ON HILBERT FUNCTIONS OF REDUCED AND OF INTEGRAL ALGEBRAS*

Leslie G. ROBERTS
Department of Mathematics and Statistics, Queen’s University, Kingston, Ontario, Canada K7L 3N6

Moshe ROITMAN
Department of Mathematics and Computer Sciences, University of Haifa, Mount Carmel, Haifa 31999, Israel

Communicated by C.A. Weibel
Received 28 January 1987
Revised 20 July 1987

We prove that for any finite field k, there exist differentiable O-sequences which are not Hilbert functions of reduced graded k-algebras. We discuss when generic Hilbert functions and the Hilbert function of a complete intersection can be Hilbert functions of reduced or of integral graded algebras.

Introduction

We study in this paper Hilbert functions of reduced and of integral standard graded algebras. For background on Hilbert functions see [10] and [5]. Throughout this paper, k will always be a field. We will denote by R the ring k[Xₙ,...,Xₙ], where X₀,...,Xₙ are indeterminates and by $\bar{R}$ the ring k[X₁,...,Xₙ]. We recall from [10] that a (standard) graded k-algebra is a graded k-algebra $A = \bigoplus_{i \geq 0} A_i$ with $A_0 = k$ which is generated by finitely many homogeneous elements of degree 1. Equivalently, A is isomorphic (as a graded k-algebra) to $R/J$ where $J \neq R$ is a homogeneous ideal. The Hilbert function $H_A$ of A is defined by $H_A(i) = \dim_k A_i$ for $i \geq 0$ and $H_A(i) = 0$ for $i < 0$. If $J$ is a homogeneous ideal in $R$, the function $H_{R/J}$ will be called the Hilbert function corresponding to $J$. All graded k-algebras will be standard and sometimes (if clear from the context) we will drop the term ‘graded’.

A function $H : \mathbb{Z} \to \mathbb{Z}$ is the Hilbert function of a graded k-algebra for some field k if and only if H is an O-sequence (see [10]). We recall that an O-sequence $H$ is

* This work was partially supported by an NSERC grant. M. Roitman thanks Queen’s University for its hospitality.
zero-dimensional if and only if \( H(n) = c \) for \( n \gg 0 \), where \( c > 0 \) (c is called the degree of \( H \)). The notation \( d_0, d_1, \ldots, d_n \rightarrow \) for an \( O \)-sequence \( H \) means that \( H(i) = d_n \) for \( i \geq n \). Most of our results are for graded algebras of Krull dimension 1, thus with zero-dimensional Hilbert functions.

For any function \( F : \mathbb{Z} \rightarrow \mathbb{Z} \) we define \( \Delta F(i) := F(i) - F(i-1) \) and \( \delta F(i) := \sum_{j=0}^{i} F(j) \). The function \( \delta F \) is called the lifting of \( F \). An \( O \)-sequence \( H \) is differentiable if \( \Delta H \) is also an \( O \)-sequence. For any field \( k \), the Hilbert function of a reduced graded \( k \)-algebra is differentiable. By [4], for \( k \) infinite, the converse is also true and furthermore, a given differentiable \( O \)-sequence \( H \) is the Hilbert function of a reduced graded \( k \)-algebra provided \( |k| \) is sufficiently big. (For any finite set \( S \), \(|S| \) is the number of elements in \( S \).) The original motivating problem for this paper was "What happens in general if \( k \) is finite?". We show in Section 1 that for any finite field \( k \) there are differentiable \( O \)-sequences which are not Hilbert functions of reduced graded algebras and provide explicit examples.

In Section 2 we introduce the generic Hilbert function \( H \) of \( N \) points in \( \mathbb{P}^n \). Then \( H \) is differentiable, hence by the above discussion is the Hilbert function of a reduced \( k \)-algebra provided \( |k| \) is large enough. We prove that \( H \) is actually the Hilbert function of an integral \( k \)-algebra under suitable assumptions on \( k \), for example if \( k \) is a finitely generated infinite field (see Theorems 2.2, 2.3 and 2.5 to the end of the section). In Section 3 we discuss the Hilbert function \( G \) of a complete intersection. For any field \( k \), \( G \) is the Hilbert function of a reduced \( k \)-algebra (Theorem 3.2), so we turn our attention to whether or not \( G \) is the Hilbert function of an integral \( k \)-algebra. This is the case for \( k = \mathbb{Q} \) (Theorem 3.4), but if \( k \) is finite we cannot decide in all cases. In Section 4 we make further remarks about the Hilbert function of an integral domain. In particular Theorem 4.5 shows that an \( O \)-sequence \( H \) must in general satisfy conditions much stronger than differentiability in order to be the Hilbert function of an integral domain. We also describe numerical evidence that shows that our cardinality assumption in Theorems 2.2 and 2.3 is stronger than necessary.

An important method of producing \( k \)-algebras of a particular type with given Hilbert function is by the lifting of ideals (see [3] and [9]). We use the terminology of [9]. We recall that if \( A \) and \( A' \) are \( k \)-algebras, the algebra \( A' \) is a lifting of \( A \) if and only if there exists in \( A' \) a homogeneous element \( x \) of degree 1 which is not a zero-divisor such that the graded \( k \)-algebras \( A \) and \( A'/xA' \) are isomorphic. We have: \( H_A = \Delta H_{A'} \). Furthermore, if \( I \) and \( I' \) are homogeneous ideals in \( k[X_1, \ldots, X_n] \) and \( k[X_0, \ldots, X_n] \) respectively, then \( I' \) is a lifting of \( I \) (or \( I' \) lifts \( I \)) if and only if the \( k \)-algebra \( A' := k[X_0, \ldots, X_n]/I' \) is a lifting of \( A := k[X_1, \ldots, X_n]/I \) [9, Proposition 2].

Let \( H \) be a differentiable \( O \)-sequence with \( H(1) = n + 1 \). Then \( \Delta H \) is the Hilbert function of \( R/J \) for some homogeneous ideal \( J \) (see [10]). If the ideal \( I \) of \( R \) lifts \( J \), then \( R/I \) has Hilbert function \( H \). Thus in order to show that \( H \) is the Hilbert function of a reduced (respectively integral) \( k \)-algebra it suffices to find a homogeneous ideal \( J \) in \( R \) such that \( H_{R/J} = \Delta H \) and \( J \) lifts to a radical (respectively) prime ideal. We will say that an \( O \)-sequence \( H \) is liftable to the Hilbert function of a reduced
Hilbert functions

87

(integral) graded \(k\)-algebra if \(\int H\) is the Hilbert function of a reduced (respectively integral) graded \(k\)-algebra. Theorem 1.9 gives examples of homogeneous ideals \(J\) in \(R\) that are not liftable to a radical ideal but whose Hilbert function is liftable to the Hilbert function of a reduced graded \(k\)-algebra (so that some other ideal with the same Hilbert function as \(J\) is liftable to a radical ideal). Theorems 4.3 and 4.4 give examples of ideals that are liftable to a radical but not a prime ideal, and whose Hilbert function is liftable to the Hilbert function of an integral graded \(k\)-algebra.

For geometrical background see [7]. By a point in \(\mathbb{P}^n_k\) we mean a closed point. A finite union of points will always be given the reduced subscheme structure. The Hilbert function \(H_S\) of a closed subscheme \(S\) of \(\mathbb{P}^n_k\) is the Hilbert function of \(R/I\), where \(I\) is the corresponding saturated ideal.

1. Configurations in \(\mathbb{P}^2\)

In this section we study configurations of points in \(\mathbb{P}^2\). As an application we prove (Theorem 1.8) that for any finite field \(k\), there exists a differentiable \(O\)-sequence which is not the Hilbert function of a reduced graded \(k\)-algebra.

Definition 1.1. A \(k\)-configuration is a finite set \(S\) of \(k\)-rational points in \(\mathbb{P}^2_k\) such that the following conditions are satisfied: there exist integers \(1 \leq d_1 < d_2 < \cdots < d_m\), subsets \(S_i \subseteq S\), and distinct lines \(L_i\) such that \(S\) is the union of the \(S_i\), \(|S_i| = d_i\), \(S_i \subseteq L_i\), and \(L_i(1 < i \leq m)\) does not contain any point of \(\bigcup_{j<i} S_j\). The \(k\)-configuration \(S\) is said to be of type \((d_1, \ldots, d_m)\).

The previous definition implies that the sets \(S_i\) are disjoint. The line \(L_i\) can contain a point of \(S_j\) for \(j > i\) – at most one, otherwise \(L_i = L_j\). The type of a \(k\)-configuration is well defined (see the last remark after the next theorem).

Theorem 1.2. For \(1 \leq d_1 < \cdots < d_m\), all \(k\)-configurations in \(\mathbb{P}^2_k\) of type \((d_1, \ldots, d_m)\) \((k\) any field\) have the same Hilbert function, which will be denoted by \(H^{(d_1, \ldots, d_m)}\).

For \(i \geq 0\) and \(s = \sum_{i=1}^m d_i\), we have: \(H^{(d_1, \ldots, d_m)}(i) = s \Leftrightarrow i \geq d_m - 1\).

Proof. We use induction on \(m\). For \(m = 1\), the Hilbert function of a set of \(d_m\) collinear points is \(1 2 \ldots d_m \to\) and so both parts of the theorem hold. Let \(m > 1\). Let \(S\) be a \(k\)-configuration of type \((d_1, \ldots, d_m)\). As \(d_m - 2 \geq d_{m-1} - 1\) we have by the inductive assumption: \(H^{(d_1, \ldots, d_{m-1})}(d_m - 2) = \sum_{i=1}^{m-1} d_i\). By [4, Corollary 2.8] and the inductive assumption, we see that \(H_S\) is completely determined by \(d_1, \ldots, d_m\), explicitly:

\[
H_S(i) = \begin{cases} 
(H^{(d_1, \ldots, d_{m-1})}(i-1)) + i + 1 & \text{for } i \leq d_m - 1, \\
0 & \text{for } i \geq d_m - 1.
\end{cases}
\]

We see also: \(H^{(d_1, \ldots, d_m)}(i) = s \Leftrightarrow i \geq d_m - 1\). \(\square\)
It follows from the proof of the last theorem that \( H^{(d_1, \ldots, d_m)} \) can be obtained as follows: For any \( d \geq 1 \), let \( \tau_d \) be the sequence \( 1 \ 2 \ \ldots \ d \rightarrow \). Write down the sequences \( \tau_{d_1}, \ldots, \tau_{d_m} \), successively shifted to the left and add:

\[
\begin{array}{cccc}
\tau_{d_1} & 1 & 2 & \ldots & d_1 \\
\tau_{d_2} & 1 & 2 & 3 & \ldots & d_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\tau_{d_m} & 1 & 2 & 3 & \ldots & d_m \\
\end{array}
\]

\[
H^{(d_1, \ldots, d_m)} : 1 \ 3 \ \ldots .
\]

Explicitly: \( H^{(d_1, \ldots, d_m)}(i) = \sum_{j=1}^{m} \tau_d(j + i - 1) \).

