Combinatorics, Probability and Computing (2009) 18, 551–582.
doi:10.1017/S0963548309009894 Printed in the United Kingdom

Expressing Combinatorial Problems by Systems of Polynomial Equations and Hilbert's Nullstellensatz

J. A. LOERA[1†], J. LEE[2], S. MARGULIES[3†] and S. ONN[4‡]

[1]Department of Mathematics, University of California, Davis, California, USA
(e-mail: deloera@math.ucdavis.edu)

[2]IBM T. J. Watson Research Center, Yorktown Heights, New York, USA
(e-mail: jonlee@us.ibm.com)

[3]Department of Computer Science, University of California, Davis, California, USA
(e-mail: smargulies@ucdavis.edu)

[4]Davidson Faculty of IE & M, Technion – Israel Institute of Technology, Haifa, Israel
(e-mail: onn@ie.technion.ac.il)

Received 5 June 2007; revised 3 June 2008; first published online 28 April 2009

Systems of polynomial equations over the complex or real numbers can be used to model combinatorial problems. In this way, a combinatorial problem is feasible (*e.g.*, a graph is 3-colourable, Hamiltonian, *etc.*) if and only if a related system of polynomial equations has a solution.

For an infeasible polynomial system, the (complex) Hilbert Nullstellensatz gives a certificate that the associated combinatorial problem is infeasible. Thus, unless P = NP, there must exist an infinite sequence of infeasible instances of each hard combinatorial problem for which the minimum degree of a Hilbert Nullstellensatz certificate of the associated polynomial system grows.

In the first part of the paper, we show that the minimum degree of a Nullstellensatz certificate for the non-existence of a stable set of size greater than the stability number of the graph is the stability number of the graph. Moreover, such a certificate contains at least one term per stable set of G. In contrast, for non-3-colourability, we proved that the minimum degree of a Nullstellensatz certificate is at least four. Our efforts so far have only yielded graphs with Nullstellensatz certificates of precisely that degree.

In the second part of this paper, for the purpose of computation, we construct new polynomial encodings for the problems of finding in a graph its longest cycle, the largest planar subgraph, the edge-chromatic number, or the largest k-colourable subgraph. We include some applications to graph theory.

† Research supported in part by an IBM Open Collaborative Research Award and by NSF grant DMS-0608785.
‡ Research supported by the ISF (Israel Science Foundation) and by the fund for the promotion of research at the Technion.

1. Introduction

N. Alon [1] used the term 'polynomial method' to refer to the use of non-linear polynomials for solving combinatorial problems. Although the polynomial method is not yet as widely used by combinatorists as, for instance, polyhedral or probabilistic techniques, the literature in this subject continues to grow. Prior work on encoding combinatorial properties includes colourings [2, 11, 14, 17, 27, 30, 31, 32], stable sets [11, 26, 27, 39], matchings [15], and flows [2, 32, 33]. Non-linear encodings of combinatorial problems are often compact. This contrasts with the exponential sizes of systems of linear inequalities that describe the convex hull of incidence vectors of many combinatorial structures (see [40]).

The *polynomial method* has been mostly used to obtain theoretical results but not so much for actual computation. But recent work demonstrates that one can derive good semidefinite programming relaxations for combinatorial optimization problems from the encodings of these problems as polynomial systems (see [24] and references therein for details). Lasserre [22], Laurent [23] and Parrilo [35, 34] studied the problem of minimizing a general polynomial function $f(x)$ over an algebraic variety having only finitely many solutions. Laurent proved that when the variety consists of the solutions of a zero-dimensional ideal I, there is a way to set up the optimization problem $\min\{f(x) : x \in \text{variety}(I)\}$ as a finite sequence of semidefinite programs terminating with the optimal solution (see [23]). These SDP relaxations have been used in actual computation with great success (see, *e.g.*, [4, 12]).

The polynomial method combined with semidefinite programming is a way to approach optimization problems. In this paper, we look instead at *feasibility* or *decision* problems. Our key observation is that the sequence of SDPs is replaced by a simpler sequence of large-scale linear algebra problems. The main idea to generate these systems of linear equations is to rely on the (complex) Hilbert's Nullstellensatz. For a combinatorial feasibility problem, *e.g.*, deciding the k-colourability of graphs, we associate a system of polynomial equations J such that the system has a solution if and only if the combinatorial problem is indeed feasible. On the other hand, the famous Hilbert Nullstellensatz (see [9]) states that a system of polynomial equations $J = \{f_1(x) = 0, f_2(x) = 0, \ldots, f_r(x) = 0\}$ with complex coefficients has no solution in $\mathbb{C}^n$ if and only if there exist polynomials $\alpha_1, \ldots, \alpha_r \in \mathbb{C}[x_1, \ldots, x_n]$ such that $1 = \sum \alpha_i f_i$. Thus, if the polynomial system J has no solution, there exists a *certificate* that the associated combinatorial problem is infeasible. If the coefficients α_i have fixed degree D, the Nullstellensatz certificate is equivalent to a linear algebra system whose number of variables grows with the number of monomials of degree D. We will explain details of the construction of this linear algebra system in Section 2. The main purpose of this article is to investigate the complexity and growth of these linear algebra systems.

There are well-known *upper bounds*, due to Kollar [20], for the degrees of the coefficients α_i in the Hilbert Nullstellensatz certificate for *general* systems of polynomials, and they turn out to be sharp. For instance, the following well-known example (due to Mora, Lazard, Masser, Philippon and Kollár) shows that the degree of α_1 is at least d^m:

$$f_1 = x_1^d,\ f_2 = x_1 - x_2^d,\ \ldots,\ f_{m-1} = x_{m-2} - x_{m-1}^d,\ f_m = 1 - x_{m-1}x_m^{d-1}.$$

But polynomial systems for combinatorial optimization problems are not necessarily pathologically complicated. The natural question is: *How large are the degrees of Nullstellensatz certificates*

of infeasibility for combinatorial ideals? A fundamental result by Lazard [25] (see also [6]) proves that for combinatorial ideals, like the ones discussed in Section 2, there is an upper bound that is *linear* on the number of variables, improving the exponential bound of [20]. In Section 2 we will see that the linear bound of Lazard is tight for the stability number of graphs but it seems too pessimistic for 3-colourability.

There is a fascinating connection between the Nullstellensatz and computational complexity. As we will see in Section 2, unless P = NP, for every hard combinatorial problem there must exist an infinite sequence of infeasible instances for which the minimum degree of a Nullstellensatz certificate, for the associated system of polynomials, grows arbitrarily large. This was first observed by L. Lovász, who then proposed the problem of finding explicit graphs exhibiting such growth (see [27]). A main contribution of this article is to explicitly exhibit the growth of degree of specific families of graphs. In the first part of the paper we discuss the growth of degree for the NP-complete problems 'stable set' and '3-colourability'. We establish the following main theorem.

Theorem 1.1.

(i) *Given a graph G, let $\alpha(G)$ denote its stability number. A minimum-degree Nullstellensatz certificate for the non-existence of a stable set of size greater than $\alpha(G)$ has degree equal to $\alpha(G)$ and contains at least one term per stable set in G.*

(ii) *Every Nullstellensatz certificate for non-3-colourability of a graph has degree at least four. Moreover, in the case of a graph containing an odd-wheel or a clique as a subgraph, a minimum-degree Nullstellensatz certificate for non-3-colourability has degree exactly four.*

The motivation of our work is to use the Nullstellensatz linear algebra method as a computational tool much in the same way that linear and semidefinite programming have been used already by combinatorists. Our general scheme is as follows. If we can encode a combinatorial problem with polynomial equations in $\mathbb{R}[x_1, \ldots, x_n]$ that generate a zero-dimensional (variety is finite) ideal, then we generate the finite sequence of linear algebra systems that can help decide feasibility of our combinatorial problem. This highlights the importance of finding systems of polynomials for various combinatorial optimization problems. The second part of this paper proposes new polynomial system encodings for the problems, with respect to an input graph, of finding a longest cycle, a largest planar subgraph, a largest k-colourable subgraph, or a minimum edge colouring. In particular, we establish the following result.

Theorem 1.2.

(i) *A simple graph G with nodes $1, \ldots, n$ has a cycle of length L if and only if the following zero-dimensional system of polynomial equations has a solution.*

$$\sum_{i=1}^{n} y_i = L. \tag{1.1}$$

For every node $i = 1, \ldots, n$,

$$y_i(y_i - 1) = 0, \quad \prod_{s=1}^{n}(x_i - s) = 0, \tag{1.2}$$

$$y_i \prod_{j \in \mathrm{Adj}(i)} (x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(L-1)) = 0. \tag{1.3}$$

Here $\mathrm{Adj}(i)$ *denotes the set of nodes adjacent to node* i.

(ii) *Let* G *be a simple graph with* n *nodes and* m *edges.* G *has a planar subgraph with* K *edges if and only if the following zero-dimensional system of equations has a solution.*
For every edge $\{i, j\} \in E(G)$,

$$z_{\{ij\}}^2 - z_{\{ij\}} = 0, \quad \sum_{\{i,j\} \in E(G)} z_{\{ij\}} - K = 0.$$

For $k = 1, 2, 3$, *every node* $i \in V(G)$ *and every edge* $\{i, j\} \in E(G)$,

$$\prod_{s=1}^{n+m}(x_{\{i\}k} - s) = 0, \quad \prod_{s=1}^{n+m}(y_{\{ij\}k} - s) = 0,$$

$$s_k\Bigg(\prod_{\substack{i,j \in V(G) \\ i<j}} \big(x_{\{i\}k} - x_{\{j\}k}\big) \prod_{\substack{i \in V(G), \\ \{u,v\} \in E(G)}} \big(x_{\{i\}k} - y_{\{uv\}k}\big) \prod_{\{i,j\},\{u,v\} \in E(G)} \big(y_{\{ij\}k} - y_{\{uv\}k}\big)\Bigg) = 1.$$

For $k = 1, 2, 3$, *and for every pair of a node* $i \in V(G)$ *and incident edge* $\{i, j\} \in E(G)$,

$$z_{\{ij\}}\big(y_{\{ij\}k} - x_{\{i\}k} - \Delta_{\{ij,i\}k}\big) = 0. \tag{1.4}$$

For every pair of a node $i \in V(G)$ *and edge* $\{u, v\} \in E(G)$ *that is not incident on* i,

$$\begin{aligned} z_{\{uv\}}\big(y_{\{uv\}1} - x_{\{i\}1} - \Delta_{\{uv,i\}1}\big)\big(y_{\{uv\}2} - x_{\{i\}2} - \Delta_{\{uv,i\}2}\big) \\ \times \big(y_{\{uv\}3} - x_{\{i\}3} - \Delta_{\{uv,i\}3}\big) = 0, \\ z_{\{uv\}}\big(x_{\{i\}1} - y_{\{uv\}1} - \Delta_{\{i,uv\}1}\big)\big(x_{\{i\}2} - y_{\{uv\}2} - \Delta_{\{i,uv\}2}\big) \\ \times \big(x_{\{i\}3} - y_{\{uv\}3} - \Delta_{\{i,uv\}3}\big) = 0. \end{aligned}$$

