ON THE LIFTING PROBLEM FOR HOMOGENEOUS IDEALS IN POLYNOMIAL RINGS

Moshe ROITMAN

Department of Mathematics, University of Haifa, Mount Carmel, Haifa 31999, Israel

Communicated by C.A. Weibel
Received 18 November 1985
Revised 24 June 1986

We prove here that if $k$ is a field of zero characteristic, then any homogenous ideal in $k[\mathbb{X}, \mathbb{Y}]$ is liftable to a radical ideal. On the other hand, if $k$ is a finite field, then for any $n \geq 2$, there exist zero-dimensional monomial ideals in $k[\mathbb{X}, \ldots, \mathbb{X}_n]$ which are not liftable to radical ideals.

We deal here with the lifting problem posed in [1] (see definition below). For more background and motivation see also [2, §4].

All the rings here are commutative with unit. A graded ring here is an $\mathbb{N}$-graded ring. If $R$ is a graded ring and $0 \neq x \in R$, we denote by $l(x)$ the homogeneous component of highest degree which occurs in a homogeneous decomposition of $x$ and call it the leading form of $x$. We define $\deg x = \deg(l(x))$, $l(0) = 0$, $\deg(0) = i$ for any $i \geq 0$. For any ideal $I$ of $R$ we denote by $l(I)$ the ideal in $R$ generated by $\{l(x): x \in I\}$.

If $R$ is any ring, an ideal $I \neq R$ of $R$ is called zero-dimensional if the ring $R/I$ is zero-dimensional, that is if $\sqrt{I}$ is a finite intersection of maximal ideals. An element $u$ of $R$ is called radical if the ideal $Ru$ is radical.

If $k$ is a ring, $J$ is an ideal in $k[\mathbb{X}_0, \ldots, \mathbb{X}_n]$ and $c \in k$, let $J(c, \mathbb{X}_1, \ldots, \mathbb{X}_n) = \{F(c, \mathbb{X}_1, \ldots, \mathbb{X}_n): F(\mathbb{X}_0, \ldots, \mathbb{X}_n) \in J\}$. Clearly, $J(c, \mathbb{X}_1, \ldots, \mathbb{X}_n)$ is an ideal in $k[\mathbb{X}_1, \ldots, \mathbb{X}_n]$. If $J$ is a homogeneous ideal in $k[\mathbb{X}_0, \ldots, \mathbb{X}_n]$, then $J(0, \mathbb{X}_1, \ldots, \mathbb{X}_n)$ is homogeneous in $k[\mathbb{X}_1, \ldots, \mathbb{X}_n]$ and $J(1, \mathbb{X}_1, \ldots, \mathbb{X}_n)$ is the dehomogenization of $J$ with respect to $\mathbb{X}_0$.

If $S$ is a subset of a vector space $V$ over a field $k$, we denote by $kS$ the subspace of $V$ spanned by $S$.

Definition (Stanley [5]). A standard $G$-algebra over a ring $k$ is a graded $k$-algebra $A$ such that $A_0 = k$ and $A$ is generated (as an algebra over $k$) by a finite number of homogeneous elements of degree 1.

In order words, a standard $G$-algebra over $k$ is a graded $k$-algebra which is isomorphic to a graded $k$-algebra of the type $k[\mathbb{X}_1, \ldots, \mathbb{X}_n]/I$, where $I$ is a...
homogeneous ideal in the polynomial ring $k[X_1, \ldots, X_n]$. In this paper a standard $G$-algebra over $k$ will be called in short a $k$-algebra.

**Definition.** Let $k$ be a ring, $A$ and $A'$ $k$-algebras. The algebra $A'$ is a *lifting* of the algebra $A$ 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 (cf. Grothendieck's lifting problem, e.g. in [4]).

We express lifting of algebras over a field in terms of ideals (see Proposition 2 below):

**Definition.** Let $k$ be a ring, $I$ and $I'$ homogeneous ideals in $k[X_1, \ldots, X_n]$ and $k[X_0, \ldots X_n]$ respectively. We say that $I'$ is a lifting of $I$ if $X_0$ is not a zero-divisor mod $I'$ and there exists an automorphism $\theta$ of $k[X_1, \ldots, X_n]$ (as a graded $k$-algebra) such that $\theta(I) = I'(0, X_1, \ldots, X_n)$.

An equivalent formulation of the last condition is the following: there exists an automorphism $\phi$ of $k[X_1, \ldots, X_n]$ (as a graded $k$-algebra) such that the homomorphism of $k$-algebras $k[X_0, \ldots, X_n] \to [X_1, \ldots, X_n]$ which sends $X_0 \mapsto 0$, $X_i \mapsto \phi(X_i)$ ($1 \leq i \leq n$) induces an isomorphism of $k$-graded modules $(I', X_0)/(X_0) \cong I$. This is a possible interpretation of [1, Definition 1.7(iii)].

**Lemma 1.** Let $k$ be a field, $V$ an $n$-dimensional $k$-vector space, $W$ a subspace of $V$ and $v_1, \ldots, v_n$ vectors in $V$ which span $V$ mod $W$. Then there exists a basis \{u_1, \ldots, u_n\} of $V$ such that $u_i = v_i$ mod $W$ for $1 \leq i \leq n$.

**Proof.** We may assume that $W \neq 0$. We prove the lemma by induction on $n$ starting with $n = 1$. Let $n > 1$. If $v_1 \neq 0$, let $u_1 = v_1$. If $v_1 = 0$, let $u_1$ be any nonzero element of $W$. By the inductive assumption (with respect to the vector space $V/ku_1$), there exist vectors $u'_2, \ldots, u'_n$ in $V$ which are linearly independent mod $ku_1$ and such that $u'_i = v_i + \alpha_i u_1$ mod $W$ for $\alpha_i \in k$ ($2 \leq i \leq n$). Let $u_i = u_i - \alpha_i u_1$ for $2 \leq i \leq n$. Clearly, $u_1, \ldots, u_n$ fulfil the requirements in the lemma.

