A note on Gröbner bases and graph colorings

Amir Hashemi and Zahra Ghaeli
Abstract. In this paper, we correct a minor misstatement in [4], where J.A. De Loera demonstrates an explicit universal Gröbner basis of the radical ideal of a variety related to chromatic numbers. We show that this result does not hold when the base field is finite, and we correct it for this case.

2000 Mathematics Subject Classification: 13P10; 05C15

Keywords: graph coloring, chromatic numbers, Gröbner bases

1. Introduction

The theory of Gröbner bases is a key computational tool for studying polynomial ideals. This theory has been introduced and developed by Buchberger in 1965 (see his PhD thesis [2]) and has been applied to the problem of graph coloring in [1]. A graph with \( n \) vertices may be represented by a polynomial in \( n \) variables. This polynomial lies in a particular ideal if and only if the graph is not \( k \)-colorable. Thus, the problem of \( k \)-coloring a graph is equivalent to an ideal membership problem. The concept of Gröbner bases may be applied to solve this problem. It has been shown in [4] that the Gröbner basis of the ideal corresponding to this problem is universal, i.e. it is a Gröbner basis for any monomial ordering.

Let \( k, n \geq 2 \) be two positive integers and \( K \) be an arbitrary field. Let \( V(n,k) \) denote the set of vectors which have at most \( k \) - 1 distinct coordinates. Let also \( J(n,k) \) be the vanishing ideal of \( V(n,k) \). De Loera in [4] has proved the following theorem:

**Theorem 1.** The set of polynomials

\[
\rho(n,k) = \left\{ \prod_{1 \leq r < s \leq k} (x_{i_r} - x_{i_s}) \mid 1 \leq i_1 < \cdots < i_k \leq n \right\}
\]

is a universal Gröbner basis for \( J(n,k) \).

To prove this result, De Loera in his paper, on page 3, states that “… but no non-zero univariate polynomial belongs to \( J(n,2) \).” However, this claim (and thus this
theorem) holds only if $K$ is infinite. In the following example, we show that Theorem 1 fails when $K$ is a finite field.

**Example 1.** Let $K = \mathbb{F}_2 = \{0, 1\}$ be a field with two elements. Then $V(2, 2) = \{(0, 0), (1, 1)\}$, and therefore $x_1^2 - x_1$ and $x_2^2 - x_2$ belong to the ideal $J(2, 2) \subset \mathbb{F}_2[x_1, x_2]$. From the above notations, we have $\rho(2, 2) = \{x_1 - x_2\}$ which is not a universal Gröbner basis for $J(2, 2)$.

Extending Theorem 1 to the finite fields we prove the following theorem:

**Theorem 2.** Let $q = p^e$ where $p$ is a prime and $e$ is a positive integer. Let also $K = \mathbb{F}_q$ be a finite field with $q$ elements. Then, the set of polynomials

$$
\tau(n, k) = \left\{ \prod_{1 \leq r < s \leq k} (x_{ir} - x_{is}) \mid 1 \leq i_1 < \cdots < i_k \leq n \right\} \cup \left\{ x_i^q - x_i \mid 1 \leq i \leq n \right\}
$$

is a universal Gröbner basis for $J(n, k)$.

It is worth commenting that for the applications of Theorem 1 in [4], De Loera has used this theorem for infinite fields. Now, we give the structure of the paper. In Section 2 we prove Theorem 2. Section 3 is devoted to a correction of Example 3.4 in [4] on enumerating distinct colorings.

2. The proof of Theorem 2

In this section, we prove Theorem 2, using the proof structure of Theorem 1 in [4]. We briefly state some necessary definitions.

Let $q = p^e$ where $p$ is a prime and $e$ is a positive integer. Let $K = \mathbb{F}_q$ be a finite field with $q$ elements, $R = K[x_1, \ldots, x_n]$ be a polynomial ring and $I = \langle f_1, \ldots, f_t \rangle$ be the ideal of $R$ generated by polynomials $f_1, \ldots, f_t$. Let $f \in R$ and $\prec$ be a monomial ordering on $R$. The leading monomial of $f$ is the greatest monomial (with respect to $\prec$) which appears in $f$, and we denote it by $\text{LM}(f)$. The leading coefficient of $f$, written $\text{LC}(f)$, is the coefficient of $\text{LM}(f)$ in $f$. The leading term of $f$ is $\text{LT}(f) = \text{LC}(f) \text{LM}(f)$. The leading term ideal of $I$ is defined as

$$
\text{LT}(I) = \langle \text{LT}(f) \mid f \in I \rangle.
$$

For a finite set $G \subset R$, we denote by $\text{LT}(G)$ the monomial ideal $\langle \text{LT}(g) \mid g \in G \rangle$. A finite subset of polynomials $G \subset I$ is called a Gröbner basis for $I$ w.r.t. $\prec$ if $\text{LT}(I) = \text{LT}(G)$, see [3] for more details. A universal Gröbner basis for $I$ is a finite subset of $I$ which is a Gröbner basis w.r.t. any monomial ordering.