By the construction in [4, §3] (see also [5, §4]), every zero-dimensional differentiable \( O \)-sequence \( H \) with \( H(1) \leq 3 \) is the Hilbert function of a \( k \)-configuration, thus is of the form \( H^{(d_1, \ldots, d_m)} \) for some \( d_1, \ldots, d_m \). The last assertion follows easily also from the fact that any zero-dimensional differentiable \( O \)-sequence \( H \) satisfying \( H(1) \leq 3 \) is of the form \( f \ G \), where \( G \) is an \( O \)-sequence with \( G(1) \leq 2 \), and \( G(i) = 0 \) for \( i \) large enough. The case \( G(1) = 1 \) being trivial, assume that \( G(1) = 2 \). By [10, Theorem 2.2], \( G \) is of the form \( 1, 2, \ldots, d-1, d, e_1, e_2, \ldots, e_k, \ldots \) where \( d = e_0 \geq e_1 \geq e_2 \geq \cdots \geq e_k \geq \cdots \) and \( e_i = 0 \) for \( i \) large enough. This implies that \( H \) is of the form \( H^{(d_1, \ldots, d_m)} \) for some \( d_1, \ldots, d_m \).

For example, by the previous description of \( H^{(d_1, \ldots, d_m)} \), it easily follows that the \( O \)-sequences \( H^{(d_1, \ldots, d_m)} \) with \( d_{i+1} \geq d_i + 2 \) \( (1 \leq i < m) \) correspond to \( O \)-sequences \( G \) with \( e_{i-1} - e_i \leq 1 \) \( (i \geq 1) \). Those with \( d_{i+1} \geq d_i + 3 \) correspond to \( O \)-sequences with \( e_{i-1} - e_i \leq 1 \) and each \( e_i \) occurring at least twice \( (i \geq 1) \) (cf. Theorems 1.5 and 1.8 below).

The integers \( d_1, \ldots, d_m \) for a given \( O \)-sequence \( H \) are uniquely determined (in particular the type of a \( k \)-configuration is well defined): if \( H = H^{(d_1, \ldots, d_m)} \), then \( d_m = \sigma(H) \), \( d_{m-1} = \sigma(H^{(d_1, \ldots, d_{m-1})}) - \sigma((H - \tau_{d_m})^-) \), where \( - \) denotes shifting one place to the left, etc. (for a zero-dimensional \( O \)-sequence \( H \), \( \sigma(H) \) is the smallest \( i \) such that \( H(j) = \text{constant for } j \geq i - 1 \)).

**Lemma 1.3.** Let \( S \) be a \( k \)-configuration of type \( (d_1, \ldots, d_m) \), \( S = \bigcup_{i=1}^{m} S_i \) as in Definition 1.1. Then:

(a) \( d_m \) is the maximal number of collinear points in \( S \).

(b) If \( d_i + m - i < d_m \) for all \( 1 \leq i < m \), then \( S_m \) is the unique subset of \( S \) which consists of \( d_m \) collinear points.

**Proof.** (a) For \( 1 \leq i < m \), the line \( L_i \) contains just \( d_i \) points of \( \bigcup_{j \geq i} S_j \) and at most \( m - i \) points of \( \bigcup_{j > i} S_j \). Thus, \( L_i \) contains at most \( d_i + m - i \leq d_m \) points of \( S \). If a line \( L \) is different from \( L_i \) \( (1 \leq i \leq m) \), then \( L \) contains at most \( m \) points of \( S \) and \( m \leq d_m \). Hence, we obtain (a).

(b) If \( d_i + m - i < d_m \) for some \( i \), then \( m < d_m \), so (b) follows from the proof of (a). \( \Box \)
Theorem 1.4. Let \( k \) be a field and \( 1 \leq d_1 < d_2 < \cdots < d_m \). There exists a \( k \)-configuration of type \((d_1, \ldots, d_m) \) if \( k \) contains at least \( d_m - 1 \) elements.

Proof. We may assume that \( k \) is a finite field of \( q \) elements.

\( \Rightarrow \). The number of \( k \)-rational points on any line in \( \mathbb{P}^2_k \) is \( q + 1 \), hence \( d_m \leq q + 1 \).

\( \Leftarrow \). As \( m \leq d_m \leq q + 1 \), there exist \( m \) distinct lines \( L_1, \ldots, L_m \) in \( \mathbb{P}^2_k \) with a common intersection point \( P \). For any \( 1 \leq i < m \), let \( S_i \) be a set of \( d_i \) \( k \)-rational points on \( L_i \) different from \( P \) (recall: \( d_i \leq q \) for \( i < m \)). Let \( S_m \) be any set of \( d_m \) points on \( L_m \). Clearly, \( S := \bigcup_{i=1}^{m} S_i \) is a \( k \)-configuration of type \((d_1, \ldots, d_m) \). \( \square \)

Theorem 1.5. Let \( 1 \leq d_1 < d_2 < \cdots < d_m \). Let \( k \) be a field, \( |k| \geq d_m - 1 \). In the notation of Definition 1.1, the following conditions are equivalent:

1. For every \( k \)-configuration \( S \) of type \((d_1, \ldots, d_m) \), the sets \( S_i \) are uniquely determined by \( S \).
2. \( d_{i+1} \geq 2 \) for \( 1 \leq i < m \).

Proof. (1) \( \Rightarrow \) (2). Assume \( d_{i+1} - d_i = 1 \) for some \( 1 \leq i < m \). Let \( P \neq P' \) be \( k \)-rational points in \( \mathbb{P}^2_k \). There exist \( i + 1 \) distinct lines \( L_1, \ldots, L_{i+1} \) passing through the point \( P \). If \( i + 1 < m \), choose \( m - i - 1 \) distinct lines \( L_{i+2}, \ldots, L_m \) passing through \( P' \) which do not contain \( P \) (notice: \( |k| \geq m - i - 1 \)). For \( 1 \leq j \leq i \), let \( S_j \) be a set of \( d_j \) \( k \)-rational points on \( L_j \) such that \( P \notin S_j \) and \( S_j \) contains no points of \( L_{i+2}, \ldots, L_m \) (notice \( d_j + m - i \leq d_j + m - i \leq d_m \leq |k| + 1 \)). There exists a set \( S'_i \) of \( d_i \) \( k \)-rational points on \( L_{i+1} \) such that \( P \notin S'_i \) and \( S'_i \) contains no points of \( L_{i+2}, \ldots, L_m \) (because \( d_i + m - i \leq |k| + 1 \)). Let \( S'_{i+1} := S_i \cup \{P\} \) and \( S_{i+1} := S'_i \cup \{P\} \). There are sets of points \( S_j \) on \( L_j \) \( (i + 2 \leq j \leq m) \) such that \( S := \bigcup_{j=1}^{m} S_j \) is a \( k \)-configuration of type \((d_1, \ldots, d_m) \). Clearly, we can replace the sets \( S_i, S_{i+1} \) by \( S'_i, S'_{i+1} \) respectively and still fulfill the conditions of Definition 1.1. This contradicts (1).

(2) \( \Rightarrow \) (1). Let \( m > 1 \). We have \( d_i + m - i \leq d_m \) for \( 1 \leq i < m \). By Lemma 1.3(b), \( S_m \) is the unique subset of \( S \) consisting of \( d_m \) collinear points. Hence, \( S_m \) and \( S \setminus S_m \) are determined by \( S \). Inductively, the sets \( S_i \) \( (1 \leq i \leq m - 1) \) are determined by \( S \setminus S_m \) and so by \( S \). \( \square \)

Let \( \Omega \) be an extension field of \( k \). We recall that a closed subscheme of \( \mathbb{P}^n_\Omega \) is defined over \( k \) if and only if its defining saturated ideal in \( \Omega[X_0, \ldots, X_n] \) has a set of generators in \( k[X_0, \ldots, X_n] \). Such a subscheme can be identified with a closed subscheme of \( \mathbb{P}^n_k \). A point of degree \( d \) in \( \mathbb{P}^n_k \) is a point whose residue field is an extension of \( k \) of degree \( d \). We recall that a line \( L \) in \( \mathbb{P}^1_k \) \( (k \) a finite field) contains a point of degree \( d \) for any \( d \). Indeed, we have an isomorphism of schemes: \( L \cong \mathbb{P}^1_k \to \mathbb{A}^1_k = \text{Spec} \ k[\!X] \) under which the ideal generated by an irreducible polynomial of degree \( d \) in \( k[\!X] \) corresponds to a point of degree \( d \) on \( L \).

Theorem 1.6. Let \( k \) be a finite field of \( q \) elements, \( 1 \leq d_1 < d_2 < \cdots < d_m \) and \( d_{i+1} - d_i \geq 2 \) for \( 1 \leq i < m \). The following conditions are equivalent:
(1) There exists an $\Omega$-configuration defined over $k$ of type $(d_1, \ldots, d_m)$, for some extension field $\Omega$.

(2) $d_i = 1$ and $m \leq q^2 + 1$ or $d_i > 1$ and $m \leq q^2 + q + 1$.

