

# Low degree Nullstellensatz certificates for 3-colorability

Bo Li\*    Benjamin Lowenstein\*    Mohamed Omar

Department of Mathematics  
Harvey Mudd College  
Claremont, CA, U.S.A.

{bli,blowenstein,omar}@g.hmc.edu

Submitted: Mar 17, 2015; Accepted: Dec 31, 2015; Published: Jan 11, 2016

Mathematics Subject Classifications: 05C15, 05C50, 68W30

## Abstract

In a seminal paper, De Loera et. al introduce the algorithm NulLA (Nullstellensatz Linear Algebra) and use it to measure the difficulty of determining if a graph is not 3-colorable. The crux of this relies on a correspondence between 3-colorings of a graph and solutions to a certain system of polynomial equations over a field  $\mathbb{k}$ . In this article, we give a new direct combinatorial characterization of graphs that can be determined to be non-3-colorable in the first iteration of this algorithm when  $\mathbb{k} = GF(2)$ . This greatly simplifies the work of De Loera et. al, as we express the combinatorial characterization directly in terms of the graphs themselves without introducing superfluous directed graphs. Furthermore, for all graphs on at most 12 vertices, we determine at which iteration NulLA detects a graph is not 3-colorable when  $\mathbb{k} = GF(2)$ .

## 1 Introduction

In recent years, combinatorial optimization has flourished from algorithms that fundamentally rely on tools from algebraic geometry and commutative algebra. Work of Lasserre [9], Lovász-Schrijver [11], Sherali-Adams [13], Gouveia, Parrilo and Thomas [7], and many others have used polynomials to develop approximation algorithms for optimization problems. Another recent algorithm akin to those above is the Nullstellensatz Linear Algebra algorithm (NulLA) of De Loera et. al [4] which addresses feasibility issues in polynomial optimization. Given a set of polynomials  $f_1, f_2, \dots, f_s \in \mathbb{k}[x_1, \dots, x_n]$  for some field  $\mathbb{k}$ , NulLA's goal is to certify that the system of equations  $f_1 = 0, f_2 = 0, \dots, f_s = 0$  has no solution in  $\bar{\mathbb{k}}$ , the algebraic closure of  $\mathbb{k}$ . It exploits Hilbert's Nullstellensatz, a celebrated and fundamental theorem in algebraic geometry (see [2]).

---

\*Supported by the Department of Mathematics at Harvey Mudd College.

**Theorem 1.1** (Hilbert’s Nullstellensatz). *Let  $\mathbb{k}$  be a field and  $f_1, f_2, \dots, f_s \in \mathbb{k}[x_1, \dots, x_n]$ . The system of polynomial equations*

$$f_1 = 0, f_2 = 0, \dots, f_s = 0$$

*has no solution in  $\overline{\mathbb{k}}^n$  if and only if there are polynomials  $\alpha_1, \alpha_2, \dots, \alpha_s \in \mathbb{k}[x_1, \dots, x_n]$  such that*

$$1 = \alpha_1 f_1 + \dots + \alpha_s f_s.$$

The polynomials  $\alpha_1, \alpha_2, \dots, \alpha_s$  are referred to as a *Nullstellensatz certificate* of infeasibility; indeed they are a witness that the polynomial system  $f_1 = 0, f_2 = 0, \dots, f_s = 0$  has no solution. The maximum degree of the  $\alpha_i$ ’s is referred to as the *Nullstellensatz degree* of the system, and it is a measure of the complexity of certifying that the system of polynomial equations has no solutions. If a system of polynomial equations is known to have a Nullstellensatz certificate whose Nullstellensatz degree is a small constant (and if  $\mathbb{k}$  is finite), one can find a Nullstellensatz certificate in polynomial time in the number of variables through a sequence of linear algebra computations (see [4] for details). However, for general polynomial systems, it is well known that the degree of Nullstellensatz certificates can grow as a function of the number of variables.

The underlying paradigm in all the above algorithms is the construction of iterative approximations that are tractably computable at early stages. When applied to combinatorial optimization problems, particularly graph theoretic ones, the key problem that arises is determining the classes of graphs for which a given problem can be resolved in early iterations. For instance, when applied to the stable set problem, Gouveia, Parrilo and Thomas [7] show that the first iteration of the theta body hierarchy solves the stable set problem for perfect graphs. This result was first established by Lovász [10] by exploiting polynomials as well. NullA itself was originally introduced as a means of unfolding classes of non-3-colorable graphs that can be detected to be non-3-colorable efficiently (that is, in polynomial time in the number of variables of a given graph). In particular, the authors of [4] applied the NullA algorithm to the following algebraic formulation of graph 3-colorability due to Bayer. We will refer to this as Bayer’s formulation throughout the manuscript.