For every pair of edges $\{i, j\}, \{u, v\} \in E(G)$ (*regardless of whether or not they share an endpoint*),

$$\begin{aligned} z_{\{ij\}}z_{\{uv\}}\big(y_{\{ij\}1} - y_{\{uv\}1} - \Delta_{\{ij,uv\}1}\big)\big(y_{\{ij\}2} - y_{\{uv\}2} - \Delta_{\{ij,uv\}2}\big) \\ \times \big(y_{\{ij\}3} - y_{\{uv\}3} - \Delta_{\{ij,uv\}3}\big) = 0, \\ z_{\{ij\}}z_{\{uv\}}\big(y_{\{uv\}1} - y_{\{ij\}1} - \Delta_{\{uv,ij\}1}\big)\big(y_{\{uv\}2} - y_{\{ij\}2} - \Delta_{\{uv,ij\}2}\big) \\ \times \big(y_{\{uv\}3} - y_{\{ij\}3} - \Delta_{\{uv,ij\}3}\big) = 0. \end{aligned}$$

For every pair of nodes $i, j \in V(G)$ (*regardless of whether or not they are adjacent*),

$$\big(x_{\{i\}1} - x_{\{j\}1} - \Delta_{\{i,j\}1}\big)\big(x_{\{i\}2} - x_{\{j\}2} - \Delta_{\{i,j\}2}\big)\big(x_{\{i\}3} - x_{\{j\}3} - \Delta_{\{i,j\}3}\big) = 0,$$

$$\big(x_{\{j\}1} - x_{\{i\}1} - \Delta_{\{j,i\}1}\big)\big(x_{\{j\}2} - x_{\{i\}2} - \Delta_{\{j,i\}2}\big)\big(x_{\{j\}3} - x_{\{i\}3} - \Delta_{\{j,i\}3}\big) = 0.$$

For every Δ_{index} (*e.g.*, $\Delta_{\{ij,uv\}k}, \Delta_{\{ij,i\}k}$, *etc.*) *variable appearing in the above system,*

$$\prod_{d=1}^{n+m-1} \left(\Delta_{\text{index}} - d\right) = 0.$$

(iii) *A graph G has a k-colourable subgraph with R edges if and only if the following zero-dimensional system of equations has a solution.*

$$\sum_{\{i,j\}\in E(G)} y_{ij} - R = 0. \tag{1.5}$$

For every vertex $i \in V(G)$,

$$x_i^k = 1. \tag{1.6}$$

For every edge $\{i, j\} \in E(G)$,

$$y_{ij}^2 - y_{ij} = 0, \quad y_{ij}\left(x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_j^{k-1}\right) = 0. \tag{1.7}$$

(iv) *Let G be a simple graph with maximum vertex degree* Δ. *The graph G has edge-chromatic number* Δ *if and only if the following zero-dimensional system of polynomials has a solution. For every edge* $\{i, j\} \in E(G)$,

$$x_{ij}^{\Delta} = 1. \tag{1.8}$$

For every node $i \in V(G)$,

$$s_i\left(\prod_{\substack{j,k\in \text{Adj}(i)\\ j<k}} (x_{ij} - x_{ik})\right) = 1, \tag{1.9}$$

where Adj(i) *is the set of nodes adjacent to node i.* (*By Vizing's theorem, if the system has no solution, then G has edge-chromatic number* $\Delta + 1$.)

The paper is organized as follows. In Section 2 we show that, under the assumption that P $\neq$ NP, the minimum degree of a Nullstellensatz certificate for an NP-hard problem must grow with respect to the input size (we work out all details for 3-colourability). We explain how to generate the linear algebra systems associated with minimum-degree Nullstellensatz certificates. In Section 2.1, this time without the assumption of P $\neq$ NP, we demonstrate the degree growth of Nullstellensatz certificates for the stable set problem and show that the number of monomials in the certificate grows exponentially. This is in essence the proof of Theorem 1.1(i). Section 2.2 contains the proof of Theorem 1.1(ii). We also briefly discuss our computer experiments with non-3-colourable graphs where there is no growth of degree. Section 3 (specifically Section 3.1) contains the encoding with polynomials for the problems (1) longest cycle, (2) largest planar subgraph, (3) edge-chromatic number, and (4) largest k-colourable subgraph. We conclude in Section 3.2 with a graph theory application, by proposing a notion of *dual colouring* of graphs.

2. Nullstellensatz degree growth and combinatorics

The Hilbert Nullstellensatz states that a system of polynomial equations

$$\{f_1(x) = 0, f_2(x) = 0, \ldots, f_r(x) = 0\} \subseteq \mathbb{C}[x_1, \ldots, x_n]$$

has no solution in $\mathbb{C}^n$ if and only if there exist polynomials $\alpha_1, \ldots, \alpha_r \in \mathbb{C}[x_1, \ldots, x_n]$ such that $1 = \sum \alpha_i f_i$ (see [9]). The purpose of this section is to investigate the degree growth of the coefficients α_i. In particular, we investigate the degree growth of Nullstellensatz certificates related to systems of polynomials arising in combinatorial optimization.

Definition. For a Nullstellensatz certificate $1 = \sum_{i=1}^{r} \alpha_i f_i$, its *degree* is $\max_{1 \leqslant i \leqslant r} \{\deg(\alpha_i)\}$.

In our investigations, we will often need to find explicit Nullstellensatz certificates for specific graphs. This can be done via linear algebra. First, given a system of polynomial equations, fix a tentative degree for the coefficient polynomials α_i in the Nullstellensatz certificate. This yields a *linear* system of equations whose variables are the coefficients of the monomials of the polynomials $\alpha_1, \ldots, \alpha_r$. Then, solve this linear system. If the system has a solution, we have found a Nullstellensatz certificate. Otherwise, try a higher degree for the polynomials α_i. For the Nullstellensatz certificates, the degrees of the polynomials α_i cannot be more than known bounds (see, *e.g.*, [6, 20, 25] and references therein); thus we have a finite (but potentially long) procedure to decide whether or not a system of polynomials is feasible. An important point, which we have observed in practice, is that very low-degree certificates often work well under the linear bounds of [25] for our special ideals. We also remark that this linear algebra method finds not only a Nullstellensatz certificate (if it exists), but it finds one of the *minimum-possible degree*.

Next, we illustrate the generation of linear algebra systems from the Nullstellensatz in a concrete situation. D. Bayer established a characterization of 3-colourability via a system of polynomial equations [5], which we will use throughout this paper. In fact, one can establish that Bayer's result generalizes as follows (see [29]).

Lemma 2.1. *Graph G is k-colourable if and only if the following zero-dimensional system of equations,*

$$x_i^k - 1 = 0, \quad \textit{for every node } i \in V(G),$$
$$\sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d = 0, \quad \textit{for every edge } \{i, j\} \in E(G),$$

has a solution. Moreover, the number of solutions equals the number of distinct k-colourings multiplied by $k!$.

Example 1. Suppose that we wish to test K_4 for 3-colourability, and we assume that the α_i in the Nullstellensatz certificate all have degree 1. After encoding K_4 with the system of polynomial equations, we 'conjecture' that there exists a Nullstellensatz certificate of the following form:

$$\begin{aligned}
1 = {} & (c_0x_0 + c_1x_1 + c_2x_2 + c_3x_3 + c_4)(x_0^3 - 1) + (c_5x_0 + c_6x_1 + c_7x_2 + c_8x_3 + c_9)(x_1^3 - 1) \\
& + (c_{10}x_0 + \cdots + c_{14})(x_2^3 - 1) + (c_{15}x_0 + \cdots + c_{19})(x_3^3 - 1) \\
& + (c_{20}x_0 + \cdots + c_{24})(x_0^2 + x_0x_1 + x_1^2) + (c_{25}x_0 + \cdots + c_{29})(x_0^2 + x_0x_2 + x_2^2) \\
& + (c_{30}x_0 + \cdots + c_{34})(x_0^2 + x_0x_3 + x_3^2) + (c_{35}x_3 + \cdots + c_{39})(x_1^2 + x_1x_2 + x_1^2) \\
& + (c_{40}x_0 + \cdots + c_{44})(x_1^2 + x_1x_3 + x_3^2) + (c_{45}x_0 + \cdots + c_{49})(x_2^2 + x_2x_3 + x_3^2).
\end{aligned}$$

When we multiply out this certificate, we group together like powers of x_0, x_1, x_2, x_3 as follows:

$$1 = c_0x_0^4 + \cdots + c_{12}x_2^4 + \cdots + c_7x_1^3x_2 + \cdots + (c_{21} + c_{20} + c_{26} + c_{31})x_0^2x_1 + \cdots + (c_{34} + c_{44} + c_{49})x_3^2 + \cdots + (-c_{14} - c_{19} - c_4 - c_9).$$

Because the Nullstellensatz certificate is identically one, this identity gives rise to the following system of linear equations: $0 = c_0, 0 = c_{12}, 0 = c_7, 0 = c_{21} + c_{20} + c_{26} + c_{31}, 0 = c_{34} + c_{44} + c_{49}, \ldots, 1 = -c_{14} - c_{19} - c_4 - c_9$. In other words, we have a large-scale sparse system of linear equations that consists only of 1s and -1s. In this example, it turns out that degree 1 is not sufficient for generating a Nullstellensatz certificate, that is, this linear system has no solution. Ultimately, we discovered that degree four is required, and we were able to produce the following certificate:

$$\begin{aligned}1 = {} & \left(\frac{4}{9}x_1^4 - \frac{5}{9}x_1^3x_2 - \frac{2}{9}x_1^3x_3 - \frac{4}{9}x_1^3x_0 + \frac{2}{9}x_1^2x_2x_0 + \frac{2}{9}x_1^2x_3x_0\right)(x_1^2 + x_2x_1 + x_2^2) \\ & + \left(\frac{1}{9}x_1^4 + \frac{2}{9}x_1^3x_2 - \frac{1}{9}x_1^3x_0 - \frac{2}{9}x_1^2x_2x_0\right)(x_2^2 + x_3x_2 + x_3^2) + \frac{1}{3}x_1^3x_2(x_2^2 + x_0x_2 + x_0^2) \\ & + \left(\frac{2}{9}x_1^4 + \frac{1}{9}x_1^3x_2 + \frac{1}{9}x_1^3x_0 + \frac{2}{9}x_1^2x_2x_0\right)(x_1^2 + x_3x_1 + x_3^2) + \frac{1}{3}x_1^4(x_1^2 + x_0x_1 + x_0^2) \\ & + \left(-\frac{1}{3}x_1^4 - \frac{1}{3}x_1^3x_2\right)(x_3^2 + x_0x_3 + x_0^2) + (-x_1^3 - 1)(x_1^3 - 1). \end{aligned} \tag{2.1}$$

Our investigations of degree growth of the Nullstellensatz were motivated by the following key point.

Lemma 2.2. *If P $\neq$ NP, then there must exist an infinite family of graphs whose minimum-degree non-3-colourability Nullstellensatz certificates have unbounded growth with respect to the number of vertices and edges in the graph.*

Proof. Our proof is by contradiction with the hypothesis P $\neq$ NP. Consider a non-3-colourable graph whose 3-colourability has been encoded as the system of polynomial equations $x_i^3 - 1 = 0$ for $i \in V(G)$, and $x_i^2 + x_ix_j + x_j^2 = 0$ for $\{i, j\} \in E(G)$. Assume that every minimum-degree non-3-colourability Nullstellensatz certificate has $\deg(\alpha_i) < d$ for some constant d. We will show that P = NP by providing a polynomial-time algorithm for solving graph-3-colouring.