**Proof.** (1) $\implies$ (2). Let $S$ be an $\Omega$-configuration defined over $k$ of type $(d_1, \ldots, d_m)$. We may assume that $\Omega$ is a finite (and so a Galois) extension of $k$. Let $G := \text{Gal}(\Omega/k)$, and $\sigma \in G$. Let $S_1, \ldots, S_m$ be as in Definition 1.1. Clearly, the sets $\sigma(S_1), \ldots, \sigma(S_m)$ fulfil the requirements for $S_1, \ldots, S_m$ in Definition 1.1, so by Theorem 1.5, $\sigma(S_i) = S_i$ for all $i$. For any $i$, the lines $L_i$ and $\sigma(L_i)$ have in common the $d_i$ points of $S_i$. Hence, if $d_i > 1$, then $L_i = \sigma(L_i)$ for all $\sigma$ in $G$, so $L_i$ is defined over $k$. If $d_i > 1$, then all the lines $L_i$ are defined over $k$. As there are exactly $q^2 + q + 1$ lines in $\mathbb{P}_k^2$ defined over $k$, we obtain in this case: $m \leq q^2 + q + 1$. If $d_i = 1$, $L_i$ is defined over $k$ for $2 \leq i \leq m$ and the unique point $P$ of $S_i$ is defined over $k$. The number of lines defined over $k$ which do not contain $P$ is $q^2$, thus $m - 1 \leq q^2$, $m \leq q^2 + 1$.

(2) $\implies$ (1). Let $d_i \geq 2$. As $m \leq q^2 + q + 1$, we can pick $m$ lines: $L_1, \ldots, L_m$ in $\mathbb{P}_k^2$. There exists on $L_i$ a point $P_i$ of degree $d_i$. Let $S' := \{P_1, \ldots, P_m\}$. Let $\Omega$ be a finite extension of $k$ of degree divisible by $d_1, \ldots, d_m$. Let $S := S' \otimes_k \Omega$. We have: $S$ is an $\Omega$-configuration defined over $k$ of type $(d_1, \ldots, d_m)$.

In case $d_i = 1$, let $P_i$ be a $k$-rational point of $\mathbb{P}_k^2$. There are $q^2$ lines in $\mathbb{P}_k^2$ which do not pass through $P_i$. As $m \leq q^2 + 1$, we can pick lines $L_2, \ldots, L_m$ not passing through $P_i$. Choose a point $P_i$ of degree $d_i$ on $L_i$ ($2 \leq i \leq m$). After extending scalars to $\Omega$ as above, we obtain an $\Omega$-configuration as required.

**Lemma 1.7.** Let $1 \leq d_1 < d_2 < \cdots < d_m$, $d_{i+1} \geq d_i + 3$ for $1 \leq i < m$. Then for any field $k$, a finite set $S$ of $k$-rational points in $\mathbb{P}_k^2$ has Hilbert function $H(d_1, \ldots, d_m)$ $\Leftrightarrow$ $S$ is a $k$-configuration of type $(d_1, \ldots, d_m)$.

**Proof.** ‘$\Leftarrow$’. Obvious.

‘$\Rightarrow$’. The values of $H(d_1, \ldots, d_m)$ at $d_m - 2, d_{m-1}, d_m$ are $s - 2, s - 1, s$ respectively. By [4, Proposition 5.2], $S$ contains a set $S_m$ of $d_m$ collinear points and the Hilbert function of $S \setminus S_m$ is $H(d_1, \ldots, d_{m-1})$ (note that the two inequalities in [4, Proposition 5.2(ii)] are incorrect. They should be replaced by the inequalities $0 \leq i < d - 3$ and $i > d - 3$ respectively). By induction, we conclude that $S$ is a configuration of type $(d_1, \ldots, d_m)$.

**Theorem 1.8.** Let $k$ be a finite field of $q$ elements. Let $1 \leq d_1 < d_2 < \cdots < d_m$, $d_{i+1} \geq d_i + 3$ for $1 \leq i < m$. The following conditions are equivalent:

1. $H(d_1, \ldots, d_m)$ is the Hilbert function of a reduced graded $k$-algebra.
2. $d_i = 1$ and $m \leq q^2 + 1$ or $d_i > 1$ and $m \leq q^2 + q + 1$.

Thus, there are differentiable $O$-sequences $H$ with $H(1) = 3$ which are not Hilbert functions of reduced graded $k$-algebras.
Proof. The existence of such a reduced graded $k$-algebra is equivalent to the existence of a set $S$ of $\Omega$-rational points in $\mathbb{P}_\Omega^2$, for some extension $\Omega$ of $k$ with $S$ defined over $k$ and with $H_S = H^{(d_1, \ldots, d_n)}$. The theorem follows from Theorem 1.6 and Lemma 1.7.

Let $m \geq 2$. Note that $H^{(1,3,5,\ldots,2m-1)}(\mathbb{Q}) = C_l(m, m)$ (which is the Hilbert function of a complete intersection. See Section 3 for the definition of $C_l(m, m)$). Clearly, a set of $k$-rational points with Hilbert function $C_l(m, m)$ need not be a $k$-configuration, and we will prove in Theorem 3.2 that $C_l(m, m)$ is the Hilbert function of a reduced graded $k$-algebra for any field $k$. Thus $d_{i+1} \geq d_i + 2$ does not suffice in Lemma 1.7 or Theorem 1.8.

Example. We use the notation of Theorem 1.8. Let $k = \mathbb{F}_2$, thus $q = 2$, $q^2 + 1 = 5$. Let $m = 6$. By Theorem 1.8, $H^{(1,4,7,10,13,16)}$ is not the Hilbert function of a reduced graded $\mathbb{F}_2$-algebra. Explicitly, $H^{(1,4,7,10,13,16)}$ is the sequence

$$1 \ 3 \ 6 \ 10 \ 15 \ 21 \ 26 \ 31 \ 35 \ 39 \ 42 \ 45 \ 47 \ 49 \ 50 \ 51.$$

This is the example of lowest degree given by Theorem 1.8. It is not clear if there is a zero-dimensional differentiable $O$-sequence of lower degree which is not the Hilbert function of a graded $\mathbb{F}_2$-algebra. Of course such an $O$-sequence could not be of the type described in Theorem 1.8.

Theorem 1.9. For $1 \leq d_1 < d_2 < \cdots < d_m$ and any field $k$, $\Delta H^{(d_1, \ldots, d_m)}$ is the Hilbert function of $k[X_1, X_2]/I$, where $I$ is the ideal $(X_1^{m}, X_1^{m-1}X_2^{d_1}, \ldots, X_2^{d_m})$. For $k$ finite, $n \geq 2$, and suitable $m$, $d_i$, the ideal $\mathfrak{I}_k[X_1, \ldots, X_n]$ is not liftable to a radical ideal in $k[X_0, \ldots, X_n]$, but its Hilbert function is liftable to the Hilbert function of a reduced graded $k$-algebra.

Proof (cf. [3]). Let $K$ be an infinite extension of $k$. For $j = 1, 2$ choose distinct elements $t_{ji}$ in $K$ ($0 \leq i < m$ for $j = 1$ and $0 \leq i < d_m$ for $j = 2$). Let $S$ be the set of points $(1 : t_{1, i-1} : t_{2, i'})$ ($1 \leq i \leq m$, $1 \leq i' \leq d_i$). By [3, §2] we have: $\Delta H_S$ is the Hilbert function of $k[X_1, X_2]/I$. For $1 \leq i \leq m$, let $S_i$ be the set of points $(1 : t_{1, i-1} : t_{2, i'} - 1)$ ($1 \leq i' \leq d_i$). Thus, $S_i$ consists of $d_i$ points and clearly $S := \bigcup_{i=1}^m S_i$ is a configuration of type $(d_1, \ldots, d_m)$.

If $k$ is finite ($|k| = q$), let $1 < m \leq q^2 + 1$ and $d_1 \leq \cdots \leq d_m$. Then the ideal $\mathfrak{I}_k[X_1, \ldots, X_n]$ is not liftable to a radical ideal by [9, Theorem 9] and its proof. However, by Theorem 1.8, $H^{(d_1, \ldots, d_m)}$, which is the lifting of the Hilbert function corresponding to $I$, is the Hilbert function of a reduced graded $k$-algebra. □

2. Generic Hilbert functions

In this section we discuss the generic Hilbert function $GH(N, n)$ of $N$ points in $\mathbb{P}^n$. The $O$-sequence $GH(N, n)$ is differentiable, hence is the Hilbert function of a
reduced graded $k$-algebra provided $|k|$ is large enough. Unlike the case in Theorem 1.8, we do not know if the cardinality assumption on $k$ is necessary. In this section, we prove that if $k$ is finite (again with $|k|$ large enough), then $GH(N,n)$ is the Hilbert function of an integral graded $k$-algebra (Theorems 2.2 and 2.3). This result is extended to infinite fields in Theorem 2.5.

Let $n$ and $N$ be integers $\geq 1$. We define $GH(N,n)$ by the formula $GH(N,n)(i) = \min(\binom{n+i}{n},N)$ for $i \geq 0$. If there is a set $S$ of $N$ $k$-rational points in generic position in $\mathbb{P}^n_k$ ($n \geq 1$) [4, Definition 2.4], then $H_S(i) = GH(N,n)(i)$ for all $i \geq 0$ (such $S$ exists if $|k|$ is large enough). Thus, we will call $GH(N,n)$ the generic Hilbert function of $N$ in points in $\mathbb{P}^n$.

Note that if $A$ is an integral graded $k$-algebra whose Hilbert function is a zero-dimensional $O$-sequence of degree $d$, then Proj $A$ is isomorphic to $\text{Spec} K$, where $K$ is an extension field of $k$ of degree $d$. Thus an obvious necessary condition for $GH(N,n)$ to be the Hilbert function of an integral graded $k$-algebra is that $k$ have an extension field of degree $N$ (cf. Theorem 2.1 below).

Let $J$ be a (not necessarily homogeneous) ideal in $\mathbb{R}$. We denote by $H^\mathbb{R}_{R/J}(i)$ the dimension of the $k$-vector subspace of $\mathbb{R}/J$ generated by the image of polynomials in $\mathbb{R}$ of degree $\leq i$. Let $I$ be the homogenization of $J$ with respect to $X_0$. Then $H^\mathbb{R}_{R/J} = H_{R/I}$ [6, 141.8]. Furthermore, if $I$ is a homogeneous ideal in $\mathbb{R}$ such that $X_0$ is not a zero-divisor mod $I$, then $I$ is the homogenization with respect to $X_0$ of

$$I(1,X_1,\ldots,X_n) := \{f(1,X_1,\ldots,X_n) : f(X_0,\ldots,X_n) \in I\}$$

and so for $J=I(1,X_1,\ldots,X_n)$ we have $H^\mathbb{R}_{R/J} = H_{R/I}$. The next theorem is the basic tool used in the proofs of Theorem 2.2 and 2.3.