**Lemma 1.2** (Bayer [1]). *A graph  $G$  with vertex set  $V$  and edge set  $E$  is 3-colorable if and only if the following system of equations has a solution over an algebraically closed field  $\mathbb{k}$  with  $\text{char}(\mathbb{k})$  relatively prime to 3.*

$$0 = x_i^3 - 1 \qquad \forall i \in V \qquad (1)$$

$$0 = x_i^2 + x_i x_j + x_j^2 \qquad \forall v_i v_j \in E \qquad (2)$$

The fundamental concern then is determining combinatorial features of non-3-colorable graphs that dictate the minimum Nullstellensatz degree of infeasibility for the system in Lemma 1.2, which we denote by  $N_{\mathbb{k}}(G)$ , is a small constant. In light of this, it is natural to address the following problem, a variant of which was first asked in [3]:

**Problem 1.3.** Given a finite field  $\mathbb{k}$ , and positive integer  $d$ , characterize those graphs with  $N_{\mathbb{k}}(G) = d$ .

Computational evidence (see, for example, Table 1 of [6]) suggests that the minimum Nullstellensatz degree of a non-3-colorable under Bayer's formulation is smallest when the field of coefficients chosen is  $GF(2)$  as opposed to  $GF(p)$  for primes  $p > 2$ , so from a computational complexity perspective, it may be beneficial to begin addressing Problem 1.3 by working with Bayer's formulation when  $\mathbb{k} = GF(2)$ . A partial answer in this case was given by De Loera et. al [3] (see their paper for relevant definitions).

**Theorem 1.4** (Theorem 2.1 of [3]). For a given simple undirected graph  $G$  with vertex set  $V = \{v_1, v_2, \dots, v_n\}$  and edge set  $E$ , the polynomial system over  $GF(2)$  encoding the 3-colorability of  $G$

$$J_G = \{x_i^3 + 1 = 0, x_i^2 + x_i x_j + x_j^2 = 0 : i \in V, v_i v_j \in E\}$$

has a degree one Nullstellensatz certificate of infeasibility if and only if there exists a set  $C$  of oriented partial 3-cycles and oriented chordless 4-cycles from  $\text{Arcs}(G)$  such that

1.  $|C_{(v_i, v_j)}| + |C_{(v_j, v_i)}| \equiv 0 \pmod{2}$  for all  $v_i v_j \in E$  and
2.  $\sum_{(v_i, v_j) \in \text{Arcs}(G), i < j} |C_{(v_i, v_j)}| \equiv 1 \pmod{2}$

where  $C_{(v_i, v_j)}$  denotes the set of cycles in  $C$  in which the arc  $(v_i, v_j) \in \text{Arcs}(G)$  appears.

This characterization adds directed structure to undirected graphs, and hence does not fully capture an inherent combinatorial characterization directly from the graphs themselves. In this paper, we provide such a direct combinatorial characterization for Bayer's formulation when  $\mathbb{k} = GF(2)$ . Before introducing the combinatorial characterization, we define the following class of graphs that will play a key role.

**Definition 1.5.** A graph  $G$  with vertex set  $V = \{v_1, v_2, \dots, v_n\}$  and edge set  $E$  is covered by length 2 paths if there exists a set  $C$  of length 2 paths in  $G$  such that

1. each edge in  $E$  appears in an even number of paths in  $C$ ,
2. the number of paths  $v_i v_j v_k$  in  $C$  in which  $j < i, k$  or  $j > i, k$  is odd, and
3. if  $v_i, v_j \in V$  but  $v_i v_j \notin E$ , then the number of paths in  $C$  with  $v_i$  and  $v_j$  as endpoints is even.

*Example 1.6.* Let  $n$  be a positive integer. The graph  $W_n$ , referred to as the *wheel* graph, is the graph whose vertex set is  $\{v_1, v_2, \dots, v_n, v_{n+1}\}$  where the induced subgraph on  $V' = \{v_1, v_2, \dots, v_n\}$  is a cycle and  $v_{n+1}$  is a vertex adjacent to all vertices in  $V'$ . See Figure 1 for an example.

Without loss of generality, we may assume the cycle whose vertex set is  $V'$  has edge set  $\{v_1 v_2, \dots, v_{n-1} v_n, v_n v_1\}$ . When  $n$  is odd, the graph  $W_n$  is covered by length 2 paths, as witnessed by the set  $C = \{v_1 v_{n+1} v_2, v_2 v_{n+1} v_3, \dots, v_{n-1} v_{n+1} v_n, v_n v_{n+1} v_1\}$ . Indeed, this set satisfies all the conditions in Definition 1.5.

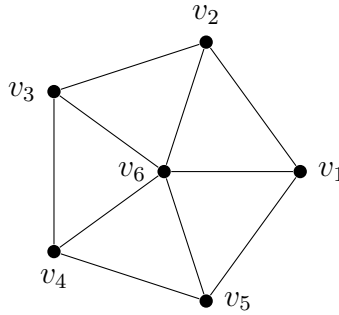


Figure 1:  $W_5$ , the wheel graph on six total vertices.

We now present the main combinatorial characterization.

**Theorem 1.7.** *Let  $G$  be a graph. Under Bayer’s formulation of 3-colorability with coefficients in the field  $\mathbb{k} = GF(2)$ ,  $N_{\mathbb{k}}(G) = 1$  if and only if  $G$  is covered by length 2 paths.*

*Example 1.8.* Let  $n$  be an odd positive integer. In Example 1.6, we saw that the graph  $W_n$  is covered by length two paths, so Theorem 1.7 establishes that NullA (applied to Bayer’s formulation when  $\mathbb{k} = GF(2)$ ) detects that this graph is non-3-colorable with a degree 1 Nullstellensatz certificate. Odd wheels are known to be non-3-colorable for both computational and algebraic reasons, but the ability for NullA to detect this with a degree 1 certificate suggests that NullA has the potential to be used not only as a computational tool but as a tool for automatic theorem proving.