**Proposition 2** (cf. Geramita et al. [1]). Let $k$ be a field, $I$ and $I'$ homogeneous ideals in $k[X_1, \ldots, X_n]$ and $k[X_0, \ldots, X_n]$ respectively. Then the ideal $I'$ is a lifting of $I$ $\iff$ the $k$-algebra $A' := k[X_0, \ldots, X_n]/I'$ is a lifting of $A := k[X_1, \ldots, X_n]/I$.

**Proof.** $\Rightarrow$. We may assume that $I = I'(0, X_1, \ldots, X_n)$. Let $J = \ker \phi$, where $\phi$ is the homomorphism of $k$-algebras $k[X_0, \ldots, X_n] \to k[X_1, \ldots, X_n]/I' = A$, which sends $X_0 \mapsto 0$, $X_i \mapsto X_i + I$ ($1 \leq i \leq n$). Clearly, $(I', X_0) \subseteq J$. Conversely, if $F \in J$, then $F(0, X_1, \ldots, X_n) \in I$, so there exists $G(X_0, \ldots, X_n)$ in $I'$ such that $G(0, X_1, \ldots, X_n) = F(0, X_1, \ldots, X_n)$, thus $F(X_0, X_1, \ldots, X_n) \in I'$ for all $X_0, X_1, \ldots, X_n \in k$.
On the lifting problem for homogeneous ideals

207

It follows that $J = (I', X_0)$. Now, $A'/X_0A'$ is isomorphic to $k[X_0, \ldots, X_n]/(I', X_0)$, so $A \cong A'/A'X_0$. As $X_0$ is not a zero-divisor mod $I'$, we conclude that $A'$ is a lifting of $A$.

As $A \cong A'/X_0A' \cong k[X_0, \ldots, X_n]/(I', X_0)$, we have a graded epimorphism $\phi: k[X_0, \ldots, X_n] \rightarrow k[X_1, \ldots, X_n]/I = A$ with $\ker \phi = (I', X_0)$. There exist in $k[X_1, \ldots, X_n]$ $n$ linearly independent forms $Y_1, \ldots, Y_n$, such that $\phi(X_i) = Y_i + I$ for $1 \leq i \leq n$. (This follows from Lemma 1 with respect to $V = (k[X_1, \ldots, X_n]), W = I_1$ and elements $u_i \in (k[X_1, \ldots, X_n])$, such that $\phi(X_i) - v_i + I$ ($1 \leq i \leq n$). Here $(k[X_1, \ldots, X_n])$, denotes the subspace of all linear forms in $k[X_1, \ldots, X_n]$ and similarly for $I_1$.) Let $\theta$ be the $k$-graded automorphism of $k[X_1, \ldots, X_n]$ which fulfils $\theta(Y_i) = X_i$ ($1 \leq i \leq n$). We have for any polynomial $F(X_0, X_1, \ldots, X_n)$ in $k[X_0, \ldots, X_n]$: $\phi(F(X_0, X_1, \ldots, X_n)) = F(0, Y_1 + I, \ldots, Y_n + I)$, hence $F(X_0, X_1, \ldots, X_n) \in \ker \phi$ if and only if $F(0, Y_1, \ldots, Y_n) \in \theta(I)$ if and only if $\theta(I) = \theta(I')(0, X_1, \ldots, X_n)$. As $X_0$ is not a zero-divisor mod $I'$, we conclude that $I'$ is a lifting of $I$. □

Definition. Let $k$ be a ring. A $k$-algebra $A$ is liftable to a reduced (respectively integral) algebra if it has a lifting which is a reduced (respectively integral) algebra. Similarly, a homogeneous ideal $I$ in $k[X_1, \ldots, X_n]$ is liftable to a radical (respectively prime) ideal if it has a lifting which is a radical (respectively prime) ideal.

Thus, if $k$ is a field, a homogeneous ideal $I$ in $k[X_1, \ldots, X_n]$ is liftable to a radical (respectively prime) ideal if and only if the algebra $k[X_1, \ldots, X_n]/I$ is liftable to a reduced algebra (respectively to an integral domain). In this paper, we deal with lifting ideals to radical or to prime ideals, that is lifting algebras to reduced or to integral algebras. Such liftings are useful e.g. in investigating Hilbert functions (cf. the proof of [1, Corollary 2.5] for reduced algebras. Some applications for integral domains will be included in a forthcoming paper of the present author with L.G. Roberts).

Lemma 3. Let $k$ be any ring, $I'$ a homogeneous ideal in $k[X_0, \ldots, X_n]$ such that $X_0$ is not a zero-divisor mod $I'$. Then $I'(0, X_1, \ldots, X_n) = \langle I'(1, X_1, \ldots, X_n) \rangle$.

Proof. Let $F(X_0, \ldots, X_n)$ be a homogeneous polynomial in $I'$ such that $F(0, X_1, \ldots, X_n) \neq 0$, $F = f_0X_0^d + \cdots + f_d$, where $f_i$ is a form of degree $i$ in $k[X_1, \ldots, X_n]$ ($0 \leq i \leq d$). We have: $F(0, X_1, \ldots, X_n) = f_d = \langle F(1, X_1, \ldots, X_n) \rangle \subseteq \langle I'(1, X_1, \ldots, X_n) \rangle$. As $I'$ is homogeneous, the ideal $I'(0, X_1, \ldots, X_n)$ is generated by $\langle F(0, X_1, \ldots, X_n): F$ homogeneous in $I' \rangle$, so $I'(0, X_1, \ldots, X_n) \subseteq \langle I'(1, X_1, \ldots, X_n) \rangle$.