(1) Given a graph G, encode it as the above system of polynomial equations.
(2) Construct and solve the associated linear system for monomials of degree $< d$.
(3) If the system has a solution, a Nullstellensatz certificate exists, and the graph is non-3-colourable: Return **no**.
(4) If the system does *not* have a solution, there does *not* exist a Nullstellensatz certificate, and the graph is 3-colourable: Return **yes**.

Now we analyse the running time of this algorithm. In step (1), our encoding has one polynomial equation per vertex and one polynomial equation per edge. Since there are $O(n^2)$ edges in a graph, our polynomial system has $n + n^2 = O(n^2)$ equations. Because every equation only contains coefficients ± 1 and is of degree three or less, encoding the graph as the above system of polynomial equations clearly runs in polynomial time.

For step (2), we note that by Corollary 3.2b of [37], if a system of linear equations $Ax = b$ has a solution, then it has a solution polynomially bounded by the bit sizes of the matrix A and the vector b (see [37] for a definition of bit size). In this case, the vector b contains only zeros and ones. To calculate the bit size of A, we recall our assumption that, for every α_i, $\deg(\alpha_i) < d$ for some constant d. Therefore, an upper bound on the number of terms in each α_i is the total number of monomials in n variables of degree less than or equal to d. Therefore, the number of terms in each α_i is

$$\binom{n+d-1}{n-1} + \binom{n+d-2}{n-1} + \cdots + \binom{n-1}{n-1} = O(n^d) + O(n^{d-1}) + \cdots + O(1) = O(n^d).$$

Because there are $O(n^2)$ equations, there are at most $O(n^{d+2})$ unknowns in the linear system, and thus, $O(n^{d+2})$ columns in A. Because the vertex equations $(x_i^3 - 1) = 0$ have two terms, and the edge equations $(x_i^2 + x_i x_j + x_j^2) = 0$ have 3 terms, there are $O(n^{d+2})$ terms in the *expanded* Nullstellensatz certificate, and $O(n^{d+2})$ rows in A. Because entries in A are $0, \pm 1$, the matrix A contains only entries of bit size at most 2. Therefore, the bit sizes of both A and b are polynomially bounded in n, and by Theorem 3.3 of [37], the linear system can be solved in polynomial time.

Therefore, we have demonstrated a polynomial-time algorithm for solving graph-3-colouring, and because graph-3-colouring is NP-complete ([16]), this implies P = NP, which contradicts our hypothesis. Therefore, $\deg(\alpha_i) \not\leq d$ for any constant d. □

Thus, in the linear algebra approach to finding a minimum-degree Nullstellensatz certificate, the existence of a universal constant bounding the degree is impossible under a well-known conjecture of complexity theory. Clearly, a similar result can be obtained for other encodings (see [29]). Note that the linear algebra method does not rely on any property that is *unique* to a particular combinatorial or NP-complete problem; the only assumption is that the problem can be *represented* as a system of polynomial equations. We will use it to find Nullstellensatz certificates of non-3-colourability and sizes of stable sets of graphs.

2.1. The Nullstellensatz and stable sets of graphs

Recall that a *stable set* or *independent set* in a graph G is a subset of vertices such that no two vertices in the subset are adjacent. The maximum size $\alpha(G)$ of a stable set is called the *stability number* of G. The problem of finding a stable set in a graph can be encoded as the following system of polynomial equations.

Lemma 2.3 (Lovász [27]). *Graph G has stability number at least k if and only if the following zero-dimensional system of equations,*

$$\begin{aligned} x_i^2 - x_i &= 0, \quad \textit{for every node } i \in V(G), \\ x_i x_j &= 0, \quad \textit{for every edge } \{i, j\} \in E(G), \\ \sum_{i=1}^{n} x_i &= k, \end{aligned}$$

has a solution.

Lovász [27] stated the challenge of finding an explicit family of graphs with growth in the minimum degree of their Nullstellensatz certificates. Here we solve his challenge for the stable set problem. Note that we do not assume P $\neq$ NP. Our main result is stated in Theorem 1.1: for every graph G, there exists a Nullstellensatz certificate of degree $\alpha(G)$ (the stability number of G), certifying that G has no stable set of size greater than $\alpha(G)$; moreover, this is the minimum-possible degree for all graphs. In what follows, for any graph G with stability number $\alpha(G)$ and an integer $r \geqslant 1$, the Nullstellensatz certificate has the general form

$$1 = A\left(-(\alpha(G)+r) + \sum_{i=1}^{n} x_i\right) + \sum_{i\in V(G)} Q_i(x_i^2 - x_i) + \sum_{\{i,j\}\in E(G)} Q_{ij}(x_i x_j). \tag{2.2}$$

In this section, we refer to the coefficient polynomials using these particular letters (that is, A, Q_i, Q_{ij}, *etc.*)

Lemma 2.4. *For any graph G and a Nullstellensatz certificate*

$$1 = A\left(-(\alpha(G)+r) + \sum_{i=1}^{n} x_i\right) + \sum_{i\in V(G)} Q_i(x_i^2 - x_i) + \sum_{\{i,j\}\in E(G)} Q_{ij}(x_i x_j), \tag{2.3}$$

certifying that G has no stable set of size $(\alpha(G)+r)$ (*with* $r \geqslant 1$)*, we can construct a 'reduced' Nullstellensatz certificate*

$$1 = A'\left(-(\alpha(G)+r) + \sum_{i=1}^{n} x_i\right) + \sum_{i\in V(G)} Q'_i(x_i^2 - x_i) + \sum_{\{i,j\}\in E(G)} Q'_{ij}(x_i x_j),$$

satisfying the following.

(1) *The coefficient A' multiplying $-(\alpha(G)+r) + \sum_{i=1}^{n} x_i$ has only square-free monomials supported on stable sets of G, and thus* $\deg(A') \leqslant \alpha(G)$.
(2) $\max\{\deg(A), \deg(Q_i), \deg(Q_{ij})\} = \max\{\deg(A'), \deg(Q'_i), \deg(Q'_{ij})\}$. *Thus, if the original Nullstellensatz certificate has minimum degree, the 'reduced' certificate also has minimum degree.*

Proof. Let I be the ideal generated by $x_i^2 - x_i$ (for every node $i \in V(G)$), and $x_i x_j$ (for every edge $\{i,j\} \in E(G)$). Furthermore, let $B := -(\alpha(G)+r) + \sum_{i=1}^{n} x_i$. We apply reductions modulo I to (2.3). If a non-square-free monomial appears in polynomial A, say $x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_k}^{\alpha_k}$ with at least one $\alpha_j > 1$, then we can subtract the polynomial $x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots, x_{i_j}^{\alpha_j - 2} x_{i_k}^{\alpha_k} B(x_{i_j}^2 - x_{i_j})$ from AB and simultaneously add it to $\sum Q_s(x_s^2 - x_s)$. Thus, eventually we obtain a new certificate that has only square-free monomials in A'. Furthermore, if Q'_s has new monomials, they are of degree less than or equal to what was originally in A.

Similarly, if $x_{i_1} x_{i_2} \cdots x_{i_k}$ appears in A, but $x_{i_1} x_{i_2} \cdots x_{i_k}$ contains an edge $\{i,j\} \in E(G)$ (if $x_i x_j$ divides $x_{i_1} x_{i_2} \cdots x_{i_k}$), then we can again subtract $B(x_{i_1} x_{i_2} \cdots x_{i_k}/x_i x_j)(x_i x_j)$ from AB, and, at the same time, add it to $\sum_{\{i,j\}\in E(G)} Q_{ij} x_i x_j$. Furthermore, the degree is maintained, and we have reached the form we claim exists for A'. □

We now show that, for *every* graph, there exists an explicit Nullstellensatz certificate of degree $\alpha(G)$. In order to prove this claim, we introduce the following notation. Let S_i be the set of all stable sets of size i in G. For any stable set $I \in S_i$, if I consists of the vertices $\{c_1, c_2, \ldots, c_i\}$, then $x_I := x_{c_1} x_{c_2} \cdots x_{c_i}$, and we refer to the monomial x_I as a 'stable set'. We define $S_0 := \emptyset$, and $x_\emptyset = 1$. If we say $I \cup k \in S_{i+1}$, we explicitly mean that $I \cap k = \emptyset$, and that $x_I x_k$ is a square-free stable-set monomial of degree $i+1$. If $I \cup k \notin S_{i+1}$, we explicitly mean that $I \cap k = \emptyset$ but $I \cup k$ contains at least one edge $\{k, c_j\}$. In other words, $x_I x_k$ is a square-free non-stable-set monomial of degree $i+1$. In this case, let $\min_k(I)$ denote the *smallest* $c_j \in I$ such that $\{k, c_j\} \in E(G)$. Finally, let

$$P_i := \sum_{I \in S_i} x_I, \quad \text{with} \quad P_0 := 1, \quad \text{and} \quad L_i := \frac{iL_{i-1}}{\alpha(G) + r - i}, \quad \text{with} \quad L_0 := \frac{1}{\alpha(G) + r}.$$

Theorem 2.5. *Given a graph G, there exists a Nullstellensatz certificate of degree $\alpha(G)$ certifying the non-existence of a stable set of size $\alpha(G) + r$ (for $r \geqslant 1$) such that*

$$1 = A\left(-(\alpha(G) + r) + \sum_{i=1}^{n} x_i\right) + \sum_{\{u,v\} \in E(G)} Q_{uv} x_u x_v + \sum_{k=1}^{n} Q_k (x_k^2 - x_k), \tag{2.4}$$

where

$$A = -\sum_{i=0}^{\alpha(G)} L_i P_i, \quad Q_{uv} = \sum_{i=1}^{\alpha(G)} \left(\sum_{\substack{I \in S_i : I \cup v \notin S_{i+1} \text{ and} \\ \min_v(I) = u}} L_{i+1} x_{I \setminus u} \right) \quad \text{and}$$

$$Q_k = \sum_{i=0}^{\alpha(G)} \left(\sum_{I \in S_i : I \cup k \in S_{i+1}} L_{i+1} x_I \right).$$

Proof. Our proof is the direct verification of (2.4). For convenience of notation, we let

$$B := -(\alpha(G) + r) + \sum_{i=1}^{n} x_i, \quad C := \sum_{\{u,v\} \in E(G)} Q_{uv} x_u x_v \quad \text{and} \quad D := \sum_{k=1}^{n} Q_k (x_k^2 - x_k).$$

It is easy to see that

$$-L_0 P_0 \big(-(\alpha(G) + r)\big) = -\frac{1}{\alpha(G) + r} \big(-(\alpha(G) + r)\big) = 1.$$

We will now show that the coefficient for every other monomial in (2.4) simplifies to zero. We begin by observing that every monomial in A, Q_k or Q_{uv} is a stable set, and furthermore, that the stable-set monomials in Q_k do not contain the variable x_k, and the stable-set monomials in Q_{uv} contain neither x_u nor x_v. Therefore, in the expanded certificate $AB + C + D$, only three types of monomials appear: square-free stable-set monomials, square-free non-stable-set monomials, and stable-set monomials with exactly one variable squared.

- **Square-free stable set.** Let $I = \{c_1, c_2, \ldots, c_m\}$ be any stable set of size m. The monomial x_I is created in AB in two ways: $x_{I \setminus c_k} x_{c_k}$ (formed m times, one for each c_k), or $x_I \big(-(\alpha(G) + r)\big)$.

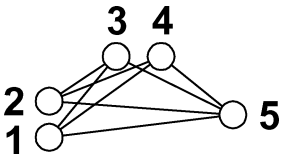

Figure 1. Turán graph $T(5,3)$.