**Proof of Theorem 2.** The following lemma gives a set of conditions for a universal Gröbner basis ([4], Lemma 2.1).
Lemma 1. Let $I \subset R$ be an ideal and let $G = \{g_1, \ldots, g_t\} \subset I$ be a set of polynomials such that each $g_i$ is a product of linear factors in $x_1, \ldots, x_n$. Further, assume that for any $g \in G$ and for any permutation $\sigma$ on the set $\{1, \ldots, n\}$, we have $g(\sigma(x_1), \ldots, \sigma(x_n)) \in G$. If $G$ is a Gröbner basis for $I$ w.r.t. a particular monomial ordering, then it is a universal Gröbner basis for $I$.

In order to apply Lemma 1 to $\tau(n, k)$, we must prove the following three claims:

- Any $g \in \tau(n, k)$ factors into linear factors in $R$.
- $g(\sigma(x_1), \ldots, \sigma(x_n)) \in \tau$ for each $g \in \tau(n, k)$ and any permutation $\sigma$ on the set $\{1, \ldots, n\}$.
- $\tau(n, k)$ is a Gröbner basis for $J(n, k)$ w.r.t. a particular monomial ordering.

For the first item, it is enough to prove that $x_i^q - x_j$ for any $i$ factors into linear factors. We show that $J(n; k)$ is true for where $n = 2$. We proceed by induction on $n$ and $k$. Let $f$ be an element of $\tau(n, 2)$, and let $\deg f = m$. By induction on $k$ the result is true for $J(n, r)$ for where $k > r \geq 2$. We prove by induction on $k^2 / n$. We show that $J(k, k)$ is generated by the set $\{\prod_{1 \leq i \leq j \leq k} (x_i - x_j) \mid \sum_{1 \leq i \leq j \leq k} q_{ij} \}$ for any $k$. By Buchberger criterion and Buchberger first criterion (see [3], pages 85 and 104) we can prove easily that the set $B = \{x_i^q - x_j^q - x_k \}$ is a Gröbner basis for the ideal that it generates. Let $f$ be an element of $J(k, k)$ and $\tilde{f}$ be the remainder of the division of $f$ by $B$. It is worth noting that since $B$ is a Gröbner basis, this remainder is unique (see [3], Proposition 1 page 82). Since $\tilde{f} \in J(k, k)$, regardless of whether $\tilde{f}$ is zero or non-zero $\tilde{f}(a_1, \ldots, a_k) = 0$ for any $(a_1, \ldots, a_k) \in V(k, k)$.

In $V(k, k)$, every $k$-dimensional point has at most $k - 1$ distinct entries. Thus, if any two entries (such as $x_i$ and $x_j$) are equal, even if the other $k - 2$ entries are distinct,
the point is still contained in \( V(k, k) \). Therefore, since \( \tilde{f} \) vanishes on every point in \( V(k, k) \) then we have \((x_i - x_j) \mid f\) for \(1 \leq i < j \leq k\), and \( f \in \tau(k, k)\). This settles the case \( n = k\).

Now by induction hypothesis the result is true for \( J(r, k) \) with \( n > r \geq k \). We have to prove that \( \text{LT}(f) \in \text{LT}(\tau(n, k)) \) for any \( f \in J(n, k) \). Let \( B = \{x_1^n - x_1, \ldots, x_n^n - x_n\} \), which is a Gröbner basis for the ideal that it generates. Let \( f' \) be the remainder of the division of \( f \) by \( B \). We have \( f' \in J(n, k) \). If \( f' \neq 0 \), we construct an auxiliary polynomial. Let \( S \subseteq \{1, \ldots, n-1\} \). We denote by \( f_S \) the polynomial obtained from \( f \) by substituting \( x_n \) for each variable \( x_i \) for \( i \in S \). Thus, for a non-empty set \( S \) the polynomial \( f_S \in J(r, k) \) with \( r = n - |S| \) where \(|S|\) denotes the size of \( S \). Let

\[
g = \sum_{S \subseteq \{1, \ldots, n-1\}} (-1)^{|S|} f_S.
\]