On the other hand, let $F(X_0, \ldots, X_n) \in I'$ such that $t = \langle F(1, X_1, \ldots, X_n) \rangle \neq 0$, $F(X_0, X_1, \ldots, X_n) = F_0 + \cdots + F_d$, where $F_i$ is a form of degree $i$ in
\[ \kappa[X_0, \ldots, X_n] \ (0 \leq i \leq d) \]. Let \( G = \sum_{i=0}^{d} X_0^{d-i}F_i \), so \( G \in I' \), \( G \) is homogeneous and \( l(G(1, X_1, \ldots, X_n)) = t \). Let \( H = G/X_0 \), where \( r \geq 0 \) is the maximal power of \( X_0 \) dividing \( G \). As \( X_0 \) is not a zero-divisor mod \( I' \), it follows that \( H \in I' \). We also have: \( H \) is homogeneous, \( H(0, X_1, \ldots, X_n) \neq 0 \) and \( l(H(1, X_1, \ldots, X_n)) = t \). As we saw at the beginning of the proof, the following holds: \( H(0, X_1, \ldots, X_n) = I'(H(1, X_1, \ldots, X_n)) = I' \). Finally, \( I'(0, X_1, \ldots, X_n) = l(I'(1, X_1, \ldots, X_n)) \). \( \square \)

From Lemma 3, we obtain immediately

**Proposition 4.** Let \( k \) be a ring, \( I' \) a homogeneous ideal in \( \kappa[X_0, \ldots, X_n] \) such that \( X_0 \) is not a zero-divisor mod \( I' \). Let \( I \) be a homogeneous ideal in \( \kappa[X_1, \ldots, X_n] \). Then \( I' \) is a lifting of \( I \) if and only if there exists a graded \( k \)-automorphism \( \theta \) of \( \kappa[X_1, \ldots, X_n] \) such that \( \theta(I) = l(I'(1, X_1, \ldots, X_n)) \). \( \square \)

In this paper, we use the approach to the lifting problem indicated by the last proposition.

**Proposition 5.** Let \( k \) be any ring, \( I \) a homogeneous ideal in \( \kappa[X_1, \ldots, X_n] \). The following properties are equivalent:

1. \( I \) is liftable to a radical (respectively prime) ideal.
2. There exists a radical (respectively prime) homogeneous ideal \( I' \) in \( \kappa[X_0, \ldots, X_n] \) such that \( X_0 \) is not a zero-divisor mod \( I' \) and \( I'(0, X_1, \ldots, X_n) = I \).
3. There exists a radical (respectively prime) ideal \( \hat{I} \) in \( \kappa[X_1, \ldots, X_n] \) such that \( l(\hat{I}) = I \).

**Proof.** (1) \( \Rightarrow \) (2). Let \( J \) be a radical (respectively prime) homogeneous ideal in \( \kappa[X_0, \ldots, X_n] \) such that \( X_0 \) is not a zero-divisor mod \( J \) and \( J(0, X_1, \ldots, X_n) = \theta(I) \) for some automorphism \( \theta \) of \( \kappa[X_1, \ldots, X_n] \). Let \( \theta' \) be the automorphism of \( \kappa[X_0, \ldots, X_n] \) (as a \( k \)-graded algebra) which fulfills: \( \theta'(X_0) = X_0 \) and \( \theta'(X_i) = \theta(X_i) \) for \( 1 \leq i \leq n \). Define \( I' = \theta^{-1}(J) \). Clearly, \( I' \) is a radical (respectively prime) homogeneous ideal in \( \kappa[X_0, \ldots, X_n] \), \( X_0 \) is not a zero-divisor mod \( I' \) and \( I'(0, X_1, \ldots, X_n) = I \).

(2) \( \Rightarrow \) (3). Let \( I' \) be an ideal in \( \kappa[X_0, \ldots, X_n] \) which fulfills the properties in (2). Let \( \hat{I} = I'(1, X_1, \ldots, X_n) \). By [6, Chapter VII, §5, Theorem 18], which holds for any ring \( k \), \( \hat{I} \) is a radical (respectively prime) ideal in \( \kappa[X_1, \ldots, X_n] \). By Lemma 3, we have \( l(\hat{I}) = I'(0, X_1, \ldots, X_n) = I \), so (3) holds.

(3) \( \Rightarrow \) (1). If \( \hat{I} \) is a radical (respectively prime) ideal in \( \kappa[X_1, \ldots, X_n] \) such that \( l(\hat{I}) = I \), let \( I' \) be the homogenization of \( \hat{I} \) in \( \kappa[X_0, \ldots, X_n] \) with respect to \( X_0 \). Hence \( X_0 \) is not a zero-divisor mod \( I' \). Using [6, Chapter VII, §5, Theorems 17 and 18], which hold for any ring \( k \), we obtain \( \hat{I} = I'(1, X_1, \ldots, X_n) \) and \( I' \) is a radical (respectively prime) ideal. By Lemma 3, \( I = l(I'(1, X_1, \ldots, X_n)) = I'(0, X_1, \ldots, X_n) \). Hence \( I' \) is a radical (respectively prime) lifting of \( I \). \( \square \)
Lemma 6. Let $I$ be an ideal in a graded ring $R$. Then the set of homogeneous elements in $l(I)$ equals the set of the leading forms of elements in $I$.