Thus, the coefficient for x_I in AB is

$$-mL_{m-1} - L_m\big(-(\alpha(G)+r)\big) = -m\frac{L_m(\alpha(G)+r-m)}{m} + L_m(\alpha(G)+r) = mL_m.$$

The monomial x_I does not appear in C, because x_I is a stable-set monomial. However, the monomial x_I is produced by $x_{I\setminus c_k}(-x_{c_k})$ in D (formed m times, one for each c_k), and the coefficient for x_I in D is $-mL_m$. Therefore, we see that

$$\underbrace{mL_m}_{\text{from } AB} \underbrace{-mL_m}_{\text{from } D} = 0.$$

- **Square-free non-stable set.** Let $I = \{c_1, c_2, \ldots, c_{m-1}, u\}$ be any stable set of size m, and consider the monomial $x_I x_v$ where $u = \min_v I$ and $\{u,v\} \in E(G)$. Now, consider all $\binom{m+1}{m}$ subsets of $\{c_1, c_2, \ldots, c_{m-1}, u, v\}$, and let M be the number of stable sets among those $\binom{m+1}{m}$ subsets. Each of those M subsets appears as a stable-set monomial in A. Therefore, the monomial $x_I x_v$ is created M times in AB, and the coefficient for $x_I x_v$ in AB is $-ML_m$. The monomial $x_I x_v$ does not appear in D, because it is a non-stable-set monomial, and it appears exactly M times in C. Therefore, the coefficient for $x_I x_v$ in C is ML_m, and we see that

$$\underbrace{-ML_m}_{\text{from } AB} + \underbrace{ML_m}_{\text{from } C} = 0.$$

- **Stable set with one variable squared.** Let $I = \{c_1, c_2, \ldots, c_{m-1}, k\}$ be any stable set of size m, and consider the monomial $x_{I\setminus k}x_k^2$. This monomial is created in AB by the direct product $x_I x_k$, and the coefficient is $-L_m$. This monomial is not created in C, because it contains no edges, and it is created in D by $x_{I\setminus k}x_k^2$. Thus, the coefficient for $x_I x_k$ in D is L_m, and we see that

$$\underbrace{-L_m}_{\text{from } AB} + \underbrace{L_m}_{\text{from } D} = 0.$$

Therefore, we have shown that the constant term in $AB + C + D$ is one, and the coefficient for every other monomial is zero. Therefore, (2.4) is a Nullstellensatz certificate of degree $\alpha(G)$. □

Example 2. We display a certificate from Theorem 2.5. Figure 1 depicts the Turán graph $T(5,3)$. It is clear that $\alpha(T(5,3)) = 2$. Therefore, we 'test' for a stable set of size 3. The

certificate is

$$\begin{aligned}1 = {} & \left(\frac{1}{3}x_4 + \frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_3 + \left(\frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_4 + \left(\frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_5 + \left(\frac{1}{3}x_4 + \frac{1}{3}\right)x_2x_3 \\ & + \left(\frac{1}{3}\right)x_2x_4 + \left(\frac{1}{3}\right)x_2x_5 + \left(\frac{1}{3}x_4 + \frac{1}{3}\right)x_3x_5 + \left(\frac{1}{3}\right)x_4x_5 + \left(\frac{1}{3}x_2 + \frac{1}{6}\right)(x_1^2 - x_1) \\ & + \left(\frac{1}{3}x_1 + \frac{1}{6}\right)(x_2^2 - x_2) + \left(\frac{1}{3}x_4 + \frac{1}{6}\right)(x_3^2 - x_3) + \left(\frac{1}{3}x_3 + \frac{1}{6}\right)(x_4^2 - x_4) \\ & + \left(\frac{1}{6}\right)(x_5^2 - x_5) + \underbrace{\left(-\frac{1}{3}(x_1x_2 + x_3x_4) - \frac{1}{6}(x_1 + x_2 + x_3 + x_4 + x_5) - \frac{1}{3}\right)}_{\text{stable-set polynomial}} \\ & \times (x_1 + x_2 + x_3 + x_4 + x_5 - 3).\end{aligned}$$

Note that the coefficient for the stable-set polynomial contains one monomial for every stable set in $T(5,3)$. For example, note that the term $-\frac{1}{3}x_1x_2$ corresponds to the stable set formed by vertices 1 and 2 in Figure 1. Furthermore, note that every monomial in every coefficient is also a stable set in $T(5,3)$.

We will now prove that the stability number $\alpha(G)$ is the minimum degree for any Nullstellensatz certificate for the non-existence of a stable set of size greater than $\alpha(G)$. To prove this, we rely on two lemmas. For convenience of notation, in the next two lemmas, we let

$$B := -(\alpha(G) + r) + \sum_{i=1}^{n} x_i, \quad C := \sum_{\{i,j\} \in E(G)} Q'_{ij}x_ix_j \quad \text{and} \quad D := \sum_{i=1}^{n} Q'_i(x_i^2 - x_i).$$

Lemma 2.6. *Let G be a graph, and let*

$$1 = A'\left(-(\alpha(G) + r) + \sum_{i=1}^{n} x_i\right) + \sum_{\{i,j\} \in E(G)} Q'_{ij}x_ix_j + \sum_{i=1}^{n} Q'_i(x_i^2 - x_i), \tag{2.5}$$

be a reduced *(via Lemma 2.4) Nullstellensatz certificate proving the non-existence of a stable set of size $\alpha(G) + r$ (for $r \geqslant 1$). Then the constant term in A' is $-L_0$, and the coefficient for x_i in A' is $-L_1$.*

Proof. The certificate presented in (2.5) must simplify to one. A constant only appears in the expanded certificate $A'B + C + D$ via the product of a constant term in A' and the constant term in B. Therefore, letting β_0 be the constant term in A', we see

$$-(\alpha(G) + r)\beta_0 = 1 \quad \Longrightarrow \quad \beta_0 = -\frac{1}{\alpha(G) + r} = -L_0.$$

Now let β_i be the coefficient of x_i in A' and let $D = \deg(Q'_i)$. Therefore,

$$Q'_i = M_Dx_i^D + M_{D-1}x_i^{D-1} + \cdots + M_1x_i + M_0 + \text{other terms in } Q'_i \text{ that are not powers of } x_i.$$

Now consider the coefficients for x_i, x_i^2 in the expanded certificate $A'B + C + D$, which must simplify to zero:

$$\begin{aligned} \mathbf{x_i}: &\quad 0 = \beta_i\big(-(\alpha(G)+r)\big) - M_0 - L_0, \\ \mathbf{x_i^2}: &\quad 0 = \beta_i + M_0 - M_1. \end{aligned}$$

Now consider the coefficients for the monomials $x_i^{D+2}, x_i^{D+1}, \ldots, x_i^3$ in the expanded certificate $A'B + C + D$, which are $M_D, -M_D + M_{D-1}, -M_{D-1} + M_{D-2}, \ldots, -M_2 + M_1$. Each of these coefficients must simplify to zero, which implies each of these equations is equal to zero. Note that when the coefficients for $x_i^{D+2}, x_i^{D+1}, \ldots, x_i^3, x_i^2$ are summed together in *one* equation, we have a telescopic sum yielding $\beta_i + M_0 = 0$. Therefore, the equation for x_i becomes

$$\begin{aligned} \beta_i\big(-(\alpha(G)+r)\big) + \beta_i - L_0 &= 0, \\ \beta_i(\alpha(G)+r) - \beta_i &= -L_0, \\ \beta_i &= -\frac{L_0}{\alpha(G)+r-1}, \\ \beta_i &= -L_1. \end{aligned}$$

Thus, we see that coefficient of x_i in A' is equal to $-L_1$. □

Lemma 2.7. *Let G be a graph, and let*

$$1 = A'\left(-(\alpha(G)+r) + \sum_{i=1}^{n} x_i\right) + \sum_{\{i,j\}\in E(G)} Q'_{ij} x_i x_j + \sum_{i=1}^{n} Q'_i(x_i^2 - x_i), \tag{2.6}$$

be a reduced (*via Lemma 2.4*) *Nullstellensatz certificate proving the non-existence of a stable set of size $\alpha(G)+r$ (for $r \geqslant 1$). Let $I = \{c_1, c_2, \ldots, c_{m+1}\}$ be a stable set in G. If the coefficient for $x_{I\setminus c_i}$ in A' is $-L_m$, then the coefficient for x_I in A' is $-L_{m+1}$.*

Proof. Let β_I be the coefficient for x_I in A', denote $x_I^\gamma := x_{c_1}^{\gamma_1} \cdots x_{c_{m+1}}^{\gamma_{m+1}}$ by x_I^γ, set $N = \max\{\deg(Q'_{c_1}), \ldots, \deg(Q'_{c_{m+1}})\}$, and let N_γ be the set of $\{\gamma_1, \ldots, \gamma_{m+1}\}$-tuples such that $\gamma_i \geqslant 0$ and $\sum_{i=1}^{m+1} \gamma_i \leqslant N$. Therefore, let

$$Q'_{c_i} = \sum_{\gamma\in N_\gamma} M_{I^\gamma}^{c_i} x_I^\gamma + \text{other terms in } Q'_{c_i}.$$

Now consider the coefficients for $x_I, x_{I\setminus c_i} x_{c_i}^2$ in the expanded certificate $A'B + C + D$.

- $\mathbf{x_I}$. This monomial is formed in two ways in $A'B$, $x_I\big(-(\alpha(G)+r)\big)$, or $x_{I\setminus c_i} x_{c_i}$ (formed $m+1$ times, once for each c_i), and formed in one way in D, $x_{I\setminus c_i}(-x_{c_i})$ (formed $m+1$ times, once

for each c_i), yielding

$$\beta_I\big(-(\alpha(G)+r)\big) - (m+1)L_m - \underbrace{\sum_{i=1}^{m+1} M_{I\setminus c_i}^{c_i}}_{\mathrm{E}} = 0. \tag{2.7}$$

- $\mathbf{x_{I\setminus c_i} x_{c_i}^2}$. This monomial is formed in one way in $A'B$, $x_I x_{c_i}$, and formed in three ways in D, $x_I(-x_{c_i})$, $x_{I\setminus c_i}x_{c_i}^2$, or $x_{c_i}^2 x_{I\setminus\{c_i\cup c_j\}}(-x_{c_j})$ (formed m times, once for each c_j with $j\neq i$), yielding

$$\beta_I - M_I^{c_i} + M_{I\setminus c_i}^{c_i} - \sum_{\substack{j=1\\ j\neq i}}^{m+1} M_{I\setminus(c_i\cup c_j)}^{c_j} = 0. \tag{2.8}$$

Now we will consider (2.8) for *each individual* c_i, with $i = 1,\ldots,m+1$, and sum those $m+1$ equations. This yields

$$(m+1)\beta_I - \sum_{i=1}^{m+1} M_I^{c_i} + \underbrace{\sum_{i=1}^{m+1} M_{I\setminus c_i}^{c_i}}_{\mathrm{E}} - \sum_{i=1}^{m+1}\sum_{\substack{j=1\\ j\neq i}}^{m+1} M_{I\setminus(c_i\cup c_j)}^{c_j} = 0. \tag{2.9}$$

Notice that part E in (2.9) is equal to part E in (2.7). Now, as in Lemma 2.6, we sum (2.9) with the equations for the coefficients of *every other monomial* x_I^γ in Q'_{c_i}, excluding x_I (and thus (2.7)). As before, every $M_{I^\gamma}^{c_i}$ appears in exactly two equations, once with a positive sign and once with a negative sign, (corresponding to the multiplication $x_{c_i}^2$ and $-x_{c_i}$, respectively). Thus, when (2.9) is summed with the equations corresponding to every other monomial *excluding* x_I, the sum will telescope and every $M_{I^\gamma}^{c_i}$ *excluding part E* will cancel. The negative component for part E is contained in (2.7), which is *not* included in this sum, which is why part E does *not* cancel. Thus, we see

$$(m+1)\beta_I = -\underbrace{\sum_{i=1}^{m+1} M_{I\setminus c_i}^{c_i}}_{\mathrm{E}}. \tag{2.10}$$

Substituting (2.10) into (2.7), we see

$$\begin{aligned}
\beta_I\big(-(\alpha(G)+r)\big) - (m+1)L_m + (m+1)\beta_I &= 0,\\
\beta_I(\alpha(G)+r) - (m+1)\beta_I &= -(m+1)L_m,\\
\beta_I &= -\frac{(m+1)L_m}{\alpha(G)+r-(m+1)},\\
\beta_I &= -L_{m+1}.
\end{aligned}$$

Thus, the coefficient of x_I in A' is equal to $-L_m$. □

Using Lemmas 2.6 and 2.7, we can now prove the main theorem of this section.