We claim that \( \text{LT}(g) \in \text{LT}(\tau(n, k)) \). Note that from the definition of \( f \) we can replace \( \tau(n, k) \) by \( \rho(n, k) \) in this claim. The rest of the proof is exactly the same as the latter part of the proof of Theorem 1 in [4]. However, for the sake of completeness, we provide it here. If we substitute \( x_n \) for any \( x_i \) with \( 1 \leq i \leq n - 1 \) then we get the zero polynomial (note that \( \deg(\tilde{f}) \leq q \)). Thus \((x_1 - x_n) \cdots (x_{n-1} - x_n) \mid g\), and therefore we can write it as \( g = (x_1 - x_n) \cdots (x_{n-1} - x_n) h \) for some polynomial \( h \in R \). Since \( g \in J(n, k) \) if we expand \( h \) as a polynomial in \( x_n \), its coefficients \( L_i \) belongs to \( J(n-1, k-1) \). By the induction hypothesis \( \text{LT}(L_i) \in \text{LT}(\rho(n-1, k-1)) \). We observe that \( \text{LT}(h) = \text{LT}(L_j)x_n^j \) for some \( j \) and thus \( \text{LT}(g) = x_1x_2\cdots x_{n-1}\text{LT}(L_j)x_n^j \). Since \( \text{LT}(L_j) \) is divisible by some element of \( \text{LT}(\rho(n-1, k-1)) \), then \( x_1x_2\cdots x_{n-1}\text{LT}(L_j) \) is divisible by some monomial in \( \text{LT}(\rho(n, k)) \) as desired.

If \( \text{LT}(g) = \text{LT}(f) \) we are done. Otherwise, \( \text{LT}(g) \prec \text{LT}(f) \) (since we use lexicographical ordering). But, in the definition of \( g \) the set \( S \) may be empty. In this case \( f_S = \tilde{f} \) and we can write \( g \) as

\[
g = \tilde{f} + \sum_{S \neq \emptyset \text{ and } S \subseteq \{1, \ldots, n-1\}} (-1)^{|S|} f_S.
\]

This follows that \( \text{LT}(\tilde{f}) = \text{LT}(f_S) \) for a non-empty set \( S \subseteq \{1, \ldots, n-1\} \). We observe that \( f_S \in J(r, k) \) for \( n > r \geq k \) and then \( \text{LT}(f) = \text{LT}(f_S) \in \text{LT}(\rho(r, k)) \) by the induction hypothesis. Finally, for \( n > r \geq k \), we have \( \rho(r, k) \subseteq \rho(n, k) \), and this ends the proof of the theorem.

\[ \square \]

3. Enumerating distinct colorings

In this section, we correct an error in Example 3.4 in [4] to compute the number of distinct 3-colorings of the two-by-four grid graph.

In [4], De Loera has applied Theorem 1 to the general question of enumerating distinct colorings of a graph (see Lemma 3). For this, we need some definitions. Let
us denote by $\pi(G, k)$ the number of distinct $k$-colorings of a graph $G$. Let also $P_G$ be the polynomial associated with the labeling of a graph $G$, i.e. if $V = \{x_1, \ldots, x_n\}$ is the set of vertices and $E(G)$ is the set of edges of $G$ then

$$P_G = \prod_{i<j \text{ and } x_i, x_j \in E(G)} (x_i - x_j).$$

Now we recall the definition of the degree of an ideal. Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring where $K$ is an infinite field. Let $X$ be a graded $R$-module and $\delta$ be a positive integer. We denote by $X_\delta$ the set of elements of $X$ of degree $\delta$. Let $I$ be a homogeneous ideal. The Hilbert series of $I$ is the power series $HS_I(t) = \sum_{s=0}^{\infty} HF_I(s) t^s$ where $HF_I(s)$ (the Hilbert function of $I$) is the dimension of $(R/I)_s$ as a $K$-vector space.

**Proposition 1.** We have $HS_I(t) = N(t)/(1-t)^d$ where $N(t)$ is a polynomial which is not multiple of $1-t$, and $d$ is the dimension of $I$.

For the proof of this proposition see [5], Theorem 7, Chapter 11. Now, using this proposition we could define the degree of an ideal.

**Definition 1.** The degree of the ideal $I$, noted by $\deg(I)$, is $N(1)$ where $N$ is the numerator of $HS_I$.

We recall that the ideal $I : P_G^\infty$ is defined as

$$I : P_G^\infty = \{f \in R \mid f^m P_G \in I \text{ for some } m > 0\}.$$

Using these notations, we have the following result (see [4], Proposition 3.3).