**Theorem 2.1.** Let $k$ be a field, and $N,n$ integers $\geq 1$. Let $d$ be defined by $\binom{n+d}{n} \leq N < \binom{n+d+1}{n}$ and let $r = N - \binom{n+d}{n}$. The following conditions are equivalent:

1. There is a homogeneous prime ideal $P$ such that $GH(N,n)$ is the Hilbert function of the integral domain $k[X_0,\ldots,X_n]/P$.

2. There exist
   - a set of monomials $\{X^{\lambda} \}_{\lambda \in \Lambda}$ in $k[X_1,\ldots,X_n]$ which consists of all monomials of degree $\leq d$ and $r$ monomials of degree $d+1$,
   - a field extension $L$ of $k$ and elements $s_1,\ldots,s_n$ of $L$ such that the set $\{s^\lambda \}_{\lambda \in \Lambda}$ is a $k$-basis for $L$.

**Proof.** Assume that (1) holds. Without loss of generality we can assume that $X_0 \notin P$. Let $M = P(1,X_1,\ldots,X_n)$, so $M$ is prime in $\mathbb{R}$ and $H^\mathbb{R}_{R/M} = H_{R/P} = GH(N,n)$. Let $L := k[X_1,\ldots,X_n]/M$, and let $s_i$ be the image of $X_i$ in $L$. It follows from the definitions of $H^\mathbb{R}$ and $GH(N,n)$ that there exists a set of monomials $\{s^\lambda \}_{\lambda \in \Lambda}$ as in (2) which is a $k$-basis for $L$. As $L$ is an integral domain and an $N$-dimensional vector space over $k$, we see that $L$ is a field.

If (2) holds, let $M := \ker(k[X_1,\ldots,X_n] \to L)$ (where $X_i$ is mapped to $s_i$) and let $P$
be the homogenization of \(M\) with respect to \(X_0\). Then \(P\) is prime in \(R\) and \(H_{R/p} = H^{R/M}_p = \text{GH}(N, n)\), thus (1) holds. □

It follows directly from the definitions that if \(J\) is a homogeneous ideal in \(R\), then the algebras \(R/J\) and \(\bar{R}/(X_1, \ldots, X_n)^d\) have the same Hilbert function if and only if \(J = (X_1, \ldots, X_n)^d\). Hence, \((X_1, \ldots, X_n)^d\) is liftable to a radical (respectively prime) ideal in \(R\) if and only if the Hilbert function of \(k[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^d\) is liftable to the Hilbert function of a reduced (respectively integral) \(k\)-algebra. Furthermore, we have \(H_{R/(X_1, \ldots, X_n)^d} = \Delta \text{GH}(N, n)\) where \(N = \binom{n+d-1}{n} - 1\). Thus, Theorem 2.1 generalizes [9, Lemma 11].

As usual, if \(a\) is a real number, \([a]\) denotes the largest integer \(\leq a\).

**Theorem 2.2** (cf. [9, Proposition 12]). If \(q \geq \frac{1}{2} d + 2\) (equivalently, \(q \geq \lceil \frac{1}{2} (d + 5) \rceil\)), then the ideal \((X, Y)^d\) of \(F_q[X, Y]\) is liftable to a prime ideal.

**Proof.** Let \(N = \binom{d+1}{2}\), the number of monomials in \(k[X, Y]\) of degree \(< d\). Let \(m = \lceil \frac{1}{2} (d + 1) \rceil\) and \(r = N/m\), that is (as pairs of integers)

\[
(m, r) = \begin{cases} 
\left(\frac{1}{2} d, d + 1\right) & \text{if } d \text{ is even}, \\
\left(\frac{1}{2} (d + 1), d\right) & \text{if } d \text{ is odd}.
\end{cases}
\]

We have by assumption: \(q > 2, m \leq q - 2\). Let \(k = \mathbb{F}_q\). Let \(L\) be a field extension of \(k\) of degree \(N\). Let \(s \in L, [k(s): k] = r\). We search for a generator \(t\) of \(L\) over \(k\) such that the elements \(s^i t^j\) (\(0 \leq i + j < d\)) are \(k\)-linearly independent, thus finishing the proof by Theorem 2.1.

An element of \(L\) is not a generator of \(L\) over \(k\) if and only if it belongs to some proper subfield \(L'\) of \(L\), thus \([L': k] \leq N - 1\). It follows that the number of generators of \(L\) over \(k\) is at least

\[
q^N - \sum_{i=1}^{N-1} q^i > q^N - \frac{q^N}{q - 1} = q^N \frac{q - 2}{q - 1}
\]

(cf. [8, remark after Example 3.26]).

On the other hand, if \(t\) generates \(L\) over \(k\) (or even just over \(k(s)\)) and \(t\) is a root of a polynomial \(f(Y) := \sum_{0 \leq i + j < d} a_{iy} s^i Y^j\), where \(a_{iy}\) are in \(k\) not all 0, then \(f(Y) \neq 0\), because \([k(s): k] = r \geq d\). As \([k(s)(t): k(s)] = m\), \(t\) has \(m\) distinct conjugates over \(k(s)\) and as \(\deg f(Y) < d \leq 2m\), we see that \(f(Y)\) has at most \(m\) roots which are generators of \(L\) over \(k(s)\). The number of polynomials \(f(Y)\), as above after identifying proportional polynomials, is \((q^N - 1)/(q - 1)\). Thus, the total number of roots of such polynomials which are generators of \(L\) over \(k(s)\) is at most \((q^N - 1)/(q - 1) \cdot m \leq (q^N - 1) \cdot (q - 2)/(q - 1)\) the number of generators of \(L\) over \(k\). Hence, there exists a generator \(t\) of \(L\) over \(k\) such that \(f(t) \neq 0\) for all polynomials \(f(Y)\) as above, that is the elements \(s^i t^j\) (\(0 \leq i + j < d\)) are \(k\)-linearly independent. □
Theorem 2.3. Let \( n \geq 1, N \geq 1, \) and \(|k| = q\). If \( N < \binom{n+q}{n} \), then \( \text{GH}(N, n) \) is the Hilbert function of an integral graded \( k \)-algebra.

Proof. If \( n = 1, N \geq 1, |k| < \infty \), then \( \text{GH}(N, n) \) is always the Hilbert function of an integral graded \( k \)-algebra since there is an irreducible polynomial of degree \( N \) in \( k[X] \). Assume now \( n \geq 2 \).

Define \( d \) by the inequalities \( \binom{n+d}{n} \leq N < \binom{n+d+1}{n} \). The hypothesis is equivalent to \( q > d + 1 \).

If \( d = 0 \), then \( 1 \leq N < n + 1 \), so let \( s_1, \ldots, s_N \) be a basis for a field extension of \( k \) of degree \( N \). Thus, we conclude by Theorem 2.1 that \( F \) is the Hilbert function of an integral \( k \)-algebra.

Let \( d > 0 \). Let \( r := N - \binom{n+d}{n} \) and let \( \mathcal{P} \) be the set of all monomials of degree \( \leq d \) together with \( r \) monomials of degree \( d + 1 \) which are distinct from \( X_n^{d+1} \). Let \( L \) be an extension of \( k \) of degree \( N \). We obtain successively elements \( s_1, \ldots, s_m \) of \( L \) (\( 1 \leq m \leq n \)) such that the elements \( s_1^i \ldots s_m^i \) for \( X_1^i \ldots X_m^i \) in \( \mathcal{P} \), are \( k \)-linearly independent. If \( m = 1 \), let \( s_1 \) be a generator of \( L \) over \( k \). The minimal polynomial of \( s_1 \) over \( k \) is of degree \( N > d + 1 \). As all monomials in \( \mathcal{P} \) are of degree \( \leq d + 1 \), we conclude that the elements \( s_1^i \), where \( X_1^i \in \mathcal{P} \), are \( k \)-linearly independent. Let \( 1 < m \leq n \) and let \( s_1, \ldots, s_{m-1} \) be the elements already obtained inductively. Consider the polynomial \( f(X) = \sum a_{i_1, \ldots, i_m} s_1^{i_1} \ldots s_m^{i_m} X_1^{i_{m-1}} \ldots X_m^{i_1} \), where the summation is over all sequences \( (i_1, \ldots, i_m) \) such that \( X_1^{i_1} \ldots X_m^{i_m} \) is in \( \mathcal{P} \) and the coefficients \( a_{i_1, \ldots, i_m} \) are in \( k \) not all 0. Fix \( i_m \) such that \( a_{i_1, \ldots, i_m} \neq 0 \) for some \( i_1, \ldots, i_m-1 \). Then, since \( X_1^{i_1} \ldots X_m^{i_m} \in \mathcal{P} \) implies \( X_1^{i_1} \ldots X_m^{i_{m-1}} \in \mathcal{P} \), by the inductive assumption, the coefficient of \( X_1^{i_1} \) in \( f(X) \) is not zero, so \( f(X) \neq 0 \).

If \( m < n \), then by identifying proportional polynomials, we obtain at most \( (q^{N-1} - 1)/(q - 1) \) polynomials of this type (recall: \( d > 0 \), so \( X_n \in \mathcal{P} \)). The total number of roots of such polynomials is at most

\[
\frac{q^{N-1} - 1}{q - 1} < \frac{q^{N-1}}{q - 1} < q \frac{q^N}{q - 1} \leq q^N.
\]

Hence, there exists \( s_m \) in \( L \) such that \( f(s_m) \neq 0 \) for all polynomials \( f \) as above.