Theorem 2.8. *Given a graph G, any Nullstellensatz certificate for the non-existence of a stable set of size greater than $\alpha(G)$ has degree at least $\alpha(G)$.*

Proof. Our proof is by contradiction. Let

$$1 = A\left(-(\alpha(G)+r) + \sum_{i=1}^{n} x_i\right) + \sum_{\{i,j\}\in E(G)} Q_{ij}x_ix_j + \sum_{i=1}^{n} Q_i(x_i^2 - x_i)$$

be any Nullstellensatz certificate for the non-existence of a stable set of size $\alpha(G)+r$, with $r \geqslant 1$, such that $\deg(A), \deg(Q_i), \deg(Q_{ij}) < \alpha(G)$, and let

$$1 = A'\underbrace{\left(-(\alpha(G)+r) + \sum_{i=1}^{n} x_i\right)}_{B} + \underbrace{\sum_{\{i,j\}\in E(G)} Q'_{ij}x_ix_j}_{C} + \underbrace{\sum_{i=1}^{n} Q'_i(x_i^2 - x_i)}_{D} \tag{2.11}$$

be the reduced certificate via Lemma 2.4. The proof of Lemma 2.4 implies $\deg(A') \leqslant \deg(A) < \alpha(G)$. Let $M = \{c_1, c_2, \ldots, c_{\alpha(G)}\}$ be any maximum stable set in G. Via Lemma 2.6, we know that x_{c_1} appears in A' with the non-zero coefficient $-L_1$, which implies (via Lemma 2.7) that $x_{c_1}x_{c_2}$ appears in A' with non-zero coefficient $-L_2$, which implies that $x_{c_1}x_{c_2}x_{c_3}$ appears in A' and so on. In particular, $x_{c_1}x_{c_2}\cdots x_{c_{\alpha(G)}}$ appears in A' with non-zero coefficient $-L_{\alpha(G)}$. This contradicts our assumption that $\deg(A') < \alpha(G)$. Therefore, there can be no Nullstellensatz certificate with $\deg(A) < \alpha(G)$; thus, the degree of *any* Nullstellensatz certificate is at least $\alpha(G)$. □

Lemmas 2.6 and 2.7 also give rise to the following corollary.

Corollary 2.9. *Given a graph G, any Nullstellensatz certificate for the non-existence of a stable set of size greater than $\alpha(G)$ contains at least one monomial for every stable set in G.*

Proof. Given any Nullstellensatz certificate, we create the reduced certificate via Lemma 2.4. The proof of the Lemma 2.4 implies that the number of terms in A is equal to the number of terms in A'. Via Lemmas 2.6 and 2.7, A' contains one monomial for every stable set in G. Therefore, A also contains one monomial for every stable set in G. □

This brings us to the last theorem of this section.

Theorem 2.10. *Given a graph G, a minimum-degree Nullstellensatz certificate for the non-existence of a stable set of size greater than $\alpha(G)$ has degree equal to $\alpha(G)$ and contains at least one term for every stable set in G.*

Proof. This theorem follows directly from Theorems 2.5 and 2.8, and Corollary 2.9. □

Finally, our results establish new lower bounds for the degree and number of terms of Nullstellensatz certificates. In earlier work, researchers in logic and complexity showed both logarithmic and linear growth of degree of the Nullstellensatz over finite fields or for special instances, *e.g.*,

Nullstellensatz related to the pigeonhole principle (see [7], [18] and references therein). Our main complexity result below settles a question of Lovász [27].

Corollary 2.11. *There exist infinite families of graphs G_n, on n vertices, such that the degree of a minimum-degree Nullstellensatz certificate grows linearly in n and, at the same time, the number of terms in the coefficient polynomials of the Nullstellensatz certificate is exponential in n.*

Proof. We give two concrete families that prove the statement. First, the disjoint union of $n/3$ triangles has exactly $4^{n/3} - 1$ stable sets and the minimum degree of the Nullstellensatz certificate is $n/3$. Second, the complements of complete graphs have $\alpha(G) = n$, and the number of stable sets is 2^n. □

It is worth emphasizing that the Nullstellensatz certificates are extremely dense as all square-free monomials representing stable sets appear in them. This represents a serious obstacle for computation and, in this case, shows that the computation of Hilbert's Nullstellensatz is at least as hard as counting all possible stable sets inside a graph, which is known to be $\#P$-complete, even for graphs of low vertex-degree [13].

2.2. The Nullstellensatz and 3-colourability

In this subsection, we investigate the degree growth of Nullstellensatz certificates for the non-3-colourability of graphs, using the polynomial encoding previously introduced in Lemma 2.1.

2.2.1. Minimum-degree Nullstellensatz certificates. Curiously, every non-3-colourable graph that we have investigated thus far has a minimum-degree Nullstellensatz certificate of degree four. We begin by proving that four is indeed a lower bound on the degree of non-3-colourability certificates.

Theorem 2.12. *Every Nullstellensatz certificate for non-3-colourability has degree* at least *four.*

Proof. Our proof is by contradiction. Suppose there exists a Nullstellensatz certificate of degree three or less. Such a certificate has the following form:

$$1 = \sum_{i=1}^{n} P_{\{i\}}(x_i^3 - 1) + \sum_{\{i,j\}\in E} P_{\{ij\}}(x_i^2 + x_i x_j + x_j^2), \tag{2.12}$$

where $P_{\{i\}}$ and $P_{\{ij\}}$ represent general polynomials of degree less than or equal to three. To be precise,

$$P_{\{i\}} = \sum_{s=1}^{n} a_{\{i\}s} x_s^3 + \sum_{s=1}^{n} \sum_{\substack{t=1 \\ t\neq s}}^{n} b_{\{i\}st} x_s^2 x_t + \sum_{s=1}^{n} \sum_{t=s+1}^{n} \sum_{u=t+1}^{n} c_{\{i\}stu} x_s x_t x_u + \sum_{s=1}^{n} \sum_{t=1}^{n} d_{\{i\}st} x_s x_t + \sum_{s=1}^{n} e_{\{i\}s} x_s + f_{\{i\}},$$

and

$$P_{\{ij\}} = \sum_{s=1}^{n} a_{\{ij\}s} x_s^3 + \sum_{s=1}^{n} \sum_{\substack{t=1 \\ t \neq s}}^{n} b_{\{ij\}st} x_s^2 x_t + \sum_{s=1}^{n} \sum_{t=s+1}^{n} \sum_{u=t+1}^{n} c_{\{ij\}stu} x_s x_t x_u + \sum_{s=1}^{n} \sum_{t=1}^{n} d_{\{ij\}st} x_s x_t + \sum_{s=1}^{n} e_{\{ij\}s} x_s + f_{\{ij\}}.$$

Because we work with undirected graphs, note that $a_{\{ij\}s} = a_{\{ji\}s}$, and this fact applies to all coefficients a to f. Note also that when $\{i, j\}$ is not an edge of the graph, $P_{ij} = 0$ and thus $a_{\{ij\}s} = 0$. Again, this fact holds for all coefficients a to f.

When $P_{\{i\}}$ multiplies $(x_i^3 - 1)$, this generates cross-terms of the form $P_{\{i\}} x_i^3$ and $-P_{\{i\}}$. In particular, this generates monomials of degree six or less. Notice that $P_{\{ij\}}(x_i^2 + x_i x_j + x_j^2)$ does *not* generate monomials of degree six, only monomials of degree five or less. We begin the process of deriving a contradiction from (2.12) by considering all monomials of the form $x_s^3 x_i^3$ that appear in the expanded Nullstellensatz certificate. These monomials are formed in only *two* ways: either (1) $x_s^3(x_i^3 - 1)$, or (2) $x_i^3(x_s^3 - 1)$. Therefore, the n^2 equations for $x_s^3 x_i^3$ (denoted as $I.1$ to $I.n^2$) are either $a_{\{i\}i} = 0$ for x_i^6, or $a_{\{s\}i} + a_{\{i\}s} = 0$ for $x_s^3 x_i^3$. Summing these equations, we see

$$0 = \sum_{i=1}^{n} \sum_{s=1}^{n} a_{\{i\}s}. \tag{2.13}$$

Let us now consider monomials of the form $x_s^2 x_t x_i^3$ (with $s \neq t$). These monomials are formed in only *one* way: by multiplying $b_{\{i\}st} x_s^2 x_t$ by x_i^3. Therefore, because the coefficient for $x_s^2 x_t x_i^3$ must simplify to zero in the expanded Nullstellensatz certificate, $b_{\{i\}st} = 0$ for all $b_{\{i\}}$. When we consider monomials of the form $x_s x_t x_u x_i^3$ (with $s < t < u$), we see that $c_{\{i\}stu} = 0$ for all $c_{\{i\}}$, for the same reasons as above.

As we continue toward our contradiction, we now consider monomials of degree three in the expanded Nullstellensatz certificate. In particular, we consider the coefficient for x_s^3. The monomial x_s^3 is generated in three ways: (1) $f_{\{s\}}(x_s^3 - 1)$, (2) $a_{\{i\}s} x_s^3 (x_i^3 - 1)$ (from the vertex polynomials), and (3) $e_{\{st\}s} x_s (x_s^2 + x_s x_t + x_t^2)$ (from the edge polynomials). The n equations for x_s^3 are of the following form:

$$0 = f_{\{s\}} - \sum_{i=1}^{n} a_{\{i\}s} + \sum_{t \in \mathrm{Adj}(s)} e_{\{1s\}1}.$$

Summing these equations, we see

$$0 = \sum_{i=1}^{n} f_{\{i\}} - \left(\sum_{i=1}^{n} \sum_{s=1}^{n} a_{\{i\}s} \right) + \sum_{s=1}^{n} \sum_{t \in \mathrm{Adj}(s)}^{n} e_{\{st\}s}. \tag{2.14}$$

Because the degree-three-or-less Nullstellensatz certificate (2.12) is identically one, the constant terms must sum to one. Therefore, we know $\sum_{i=1}^{n} f_{\{i\}} = -1$. Furthermore, recall that $e_{\{st\}s} = 0$ if the undirected edge $\{s, t\}$ does not exist in the graph. Therefore, applying (2.13) to (2.14), we

have the following equation:

$$1 = \sum_{\substack{s,t=1,\\ s\neq t}}^{n} e_{\{st\}s}. \tag{2.15}$$

To give a preview of our overall proof strategy, the equations to come will ultimately show that the right-hand side of (2.15) also equals zero, which is a contradiction.