Proof. We have to show that any homogeneous element $t$ in $l(I)$ is a leading form of an element in $I$. There exists a representation $t = \Sigma r_i l(a_i)$, where $r_i$ are homogeneous in $R$, $a_i$ are in $I$ and $\deg(r_i l(a_i)) = \deg t$ for all $i$. It follows that $t = l(\Sigma r_i a_i)$. \qed

Lemma 7. Let $R$ be a graded ring with $R_0 = k$, a field. Let $I$ be an ideal of $R$. Then $\dim_k R/I = \dim_k R/l(I)$. Furthermore, if $S$ is a set of homogeneous elements in $R$, then we have

- If $\overline{S}$ spans the $k$-vector space $\overline{R} = R/l(I)$, then $S$ is also a set of $k$-generators mod $I$.
- If $S$ is a linearly independent set over $k$ mod $l(I)$, then $S$ has the same property also mod $I$.
- If $S$ is a $k$-basis mod $l(I)$, then $S$ is a $k$-basis also mod $I$.

Proof. Let $S$ be a set of homogeneous elements. Assume that $S$ is a set of generators mod $l(I)$. If $R \neq kS+I$, let $x$ be an element of minimal degree in $R\setminus (kS+I)$. As $R = kS + l(I)$, we have $l(x) = u + v$, for some homogeneous elements $u$ in $kS$, $v$ in $l(I)$, such that $\deg x = \deg u = \deg v$. By Lemma 6, there exists $y \in I$ such that $l(y) = v$. We have $\deg(x - u - y) < \deg x$, so $x - u - y \in kS + I$, a contradiction. It follows that $S$ is a set of $k$-generators mod $I$.

Assume now that $S$ is linearly independent mod $l(I)$. If $S$ is linearly dependent mod $I$, then there exists $x \in I$, $x = \Sigma_{i=1}^m \alpha_i s_i$, with $\alpha_i \in k$, $\alpha_m \neq 0$, $s_i \in S$ and $\deg x = \deg s_m > \deg s_i$ for $1 \leq i \leq m$. It follows that

$$l(x) = \sum_{i: \deg s_i = \deg s_m} \alpha_i s_i$$

so

$$\sum_{i: \deg s_i = \deg s_m} \alpha_i s_i \equiv 0 \pmod{l(I)},$$

a contradiction.

It follows that $S$ is linearly independent mod $I$. The rest of the lemma follows directly from the assertions proved above. \qed

In the notation of Lemma 7, if $S$ is a set of homogeneous elements which is a $k$-basis mod $I$, then $S$ is not necessarily a set of $k$-generators nor linearly independent mod $l(I)$. Indeed, if $I$ is not homogeneous, then let $s$ be a homogeneous element in $l(I)\setminus I$. Let $S$ be a set of homogeneous elements which contain $s$
and is a basis mod $I$. Then $S$ is linearly dependent mod $l(I)$, because $s \in S \cap l(I)$. $S$ is not a set of generators mod $l(I)$, otherwise we can choose a subset $S_1$ of $S$ which is a basis mod $l(I)$, and so also mod $I$ by Lemma 7. As $S_1$ is a basis mod $l(I)$, we have $s \not\in S_1$, so $S_1 \not\subseteq S$, but $S_1$ and $S$ are bases mod $I$, a contradiction.

We now present a simplified version of the proof of [1, Theorem 2.2]:

**Theorem 8** (Geramita et al. [1, Theorem 2.2]. Let $I$ be an ideal in $k[X_1, \ldots, X_n]$ generated by a finite set $M$ of monomials, $k$ a field with at least $e$ elements, where $e = \max\{a; \text{there exists a monomial } X_1^{a_1} \cdots X_n^{a_n} \text{ in } M \text{ with } a_i = a \text{ for some } i\}$. Then $I$ is liftable to a radical ideal.

**Proof.** Let $L$ be an infinite field which contains $k$. For any $1 \leq j \leq n$ choose an infinite set of distinct elements $t_{j,0}, \ldots, t_{j,e-1}$ in $k$. We associate with any monomial $X_1^{a_1} \cdots X_n^{a_n}$ which is not in $I$ the point $(t_{1,b_1}, \ldots, t_{n,b_n})$ in $L^n$. Let $V$ be the set of all these points and let $\hat{I}$ be the set of all the polynomials in $k[X_1, \ldots, X_n]$ which vanish on $V$. For any monomial $X_1^{a_1}X_2^{a_2} \cdots X_n^{a_n}$ in $M$, we have $f(X_1, \ldots, X_n) = \Pi_{j=1}^n \Pi_{i=0}^{a_i-1} (X_j - t_{i,j}) \subseteq \hat{I}$. Indeed, if $X_1^{b_1} \cdots X_n^{b_n} \not\in I$, then for some $j$ we have $a_j > b_j$, so $X_j - t_{i,j}$ occurs in the product $\Pi_{i=0}^{a_i-1} (X_j - t_{i,j})$. It follows that $f(X_1, \ldots, X_n)$ vanishes at the point $(t_{1,b_1}, \ldots, t_{n,b_n})$ which is associated with the monomial $X_1^{b_1} \cdots X_n^{b_n}$, so $f \in \hat{I}$. As $l(f) = X_1^{b_1} \cdots X_n^{b_n}$, we conclude $l(\hat{I}) \supseteq I$.