Theorem 1.7 also allows us to establish, combinatorially, that a graph does not have a degree 1 NullA certificate (under Bayer’s formulation when  $\mathbb{k} = GF(2)$ ).

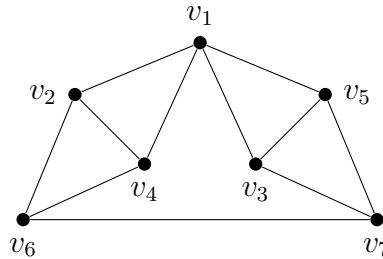


Figure 2: Moser spindle.

**Proposition 1.9.** *Let  $G$  be the Moser spindle (depicted in Figure 2). The graph  $G$  does not have a degree 1 NullA certificate under Bayer’s formulation when  $\mathbb{k} = GF(2)$ .*

*Proof.* Using Theorem 1.7, we will show that  $N_{\mathbb{k}}(G) > 1$  when  $\mathbb{k} = GF(2)$ . Suppose otherwise. By Theorem 1.7,  $G$  is covered by length 2 paths, which we refer to collectively as  $C$ .

We claim that the edge  $v_6v_7$  can not be an edge in any length 2 path in  $C$ . Indeed, assume without loss of generality that the path  $v_6v_7v_k$  is in  $C$  for some vertex  $k \notin \{6, 7\}$ . Since the edge  $v_6v_7$  is not on a 3-cycle,  $v_6v_k$  is not an edge. Moreover, since the edge  $v_6v_7$  is not on a 4-cycle,  $v_6v_7v_k$  is the only member of  $C$  whose endpoints are  $v_6$  and  $v_k$ . But this is impossible because  $v_6v_k$  is not an edge, so the number of paths in  $C$  with  $v_6$  and  $v_k$  as endpoints must be even. Hence, there are no length 2 paths in  $C$  of the form  $v_6v_7v_k$ .

Now since  $v_6v_7v_k$  is not a member of  $C$  for any  $k$ ,  $C$  certifies through Theorem 1.7 that  $N_{\mathbb{k}}(G \setminus v_6v_7) = 1$ . But this is a contradiction because  $G \setminus v_6v_7$  is 3-colorable. Thus, no set  $C$  with the desired property exists, so  $N_{\mathbb{k}}(G) \neq 1$ .  $\square$

Proposition 1.9 generalizes directly in the following way, providing a combinatorial obstruction to existence of a degree 1 Nullstellensatz certificate for Bayer's formulation when  $\mathbb{k} = GF(2)$ .

**Corollary 1.10.** *Let  $\mathbb{k} = GF(2)$ , and suppose  $G$  is a non-3-colorable graph that contains an edge  $e$  for which the following are true:*

- $G \setminus e$  is 3-colorable, and
- $e$  is not an edge in a 3-cycle nor a 4-cycle of  $G$ .

Then  $N_{\mathbb{k}}(G) > 1$ .

*Remark 1.11.* One of the most celebrated constructions of very hard instances of graph 3-colorability is a construction of Mizuno and Nishihara [12]. Corollary 1.10 is consistent with their findings. Indeed, in all the graphs they present in Figure 3 (see [12]), the removal of any edge leaves a 3-colorable graph, and each of these graphs has an edge that does not lie on 3 or 4-cycle. This implies that when  $\mathbb{k} = GF(2)$ ,  $N_{\mathbb{k}}(G) > 1$  for such graphs  $G$ , so computationally determining that they are not 3-colorable is not immediate under the NullA paradigm.

Alongside our combinatorial characterization, in Section 3 we begin the program of determining the Nullstellensatz degree of Bayer's formulation (with coefficients in  $GF(2)$ ) for small non-3-colorable graphs. Most notably we prove

**Theorem 1.12.** *If  $\mathbb{k} = GF(2)$  and  $|V(G)| \leq 12$ , then  $N_{\mathbb{k}}(G) \leq 4$ .*

## 2 Characterizing Degree 1 Certificates

This section is dedicated to proving Theorem 1.7, and in particular developing a combinatorial characterization of non-3-colorable graphs  $G$  for which  $N_{\mathbb{k}}(G) = 1$  (under Bayer's formulation with coefficients in  $GF(2)$ ). We begin with a technical proposition that will be needed throughout:

**Proposition 2.1.** *For a graph  $G$  with vertex set  $V = \{v_1, v_2, \dots, v_n\}$  and edge set  $E$ , the following are equivalent for Bayer's formulation when  $\mathbb{k} = GF(2)$ :*

1.  $N_{\mathbb{k}}(G) = 1$ .