Now we will consider the monomial $x_s^2 x_t$ (with $s \neq t$). We recall that $b_{\{i\}st} = 0$ for all $b_{\{i\}}$ (where $b_{\{i\}st}$ is the coefficient for $x_s^2 x_t$ in the ith vertex polynomial). Therefore, we do *not* need to consider $b_{\{i\}st}$ in the equation for the coefficient of monomial $x_s^2 x_t$. In other words, we only need to consider the edge polynomials, which can generate this monomial in two ways: (1) $e_{\{st\}s} x_s \cdot x_s x_t$, and (2) $e_{\{si\}t} x_t \cdot x_s^2$. The $2\binom{n}{2}$ equations for these coefficients are of the following form:

$$0 = e_{\{st\}s} + \sum_{i\in \mathrm{Adj}(s)} e_{\{si\}t}.$$

Summing these equations, we see

$$\sum_{s=1}^{n}\sum_{\substack{t=1,\\ t\neq s}}^{n} e_{\{st\}s} + \underbrace{\left(\sum_{s=1}^{n}\sum_{t\in \mathrm{Adj}(s)} e_{\{st\}t}\right)}_{\text{partial sum A}} + \underbrace{\left(\sum_{s=1}^{n}\sum_{t\in \mathrm{Adj}(s)}\sum_{\substack{u=1,\\ u\neq s,t}}^{n} e_{\{st\}u}\right)}_{\text{partial sum B}} = 0. \tag{2.16}$$

However, recall that $e_{\{st\}u} = 0$ when $\{s,t\}$ does not exist in the graph, and also that $e_{\{st\}t} = e_{\{ts\}t}$. Thus, we can rewrite partial sum A from (2.16) as

$$\sum_{s=1}^{n}\sum_{t\in \mathrm{Adj}(s)} e_{\{st\}t} = \sum_{s=1}^{n}\sum_{\substack{t=1,\\ t\neq s}}^{n} e_{\{st\}t} = \sum_{s=1}^{n}\sum_{\substack{t=1,\\ t\neq s}}^{n} e_{\{ts\}t}.$$

Substituting the above into (2.16) yields

$$2\sum_{\substack{s,t=1,\\ s\neq t}}^{n} e_{\{st\}s} + \underbrace{\left(\sum_{s=1}^{n}\sum_{t\in \mathrm{Adj}(s)}\sum_{\substack{u=1,\\ u\neq s,t}}^{n} e_{\{st\}u}\right)}_{\text{partial sum B}} = 0. \tag{2.17}$$

Finally, we consider the monomial $x_s x_t x_u$ (with $s < t < u$). We have already argued that $c_{\{i\}stu} = 0$ for all $c_{\{i\}}$ (where $c_{\{i\}stu}$ is the coefficient for $x_s x_t x_u$ in the ith vertex polynomial). Therefore, as before, we need only consider the edge polynomials, which can generate this monomial in three ways: (1) $e_{\{st\}u} x_u \cdot x_s x_t$, (2) $e_{\{su\}t} x_t \cdot x_s x_u$, and (3) $e_{\{tu\}s} x_s \cdot x_t x_u$. As before, these coefficients must cancel in the expanded certificate, which yields $\binom{n}{3}$ equations of the following form:

$$0 = e_{\{st\}u} + e_{\{su\}t} + e_{\{tu\}s}.$$

Summing these equations, we see

$$\sum_{s=1}^{n-2}\sum_{t=s+1}^{n-1}\sum_{u=t+1}^{n} \left(e_{\{st\}u} + e_{\{su\}t} + e_{\{tu\}s}\right) = 0. \tag{2.18}$$

Now we come to the critical argument of the proof. We claim that the following equation holds:

$$\left(\sum_{s=1}^{n}\sum_{t\in \mathrm{Adj}(s)}\sum_{\substack{u=1,\\ u\neq s,t}}^{n} e_{\{st\}u}\right) = 2\left(\sum_{s=1}^{n-2}\sum_{t=s+1}^{n-1}\sum_{u=t+1}^{n}\left(e_{\{st\}u}+e_{\{su\}t}+e_{\{tu\}s}\right)\right). \tag{2.19}$$

Notice that the left-hand and right-hand sides of this equation consist only of coefficients $e_{\{st\}u}$ with s,t,u distinct. Consider any such coefficient $e_{\{st\}u}$. Notice that $e_{\{st\}u}$ appears exactly *once* on the right-hand side of the equation. Furthermore, either $e_{\{st\}u}$ appears exactly *twice* on the left-hand side of this equation (because $s \in \mathrm{Adj}(t)$ implies $t \in \mathrm{Adj}(s)$), or $e_{\{st\}u} = 0$ (because the edge $\{s,t\}$ does not exist in the graph). Therefore, (2.19) is proved. Applying this result (and (2.18)) to (2.17) gives us the following:

$$\sum_{\substack{1\leqslant s,t\leqslant n\\ s\neq t}} e_{\{st\}s} = 0. \tag{2.20}$$

But (2.20) contradicts (2.15) ($1 = 0$), thus there can be no certificate of degree less than four. □

It is important to note that when we try to construct certificates of degree four or greater, the equations for the degree-six monomials become considerably more complicated. In this case, the edge polynomials *do* contribute monomials of degree six, which causes the above argument to break.

2.2.2. Cliques, odd-wheels and their Nullstellensatz certificates...

Theorem 2.13. *For K_n with $n \geqslant 4$, a minimum-degree Nullstellensatz certificate for non-3-colourability has degree four.*

Proof. It is easy to see that K_4 is a subgraph of K_5, which is a subgraph of K_6, and so on. If H is a subgraph of G, and H has a minimum-degree non-3-colourability Nullstellensatz certificate of degree k, then G also has a minimum-degree non-3-colourability Nullstellensatz certificate of degree k. Thus, because K_4 has a degree-four Nullstellensatz certificate ((2.1)), K_n with $n \geqslant 4$ also has a degree-four certificate. □

The odd-wheels consist of an odd-cycle rim, with a centre vertex connected to all other vertices. The $(2k+1)$-odd-wheel refers to a rim of length $2k+1$, which implies that the actual graph contains $2k+2$ vertices, and $4k+2$ edges. It is easy to see that the odd-wheels are non-3-colourable. It is natural to ask about the degree of a minimum-degree Nullstellensatz certificate for non-3-colourability.

Theorem 2.14. *The $(2k+1)$-odd-wheel has a minimum-degree Nullstellensatz certificate for non-3-colourability of degree four.*

Proof. Our proof is by induction on k. We will show that for every k, we can construct a certificate of degree four with very particular properties. By Theorem 2.12, any certificate of

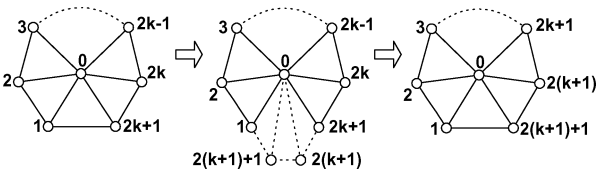

Figure 2. Here we show the evolution of the $(2k+1)$-odd-wheel to the $(2(k+1)+1)$-odd-wheel.

degree four is minimal. Our base case is $k=1$. The 3-odd-wheel is isomorphic to K_4 (the 4-complete graph), and a certificate of degree four was previously displayed in (2.1). Based on that equation, we denote the non-3-colourability certificate for the 3-odd-wheel as follows:

$$1 = \alpha_1 v_1 + \alpha_{\{12\}} e_{\{12\}} + \alpha_{\{23\}} e_{\{23\}} + \widetilde{\alpha} e_{\{13\}} + \alpha_{\{20\}} e_{\{20\}} + \alpha_{\{10\}} e_{\{10\}} + \alpha_{\{30\}} e_{\{30\}},$$

where $v_1 = x_1^3 - 1$, and $e_{\{ij\}} = x_i^2 + x_i x_j + x_j^2$ and $\alpha_1, \alpha_{\{ij\}}$ and $\widetilde{\alpha}$ denote polynomials of degree four in $\mathbb{R}[x_0, x_1, x_2, x_3]$. In particular, via (2.1), we see

$$\widetilde{\alpha} = \frac{2}{9}x_1^4 + \frac{1}{9}x_1^3 x_2 + \frac{1}{9}x_1^3 x_0 + \frac{2}{9}x_1^2 x_2 x_0. \tag{2.21}$$

For our induction hypothesis, we assume that there exists a degree-four certificate for the $(2k+1)$-odd-wheel of the following specific form:

$$1 = \gamma_1 v_1 + \gamma_{\{12\}} e_{\{12\}} + \cdots + \gamma_{\{2k,2k+1\}} e_{\{2k,2k+1\}} + \widetilde{\alpha} e_{\{1,2k+1\}} + \gamma_{\{10\}} e_{\{10\}} + \cdots + \gamma_{\{0,2k+1\}} e_{\{0,2k+1\}}, \tag{2.22}$$

where $\gamma_1, \gamma_{\{ij\}}$ denote polynomials of degree four in $\mathbb{R}[x_0, x_1, \ldots, x_{2k+1}]$. Note in particular that the coefficient for the edge $\{1, 2k+1\}$ in the $(2k+1)$-odd-wheel certificate is exactly the same as the coefficient for the $\{1,3\}$ edge in the 3-odd-wheel certificate: both are equal to $\widetilde{\alpha}$.

Now, we will show that there exists a degree-four certificate for the $\big(2(k+1)+1\big)$-odd-wheel such that the coefficient for the $\{1, 2(k+1)+1\}$ edge is still $\widetilde{\alpha}$. In Figure 2, we can see that the topological difference between the $(2k+1)$-odd-wheel and the $(2(k+1)+1)$-odd-wheel is that the edge $\{1, 2k+1\}$ is lost, and the $2(k+1), 2(k+1)+1$ vertices are gained, along with associated edges

$$\big\{\big(2k+1, 2(k+1)\big), \big(2(k+1), 2(k+1)+1\big), \big(1, 2(k+1)+1\big), \big(0, 2(k+1)\big), \big(0, 2(k+1)+1\big)\big\}.$$

Suppose there exists an algebraic relation or syzygy of the specific form

$$\begin{aligned}\widetilde{\alpha} e_{\{1,2k+1\}} = {} & \widetilde{\alpha} e_{\{1,2(k+1)+1\}} + \beta_{\{2k+1,2(k+1)\}} e_{\{2k+1,2(k+1)\}} \\ & + \beta_{\{2(k+1),2(k+1)+1\}} e_{\{2(k+1),2(k+1)+1\}} + \beta_{\{01\}} e_{\{01\}} + \beta_{\{0,2k+1\}} e_{\{0,2k+1\}} \\ & + \beta_{\{0,2(k+1)\}} e_{\{0,2k+1\}} + \beta_{\{0,2(k+1)+1\}} e_{\{0,2(k+1)+1\}},\end{aligned} \tag{2.23}$$

where $\beta_{\{ij\}} \in \mathbb{R}[x_0, x_1, x_2, x_{2k+1}, x_{2(k+1)}, x_{2(k+1)+1}]$ and $\deg(\beta_{\{ij\}}) = 4$. Note that the coefficients for $e_{\{1,2k+1\}}$ and $e_{\{1,2(k+1)+1\}}$ are the same: both are equal to $\widetilde{\alpha}$. Therefore, in order to construct a degree-four certificate for the $\big(2(k+1)+1\big)$-odd-wheel, we can simply substitute (2.23) for the $\widetilde{\alpha} e_{\{1,2k+1\}}$ term in (2.22). Thus, demonstrating the existence of a syzygy such as (2.23) will conclude our proof.