Assume that $l(\hat{I}) = I$ and let $u \in l(\hat{I}) \setminus I$. We may assume that $u$ is a linear combination over $k$ of distinct monomials which do not belong to $I$. Let $M_1, \ldots, M_m$ be all the monomials that are divisors of the monomials which occur in this linear combination, hence $M_i \not\subseteq I$ for $1 \leq i \leq m$. Let $P_1, \ldots, P_m$ be the points in $L^n$ associated with $M_1, \ldots, M_m$. Let $I_0$ be the set of all the polynomials in $L[X_1, \ldots, X_n]$ vanishing at $P_1, \ldots, P_m$. We have $I_0 \supseteq \hat{I}[L[X_1, \ldots, X_n]]$, so $l(I_0) \supseteq l(\hat{I})$, $u \in l(I_0)$. By the argument above, if $M$ is a monomial different from $M_1, \ldots, M_m$, then $M \in l(I_0)$. As $u \in l(I_0)$, we conclude $\dim_L L[X_1, \ldots, X_n]/l(I_0) < m$. On the other hand, $I_0$ is the ideal in $L[X_1, \ldots, X_n]$ of all the polynomials vanishing at a set of $m$ distinct $L$-rational points (namely $\{P_1, \ldots, P_m\}$), hence $\dim_L L[X_0, \ldots, X_n]/I_0 = m$. Using Lemma 7 we obtain: $m = \dim_L L[X_0, \ldots, X_n]/I_0 = \dim_L L[X_1, \ldots, X_n]/l(I_0) < m$, a contradiction. Thus, $l(\hat{I}) = I$. As $\hat{I}$ is radical, it follows from Proposition 5 that $I$ is liftable to a radical ideal. □

By Theorem 8 we see that any monomial ideal in $k[X_1, \ldots, X_n]$, where $k$ is an infinite field, is liftable to a radical ideal. Over a finite field this is false.

**Theorem 9.** For any finite field $k$ and for any $n \geq 2$, there exists a zero-dimensional monomial ideal in $k[X_1, \ldots, X_n]$ which is not liftable to a radical ideal.
Proof. First consider the case $n = 2$. Let $m > |k|$. Let $I = (X^m, X^{m-1}Y^t_1, \ldots, XY^{m-1}, Y^m)$, where $r_1, \ldots, r_m$ are positive integers which fulfil the following conditions defined recursively: $r_0 = 0$. Let $0 \leq i \leq m - 1$. Let $J$ be an ideal which is generated by $i + 1$ polynomials with leading forms $X^m, X^{m-1}Y^t_1, \ldots, X^{m-i}Y^t_i$ and contains a polynomial with leading forms $X^m X^{m-i}Y^t_i$ for some $t \geq 0$. Let $t(J)$ be the minimal possible $t$. As the number of ideals $J$ as above is finite we can choose $r_{i+1}$ such that $r_{i+1} > t(J)$ for all $J$ as above and $r_{i+1} > r_i$. For example we can choose $r_i > 0$ arbitrarily.

Clearly, $I$ is a zero-dimensional monomial ideal. We claim that $I$ is not liftable to a radical ideal. Assume the contrary. By Proposition 5 there exists a radical ideal $\tilde{I}$ in $k[X_1, \ldots, X_n]$ such that $l(\tilde{I}) = I$. For any homogeneous $f \in I$, choose $\tilde{f}$ in $\tilde{I}$ such that $l(\tilde{f}) = f$. Let $g_i$ be the GCD of the polynomials $(X^m)^{r_i}, (X^{m-i}Y^t_i)^{r_i}, \ldots, (X^{m-1}Y^t_1)^{r_i}$ (for $0 \leq r_i \leq m - 1$). For any $i$, let $g_i$ be the GCD of the polynomials $(X^m)^{r_i}, X^{m-i}Y^t_i, \ldots, X^{m-1}Y^t_i$. We see that $l(g_i) = a_i X^m$ for some $a_i \neq 0$ in $k$ and $0 \leq i \leq m - 1$. Replacing $g_i$ by $a_i^{-1} g_i$ we may assume: $l(g_i) = X^m$.

We claim by induction on $i$ that $s_i = m - i$ for $0 \leq i \leq m - 1$. The case $i = 0$ is obvious. Let $0 < i < m - 1$. Assume $s_i < m - i$. Let $h_i$ be a polynomial in $((X^m)^{r_i}, \ldots, (X^{m-1}Y^t_i)^{r_i})$ such that $l(h_i)$ is of the form $X^m X^{m-i}Y^t_i$ with $t$ minimal. We have by definition: $t < r_{i+1} < \cdots < r_m$. On the other hand, for $0 < j < i$, we have $m - i - 1 < m - j$, so the monomial $X^m X^{m-i}Y^t_i$ is not divisible by any of the monomials $X^m, X^{m-1}Y^t_i, \ldots, Y^{m-1}$. It follows that $X^m X^{m-i}Y^t_i \not\in ((X^m)^{r_i}, \ldots, (X^{m-1}Y^t_i)^{r_i})$, contradicting the assumption $l(h_i) = X^m$. It follows that $l(h_i) = X^{m-i}$ for $0 < i < m - 1$.

We have: $g_{m-1} g_{m-2} \cdots g_0 = (X^m)^{r_i}$. As $l(g_{m-1}) = X$, we obtain $g_{m-1} = X + a_{m-1}$ for some $a_{m-1}$ in $k$. We have $l(g_{m-2} g_{m-1}) = X$, so $g_{m-2} g_{m-1} = X + a_{m-2}$ for some $a_{m-2}$ in $k$. Finally we conclude $g_0 = (X^m) = \prod_{i=1} (X + a_i)$, with $a_i \in k$. As $m > |k|$, we may assume $a_i = a_2$. As $\tilde{I}$ is radical, $\prod_{i=2} (X + a_i) \in \tilde{I}$, so $X^m \in l(\tilde{I}) \setminus I$, a contradiction. It follows that $I$ is not liftable to a radical ideal.