2. 1 is a  $\mathbb{k}$ -linear combination of

$$x_i^3 + 1 \qquad \qquad \qquad \forall v_i \in V \qquad (3)$$

$$x_k(x_i^2 + x_i x_j + x_j^2) \qquad \qquad \forall v_i v_j \in E, v_k \in V \qquad (4)$$

3. 1 is a  $\mathbb{k}$ -linear combination of

$$x_i^2 x_j + x_i x_j^2 + 1 \qquad \qquad \qquad \forall v_i v_j \in E \qquad (5)$$

$$x_i^2 x_k + x_i x_j x_k + x_j^2 x_k \qquad \forall v_i v_j \in E, v_k \in V, v_i \neq v_k \neq v_j \qquad (6)$$

4. 1 is a  $\mathbb{k}$ -linear combination of

$$x_i^2 x_j + x_i x_j^2 + 1 \qquad \qquad \qquad \forall v_i v_j \in E \qquad (7)$$

$$x_i^2 x_k + x_j^2 x_k + x_i x_j^2 + x_i x_k^2 \qquad \forall v_i v_j \in E, v_j v_k \in E \qquad (8)$$

The above proposition finds alternate and equivalent sets of polynomials whose solution sets are the same as that of the system in Lemma 1.2. The last set of polynomials are particularly useful in uncovering our combinatorial characterization. The equivalence of the first three sets was proven in Theorem 2.1 of [3]. The equivalence to the last set of polynomials follows an argument similar to the proof of Theorem 2.1 in [3]. For completeness, we include a proof of this equivalence in the appendix.

In proving Theorem 1.7, we will repeatedly appeal to the following immediate proposition:

**Proposition 2.2.** *Let  $G$  be a graph with vertex set  $V = \{v_1, v_2, \dots, v_n\}$  and edge set  $E$ , and suppose  $G$  is covered by a set  $C$  of length 2 paths. The following statements are equivalent:*

1. *The number of pairs  $v_i, v_j \in V$  with  $i < j$  for which there are an odd number of paths in  $C$  containing  $v_i$  with  $v_j$  as an endpoint, is itself an odd number.*
2. *The sum over all pairs  $i < j$  of the number of paths in  $C$  containing  $v_i$  with  $v_j$  as an endpoint is odd.*
3. *The number of paths  $v_i v_j v_k$  in  $C$  in which  $j < i, k$  or  $j > i, k$  is odd.*

We omit the proof of Proposition 2.2 but illustrate an example. Consider the wheel graph  $W_5$  as depicted in Figure 1, and the set  $C = \{v_1 v_6 v_2, v_2 v_6 v_3, v_3 v_6 v_4, v_4 v_6 v_5, v_5 v_6 v_1\}$  of length 2 paths that  $G$  is covered by. All three conditions in Proposition 2.2 are satisfied. For condition 1, the pairs  $\{v_1, v_2\}$ ,  $\{v_2, v_3\}$ ,  $\{v_3, v_4\}$ ,  $\{v_4, v_5\}$ ,  $\{v_1, v_5\}$  each have exactly 1 path in  $C$  as their endpoints, and all other pairs have 0 paths as their endpoints, so the total number of pairs in question is 5. For condition 2, the pairs  $\{i, j\}$ , with  $i < j$ , for which there are paths containing  $v_i$  with  $v_j$  as an endpoint are  $\{1, 2\}$ ,  $\{2, 3\}$ ,  $\{3, 4\}$ ,  $\{4, 5\}$ ,  $\{1, 5\}$ ,

so that total in question is also 5. This follows directly from condition 1 because  $v_6$  is never an endpoint of a path. Finally, every path in  $v_i v_j v_k$  in  $C$  has  $j > i, k$ , so the total in question here is also 5.

We now move on to the main result:

*Proof.* (of Theorem 1.7) Throughout this proof, for any set of polynomials  $S$  in a polynomial ring whose coefficients are in  $\mathbb{k}$ , we denote by  $\langle S \rangle_{\mathbb{k}}$  the linear span of  $S$  over  $\mathbb{k}$ . Let  $F$  be the following set of polynomials:

$$x_i^2 x_j + x_i x_j^2 + 1 \qquad \forall v_i v_j \in E \qquad (9)$$

$$x_i^2 x_k + x_j^2 x_k + x_i x_j^2 + x_i x_k^2 \qquad \forall v_i v_j \in E, v_j v_k \in E \qquad (10)$$

By Proposition 2.1, we know that  $N_{\mathbb{k}}(G) = 1$  if and only if  $1 \in \langle F \rangle_{\mathbb{k}}$ , so we must show that  $1 \in \langle F \rangle_{\mathbb{k}}$  if and only if  $G$  is covered by a set  $C$  of length 2 paths.

First suppose  $G$  is covered by a set of length 2 paths  $C$ . Consider the set  $H \subset F$  consisting of the following polynomials:

1.  $x_i^2 x_k + x_j^2 x_k + x_i x_j^2 + x_i x_k^2$  for each path  $v_i v_j v_k \in C$ , and
2.  $x_i x_j^2 + x_j x_i^2 + 1$  for each  $v_i, v_j \in V$  with  $i < j$  such that the number of length 2 paths in  $C$  containing  $v_i$  and having  $v_j$  as an endpoint is odd.