This special syzygy was indeed found explicitly via computer and it is listed below for the 3-odd-wheel to the 5-odd-wheel. For space considerations we do not list it for general k; however, it can be easily generalized to match the indices of (2.23) via the following variable substitutions: $x_3 \to x_{2k+1}$, $x_4 \to x_{2(k+1)}$, $x_5 \to x_{2(k+1)+1}$. Notice that $\widetilde{\alpha} \in \mathbb{R}[x_0, x_1, x_2]$. Therefore, $\widetilde{\alpha}$ is invariant under this substitution.

$$
\begin{aligned}
0 = &- \underbrace{\left(\frac{2}{9}x_1^4 + \frac{1}{9}x_1^3x_2 + \frac{1}{9}x_1^3x_0 + \frac{2}{9}x_1^2x_2x_0\right)}_{\widetilde{\alpha}} \underbrace{(x_1^2 + x_3x_1 + x_3^2)}_{e_{\{13\}}} \\
&+ \underbrace{\left(\frac{2}{9}x_1^4 + \frac{1}{9}x_1^3x_2 + \frac{1}{9}x_1^3x_0 + \frac{2}{9}x_1^2x_2x_0\right)}_{\widetilde{\alpha}} \underbrace{(x_1^2 + x_5x_1 + x_5^2)}_{e_{\{15\}}} \\
&+ \left(\frac{2}{9}x_1^3x_0 + \frac{1}{9}x_1x_2x_0x_5 - \frac{1}{9}x_1x_2x_4x_5 - \frac{1}{9}x_1x_3x_0^2 - \frac{2}{9}x_1x_3x_0x_4 - \frac{2}{9}x_2x_0^3\right. \\
&\left. - \frac{1}{9}x_2x_0^2x_4 + \frac{1}{9}x_4^4\right) \underbrace{(x_3^2 + x_3x_4 + x_4^2)}_{e_{\{34\}}} \\
&+ \left(-\frac{2}{9}x_1^4 - \frac{2}{9}x_1^2x_2x_0 - \frac{1}{9}x_1^2x_2x_4 + \frac{1}{9}x_1^2x_0x_4 - \frac{1}{9}x_1x_2x_3x_0 + \frac{1}{9}x_1x_2x_3x_4 - \frac{1}{9}x_1x_2x_0^2\right. \\
&\left. + \frac{1}{9}x_1x_2x_4^2 - \frac{2}{9}x_0^4 + \frac{1}{9}x_0^3x_4 - \frac{1}{9}x_4^4 + \frac{1}{9}x_4^3x_5 - \frac{1}{9}x_4x_5^3\right) \underbrace{(x_4^2 + x_4x_5 + x_5^2)}_{e_{\{45\}}} \\
&+ \left(-\frac{1}{3}x_1x_3x_0^2 - \frac{2}{9}x_3x_0x_4^2 - \frac{5}{9}x_1x_3^2x_0 - \frac{1}{3}x_1^2x_3x_0 + \frac{2}{9}x_1^2x_4x_5 + \frac{2}{9}x_0^2x_4x_5 - \frac{1}{9}x_1x_4x_5^2\right. \\
&+ \frac{2}{9}x_3^2x_0x_4 + \frac{2}{9}x_2x_3x_4^2 + \frac{1}{9}x_1^2x_2x_3 - \frac{1}{9}x_1^2x_2x_5 + \frac{2}{9}x_1^3x_3 - \frac{2}{9}x_1^3x_5 + \frac{1}{9}x_1^2x_0x_5 \\
&- \frac{2}{9}x_1^2x_0^2 + \frac{2}{9}x_1^2x_4^2 - \frac{4}{9}x_1x_3^2x_4 - \frac{2}{3}x_1x_3x_0x_4 - \frac{4}{9}x_1x_0x_4x_5 - \frac{5}{9}x_1x_0^2x_4 - \frac{4}{9}x_1x_0x_4^2 \\
&- \frac{1}{9}x_1x_0x_5^2 - \frac{1}{9}x_1x_4^2x_5 - \frac{2}{9}x_1x_0^3 + \frac{2}{9}x_2x_3^2x_0 + \frac{1}{9}x_2x_3^2x_4 - \frac{1}{9}x_2x_3x_5^2 + \frac{2}{9}x_2x_0x_4^2 \\
&+ \frac{1}{3}x_2x_3x_0x_4 - \frac{1}{9}x_2x_3x_0x_5 + \frac{1}{9}x_2x_4^3 - \frac{4}{9}x_3^3x_0 - \frac{1}{3}x_3^4 - \frac{1}{9}x_3^3x_4 \\
&\left. + \frac{2}{9}x_3^2x_4^2 + \frac{2}{9}x_0^2x_5^2 - \frac{1}{9}x_0x_4^3\right) \underbrace{(x_0^2 + x_0x_1 + x_1^2)}_{e_{\{01\}}} \\
&+ \left(\frac{2}{9}x_1^4 + \frac{1}{9}x_1^3x_2 + \frac{4}{9}x_1^3x_0 + \frac{4}{9}x_1^3x_4 - \frac{1}{9}x_1^2x_2x_4 + \frac{1}{3}x_1^2x_3^2 + \frac{1}{9}x_1^2x_3x_0 + \frac{1}{9}x_1^2x_3x_4\right. \\
&+ \frac{5}{9}x_1^2x_0^2 + \frac{5}{9}x_1^2x_0x_4 + \frac{2}{9}x_1^2x_4^2 - \frac{2}{9}x_1x_2x_0^2 - \frac{1}{9}x_1x_2x_0x_4 - \frac{1}{9}x_1x_2x_0x_5 \\
&+ \frac{1}{9}x_1x_2x_4x_5 + \frac{1}{3}x_1x_3^2x_0 + \frac{2}{9}x_1x_3x_0^2 + \frac{1}{3}x_1x_3x_0x_4 + \frac{1}{3}x_3^2x_0^2 \\
&\left. - \frac{1}{9}x_3x_0^3 - \frac{1}{9}x_3x_0^2x_4 - \frac{2}{9}x_3x_0x_4^2 - \frac{2}{9}x_0^4 - \frac{2}{9}x_0^3x_4\right) \underbrace{(x_0^2 + x_0x_3 + x_3^2)}_{e_{\{03\}}}
\end{aligned}
$$

$$
\begin{aligned}
&+\Big(\frac{1}{9}x_1^3x_5-\frac{2}{9}x_1^2x_2x_3+\frac{1}{9}x_1^2x_2x_5-\frac{4}{9}x_1^2x_3^2-\frac{1}{9}x_1x_2x_3x_4+\frac{1}{9}x_1x_2x_0^2-\frac{1}{9}x_1x_2x_4^2\\
&+\frac{1}{9}x_1x_3x_0^2+\frac{2}{9}x_1x_3x_0x_4+\frac{1}{3}x_1x_0^3+\frac{1}{9}x_1x_0^2x_4+\frac{1}{9}x_1x_0^2x_5+\frac{1}{9}x_2x_3x_0x_5\\
&+\frac{1}{9}x_2x_3x_5^2+\frac{2}{9}x_3^3x_0+\frac{1}{9}x_3^2x_0x_4-\frac{1}{9}x_3^2x_4^2+\frac{1}{3}x_3x_0^3\\
&+\frac{1}{9}x_3x_0x_4^2-\frac{1}{9}x_3x_4^3+\frac{2}{9}x_0^4\Big)\underbrace{(x_0^2+x_0x_4+x_4^2)}_{e_{\{04\}}}\\
&+\Big(-\frac{1}{9}x_1^3x_2+\frac{1}{9}x_1^3x_4+\frac{1}{9}x_1^2x_2x_3+\frac{1}{9}x_1^2x_2x_4-\frac{1}{9}x_1^2x_0^2+\frac{2}{9}x_1x_2x_3x_0-\frac{1}{9}x_1x_2x_3x_4\\
&+\frac{1}{9}x_1x_2x_0^2-\frac{1}{9}x_1x_2x_4^2-\frac{1}{9}x_1x_0^3+\frac{1}{9}x_1x_0^2x_4-\frac{1}{9}x_2x_3x_0x_4-\frac{1}{9}x_2x_3x_4^2\\
&-\frac{1}{9}x_0x_4^2x_5-\frac{1}{9}x_0x_4x_5^2+\frac{1}{9}x_4^2x_5^2+\frac{1}{9}x_4x_5^3\Big)\underbrace{(x_0^2+x_0x_5+x_5^2)}_{e_{\{05\}}}.
\end{aligned}
$$

□

Finally, the reader may easily observe that Theorem 1.1(ii) follows directly from Theorem 2.13, Theorem 2.14, and the fact that when H is a subgraph of G, and H has a minimum-degree non-3-colourability Nullstellensatz certificate of degree k, then G also has a minimum-degree non-3-colourability Nullstellensatz certificate of degree k.

2.2.3. Computer generation of Nullstellensatz certificates for non-3-colourable graphs... To deal with various non-3-colourable graphs, we implemented an exact-arithmetic linear system solver for the purpose of finding explicit Nullstellensatz certificates (we had previously observed that the systems of linear equations were numerically unstable in floating-point arithmetic). With our implementation we ran several experiments. The systems of linear equations are also quite large in practice, as the bound on the degree of the polynomial coefficients grows. Thus we need ways to reduce the number of unknowns.

We will not discuss *ad hoc* methods we used to deal with the particular polynomial system at hand (see [29]), but let us at least observe one useful trick for reducing the size of our systems of linear equations. Instead of allowing *all* monomials of degree $\leqslant d$ to appear in the construction of the linear system of equations, we can randomly set unknowns in the linear system of equations to be equal to zero, *e.g.*, set each variable to 0 with probability p, independently, to get a smaller system.

This heuristic worked quite well. In Figure 3 we see the results of a probabilistic search for Nullstellensatz certificates. On the x-axis is the probability p of keeping an unknown in the linear system. Thus, if $p = 0.1$, 90% of the time we set the unknown to 0, and only 10% of the time, we keep it in the system. For the cliques and odd-wheels, we know that there is always a certificate of degree four. For every probability $0.1, 0.2, \ldots, 1$ we performed 100 searches for a degree-four certificate. For the cliques and odd-wheels at $p = 0.1$ and $p = 0.2$, we almost never found certificates. But for $p = 0.4$, we found certificates 95% of the time. In practice, we can reduce the number of variables in the linear system by 60%, and still find a Nullstellensatz certificate 90% of the time.