For $n > 2$, let $I_n = (I, X_3, \ldots, X_n)$. (Here we denote $X = X_1, Y = X_2$). Clearly $I_n$ is a monomial zero-dimensional ideal in $k[X_1, X_2, \ldots, X_n]$. Assume that $I_n$ is liftable to a radical ideal, then by Proposition 5 there exists a radical ideal $\tilde{I}_n$ in $k[X_1, \ldots, X_n]$ such that $l(\tilde{I}_n) = I_n$. Let $X_i - a_i \in \tilde{I}_n$, $a_i \in k$, $3 \leq i \leq n$. Let $\tilde{I} = \tilde{I}_n(X_1, X_2, a_3, \ldots, a_n) \subseteq k[X_1, X_2]$. We have $k[X_1, X_2] / \tilde{I} \cong k[X_1 \ldots X_n] / \tilde{I}_n$, so $\tilde{I}$ is radical. It is easy to show that $l(\tilde{I}) = I$, contradicting the fact that $I$ is not liftable to a radical ideal. It follows that $I_n$ is not liftable to a radical ideal.

Theorem 10. Any homogeneous ideal in $k[X, Y]$, where $k$ is a field of zero characteristic, is liftable to a radical ideal.
Proof. Let $R = k[X, Y]$. We prove the theorem first for zero-dimensional homogeneous ideals. If the theorem does not hold for such ideals, let $I$ be a maximal counterexample, so $I 
eq R$. As $R/RX$ is a graded principal ideal ring, there exists a homogeneous element $f$ in $I$ such that $I = (RX \cap I) + Rf$. Let $J = (I : X)$, so $(RX) \cap I = JX$. As $I$ is zero-dimensional we have $J \supseteq I$ (take e.g. $X^m \in I$, with $m > 0$ minimal and then $X^{m-1} \in JI$). We have also $X \not| f$. By assumption and by Proposition 5 there exists a radical ideal $\hat{J}$ in $k[X, Y]$ such that $l(\hat{J}) = J$. (In case $J = R$, take $\hat{J} = R$.) Let $u$ be an element in $\hat{J}$ such that $l(u) = f \pmod{(RX \cap I)}$ (so $\deg u = \deg f$, $X \not| l(u)$) and the number of distinct (non-associate) prime factors in a prime decomposition of $u$ is maximal among all such elements. If $u$ is not radical, let $u = u_1v_1$, where $u_1$ is a prime element. Let $d = \deg u_1$. As $k$ is infinite and $X \not| u$ we can choose $a \in k$ such that $u_1 + aX^d$ is not associated with any prime factor of $u_1v$. Let $u' - (u_1 + aX^d)u_1v$. As $\hat{J}$ is radical, we have $u_1v \not\in \hat{J}$, so $u' \in \hat{J}$. We have $l(u') = l(u) + aX^dl(u_1v)$ and $l(u_1v) \in I$, $X^dl(u_1v) \in I$, so $l(u') = f \pmod{RX \cap I}$. The number of distinct prime factors of $u'$ is strictly greater than that of $u$, a contradiction. It follows that $u$ is radical. Let $c(X)$ be the discriminant of $u$ as a polynomial in $Y$ over $k(X)$. We have $c(X) \neq 0$, because $k$ is of zero characteristic and any irreducible polynomial in $Y$ over $k(X)$ has distinct roots in a splitting field. Choose $a \in k$ such that $X - a$ does not belong to any of the primes associated with $\hat{J}$ and $c(a) \neq 0$. It follows that $u(a, Y)$ is radical, so the ideal $(X - a, u(X, Y))$ is radical. Let $\hat{J} = (X - a, u) \cap \hat{J}$. Clearly $\hat{J}$ is radical. We claim that $l(\hat{J}) = I$. As $I = (RX \cap I) + Rl(u)$, if $g$ is a homogeneous element of $I_1$ then $g = jX + rl(u)$ for some homogeneous elements $j$ in $J$ and $r$ in $R$. Let $\hat{j} \in \hat{J}$ such that $l(\hat{j}) = j$. For $\hat{g} = \hat{j}(X - a) + ru$ we have $l(\hat{g}) = g$ and $\hat{g} \in (X - a, u) \cap \hat{J}$. It follows that $l \subseteq l(\hat{J})$. On the other hand, let $v \in I$, so $v = r(X - a) + su$ for some $r, s \in R$, $s \in k[Y]$. We have: $v \in \hat{J}$, so $r(X - a) \in J$ and as $X - a$ is not a zero-divisor mod $\hat{J}$, we have $r \in \hat{J}$. This proves that $\hat{J} = \hat{j}(X - a) + Ru$. As $X \not| l(u)$ and $s \in k[Y]$, the leading forms of $r(X - a)$ and $su$ cannot cancel each other so there are the following possibilities: $l(v) = l(r)X + l(s)l(u), l(v) = l(r)X$ and $l(v) = l(s)l(u)$. In each case, taking into account the facts: $l(r) \in J$, $l(r)X \in I$, $l(s) \in I$, we obtain $l(v) \in I$, so $I = l(\hat{J})$. By Proposition 5, $I$ is liftable to a radical ideal.