We claim  $1 \in \langle H \rangle_{\mathbb{k}}$  and hence  $1 \in \langle F \rangle_{\mathbb{k}}$ . Observe that the non-constant monomials appearing in  $F$  (and hence in  $H$ ) are all of the form  $x_r^2 x_s$ , where  $v_r, v_s \in V$  are arbitrary. We start by showing that the coefficient of  $x_r^2 x_s$  in  $\sum_{h \in H} h$  is 0 in  $\mathbb{k}$ , and so all non-constant terms in  $\sum_{h \in H} h$  vanish. An  $x_r^2 x_s$  term appears in one of four ways:

- (a) one  $x_r^2 x_s$  term for each path in  $C$  with  $v_r$  and  $v_s$  as endpoints,
- (b) one  $x_r^2 x_s$  term for each path in  $C$  with  $v_r$  as the middle vertex and  $v_s$  as an endpoint,
- (c) one  $x_r^2 x_s$  term if there are an odd number of paths in  $C$  containing  $v_r$  with  $v_s$  as an endpoint,
- (d) one  $x_r^2 x_s$  term if there are an odd number of paths in  $C$  containing  $v_s$  with  $v_r$  as an endpoint.

The coefficient of the  $x_r^2 x_s$  in the combined contribution from the terms in (a) and (b) is the parity of the number of paths in  $C$  containing  $v_r$  with  $v_s$  as an endpoint. By our assumption on  $C$ , there are even number of paths in  $C$  containing  $v_r v_s$  as an edge, so the coefficient of the  $x_r^2 x_s$  in the combined contribution from (a) and (b) is the parity of the number of paths in  $C$  containing  $v_r$  and  $v_s$  as endpoints. The coefficient of  $x_r^2 x_s$  in the combined contribution from the terms in (c) and (d) is the number of paths in  $C$  containing  $v_r$  and  $v_s$ . By our assumption on  $C$ , this is again the parity of the number of paths in  $C$  containing  $v_r$  and  $v_s$  as endpoints. Thus, the coefficient of  $x_r^2 x_s$  in the combined contribution from the terms in (a),(b),(c),(d) is 0 in  $\mathbb{k}$ . Finally we need to

discern the constant term of  $\sum_{h \in H} h$ . The constant term is the parity of the number of summands of the form (2). But this is immediately 1 by condition (2) of Definition 1.5 and Proposition 2.2, so the constant term in  $\sum_{h \in H} h$  over  $\mathbb{k}$  is 1.

We must now show that if  $N_{\mathbb{k}}(G) = 1$ , then such a set  $C$  exists. In that light, Proposition 2.1 asserts the existence of a set  $H$  of polynomials of the form (9) and (10) with  $\sum_{h \in H} h = 1$ . Let  $H^*$  be the restriction of  $H$  to the polynomials in (10). Construct  $C$  to consist of the paths  $v_i v_j v_k$  for which  $x_i^2 x_k + x_j^2 x_k + x_i x_j^2 + x_i x_k^2$  appears in  $\sum_{h \in H^*} h$  with a non-zero coefficient.

Suppose  $v_r v_s \in E$ , define  $S_{r,s}$  to be the sum (in  $\mathbb{k}$ ) of the coefficients of the monomials  $x_r^2 x_s$  and  $x_r x_s^2$  appearing in  $\sum_{h \in H^*} h$ . Since  $\sum_{h \in H} h = 1$ , and the only other summand of  $\sum_{h \in H} h$  not in  $\sum_{h \in H^*} h$  is  $x_r^2 x_s + x_r x_s^2 + 1$ ,  $S_{r,s}$  is 0 in  $\mathbb{k}$ . However, the contribution of a single summand  $x_i^2 x_k + x_j^2 x_k + x_i x_j^2 + x_i x_k^2$  in  $\sum_{h \in H^*} h$  to  $S_{r,s}$  is 1 precisely when  $v_r v_s$  is an edge on the path  $v_i v_j v_k$ , 2 if  $v_r$  and  $v_s$  are endpoints of  $v_i v_j v_k$ , and 0 otherwise. Since  $S_{r,s}$  is 0 in  $\mathbb{k}$ , we deduce that the edge  $v_r v_s$  lies on an even number of paths in  $C$ .

If  $v_r, v_s \in V$  but  $v_r v_s \notin E$ , then any  $x_r^2 x_s$  term in  $\sum_{h \in H} h$  appears in  $\sum_{h \in H^*} h$ , so the coefficient of  $x_r^2 x_s$  in  $\sum_{h \in H^*} h$  is 0 in  $\mathbb{k}$ . But  $x_r^2 x_s$  appears once in the summand of  $H^*$  corresponding to the path  $v_i v_j v_k$  precisely when  $v_r$  and  $v_s$  are endpoints of  $v_i v_j v_k$ . Thus, the number of paths whose endpoints are  $v_r$  and  $v_s$  is even.

