5\,p^i - 6 & \text{if } i \geq 1 \text{ is odd.} \end{cases}$$
(b) If $p \equiv 4 \mod 5$ then $g_1 = (x_1 - 1) q_1\, q_2$ with irreducible quadratic polynomials $q_1, q_2 \in K[x_1]$. Hence it suffices to pass to $K_3 = \mathbb{F}_{p^2}$ in order to split $g_1$ into distinct linear factors. We get $e' = 2$ and $\psi(0) = -4$, $\psi(1) = -4$ in Step 6. Therefore, the period length of $\psi$ is $m = 1$ and $\mathrm{HK}_R(i) = 5\,p^i - 4$ for all $i \geq 0$.
(c) If $p \equiv 1 \mod 5$ then $g_1 = (x_1 - a_1) \cdots (x_5 - a_5)$ with distinct numbers $a_1, \ldots, a_5 \in K$. Hence $e' = 1$ and $\psi(0) = -4$ implies $\mathrm{HK}_R(i) = 5\,p^i - 4$ for all $i \geq 0$.

Generalizing the cases, where $g_n \in K[x_n]$ splits into distinct linear factors, we have the following result.

PROPOSITION 6.4. *Let $\mathbb{X} = \{p_1, \ldots, p_s\}$ be a set of $s$ distinct $\mathbb{F}_p$-rational points in $\mathbb{P}^n$. Then the Hilbert–Kunz function of the homogeneous coordinate ring $R$ of $\mathbb{X}$ is*
$$\mathrm{HK}_R(i) = s\,p^i - s + 1 \qquad \textit{for all } i \geq 0.$$

PROOF. In Algorithm 5.4 we have $\mathrm{mult}(R) = s$, the ring $R$ is Cohen–Macaulay with non-zerodivisor $\bar{x}_0$, and the primary decomposition of $I$ is $I =$

$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$, where the homogeneous vanishing ideal $\mathfrak{p}_i$ of $p_i$ is defined over $\mathbb{F}_p$. Hence we get $e = 1$, $\psi(0) = 1 - s$, and the claimed Hilbert–Kunz function. □

Notice that, in stark contrast to the usual Hilbert function, the Hilbert–Kunz function does not depend on the geometry of the point set. Finally, we look at a couple of examples of 1-dimensional graded rings which are not as nice as the ones above, so that the first steps of the algorithm actually have some work to do.

EXAMPLE 6.5. Let $K = \mathbb{F}_3$, let $I = \langle x_0^3 - x_0x_1^2,\, x_1^3 + x_1^2x_2,\, x_0^2 - x_2^2\rangle \subset K[x_0, x_1, x_2]$, and let $R = K[x_0, x_1, x_2]/I$. In Step 1 of Algorithm 5.4 we find $\mathrm{mult}(R) = 2$. In Step 2 we discover that $R$ is not a Cohen–Macaulay ring, since $I' = I : \langle x_0, x_1, x_2\rangle^\infty = \langle x_1 + x_2,\, x_0^2 - x_2^2\rangle$ contains $I$ properly.

The computation of the Hilbert–Kunz function of $R' = K[x_0, x_1, x_2]/I'$ yields $\mathrm{HK}_R(i) = 2 \cdot 3^i - 1$ for all $i \geq 0$. Hence we get $N' = 0$ in Step 3 of Algorithm 3.1. In Step 2 of this algorithm we compute $\mathrm{HS}_R(z) = (1 + 2z + 2z^2 - 2z^4 - z^5)/(1 - z)$ and $\mathrm{HS}_{R'}(z) = (1 + z)/(1 - z)$. This yields $p(z) = z^4 + 3z^3 + 3z^2 + z$, $r = 4$, and $c = 8$. Consequently, the Hilbert–Kunz function of $R$ is given by Step 4 of Algorithm 3.1 in degree $\geq \min\{i \mid 3^i \geq 5\} = 2$. Since the period length of $\mathrm{HK}_{R'}$ is $m = 1$, we calculate $\varphi_0 = -1 + 8 = 7$. After determining $\mathrm{HK}_R(1) = 11$ individually, we conclude that

$$\mathrm{HK}_R(i) = \begin{cases} 1 & \text{for } i = 0, \\ 11 & \text{for } i = 1, \\ 2 \cdot 3^i + 7 & \text{for } i \geq 2. \end{cases}$$