Assume now that $I \neq 0$ is not zero-dimensional. Let $g$ be the GCD of all the elements in $I$, so $I = Kg$ with $K$ homogeneous zero-dimensional or $K = R$. Let $K$ be a radical ideal in $K[X, Y]$ such that $l(K) = K$. Let $g = g_1g_2 \ldots g_m$ be a prime decomposition of $g$. Choose $a_1, \ldots, a_m$ in $k$ such that $g_1 - a_1, \ldots, g_m - a_m$ are not associates and $g_i - a_i$ is not a zero-divisor mod $\hat{K}$ for each $i$. It follows that $g_i - a_1, \ldots, g_m - a_m$ are nonassociated primes and for $u = \prod_{i=1}^{m} (g_i - a_i)$ we have $Ru + \hat{K} = R$. Let $\hat{I} = \hat{K}u = \hat{K} \cap Ru$. Clearly, $I$ is radical and $l(\hat{I}) = I$. By Proposition 5, $I$ is liftable to a radical ideal. □

Lemma 11. Let $k$ be a field. Then the ideal $(X_1, \ldots, X_n)$ in $k[X_1, \ldots, X_n]$ is liftable to a prime ideal $\iff$ there exists an algebraic extension $k(s_1, \ldots, s_n)$ of $k$
such that the elements \( s_1^{i_1} \cdots s_n^{i_n} \) \( (0 \leq i_1 + \cdots + i_n < r) \) form a basis for \( k(s_1, \ldots , s_n) \) as a vector space over \( k \).

**Proof.** \( \Rightarrow \). By Proposition 5 there exists a prime ideal \( m \) in \( k[X_1, \ldots , X_n] \) such that \( l(m) = (X_1, \ldots, X_n)' \) and so \( m \) is maximal. Let \( s_i = \bar{x}_i \in k[X_1, \ldots, X_n]/m \) \( (1 \leq i \leq n) \). We have: \( k[X_1, \ldots, X_n]/m = k(s_1, \ldots, s_n) \) is an algebraic extension of \( k \) and the elements \( s_1^{i_1} \cdots s_n^{i_n} \) \( (0 \leq i_1 + \cdots + i_n < r) \) are linearly independent over \( k \) (linear dependence would imply the existence in \( m \) of a non-zero polynomial of total degree \( < r \), contradicting the fact that \( l(m) = (X_1, \ldots, X_n)' \)).

The elements \( s_1^{i_1} \cdots s_n^{i_n} \) \( (0 \leq i_1 + \cdots + i_n < r) \) form a basis of \( k[X_1, \ldots, X_n]/m \) by Lemma 7. (Alternatively, as \( l(m) = (X_1, \ldots, X_n)' \), any monomial in \( s_1, \ldots, s_n \) of total degree \( r \) is a linear combination of the elements \( s_1^{i_1} \cdots s_n^{i_n} \) \( (0 \leq i_1 + \cdots + i_n < r) \) and therefore so is any other monomial in \( s_1, \ldots, s_n \) of any degree. Use Lemma 7.)

\( \Leftarrow \). Let \( m \) be the ideal of all the polynomials in \( k[X_1, \ldots, X_n] \) vanishing at the point \( (s_1, \ldots, s_n) \). We have: \( m \) is a maximal ideal because \( k[X_1, \ldots, X_n]/m \cong k(s_1, \ldots, s_n) \). For any monomial \( M(X_1, \ldots, X_n) \) of degree \( r \), there are scalars \( a_{i_1, \ldots, i_n}^{(M)} \) in \( k \) such that

\[
M(s_1, \ldots, s_n) = \sum_{0 \leq i_1 + \cdots + i_n < r} a_{i_1, \ldots, i_n}^{(M)} s_1^{i_1} \cdots s_n^{i_n}.
\]

Let

\[
f_M = M(X_1, \ldots, X_n) - \sum_{0 \leq i_1 + \cdots + i_n < r} a_{i_1, \ldots, i_n}^{(M)} X_1^{i_1} \cdots X_n^{i_n}.
\]

We have: \( f_M \in m \) for all \( M \), so \( l(m) \supseteq (X_1, \ldots, X_n)' \). On the other hand, as the set \( \{s_1^{i_1} \cdots s_n^{i_n} : 0 \leq i_1 + \cdots + i_n < r\} \) is a basis of \( k(s_1, \ldots, s_n) \) over \( k \), we have

\[
\dim_k k[X_1, \ldots, X_n]/m = \binom{n + r - 1}{n},
\]

the number of monomials in \( n \) indeterminates of degree \( < r \). By Lemma 7,

\[
\dim_k \frac{k[X_1, \ldots, X_n]}{l(m)} = \binom{n + r - 1}{n},
\]

so

\[
\dim_k \frac{k[X_1, \ldots, X_n]}{l(m)} = \dim_k \frac{k[X_1, \ldots, X_n]}{(X_1, \ldots, X_n)'},
\]

so \( l(m) = (X_1, \ldots, X_n)' \).

We conclude that \( (X_1, \ldots, X_n)' \) is liftable to a prime ideal. \( \square \)

**Proposition 12.** Let \( k \) be a finite field, \( r \geq 1 \) and assume \( |k| \geq r \). Then, for any \( n \geq 1 \), the ideal \( (X_1, \ldots, X_n)' \) in \( k[X_1, \ldots, X_n] \) is liftable to a prime ideal.
Proof. Let $L$ be a field extension of degree $N$ over $k$, where $N = \binom{n}{r}^{-1}$ is the number of monomials of degree $< r$ in $X_1, \ldots, X_n$. Let $|k| = q$, so $|L| = q^N$.