Each edge  $v_i v_j$  with  $i < j$  contributes a 1 to the sum  $\sum_{h \in H} h$ . Moreover, for such pairs  $i, j$  the monomial  $x_i^2 x_j$  appears an odd number of times in  $H^*$ . We know  $x_i^2 x_j$  appears in  $H^*$  once for each path in  $C$  whose endpoints are  $v_i$  and  $v_j$  and once for each path in  $C$  with  $v_i$  as a midpoint and  $v_j$  as an endpoint. This is equivalent to  $x_i^2 x_j$  appearing in  $H^*$  once for each path in  $C$  containing  $v_i$  with  $v_j$  as an endpoint. Since the number of 1s appearing in  $\sum_{h \in H} h$  is odd, there are an odd number of  $i, j$  pairs with  $i < j$  such that the number of paths in  $C$  containing  $i$  with  $j$  as an endpoint is odd. By Proposition 2.2, this establishes condition (2) of Definition 1.5.  $\square$

### 3 NullA on Small Graphs and Future Directions

Section 2 equipped us with a complete combinatorial understanding of the graphs  $G$  for which  $N_{\mathbb{k}}(G) = 1$  when  $\mathbb{k} = GF(2)$ . By Theorem 2.1 of [6],  $N_{\mathbb{k}}(G) \equiv 1 \pmod{3}$ , so in investigating Problem 1.3, the next natural step is determining when  $N_{\mathbb{k}}(G) = 4$ . This section is devoted to a systematic study of this for small graphs. We first remark that, in order to find graphs with low minimum Nullstellensatz degree, we only need to focus on a subclass of non-3-colorable graphs.

**Definition 3.1** (Definition 5.1.4 of [14]). A non-3-colorable graph  $G$  is *4-critical* if for any edge  $e \in E(G)$ ,  $G \setminus e$  is 3-colorable.

The following observation is fundamental for our purposes. See Chapter 5 of [14] for a discussion of this.

**Lemma 3.2** ([14]). *Every non-3-colorable graph has a 4-critical subgraph.*



$ V $	$N_{\mathbb{k}}(G) = 1$	$N_{\mathbb{k}}(G) = 4$	Total 4-critical graphs
4	1	0	1
5	0	0	0
6	1	0	1
7	1	1	2
8	2	3	5
9	5	16	21
10	13	137	150
11	38	1183	1221
12	141	14440	14581
Total	202	15780	15982

Table 1:  $N_{\mathbb{k}}(G)$  for 4-critical graphs on at most 12 vertices when  $\mathbb{k} = GF(2)$ .

In light of the previous lemma, the following lemma tells us that 4-critical graphs provide upper bounds for the minimum Nullstellensatz degree of general non-3-colorable graphs.

**Lemma 3.3** (Lemma 3.14 of [5]). *If  $H$  and  $G$  are non-3-colorable graphs with  $H$  a subgraph of  $G$ , then  $N_{\mathbb{k}}(H) \geq N_{\mathbb{k}}(G)$ .*

Lemma 3.2 and Lemma 3.3 suggest that we solely focus on minimum degree Nullstellensatz certificates for 4-critical graphs. We computed minimum degree Nullstellensatz certificates for all such graphs on at most 12 vertices. A summary of the results is illustrated in Table 1. Some of the graphs represented in the data table are ones we have seen so far. For instance, the only 4-critical graph  $G$  with  $|V(G)| = 4$  is the complete graph on four vertices, which is the wheel  $W_3$ . The graph on the fewest number of vertices whose minimum degree Nullstellensatz certificate is 4 is the Moser spindle. One particular degree 4 certificate, consistent with the vertex labeling in Figure 2 is the following:

$$\begin{aligned}
1 = & (x_1x_2x_6 + x_1x_2x_7 + x_1x_4x_6 + x_1x_4x_7 + x_2x_6x_7 + x_4x_6x_7)(x_1^3 + 1) \\
& + (x_1^2x_6 + x_1^2x_7 + x_1x_6x_7)(x_2^3 + 1) + (1)(x_3^3 + 1) \\
& + (x_4 + x_7 + x_1^2x_4x_6 + x_1^2x_4x_7 + x_1x_4x_6x_7)(x_1^2 + x_1x_2 + x_2^2) \\
& + (x_1)(x_1^2 + x_1x_3 + x_3^2) + (x_1 + x_6 + x_7 + x_1^2x_2x_6 + x_1^2x_2x_7 + x_1x_2x_6x_7)(x_1^2 + x_1x_4 + x_4^2) \\
& + (x_3 + x_7)(x_1^2 + x_1x_5 + x_5^2) + (x_1 + x_2 + x_6 + x_1^2x_2x_6 + x_1^2x_2x_7 + x_1x_2x_6x_7)(x_2^2 + x_2x_4 + x_4^2) \\
& + (x_1 + x_2 + x_7)(x_2^2 + x_2x_6 + x_6^2) + (x_1 + x_7)(x_3^2 + x_3x_5 + x_5^2) + (x_3)(x_3^2 + x_3x_7 + x_7^2) \\
& + (x_2 + x_7)(x_4^2 + x_4x_6 + x_6^2) + (x_1 + x_3)(x_5^2 + x_5x_7 + x_7^2) + (x_1)(x_6^2 + x_6x_7 + x_7^2)
\end{aligned}$$

These observations now allow us to prove Theorem 1.12.