**Lemma 3.** $\pi(G, k - 1) = \deg(J(n, k) : P_G^\infty)$.

**Example 2.** In this example, we compute the number of distinct 3-colorings of the two-by-four grid graph $H$, and we correct an error of Example 3.4 in [4] to compute it. This graph has eight vertices $x_1, \ldots, x_8$ and ten edges $x_1x_2, x_2x_3, x_3x_4, x_4x_5, x_5x_6, x_6x_7, x_7x_8, x_1x_8, x_2x_7, x_3x_6$. We have to compute the degree of the ideal $J(8, 4) : P_H^\infty$. In order to speed up the computation, De Loera has proposed to use the factorization of $P_H$ to compute the generators of the saturation ideals $J(8, 4) : (x_i - x_j)^\infty$ for each of the edges of $H$. He has claimed that if one computes these ten ideals, then their intersection is precisely equal to $J(8, 4) : P_H^\infty$ (we denote this intersection by $I$). But, this equality does not hold. Using MAPLE11, we can compute $I$ and its Hilbert series where the latter is equal to

$$t^{13} + 6t^{12} + 22t^{11} + 55t^{10} + 106t^9 + 159t^8 + 190t^7 + 175t^6 + 126t^5 + 70t^4 + 35t^3 + 15t^2 + 5t + 1)/(1-t)^3.$$

---

1After the submission of the paper, an anonymous referee pointed out that Example 3.4 in [4] remains true if we replace “intersection” by ”sum”. He/She provided also a Macaulay2 code to verify this statement, see [http://amirhashemi.iut.ac.ir/software.html](http://amirhashemi.iut.ac.ir/software.html).
Therefore \( \text{deg}(I) = 966 \) which is not equal to \( \pi(H, 3) \), because we will see further that the number of distinct 3-colorings of \( H \) is 26. Let us see a simple example illustrating the difference between the above ideals. Let \( C_4 \) be the 4-cycle graph with the vertices \( y_1, \ldots, y_4 \) and the edges \( y_1y_2, y_2y_3, y_3y_4, y_4y_1 \). We would like to compute \( \pi(C_4, 2) \). We observe that \( J(1; C_4) \) is equal to \( \langle y_1 - y_3, y_2 - y_4 \rangle \), i.e. \( \pi(C_4, 2) = 1 \). On the other hand,

\[
\bigcap_{y_i, y_j \in E(C_4)} J(4, 3) : (y_i - y_j)_{\infty} = \langle y_1 - y_4, y_3 - y_4 \rangle \cap \langle y_1 - y_2, y_3 - y_4 \rangle \\
\cap \langle y_1 - y_3, y_2 - y_3 \rangle \cap \langle y_1 - y_4, y_2 - y_3 \rangle \\
\cap \langle y_1 - y_4, y_2 - y_4 \rangle \cap \langle y_2 - y_4, y_3 - y_4 \rangle \\
\cap \langle y_1 - y_3, y_2 - y_4 \rangle
\]

which is not equal to \( J(4, 3) : P_{C_4}^\infty \). The Hilbert series of this intersection is equal to \( (t^3 + 3t^2 + 2t + 1)/(1-t)^2 \), and therefore its degree is 7.

Now, we compute \( \pi(H, 3) \). Computing \( J(8; H) \) is not feasible in less than 12 hours (timings in this paper were conducted on a personal computer with 3.2GHz, 2×Intel(R)-Xeon(TM) Quad core, 24 GB RAM and 64 bits under the Linux operating system). In order to speed up the computation, we use the following simple result (see [3], Theorem 11, page 196).

**Lemma 4.** Let \( L \subset R \) be a radical ideal and \( f \in R \). Let \( L \cap \langle f \rangle = \langle g_1, \ldots, g_\ell \rangle \). Then \( \langle g_1/f, \ldots, g_\ell/f \rangle \) is a generating set for the ideal \( L : f^\infty \).

**Proof.** It is enough to prove that any polynomial \( g \in L : f^\infty \) belongs to \( \langle g_1/f, \ldots, g_\ell/f \rangle \). We know that \( gf^m \in L \) for some integer \( m \). This follows that \( (gf)^m \in L \), and therefore \( gf \in L \cap \langle f \rangle \). Thus, \( g \in \langle g_1/f, \ldots, g_\ell/f \rangle \).  

We can compute \( J(8, 4) \cap \langle P_H \rangle \) and then a generating set for \( J(8, 4) : P_H^\infty \) in 2152.549 seconds. The Hilbert series of this ideal is equal to \( (8t^3 + 12t^2 + 5t + 1)/(1-t)^3 \), and therefore its degree is equal to 26.

**Acknowledgement**

The authors would like to thank an anonymous referee for very useful comments on a previous draft.

**References**


nach einem nulldimensionalen Polynomideal.)  Innsbruck: Univ. Innsbruck, Mathematisches Institut (Diss.), 1965.


Authors’ addresses

Amir Hashemi
Department of Mathematical Sciences,, Isfahan University of Technology, Isfahan, 84156-83111, Iran
E-mail address: Amir.Hashemi@cc.iut.ac.ir

Zahra Ghaeli
Department of Mathematical Sciences,, Isfahan University of Technology, Isfahan, 84156-83111, Iran
E-mail address: z.ghaeli@math.iut.ac.ir