EXAMPLE 6.6. Let $K = \mathbb{F}_3$, let $I = \langle x_0^3 - x_0x_1^2,\, x_1x_2 + x_2^2,\, x_1x_3 - x_3^2\rangle$, and let $R = K[x_0, \ldots, x_3]/I$. After computing $\mathrm{mult}(R) = 12$, we check that $R$ is already a Cohen–Macaulay ring. It turns out to be not easy to find a linear non-zerodivisor in $R$. Hence we extend $K$ to $K_2 = \mathbb{F}_9 = \mathbb{F}_3[t]/\langle t^2 + 1\rangle$. For the ring $R' = K_2[x_0, \ldots, x_3]/I\,K_2[x_0, \ldots, x_3]$, the element $x_0 - t\,x_1$ is a linear non-zerodivisor. Hence we have to perform a linear change of coordinates and get a Cohen–Macaulay ring $R'' = K_2[x_0, \ldots, x_3]/I_2$ with $I_2 = \langle x_0^3 - x_0x_1^2 + tx_1^3,\, x_1x_2 + x_2^2,\, x_1x_3 - x_3^2\rangle$ and a linear non-zerodivisor $\bar{x}_0 \in R''_1$.

Also the next step turns out to be more cumbersome than usual. After dehomogenization, we have to bring the ideal $J = \langle tx_1^3 - x_1^2 + 1,\, x_1x_2 + x_2^2,\, x_1x_3 - x_3^2\rangle$ into normal $x_3$-position. Unless we are very lucky, we have to try quite a few vectors $(c_1, c_2) \in (K_2)^2$ (or extend the field considerably until it has $q = 81 > \binom{12}{2}$ elements) to find a suitable linear coordinate transformation. Finally, the computation proceeds as usual and yields $\mathrm{HK}_R(i) = 12 \cdot 3^i - 11$ for $i \geq 0$.

The algorithm can also be applied to schemes of double points, sets of reduced points defined over proper extension fields of $\mathbb{F}_p$, and so on. We leave it to the reader to experiment with it and prove some of the many conjectures suggested by these computations.

**Acknowledgements.** The author thanks Ernst Kunz for stimulating discussions about the topic of this paper, Volker Augustin for a prototype implementation of the algorithms and for pointing out some inaccuracies in a preliminary version, and to the organizers of the "Effect" series of conferences for providing a hospitable environment leading to fruitful discussions and successful research.

## References

1. Augustin V., *Effektive Berechnung von Hilbert–Kunz Funktionen*, Diploma thesis, Universität Regensburg, 2001.
2. The CoCoA Team, CoCoA: *a system for doing Computations in Commutative Algebra*, available at `http://cocoa.dima.unige.it`
3. Kreuzer M., *On the canonical module of a 0-dimensional scheme*, Can. J. Math., **46** (1994), 357–379.
4. Kreuzer M., Robbiano L., *Computational Commutative Algebra 1*, Springer, Heidelberg, 2000.
5. Kreuzer M., Robbiano L., *Computational Commutative Algebra 2*, Springer, Heidelberg, 2005.
6. Monsky P., *The Hilbert–Kunz function*, Math. Ann., **263** (1983), 43–49.
7. Kunz E., *Characterization of regular local rings of characteristic p*, Amer. J. Math., **91** (1969), 772–784.
8. Kunz E., *On Noetherian rings of characteristic p*, Amer. J. Math., **98** (1976), 999–1013.
9. Zariski O., Samuel P., *Commutative Algebra*, Vol. II, Springer, New York, 1960.

*Received February 21, 2007*

Fakultät für Informatik und Mathematik
Universität Passau
D-94030 Passau
Germany
*e-mail*: `Martin.Kreuzer@uni-passau.de`