*Proof.* (of Theorem 1.12) By Lemma 3.2, every non-3-colorable graph  $G$  on at most 12 vertices has a 4-critical subgraph  $H$ . By Table 1,  $N_{\mathbb{k}}(H) \in \{1, 4\}$ . Lemma 3.3 implies  $N_{\mathbb{k}}(G) \leq N_{\mathbb{k}}(H)$ . The result then follows by Theorem 2.1 of [6].  $\square$

Many pertinent questions arise from our study of the minimum Nullstellensatz degree of graphs under Bayer's formulation. First and foremost, unless  $P=NP$ , one should expect to find a family of graphs for which the minimum Nullstellensatz degree grows arbitrarily large (see Lemma 3.2 of [5] for a discussion of this). As evidenced by Table 1, an exhaustive search of the almost 16,000 4-critical graphs on at most 12 vertices indicates that a first step in this direction is to address the following problem:

**Problem 3.4.** *For any positive integer  $t$ , find a graph  $G$  for which  $N_{\mathbb{k}}(G) > t$ .*

After exhaustive experimentation, the authors of [5] have yet to see an example resolving Problem 3.4 when  $t = 4$  for any finite field  $\mathbb{k}$ . One possible method for addressing Problem 3.4 is understanding what happens to the minimum Nullstellensatz degree under the famous Hajós construction. In his seminal paper [8], Hajós defined a recursively constructed class of graphs, which he called 4-constructible, in the following way:

- i)  $K_4$  is 4-constructible.
- ii) For any two non-adjacent vertices  $u$  and  $v$  in a 4-constructible graph  $G$ , the graph obtained from  $G$  by adding an edge  $e$  incident to  $u$  and  $v$  and contracting  $e$  is also 4-constructible.
- iii) (Hajós Construction) For any two 4-constructible graphs  $G$  and  $H$ , with  $vw$  an edge of  $G$ , and  $xy$  an edge of  $H$ , the graph obtained by identifying  $v$  and  $x$ , removing  $vw$  and  $xy$ , and adding the edge  $wy$  is also 4-constructible.

Hajós proved that the set of 4-constructible graphs is precisely the set of 4-critical graphs, so it is fundamental for us to determine what changes in the minimum Nullstellensatz degree of graphs when applying these constructions. Observe  $N_{\mathbb{k}}(K_4) = 1$ , and by Lemma 3.14 of [5], the minimum Nullstellensatz degree will not increase by applying construction ii). This leads us to the following fundamental question:

**Problem 3.5.** *Let  $G$  and  $H$  be 4-critical graphs. What is the relationship between  $N_{\mathbb{k}}(G)$ ,  $N_{\mathbb{k}}(H)$  and the minimum Nullstellensatz degree of the graph obtained from  $G$  and  $H$  by applying the Hajós construction?*

## Acknowledgments

The authors thank Jesus De Loera and Susan Margulies for fruitful discussions, the anonymous referees for their helpful feedback, and Eric Stucky for his assistance in typesetting. We also thank the referees for very helpful comments on edits to and the restructuring of the article.

## A Appendix

Here, we give a complete proof of Proposition 2.1. The equivalence of the first three sets of polynomials was proven in Theorem 2.1 of [3], so we proceed by establishing the

equivalence of the fourth set of polynomials with the third. First, suppose we are given a polynomial  $x_i^2x_k + x_j^2x_k + x_ix_j^2 + x_ix_k^2$  in (8). Observe that

$$x_i^2x_k + x_j^2x_k + x_ix_j^2 + x_ix_k^2 = (x_i^2x_k + x_ix_jx_k + x_j^2x_k) + (x_j^2x_i + x_jx_kx_i + x_k^2x_i)$$

since  $\text{char}(\mathbb{k})=2$ . The two summands on the right are polynomials in (6) because  $v_iv_j$  and  $v_jv_k$  lie in  $E$ , so any polynomial in (8) is a  $\mathbb{k}$ -linear combination of polynomials in (6), and hence the fourth condition implies the third.

Now suppose the third condition holds, and we expressed 1 as a  $\mathbb{k}$ -linear combination of the polynomials in (5) and (6) as follows:

$$1 = \sum_{v_iv_j \in E} \alpha_{ij}(x_i^2x_j + x_ix_j^2 + 1) + \sum_{\substack{v_iv_j \in E \\ v_k \notin \{v_i, v_j\}, k \in V}} \beta_{ijk}(x_i^2x_k + x_ix_jx_k + x_j^2x_k). \quad (11)$$

Fix vertices  $v_i, v_j, v_k \in V$  with  $v_iv_j \in E$ . When the right-hand side of (11) is expanded, the coefficient of  $x_ix_jx_k$  must be 0. We now focus on the contribution of the polynomials in (5) and (6) to coefficient of  $x_ix_jx_k$  on the right-hand side for a fixed set of vertices  $\{v_i, v_j, v_k\}$ . Without loss of generality, we can demand  $v_iv_j \in E$ .

First, suppose neither  $v_iv_k$  nor  $v_jv_k$  are edges of  $G$ . Then the coefficient of  $x_ix_jx_k$  is  $\beta_{ijk}$ . Comparing both sides of (11) implies  $\beta_{ijk} = 0$ , and hence the polynomial  $x_i^2x_k + x_ix_jx_k + x_j^2x_k$  does not appear at all on the right-hand side of (11).