Let \( m = n \). Using a similar argument, we see that the total number of roots of polynomials \( f(X) \) as above is at most

\[
\frac{q^{N-1} - 1}{q - 1} \leqq \frac{q^N}{q - 1} - 1 < q^N.
\]

(Recall: \( X_n^{d+1} \notin \mathcal{P} \), thus \( \deg f(X) \leq d \)). By Theorem 2.1 we conclude that \( \text{GH}(N, n) \) is the Hilbert function of an integral \( k \)-algebra. \( \square \)

Lemma 2.4. Let \( n \) and \( N \) be positive integers. Let \( \binom{n+d}{n} \leq N < \binom{n+d+1}{n} \). Let \( k \) be a field, \( A = [\prod_{i=1}^m L_i] \), a direct product of separable field extensions of \( k \), with \( \dim_k A = N \). Let \( \mathcal{P} \) be a set of monomials \( \{X^i\}_{i \in A} \) in \( \bar{R} \) which consists of all monomials of degree \( \leq d \) and \( N - \binom{n+d}{n} \) monomials of degree \( d + 1 \). Assume \( |k| > (d + 1)^m \). Then there exist elements \( s_1, \ldots, s_n \) in \( A \) such that the set \( \{s_i^j\}_{i \in A} \) is a \( k \)-basis for \( A \).
Proof. We may assume \( N > 1 \). First, assume that \( k \) is finite, \(|k| = q\). Let \( F(X) = \sum a_{i_1\ldots i_n} X_1^{i_1} \ldots X_n^{i_n} \) be a nonzero polynomial in \( R \), where the summation is over all sequences \((i_1, \ldots, i_n)\) such that \( X_1^{i_1} \ldots X_n^{i_n} \) is in \( \mathcal{P} \) and the coefficients \( a_{i_1\ldots i_n} \) are in \( k \). As \( \deg F \leq d + 1 \), by [8, Theorem 6.13] the number of solutions in \( L_i^n \) to the equation \( F(X) = 0 \) is at most \((d + 1)|L_i|^n - 1\) \( (1 \leq i \leq m) \). Thus, the number of solutions to this equation in \( A^n \) is at most
\[
\prod_{i=1}^m (|L_i|^{n-1}) = (d + 1)^m|A|^{n-1} = (d + 1)^mq^{N(n-1)}.
\]
The number of all polynomials \( F(X) \) as above, after identifying \( k \)-proportional polynomials is \((q^N - 1)/(q - 1)\). Thus, the total number of solutions in \( A^n \) to equations of the type \( F(X) = 0 \) is at most
\[
\frac{q^{N-1}}{q-1} \cdot (d + 1)^mq^{N(n-1)} = q^{Nn} \cdot \frac{(d + 1)^m}{q-1} \leq q^{Nn} = |A^n|.
\]

Hence, there exist \( s_1, \ldots, s_n \) in \( A \) such that \( F(s_1, \ldots, s_n) \neq 0 \) for all \( F \) as above. This means that the set \( \{ s^A \}_{A \in A} \) is \( k \)-linearly independent and as its cardinality is \( N \), it is a \( k \)-basis for \( A \).

Consider now the case \( k \) infinite. Let \( \mathcal{B} \) be a \( k \)-basis of \( A \), \( D \) the discriminant of \( \mathcal{B} \), thus \( D \neq 0 \). Let \( x_1, \ldots, x_r \) be all the coefficients of the products \( uv \), where \( u, v \) are in \( \mathcal{B} \), with respect to the \( k \)-basis \( \mathcal{B} \). We claim that there exist a subring \( T \) of \( k \) containing \( x_1, \ldots, x_r \) (which implies that \( D \in T \)) and a maximal ideal \( M \) of \( T \) such that \( D \in M \), \( T/M \) is a finite field and \( |T/M| > t := (d + 1)^N \).

Indeed, if \( \text{char } k = 0 \), let \( T := \mathbb{Z}[x_1, \ldots, x_r] \) and let \( C \) be the product of all primes in \( \mathbb{Z} \) which are \( \leq t \). There exists a maximal ideal \( M \) in \( T \) such that \( CD \in M \), so \( D \in M \) and \( T/M \) is finite. We have \( \mathbb{Z} \cap M = \mathbb{Z}p \) for some prime \( p > t \), hence \( |T/M| > t \).

Now, assume that \( \text{char } k \) is finite and let \( T_0 \) be the prime subfield of \( k \). If \( k \) is algebraic over \( T_0 \), let \( T \) be a finite subfield of \( k \) containing \( x_1, \ldots, x_r \) such that \( |T| > t \) and let \( M = 0 \). If \( k \) is not algebraic over \( T_0 \), let \( y \) be an element of \( k \) which is transcendental over \( T_0 \). Let \( T := T_0[y, x_1, \ldots, x_r] \). Let \( C \) be the product of all non-zero polynomials in \( T_0[y] \) of degree \( \leq t \). Let \( M \) be a maximal ideal of \( T \) such that \( CD \in M \).

Now, let \( T \) and \( M \) as above, \( k_0 := T/M \). Clearly, \( \mathcal{B} \) is a free \( T \)-basis for \( T[\mathcal{B}] \). Let \( A' := T[\mathcal{B}] / MT[\mathcal{B}] \) and let \( \mathcal{B}' \) be the canonical image of \( \mathcal{B} \) in \( A' \), thus \( \mathcal{B}' \) is a \( k_0 \)-basis for \( A' \). As \( D \in M \), the discriminant of \( \mathcal{B}' \) is nonzero. It follows that \( A' \) is a separable \( k_0 \)-algebra, thus a direct product of at most \( N \) finite field extensions of \( k_0 \). As \( |k_0| > (d + 1)^N \) and \( \dim_{k_0} A' = N \), we conclude by the first part of the proof that there exist elements \( s_1', \ldots, s_r' \) in \( A' \) such that the set \( \{ s_i^A \}_{A \in A} \) is a \( k_0 \)-basis for \( A' \). Let \( s_1, \ldots, s_r \) be elements in \( T[\mathcal{B}] \) such that \( s_1', \ldots, s_r' \) respectively are their canonical images in \( A' \). As \( \{ s_i^A \}_{A \in A} \) is a \( k_0 \)-basis for \( A' \), the matrix of the coefficients of \( \{ s_i^A \}_{A \in A} \) with respect to \( \mathcal{B} \) has a nonzero determinant. It follows that \( \{ s_i^A \}_{A \in A} \) is a \( k \)-basis for \( A \). \( \square \)
As a consequence of Theorem 2.1 and Lemma 2.4, we obtain

**Theorem 2.5.** Let $k$ be an infinite field. Assume that there exists a separable field extension of degree $N$ over $k$. Then the generic Hilbert function of $N$ points in $\mathbb{P}^n$ ($n \geq 1$) is the Hilbert function of an integral graded $k$-algebra. □

If $k$ is infinite perfect, there is a separable field extension of degree $N$ over $k$ (and hence Theorem 2.5 applies) if and only if there is an irreducible polynomial of degree $N$ over $k$. If $k$ is a finitely generated infinite field, then Theorem 2.5 also applies, by the following lemma:

**Lemma 2.6.** Let $k$ be a finitely generated infinite field. Then there exists an irreducible separable polynomial of degree $N$ over $k$ ($N \geq 1$).

**Proof.** Let $T$ be the smallest subring of $k$ and $\Omega$ a transcendence basis of $k$ over the quotient field of $T$. There exist elements $x_1, \ldots, x_n$ which are integral over $T[\Omega]$ such that $k = k_0(x_1, \ldots, x_n)$, where $k_0$ is the prime field contained in $k$. Let $A := T[\Omega, x_1, \ldots, x_n]$. Let $M_1$ be a maximal ideal of $T$. There exists a maximal ideal $M$ of $A$ which contains $M_1 \cup \Omega$. Hence $A/M$ is a finite extension of $T/M_1$, which is a finite field. Thus, $A/M$ is a finite field and so there exists in $(A/M)[X]$ a monic irreducible polynomial $f(X)$ of degree $N$. Let $f_0(X)$ be a polynomial in $A[X]$ which has $f(X)$ as canonical image. Clearly, $f_0(X)$ is irreducible and its discriminant $d$ is not 0 because $d$ is not 0 mod $M$. Hence, $f_0(X)$ is an irreducible separable polynomial of degree $N$ over $k$. □

By Theorem 2.5, if $k$ is a finitely generated infinite field (in particular if $k = \mathbb{Q}$), then any power of the ideal $(X_1, \ldots, X_n)$ in $R$ is liftable to a prime ideal. This generalizes [9, Proposition 13].

### 3. Hilbert functions of complete intersections

In this section we consider the Hilbert function $CI(d_1, \ldots, d_n)$ of a complete intersection. This $O$-sequence is always the Hilbert function of a reduced graded $k$-algebra (Theorem 3.2). Thus we try to prove that $CI(d_1, \ldots, d_n)$ is the Hilbert function of an integral graded $k$-algebra. A natural approach is to try lifting the ideal $(X_1^{d_1}, \ldots, X_n^{d_n})$ of $R$ to a prime ideal. This is always possible if $k = \mathbb{Q}$ (Theorem 3.4) but we cannot decide in all cases if $k$ is finite. Rather than lifting $(X_1^{d_1}, \ldots, X_n^{d_n})$ directly to a prime ideal of $R$ we find it more convenient to use a lifting criterion from [9]. We first define $CI(d_1, \ldots, d_n)$.

**Definition.** We denote by $CI(n; d_1, \ldots, d_r)$ ($r \leq n$) the Hilbert function of the complete intersection $R/(f_1, \ldots, f_r)$, where $R = k[X_0, \ldots, X_n]$, and $\langle f_1, \ldots, f_r \rangle$ is an $R$-
sequence with $f_i$ homogeneous of degree $d_i$. The function $\text{Cl}(n; d_1, \ldots, d_n)$ will be denoted by $\text{Cl}(d_1, \ldots, d_n)$.

Note that the Hilbert function of $k[X_1, \ldots, X_n]/(X_1^{d_1}, \ldots, X_n^{d_n})$ ($r \leq n$) is $\Delta \text{Cl}(n; d_1, \ldots, d_n)$. Now we recall the lifting criterion.