For given $a_{i_1}, \ldots, a_{i_n}$ in $k$ ($i_1 + \cdots + i_n < r$), not all zero, the number of solutions in $L^n$ to the equation

$$
\sum_{0 \leq i_1 + \cdots + i_n < r} a_{i_1} \ldots a_{i_n} X_1^{i_1} \ldots X_n^{i_n} = 0
$$

is at most $(r - 1)|L|^{n-1} = (r - 1)(q^N)^{n-1}$ [4, Theorem 6.13]. The number of all such equations, after identifying proportional equations is $(q^N - 1)/(q - 1)$. The total number of solutions in $L^n$ to such equations is at most $(r - 1) q^{N(n-1)} \cdot (q^N - 1)/(q - 1) < ((r - 1)/(q - 1)) q^{N(n-1)} q^N = |L|^n$. Therefore, there exist $s_1, \ldots, s_n$ in $L$ such that the elements $s_1^{i_1} \ldots s_n^{i_n}$ ($0 \leq i_1 + \cdots i_n < r$) are linearly independent over $k$. By Lemma 11, the ideal $(X_1, \ldots, X_n)'$ is liftable to a prime ideal. \( \square \)

We do not know if the restriction $|k| \geq r$ in Proposition 12 can be removed. For any given $n$ and $r$, using Proposition 12 and Lemma 11, one can check algorithmically if the ideal $(X_1, \ldots, X_n)'$ is liftable to a prime ideal over any finite field. For example this holds for $n = 2$ and $1 \leq r \leq 3$. (For $1 \leq r \leq 2$ this holds for any $n$ and the proof is easy. Let $n = 2$, $r = 3$. By Proposition 12 it is enough to check the case $|k| = 2$. In this case let $s$ be a root of the polynomial $X^6 + X^5 + 1$ over $k$ and $t = s^3$. We have $[k(s): k] = 6$ is the number of monomials in $X, Y$ of degree $< 3$ and the elements $1, s, t, s^2, st, t^2$ which are equal to $1, s, s^3, s^2, s^4, s^5 = s^5 + 1$ respectively are equal to each other over $k$ as $[k(s): k] = 6$. By Lemma 11 we conclude that $(X, Y)^3$ is liftable to a prime ideal.)

**Proposition 13.** For any $n$, any power of the ideal $(X_1, \ldots, X_n)$ in $\mathbb{Q}[X_1, \ldots, X_n]$ is liftable to a prime ideal.

**Proof.** Let $r \geq 1$, $N = \binom{n}{r}^{-1}$ = the number of monomials in $n$ indeterminates of degree $< r$ and let $p \geq r$ be a prime number. By Proposition 12 and Lemma 11, there exists an algebraic extension $F_p(s_1, \ldots, s_n)$ of $F_p = \mathbb{Z}/p\mathbb{Z}$, such that $\{s_1^{i_1} s_2^{i_2} \cdots s_n^{i_n} : 0 \leq i_1 + \cdots + i_n < r\}$ is a basis for $F_p(s_1, \ldots, s_n)$ over $F_p$. There exists an element $s$ such that $F_p(s_1, \ldots, s_n) = F_p(s)$. Let $f_0(X)$ be the minimal polynomial of $s$ over $F_p$, so $\deg f_0(X) = N$ and let $f_1(X), \ldots, f_n(X)$ be polynomials in $F_p[X]$ such that $s_i = f_i(s)$ for $1 \leq i \leq n$. Let $g_0(X), g_1(X), \ldots, g_n(X)$ be polynomials in $\mathbb{Z}[X]$, such that their canonical images in $\mathbb{Z}/p\mathbb{Z}[X]$ are $f_0(X), f_1(X), \ldots, f_n(X)$ respectively and $g_0(X)$ is a monic polynomial. Clearly $g_0(X)$ is an irreducible polynomial in $\mathbb{Z}[X]$ and also in $\mathbb{Q}[X]$. Let $t$ be a root of $g_0(X)$ in $\mathbb{C}$ and let $t_i = g_i(t)$ ($1 \leq i \leq n$). We have $[\mathbb{Q}(t): \mathbb{Q}] = \deg g_0(X) = N$, so, to finish the proof, it is enough to show that the elements $t_1^{i_1} \ldots t_n^{i_n}$ ($0 \leq i_1 + \cdots + i_n < r$) are
linearly independent over \( \mathbb{Q} \) (see Lemma 11). Let
\[
\sum_{0 \leq i_1 + \cdots + i_n < r} a_{i_1, \ldots, i_n} t_1^{i_1} \cdots t_n^{i_n} = 0,
\]
where the coefficients \( a_{i_1, \ldots, i_n} \) are in \( \mathbb{Q} \), not all 0. Multiplying all the coefficients by a non-zero rational number we can assume that all the coefficients are in \( \mathbb{Z} \) and not all of them are divisible by \( p \). Let
\[
h(X) = \sum_{0 \leq i_1 + \cdots + i_n < r} a_{i_1, \ldots, i_n} g_1(X)^{i_1} \cdots g_n(X)^{i_n}.
\]
As \( h(t) = 0 \), we have \( g_0(X)|h(X) \) in \( \mathbb{Q}[X] \), so \( h(X) = g_0(X)u(X) \), \( u(X) \in \mathbb{Q}[X] \).
As \( h(X) \in \mathbb{Z}[X] \) and \( g_0(X) \) is a monic polynomial in \( \mathbb{Z}[X] \), we obtain \( u(X) \in \mathbb{Z}[X] \), so \( h(s) = 0 \) in \( \mathbb{Z}/p\mathbb{Z}[X] \) and
\[
\sum_{0 \leq i_1 + \cdots + i_n < r} \bar{a}_{i_1, \ldots, i_n} s_1^{i_1} \cdots s_n^{i_n} = 0,
\]
a contradiction. \( \square \)

The analogue of Proposition 13 is clearly false over an algebraically closed field.

Acknowledgment

This work was prepared while the author enjoyed the warm hospitality of Queen’s University at Kingston (Ontario, Canada). I thank Professor Leslie G. Roberts (Queen’s University) for proposing to me the lifting problem and for useful discussions, suggestions and remarks concerning it. Talks with Prof. S. Geller (Texas A&M University), Prof. C.U. Jensen (University of Copenhagen) and Prof. A.V. Geramita (Queen’s University) have also been useful.

References