Now suppose all three of  $v_iv_j, v_jv_k, v_iv_k$  are all in  $E$ . The polynomials in (5) and (6) that contain  $x_ix_jx_k$  are

$$x_i^2x_k + x_ix_jx_k + x_j^2x_k, \quad x_k^2x_i + x_ix_jx_k + x_j^2x_i, \quad x_i^2x_j + x_ix_jx_k + x_k^2x_j,$$

so if any of these appear as summands of the right-hand side of (11), then exactly two of them do (since  $\text{char}(\mathbb{k})=2$ ). If none appear, we do not have to address this case, so assume exactly two appear, and without loss of generality assume they are the latter two. Then the combined contribution of these summands to the right-hand side of (11) is  $(x_k^2x_i + x_ix_jx_k + x_j^2x_i) + (x_i^2x_j + x_ix_jx_k + x_k^2x_j)$ . But observe

$$(x_k^2x_i + x_ix_jx_k + x_j^2x_i) + (x_i^2x_j + x_ix_jx_k + x_k^2x_j) = x_i^2x_j + x_k^2x_j + x_ix_j^2 + x_ix_k^2$$

which is a polynomial in (8) since  $v_iv_k, v_kv_j \in E$ .

Finally, suppose  $v_iv_k \notin E, v_jv_k \in E$ . This is the only remaining case since the case when  $v_iv_k \in E, v_jv_k \notin E$  follows by symmetry. In this case, the only polynomials in (5) and (6) that contain  $x_ix_jx_k$  as a summand are

$$x_i^2x_k + x_ix_jx_k + x_j^2x_k, \quad x_j^2x_i + x_ix_jx_k + x_k^2x_i.$$

Again, since the coefficient of  $x_ix_jx_k$  must be 0, either neither of these appear as summands in (11) or both do. Again, we only need consider the case when both appear. In this case, again since  $\mathbb{k} = GF(2)$ ,  $\beta_{ijk} = \beta_{kij} = 1$ . Observe then that the contribution of such polynomials to the right hand side of (11) is

$$(x_i^2x_k + x_ix_jx_k + x_j^2x_k) + (x_j^2x_i + x_ix_jx_k + x_k^2x_i) = x_j^2x_i + x_k^2x_i + x_kx_i^2 + x_kx_j^2,$$

and the latter polynomial is a polynomial in (8) since  $v_iv_j, v_jv_k \in E$ . Thus if 1 is a  $\mathbb{k}$ -linear combination of polynomials in (6) then it is a  $\mathbb{k}$ -linear combination of polynomials in (8).

## References

- [1] D.A. Bayer. *The Division Algorithm and the Hilbert Scheme*. PhD thesis, Harvard University, 1982.
- [2] D. Cox, J. Little, and D. O’Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, 3 edition, 2007. An introduction to computational algebraic geometry and commutative algebra.
- [3] J. De Loera, C. Hillar, P. Malkin, and M. Omar. Recognizing graph theoretic properties through polynomial ideals. *Electronic Journal of Combinatorics*, 17:R114, 2010.
- [4] J. De Loera, J. Lee, P.N. Malkin, and S. Margulies. Hilbert’s Nullstellensatz and an algorithm for proving combinatorial infeasibility. In *Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation (ISSAC 2008)*, 2008.
- [5] J. De Loera, J. Lee, S. Margulies, and S. Onn. Expressing combinatorial problems by systems of polynomial equations and Hilbert’s Nullstellensatz. *Combin. Probab. Comput.*, 18(4):551–582, 2009.
- [6] J. De Loera, S. Margulies, M. Pernpeintner, E. Riedl, G. Rolnick D., Spencer, D. Stasi, and Swenson J. Gröbner bases and nullstellensätze for graph-coloring ideals. In *Proceedings of the Twenty-seventh International Symposium on Symbolic and Algebraic Computation (ISSAC 2015)*, 2015.
- [7] J. Gouveia, P. Parrilo, and R.R. Thomas. Theta bodies for polynomial ideals. *SIAM Journal on Optimization*, 20(4):2097–2118, 2010.
- [8] G. Hajós. Über eine konstruktion nicht n-färbbarer graphen. *Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg, Math.-Nat. Reihe*, 10:116–117, 1961.
- [9] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3):796–817 (electronic), 2000/01.
- [10] L. Lovász. Stable sets and polynomials. *Discrete Math.*, 124(1-3):137–153, 1994. *Graphs and combinatorics* (Qawra, 1990).
- [11] L. Lovász and A. Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM J. Optim.*, 1(2):166–190, 1991.
- [12] K. Mizuno and S. Nishihara. Constructive generation of very hard 3-colorability instances. *Discrete Applied Mathematics*, 156(2):218–229, 2008.
- [13] H.D. Sherali and W.P. Adams. A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems. *SIAM J. Discrete Math.*, 3(3):411–430, 1990.
- [14] D.B. West. *Introduction to Graph Theory*, volume 2. Prentice Hall Upper Saddle River, 2001.