If $f$ is a nonzero polynomial in $\overline{R}$, we denote by $l(f)$ the form of highest degree occurring in $f$. If $J$ is an ideal in $\overline{R}$, we denote by $l(J)$ the ideal generated by $\{l(f) : f \in J\}$. We have by [9, Proposition 5]:

**Lifting Criterion.** A homogeneous ideal $J$ in $\overline{R}$ is liftable to a radical (respectively prime) ideal in $R$ if and only if there is a radical (respectively prime) ideal $\hat{J}$ in $\overline{R}$ such that $l(\hat{J}) = J$.

In order to verify the Lifting Criterion for the ideal $J = (X_1^{d_1}, \ldots, X_n^{d_n})$, we construct a radical (respectively prime) ideal of $R$ generated by polynomials $f_1, \ldots, f_n$ with $l(f_i) = X_i^{d_i}$ for all $i$ and use the following lemma:

**Lemma 3.1.** Let $f_1, \ldots, f_r$ be elements of $R$ such that $\langle l(f_1), \ldots, l(f_r) \rangle$ is an $R$-sequence in $R$. Then $\langle f_1, \ldots, f_r \rangle$ is an $R$-sequence and if $I$ is the ideal $(f_1, \ldots, f_r)$, then $l(I) = (l(f_1), \ldots, l(f_r))$.

**Proof.** The proof is by induction on $r$, the case $r = 1$ being obvious. Let $r > 1$. Let $f \in \langle f_1, \ldots, f_r \rangle$. Write $f = \sum_{i=1}^{r} g_i f_i$, $g_i \in R$, with deg $l(g_r)$ minimal (we define $l(0) = 0$, deg $0 = -\infty$). We want to show $l(f) \in \langle l(f_1), \ldots, l(f_r) \rangle$. This is clear by induction if $l(g_i f_i)_1 + \sum_{i=1}^{r-1} g_i f_i \neq 0$, because in this case $l(f) = l(g_i f_i) + \sum_{i=1}^{r-1} g_i f_i$, each yielding $l(f) \in \langle l(f_1), \ldots, l(f_r) \rangle$. Assume $l(g_i f_i) + l(\sum_{i=1}^{r-1} g_i f_i) = 0$. We have $l(g_r) l(f_r) = l(g_r f_r) \in l(f_1, \ldots, f_{r-1}) = (l(f_1), \ldots, l(f_{r-1}))$. As $\langle l(f_1), \ldots, l(f_r) \rangle$ is an $R$-sequence, we obtain $l(g_r) \in \langle l(f_1), \ldots, l(f_{r-1}) \rangle$. If $g_r \neq 0$, there exist $h_i \in R (1 \leq i \leq r - 1)$ such that for $g_r' := g_r \sum_{i=1}^{r-1} h_i f_i$ we have deg $l(g_r') < \deg l(g_r)$. Let $g_i = g_i + h_i f_i$. Each $g_i f_i (1 \leq i \leq r - 1)$ is contradiction. It follows that $g_r = 0$, and $l(f) \in l(f_1, \ldots, f_{r-1}) = (l(f_1), \ldots, l(f_{r-1}))$. Hence $l(f_1, \ldots, f_r) = (l(f_1), \ldots, l(f_r))$. Clearly $(f_1, \ldots, f_r) \neq R$.

We now prove that $f_r$ is not a zero-divisor modulo $(f_1, \ldots, f_{r-1})$. Indeed, let $f_r g \in (f_1, \ldots, f_{r-1})$ with $g \notin (f_1, \ldots, f_{r-1})$ and deg $l(g)$ minimal. From the minimality of deg $l(g)$ it follows that $l(g) \notin \langle l(f_1), \ldots, l(f_{r-1}) \rangle$. We have $l(f_r) l(g) \in l(f_1, \ldots, f_{r-1})$ contradicting the fact that $l(f_r)$ is not a zero-divisor modulo $(l(f_1), \ldots, l(f_{r-1}))$. It follows that $\langle f_1, \ldots, f_r \rangle$ is an $R$-sequence.

**Theorem 3.2.** The ideal $(X_1^{d_1}, \ldots, X_n^{d_n})$ of $\overline{R}$ is liftable to a radical ideal for any field $k$ and positive integers $d_1, \ldots, d_n$. Hence $\text{Cl}(d_1, \ldots, d_n)$ is the Hilbert function of a reduced graded algebra over any field.

**Proof.** Let $f_i(X)$ be a polynomial in $k[X]$ of degree $d_i$ ($1 \leq i \leq n$) that has distinct roots in an algebraic closure of $k$. Let $M := (f_1(X_1), \ldots, f_n(X_n))$. Then $M$ is a radical ideal in $k[X_1, \ldots, X_n]$ and $l(M) = (X_1^{d_1}, \ldots, X_n^{d_n})$ by Lemma 3.1.
More generally, Theorem 3.2 implies that for \( r \leq n \), the ideal \((X_1^{d_1}, \ldots, X_n^{d_n})\) of \( k[X_1, \ldots, X_n] \) is liftable to a radical ideal. A similar remark holds for other results of this type below.

**Theorem 3.3.** Let \( k \) be a finite field and let \( d_1, \ldots, d_n \) be pairwise relatively prime positive integers. Then the ideal \((X_1^{d_1}, \ldots, X_n^{d_n})\) of \( k[X_1, \ldots, X_n] \) is liftable to a prime ideal. Hence \( CI(d_1, \ldots, d_n) \) is the Hilbert function of an integral graded \( k \)-algebra.

**Proof.** Let \( f_i(X) \) be an irreducible polynomial in \( k[X] \) of degree \( d_i \) \( (1 \leq i \leq n) \). Let \( M := (f_1(X_1), \ldots, f_n(X_n)) \). Then \( M \) is a prime ideal in \( k[X_1, \ldots, X_n] \) and \( l(M) = (X_1^{d_1}, \ldots, X_n^{d_n}) \) by Lemma 3.1.

**Theorem 3.4.** For any positive integers \( d_1, \ldots, d_n \), the ideal \((X_1^{d_1}, \ldots, X_n^{d_n})\) in \( \mathbb{Q}[X_1, \ldots, X_n] \) is liftable to a prime ideal. Hence \( CI(d_1, \ldots, d_n) \) is the Hilbert function of an integral graded \( \mathbb{Q} \)-algebra.

**Proof.** Let \( p_1, \ldots, p_n \) be distinct primes. Let \( \phi \) be the homomorphism of \( \mathbb{Q} \)-algebras \( \phi : \mathbb{Q}[X_1, \ldots, X_n] \to \mathbb{Q}(\sqrt[d_1]{p_1}, \ldots, \sqrt[d_n]{p_n}) \) such that \( \phi(X_i) = \sqrt[d_i]{p_i} \) \( (1 \leq i \leq n) \). We have \((X_1^{d_1} - p_1, \ldots, X_n^{d_n} - p_n) \subseteq \ker \phi \) and \( \dim_{\mathbb{Q}} \mathbb{Q}[X_1, \ldots, X_n]/(X_1^{d_1} - p_1, \ldots, X_n^{d_n} - p_n) = \prod_{i=1}^n d_i = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[d_1]{p_1}, \ldots, \sqrt[d_n]{p_n}) \), the last equality being well known. Thus, \( M := (X_1^{d_1} - p_1, \ldots, X_n^{d_n} - p_n) \) is a maximal ideal in \( \mathbb{Q}[X_1, \ldots, X_n] \) with \( l(M) = (X_1^{d_1}, \ldots, X_n^{d_n}) \).

We recall that by the Vahlen-Capelli theorem, a polynomial of the form \( X^d - s \) over a field \( k \) is reducible if and only if \( s \) has an \( u \)th root in \( k \) for some prime divisor \( u \) of \( d \) or \( 4 \mid d \) and \( s = -4t^4 \) for some \( t \) in \( k \) (see e.g. [1, Chapter 5, Example 11, p. 212]).

**Theorem 3.5.** Let \( k \) be a finite field, \(|k| = q\), and \( d_1, \ldots, d_n \) positive integers, \( d := \prod_{i=1}^n d_i \). Assume that any prime factor of \( d \) divides \( q - 1 \). Assume also that \( 4 \nmid d \) or: \( \mathrm{char} \, k > 2 \) and \(-1 \) is a square in \( k \). Then, the ideal \((X_1^{d_1}, \ldots, X_n^{d_n})\) of \( R \) is liftable to a prime ideal.

**Proof.** Let \( s \) be a primitive element of \( k \). Any prime factor \( u \) of \( d \) divides \( q - 1 \), hence \( s \) has no \( u \)th root in \( k \). Thus, the polynomial \( X^d - s \) is irreducible over \( k \), in case \( 4 \nmid d \). Assume now that \( \mathrm{char} \, k \) is odd and \(-1 \) is a square in \( k \). The element \( s \) is not of the form \( s = -4t^4 \) for \( t \) in \( k \), because that would imply that \( s \) is a square in \( k \). Hence, the polynomial \( X^d - s \) is irreducible over \( k \) under any of our assumptions.

Let \( f_i := X_i^{d_i} - s \) and for \( 1 \leq i \leq n \), let \( f_i := X_i^{d_i} - X_{i-1}^{d_{i-1}} \). Let \( M \) be the ideal \((f_1, \ldots, f_n)\) of \( R \). We have \( R/M = k[X]/(X^d - s) \). Hence, \( M \) is a maximal ideal in \( R \) and \( l(M) = (X_1^{d_1}, \ldots, X_n^{d_n}) \). We conclude that the ideal \((X_1^{d_1}, \ldots, X_n^{d_n})\) is liftable to a prime ideal.
Theorem 3.6. Let \( d_1, \ldots, d_n \) be positive integers, \( p \) a prime such that \( p \nmid \prod_{i=1}^{n} d_i \). For any finite field \( k \) of characteristic \( p \), there exists a finite field extension \( L \) such that the ideal \((X_1^{d_1}, \ldots, X_n^{d_n})\) of \( L[X_1, \ldots, X_n] \) is liftable to a prime ideal.

Proof. By extending \( k \), we may assume that \(-1\) is a square in \( k \). Let \( d := \prod_{i=1}^{n} d_i \). As \( p \nmid d \), there is \( r \) such that \(|k|^r \equiv 1 \mod d\). Let \( L \) be a field extension of degree \( r \) over \( k \). We have \( d \mid |L| - 1 \). Hence, if \( \text{char } k \neq 2 \), we conclude the proof by the previous theorem. If \( \text{char } k = 2 \), then \( 4 \nmid d \), so we conclude again by the previous theorem. \( \square \)

Remarks. The conclusion of the last theorem can be formulated equivalently as follows: for infinitely many integers \( r \), the ideal \((X_1^{d_1}, \ldots, X_n^{d_n})\) of \( \mathbb{F}_p[X_1, \ldots, X_n] \) is liftable to a prime ideal.

Using the lifting criterion above we see that Theorem 3.6 is false for an algebraically closed field \( k \) if any of the \( d_i \)'s is greater than 1.

Lemma 3.7. Let \( k \subseteq L \) be finite fields. Then there exists a generator of \( L \) over \( k \) with trace 0, except if \( \text{char } k = 2 \) and \(|L: k| = 2\).

Proof. Let \(|k| = q\), \(|L: k| = n\) and \( T := \text{Tr}_{L/k} \). \( T: L \to k \) is a nonzero linear transformation over \( k \), hence \( \dim_k \ker T = n - 1 \), thus there are exactly \( q^{n-1} \) elements in \( L \) of zero trace.

First, assume that \( n \geq 3 \). For any field \( K \) such that \( k \subseteq K \subseteq L \), we have \(|K: k| \leq n - 2\). Hence, the number of elements of \( L \) which are not generators over \( k \) is at most

\[
\sum_{i=1}^{n-2} q^i < \frac{q^{n-1} - 1}{q - 1} < q^{n-1}.
\]

Therefore, there exists a generator \( s \) of \( L \) over \( k \) of zero trace.

Let \( n = 2 \). The number of elements in \( L \) of zero trace is \( q \). Therefore, any generator of \( L \) over \( k \) (i.e. any element in \( L \setminus k \)) has nonzero trace if and only if any element in \( k \) has zero trace, that is if and only if \( \text{char } k = 2 \). \( \square \)

Lemma 3.8. Let \( L \) be a finite field, \( x \) a generator of the multiplicative group of \( L \). Then, for any \( n \geq 3 \) there exists an irreducible polynomial \( f(Y) \) in \( L[Y] \) of the form \( f(Y) = Y^n + \sum_{i=0}^{n-2} a_i Y^i \), where \( a_{n-2} = 1 \), 0 or \( x \).

Proof. By the previous lemma, there exists an irreducible polynomial \( g(Y) \) in \( L[Y] \) of the form \( g(Y) = Y^n + d Y^{n-2} + \cdots \). We may assume that \( d \neq 0 \). Let \( d = x^r \) (\( r \geq 1 \)) and \( r' = \lfloor \frac{r}{2} \rfloor \). Let \( f(Y) := x^{-r''}g(x^{r''}Y) \). Clearly, \( f(Y) \) fulfills the requirements in the lemma. \( \square \)

Theorem 3.9. Over any finite field \( k \), \( C_1(n, m) \) is the Hilbert function of an integral graded \( k \)-algebra if \( 1 \leq m \leq 4 \).
Proof. First assume \( n \geq 3 \). Let \( L \) be a field extension of \( k \) of degree \( m \) and let \( x \) be a generator of the multiplicative group of \( L \). By Lemma 3.8, there exists an irreducible polynomial \( f(Y) \in L[Y] \) of the form \( f(Y) = Y^n + \sum_{i=0}^{n-2} a_i Y^i \), where \( a_{n-2} = 0, 1 \) or \( x \). Hence, there exists a polynomial \( g(X, Y) \in k[X, Y] \) such that \( f(Y) = g(x, Y) \) and \( \deg l(g) = n \) (any coefficient \( a_i \) can be expressed as a polynomial in \( x \) over \( k \) of degree \( \leq 3 \)). Let \( h(X) \) be the minimal polynomial of \( x \) over \( k \). Let \( M \) be the ideal \((h(X), g(X, Y))\) in \( k[X, Y] \). Clearly, \( k[X, Y]/M = L[Y]/f(Y) \), so \( M \) is a maximal ideal. Let \( u := l(g(X, Y)) \). The form \( u \) has degree \( n \) and is not divisible by \( X \), hence, by Lemma 3.1, \( l(M) = (X^n, u) \). We conclude that the ideal \((X^m, u)\) is liftable to a prime ideal so \( \text{Cl}(m, n) \) is the Hilbert function of an integral graded \( k \)-algebra.

Now, let \( n = 2 \). By the first part of the proof, we may assume also that \( m = 2 \). Take as above a field extension \( k(x) \) of degree \( m = 2 \) of \( k \) and use the fact that there exists an irreducible polynomial over \( k(x) \) of the form \( Y^2 - Y - a \).

In fact for any finite field \( k \), for \( m = 2, 3 \) and for any \( n \geq 1 \), the ideal \((X^m, Y^n)\) of \( k[X, Y] \) is liftable to a prime ideal. Indeed, if \( m = 3 \) in the above proof, then \( u = Y^n \). The preceding paragraph shows that \((X^2, Y^2)\) is liftable to a prime ideal.

Let \( k \) be a field, \( L \) an extension of degree \( m \) over \( k \). If there exists an irreducible polynomial of degree \( n \) over \( L \) of the form \( f(X) + a \), where \( f(X) \in k[X] \) and \( a \) generates \( L \) over \( k \), then the ideal \((X^m, Y^n)\) in \( k[X, Y] \) is liftable to a prime ideal. The existence of an irreducible polynomial \( f(X) + a \) over \( L \) as above is equivalent to the existence of an irreducible polynomial over \( k \) of the form \( h_1(h_2(X)) \), where \( \deg h_1 = m \) and \( \deg h_2 = n \) (see [1, Chapter 5, Exercise (10), p. 212]).

4. Hilbert functions of integral domains

In this section we make some further remarks about the Hilbert function of an integral domain and about lifting to a prime ideal.

A homogeneous ideal \( I \) in \( \mathcal{R} \) is zero-dimensional if \( \sqrt{I}=\langle X_1, \ldots, X_n \rangle \), that is, \( \dim_k \mathcal{R}/I < \infty \).

Theorem 4.1. Let \( L \) be an algebraic extension of a field \( k \) and \( I \) a homogeneous zero-dimensional ideal in \( k[X_1, \ldots, X_n] \). Assume that the degree over \( k \) of any element in \( L \) is coprime to \( \dim_k k[X_1, \ldots, X_n]/I \) (if \( L \) is a finite extension of \( k \), this holds if and only if \( [L: k] \) and \( \dim_k k[X_1, \ldots, X_n]/I \) are coprime). If \( I \) is liftable to a prime ideal, then the ideal \( lL[X_1, \ldots, X_n] \) of \( L[X_1, \ldots, X_n] \) is also liftable to a prime ideal.

Proof. Let \( M \) be a maximal ideal in \( k[X_1, \ldots, X_n] \) such that \( l(M)=I \). Clearly, \( l(M)L[X_1, \ldots, X_n] \subseteq l(M)l[X_1, \ldots, X_n] \). On the other hand, let \( B=(b_1, \ldots, b_m) \) be a basis of \( l \) over \( k \) and let \( f = \sum_{i=1}^m a_i f_i \) be a nonzero element of \( MI[X_1, \ldots, X_n] \), where \( f_i \) are nonzero elements in \( M \subseteq k[X_1, \ldots, X_n] \). Let \( d := \max \deg f_i \). Then, \[
l(f) = \sum_{I: \deg f_I = d} h_I l(f_I) \in l(M)L[X_1, \ldots, X_n].\]
Therefore, \( l(ML[X_1, \ldots, X_n]) = l(M)L[X_1, \ldots, X_n] = IL[X_1, \ldots, X_n] \). For any field \( F \) contained in \( L \) and of finite degree over \( k \), we have \( [F: k] \) and \( \dim_k k[X_1, \ldots, X_n]/M = \dim_k k[X_1, \ldots, X_n]/I \) are coprime. Hence, \( F[X_1, \ldots, X_n]/MF[X_1, \ldots, X_n] \cong k[X_1, \ldots, X_n]/M \otimes_k F \) is a field. Therefore, \( ML[X_1, \ldots, X_n] \) is a maximal ideal in \( I[X_1, \ldots, X_n] \). We conclude that the ideal \( IL[X_1, \ldots, X_n] \) is liftable to a prime ideal.

**Remark.** If \( k \) is a perfect field, \( L \) an algebraic extension of \( k \) and the ideal \( I \) of \( k[X_1, \ldots, X_n] \) is liftable to a radical ideal, then the ideal \( IL[X_1, \ldots, X_n] \) is also liftable to a radical ideal. (If \( A' \) is a reduced \( k \)-algebra which is a lifting of \( A := k[X_1, \ldots, X_n]/I \), then \( A' \otimes_k L \) is a reduced \( L \)-algebra which is a lifting of \( A \otimes_k L \cong L[X_1, \ldots, X_n]/IL[X_1, \ldots, X_n] \).)

**Example.** In order to show that \( (X, Y)^5 \) is liftable to a prime ideal over any finite field, it is enough to prove this for fields of cardinality \( < 5 \) (see e.g. Theorem 2.2 above). Using Theorem 4.1, we see that it is not necessary to check this for \( \mathbb{F}_4 \). Indeed, we have \( \dim_{\mathbb{F}_2} \mathbb{F}_2[X, Y]/(X, Y)^5 = 15 \), which is coprime to \( [\mathbb{F}_4: \mathbb{F}_2] = 2 \). Thus, the liftability for \( \mathbb{F}_4 \) follows from the liftability for \( \mathbb{F}_2 \). In fact, it can be checked that \( (X, Y)^5 \) is liftable to a prime ideal over \( \mathbb{F}_2 \) and \( \mathbb{F}_3 \) and so over any finite field.

**Theorem 4.2.** Let \( k \) be a finite field and \( I \) a zero-dimensional ideal in \( k[X, Y] \) which is liftable to a prime ideal. Then there exists an infinite field \( L \) containing \( k \) such that \( IL[X_1, \ldots, X_n] \) is liftable to a prime ideal.

**Proof.** Let \( \Omega \) be an algebraic closure of \( k \) and let \( L \) be the union of all extensions of \( k \) in \( \Omega \) of degree coprime to \( \dim_k k[X, Y]/(X^m, Y^n, XY) \). 

**Theorem 4.3.** Let \( m \geq 2, n \geq 2, k \) a field. The ideal \( (X^m, Y^n, XY) \) of \( k[X, Y] \) is liftable to a prime ideal if and only if \( m = n \) and \( k \) has a simple field extension of degree \( 2n - 1 \). On the other hand all the ideals \( (X^m, Y^n, XY) \) are liftable to radical ideals.

**Proof.** Assume that \( I := (X^m, Y^n, XY) \) is liftable to a prime ideal. Then there exists a maximal ideal \( M \) in \( k[X, Y] \) with \( l(M) = I \). Let \( L := k[X, Y]/M, \ x := X + M, \ y := Y + M \). We have \( \dim_k L = \dim_k k[X, Y]/(X^m, Y^n, XY) = m + n - 1 \), the latter equality holding because \( \{1, X, \ldots, X^{m-1}, Y, \ldots, Y^{n-1}\} \) is a basis of \( k[X, Y]/(X^m, Y^n, XY) \) over \( k \). As \( XY \in I = l(M) \), we have \( XY + aX + bY + c \in M \) for some \( a, b, c \) in \( k \). Thus \( xy + ax + by + c = 0 \), so \( y(x+b) \in k(x) \). But \( x + b \neq 0 \) because \( X \notin l(M) \), hence \( y \in k(x) \) and \( L = k(x) \). (In particular, if \( m = n \) and \( I \) is liftable to a prime ideal, then \( L \) is a simple field extension of \( k \) of degree \( 2n - 1 \).)

Now assume that \( m \neq n \) (e.g. \( m < n \)) and continue with the notation of the preceding paragraph. We have \( (y+a)(x+b) = ab - c \neq 0 \). Let \( \bar{x} := x + b, \ \bar{y} := (y + a)/(ab - c) \), so \( \bar{x}\bar{y} = 1 \) and \( L = k(\bar{x}) \). Let \( f(X) := X^d + \sum_{i=0}^{d-1} a_i X^i \) be the minimal polynomial of \( \bar{x} \) over \( k \), where \( d = m + n - 1 \). For \( r = n - 1 \) we have
Let 

\[ g(X, Y) := X^{d-r} + a_0 Y^r + \sum_{r \leq i < d} a_i X^{i-r} + \sum_{1 \leq i < r} a_i Y^{r-i}. \]

If \( n-1 > m \), then \( l(g(X, Y)) = a_0 Y^{n-1} \). As \( x \) and \( y \) are linear polynomials of \( \bar{x} \) and \( \bar{y} \), we obtain in \( M \) a polynomial with leading form \( Y^{n-1} \), contradiction. If \( n-1 = m \), we obtain in \( M \) a polynomial with leading form \( Y^{n-1} + aX^m \) for some \( a \) in \( k \), so also a polynomial with leading form \( Y^{n-1} \), contradiction.

Now, assume that \( m = n \) and \( k \) has a simple field extension of degree \( d := 2n-1. \)

Let \( f(X) \) be an irreducible polynomial in \( k[X] \) of degree \( d \). Let \( M := (f(X), XY - 1) \).

By the previous argument, we have \( Y^{m-1} f(X) \equiv g(X, Y) \mod M \) for some polynomial \( g(X, Y) \) with \( l(g(X, Y)) = X^m \), so \( X^m \in l(M) \). Considering the polynomial \( Y^m f(X) \) we obtain by a similar argument a polynomial in \( M \) with leading form \( Y^m \). It follows that \( l(M) \supseteq I \). On the other hand we have \( \dim_k k[X, Y]/M = \dim_k k[X]/(f(X)) = d \), so \( l(M) = I \). We conclude that \( I \) is liftable to a prime ideal.

In order to show that the ideal \( I = (X^m, Y^n, XY) \) is liftable to a radical ideal for any \( m \) and \( n \), let \( f(X) \) and \( g(Y) \) be polynomials of degrees \( m \) and \( n \) respectively which have just simple roots in an algebraic closure of \( k \) and such that \( f(0) = g(0) = 0 \).

Let \( J \) be the ideal \( (f(X), g(Y), XY) \) of \( k[X, Y] \). We have \( J \) is a radical ideal and \( l(J) = I \), thus \( I \) is liftable to a radical ideal (see the construction in [3, Theorem 2.2] and [9, Theorem 8]).

\[ \text{Theorem 4.4 (cf. Theorem 1.9 above and the remark after Example 4.5 in [10]). \ Let} \]

\[ k \text{ be a field. For any } n \geq 2 \text{ there exists a homogeneous ideal } I \text{ in } k[X_1, \ldots, X_n] \text{ which is liftable to a radical ideal, is not liftable to a prime ideal, but whose Hilbert function is liftable to the Hilbert function of an integral graded } k\text{-algebra.} \]

\[ \text{Proof. As in [9, Theorem 9] we may assume that } n = 2. \text{ Let } X = X_1, \ Y = X_2. \text{ Let} \]

\[ I := (X^3, XY, Y^2). \text{ The Hilbert function corresponding to } I \text{ is the Hilbert function corresponding to the complete intersection } (X^2, Y^2), \text{ so it is liftable to the Hilbert function of an integral } k\text{-algebra. By the previous theorem, the ideal } I \text{ is not liftable to a prime ideal.} \]

The remark after Example 4.5 in [10] proves more than our last theorem. Indeed, by the argument in [10], for any field \( k \) and \( I = (X^3, Y^2, XY) \), the \( k\)-algebra \( k[X, Y]/I \) is not isomorphic to a graded \( k\)-algebra which is an integral domain modulo a homogeneous regular sequence. More generally, by the same argument one can take \( I = (X^m, Y^{m+1}, XY) \), where \( m \geq 2. \)
The next theorem shows that it is much harder for an $O$-sequence to be the Hilbert function of an integral domain than to be the Hilbert function of a reduced graded $k$-algebra.

**Theorem 4.5.** Let $H$ be the Hilbert function of a domain, with $H(1)=3$, $H$ 0-dimensional. Suppose $i<j$ and $\Delta H(i) > \Delta H(j) > 0$. Then $\Delta H(j+1) < \Delta H(j)$. (That is, once $\Delta H$ starts to decrease, it decreases strictly until reaching 0).

**Proof.** Let $H$ be the Hilbert function of $A = k[X_0, X_1, X_2]/P$, where $P$ is homogeneous of height 2. Let $f$ be a homogeneous generator of $P$ of lowest degree. Let $g$ be a homogeneous element of $P$ of lowest degree that is not a multiple of $f$. The theorem follows from [2, 2.1(c)] once one notices that because $A$ is an integral domain, $\beta$ in [2] is equal to the degree of $g$, the latter clearly being the smallest integer $j$ such that $\Delta H(j) < \Delta H(j-1)$. 

For example, for any field $k$, the $O$-sequence $H := 1 \ 3 \ 4 \ 5 \rightarrow$ (so that $\Delta H = 1 \ 2 \ 1 \ 1 \ 0 \rightarrow$) is the Hilbert function of a reduced graded $k$-algebra $k$, but is not the Hilbert function of an integral graded $k$-algebra.

In fact, for any field $k$ and for all $m \geq 0$, the iterated integral

$$F_m := \left\lfloor \frac{\Delta H}{m} \right\rfloor$$

is not the Hilbert function of an integral graded $k$-algebra. In order to prove this we use an argument based on an idea due to Geramita. Assume that for some $m \geq 1$ there is a prime ideal $P$ in $\bar{R} = k[X_0, \ldots, X_{m+1}]$ with corresponding Hilbert function $F_m$ (we have $F_m(1) = m + 2$). As $F_m(2) = \binom{m+3}{2} - 2$, we see that there are in $P$ two linearly independent quadratic forms $u$ and $v$. As $P$ is prime and $P \cap \bar{R} = 0$, the forms $u$ and $v$ are prime. It follows that the Hilbert function corresponding to the ideal $(u, v)$ is Cl$(m+1; 2, 2)$, thus $F_m = \text{Cl}(m+1; 2, 2)$, which is not the case because $F_m(3) > \text{Cl}(m+1; 2, 2)$. (It is easily proved inductively, starting with $m = 0$ that for $m \geq 1$ it holds that $F_m(i) = \text{Cl}(m+1; 2, 2)(i)$ for $i \leq 2$ and $F_m(3) = \text{Cl}(m+1; 2, 2)(3) + 1$.)

The fact that iterated integration does not lead generally to the Hilbert function of an integral domain was suggested by Stanley, correcting a mistake in a previous version of this paper (cf. also the remark after Example 4.5 in [10]).

We conclude this section by remarking that one can produce explicit examples of one-dimensional integral graded $k$-algebras by choosing generators $x_1, \ldots, x_n$ of a finite degree extension field $K$ of $k$. Let $M$ be the kernel of the homomorphism $k[X_0, \ldots, X_n] \rightarrow K$ defined by sending $X_i$ to $x_i$. Let $P$ be the homogenization of $M$ with respect to $X_0$. Then $A := R/P$ is the desired graded $k$-algebra. The Hilbert function of $A$ can then be found using the discussion of $H^S$ in Section 2. This
method is suitable for numerical calculation if $k$ is finite. For $k = \mathbb{F}_2$ we verified with a computer that every zero-dimensional differentiable $O$-sequence $H$ with $H(1) = 3$ and degree $\leq 23$ not ruled out by Theorem 4.5 is the Hilbert function of an integral graded $k$-algebra. (Thus the cardinality assumption in Theorem 2.3 is far from being necessary). On the other hand we have

**Example 4.6.** Let $k$ and $a \in k$ be such that $X^{2n} - a$ is irreducible in $k[X]$ ($n \geq 4$). Let $x$ be the canonical image of $X$ in the field $k[X]/(X^{2n} - a)$. In the above discussion let $x_1 = x$, $x_2 = x^n$, and $x_3 = x^{n+1}$. Let $A$ (in the notation above) have Hilbert function $H$. Then $AH$ is the sequence $1 3 2 2 \ldots 2 0 \rightarrow (2$ repeated $n - 2$ times). Thus Theorem 4.5 is false if $H(1) > 3$. 

**References**