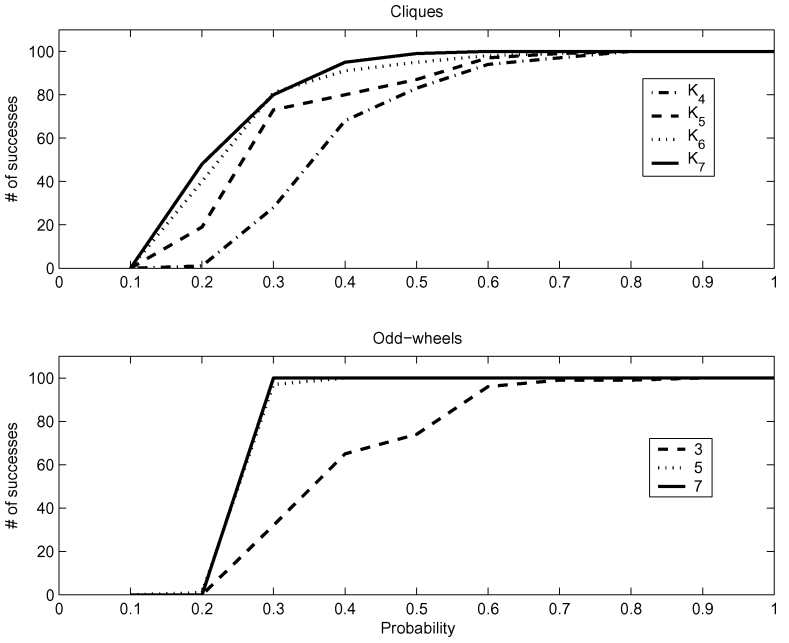

Figure 3. Probability tests on cliques and odd-wheels.

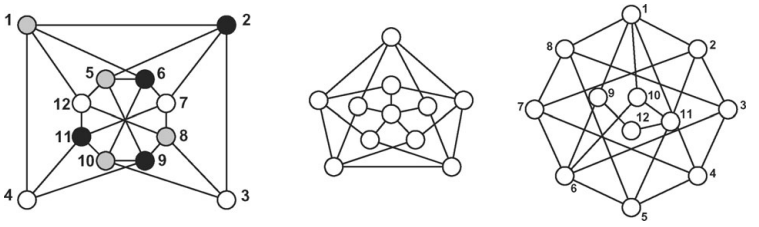

Figure 4. These graphs (from left to right) are (1) a uniquely 3-colourable graph, labelled with its unique 3-colouring [8], (2) the Grötzsch graph, and (3) the Jin graph.

We now report the results of our computational experiments. With the aid of a computer, we searched hundreds of non-3-colourable graphs, hoping to find explicit examples with growth in the certificate degree. Every graph we have investigated so far has a Nullstellensatz certificate of degree four. In contrast to the stable set case, most graphs appear to have low-degree Nullstellensatz proofs of non-3-colourability. For example, in Figure 4, we describe the Jin and Grötzch graphs, and in Figure 5, we describe the 'flower' family. Kneser graphs are described in most graph theory books. In Table 1 we present a sampling of the many graphs we tried during our computational experiments. Note that we often used our probabilistic linear algebra algorithm, selecting $p = 0.4$ as a likely threshold for feasibility.

A *uniquely* 3*-colourable* graph is a graph that can be coloured with three colours in only one way, up to permutation of the colour labels. Figure 4 displays a uniquely 3-colourable triangle-free graph [8]. Because the graph is uniquely 3-colourable, the addition of a single edge between two similarly coloured vertices will result in a new non-3-colourable graph. Table 1 also details

Table 1. Experimental investigations for flowers, Kneser graphs, the Jin graph and the Grötzch graphs. Here G denotes the uniquely colourable graph displayed in Figure 4.

Graph	Vertices	Edges	Row	Col.	p	deg
flower 8	16	32	51819	49516	0.4	4
flower 10	20	40	178571	362705	1	4
flower 11	22	44	278737	278844	0.5	4
flower 13	26	52	629666	495051	0.4	4
flower 14	28	56	923580	705536	0.4	4
flower 16	32	64	1979584	1674379	0.4	4
flower 17	34	68	2719979	2246535	0.4	4
flower 19	38	76	4862753	3850300	0.5	4
Kneser-(6,2)	15	45	39059	68811	0.5	4
Kneser-(7,2)	21	105	230861	558484	0.5	4
Kneser-(8,2)	28	210	1107881	3307971	0.5	4
Kneser-(9,2)	36	378	1107955	3304966	0.5	4
Kneser-(10,2)	45	630	15567791	36785283	0.5	4
Jin graph	12	24	12168	13150	0.4	4
Grötzsch	11	20	7903	8109	0.4	4
$G + \{(3,4)\}$	12	24	12257	13091	0.4	4
$G + \{(7,12)\}$	12	24	12201	13085	0.4	4
$G + \{(1,8)\}$	12	24	12180	13124	0.4	4
$G + \{(3,4),(12,7)\}$	12	25	12286	13804	0.4	4

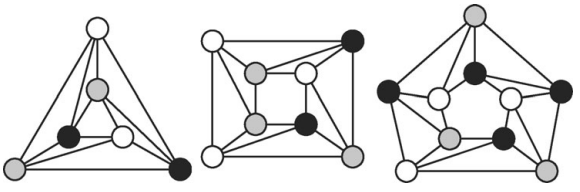

Figure 5. 3-, 4- and 5-flowers (left to right). Note that the 3-flower is 3-colourable, whereas the 4- and 5-flowers are non-3-colourable. It is easy to see that only flowers that are multiples of 3 are 3-colourable.

these experiments. Finally, we investigated all non-3-colourable graphs on six vertices or less: every one has a Nullstellensatz certificate of degree four.

3. Encodings and an applications to graph theory

Finally, we establish encodings for the combinatorial problems stated in Theorem 1.2. At the end of this section we introduce the notion of dual colouring and simultaneous chromatic numbers of graphs.

A comment about our purpose is in order. One can easily find a $0/1$ polynomial encoding for SAT, and thus construct polynomial encodings for all NP-complete problems via polynomial reductions to SAT. However, this approach is not computationally practical for us because of the blow-up in the size of the underlying linear algebra systems. We previously saw that the stable-set encoding using constraints of the form $x_i(x_i - 1)$ led to dense certificate with linear growth in degree, but other type of constraints (*e.g.*, root of unity constraints as in graph-3-colourability)

may behave better in practice with respect to the Nullstellensatz. Because we care about computation, we care about finding encodings that better capture the combinatorial structure with respect to the Nullstellensatz (this is very evident, for example, in planarity questions).

3.1. Proof of Theorem 1.1

Proof of Theorem 1.2(i). Suppose that a cycle C of length L exists in the graph G. We set $y_i = 1$ or 0 depending on whether node i is on C or not. Next, starting the numbering at any node of C, we set $x_i = j$ if node i is the jth node of C. It is easy to check that (1.1) and (1.2) are satisfied.

To verify (1.3), note that because C has length L, if vertex i is the jth node of the cycle, then one of its neighbours, say k, must be the 'follower', namely the $(j+1)$th element of the cycle. If $j < L$, then the factor $(x_i - x_k - 1) = 0$ appears in the product equation associated with the ith vertex, and the product is zero. If $j = L$, then the factor $(x_i - x_k - (L-1)) = 0$ appears, and the product is again 0. Because this is true for all vertices that are turned 'on', and for all vertices that are 'off', we have (1.3) automatically equal to zero, all of the equations of the polynomials vanish.

Conversely, from a solution of the system above, we see that L variables y_i are not zero; call this set C. We claim that the nodes $i \in C$ must form a cycle. Because $y_i \neq 0$, the polynomial of (1.3) must vanish; thus, for some $j \in C$,

$$(x_i - x_j + 1) = 0 \quad \text{or} \quad (x_i - x_j - (L-1)) = 0.$$

Note that (1.3) reduces to this form when $y_i = 1$. Therefore, either vertex i is adjacent to a vertex j (with $y_j = 1$) such that x_j equals the *next integer value* $(x_i + 1 = x_j)$, or $x_i - L = x_j - 1$ (again, with $y_j = 1$). In the second case, because x_i and x_j are integers between 1 and L, this forces $x_i = L$ and $x_j = 1$. By the pigeonhole principle, this implies that all integer values from 1 to L must be assigned to some node in C starting at vertex 1 and ending at L (which is adjacent to the node receiving 1). □

We have the following corollary.

Corollary 3.1. *A graph G has a Hamiltonian cycle if and only if the following zero-dimensional system of n variables and $2n$ equations has a solution. For every node $i \in V(G)$, we have two equations:*

$$\prod_{s=1}^{n}(x_i - s) = 0 \quad \textit{and} \quad \prod_{j \in \mathrm{Adj}(i)} (x_i - x_j + 1)(x_i - x_j - (n-1)) = 0.$$

The number of Hamiltonian cycles in the graph equals the number of solutions of the system divided by $2n$.

Proof. Clearly, when $L = n$ we can just fix all y_i to 1, and thus many of the equations simplify or become obsolete. We only have to check the last statement on the number of Hamiltonian cycles. For that, we remark that no solution appears with multiplicity because the ideal is radical. That the ideal is radical is implied by the fact that every variable appears as the only variable in

a unique square-free polynomial (see p. 246 of [21]). Finally, note that for every cycle there are n ways to choose the initial node to be labelled as 1, and then two possible directions to continue the labelling. □

Note that similar results can be established for the directed graph version; thus one can consider paths or cycles with orientation. Also note that we can use the polynomials systems above to investigate the distribution of cycle lengths in a graph (and similarly for path lengths and cut sizes). This topic has several outstanding questions. For example, a still-unresolved question of Erdős and Gyárfás [38] asks: If G is a graph with minimum degree three, is it true that G always has a cycle having length that is a power of two? Define the *cycle-length polynomial* as the square-free univariate polynomial whose roots are the possible cycle lengths of a graph (the same can be done for cuts). Considering L as a variable, the reduced lexicographic Gröbner basis (with L the last variable) computation provides us with a unique univariate polynomial on L that is divisible by the cycle-length polynomial of G.

Now we proceed to the proof of part (ii) of Theorem 1.2. For this we recall Schnyder's characterization of planarity in terms of the dimension of a poset [36]. For an n-element poset P, a *linear extension* is an order-preserving bijection $\sigma : P \to \{1, 2, \ldots, n\}$. The *poset dimension* of P is the smallest integer t for which there exists a family of t linear extensions $\sigma_1, \ldots, \sigma_t$ of P such that $x < y$ in P if and only if $\sigma_i(x) < \sigma_i(y)$ for all σ_i. The *incidence poset* $P(G)$ of a graph G with node set V and edge set E is the partially ordered set of height two on the union of nodes and edges, where we say $x < y$ if x is a node and y is an edge, and y is incident to x.

Lemma 3.2 (Schnyder's theorem [36]). *A graph G is planar if and only if the poset dimension of $P(G)$ is no more than three.*

Thus our first step is to encode the linear extensions and the poset dimension of a poset P in terms of polynomial equations. The idea is similar to our characterization of cycles via permutations.

Lemma 3.3. *Let $P = (E, >)$ be a poset, and $\mathbb{C}[x_i(k), \Delta_{ij}, s_k]$ be a polynomial ring in $p|E| + (|E|^2 - |E|) + p$ variables (where $i = 1, \ldots, |E|$, $j = 1, \ldots, |E|$, $j \neq i$, and $k = 1, \ldots, p$). Then P has poset dimension at most p if and only if the following system of equations has a solution.*

For $k = 1, \ldots, p$,

$$\prod_{s=1}^{|E|} (x_i(k) - s) = 0, \quad \text{for every } i \in \{1, \ldots, |E|\}, \quad \text{and}$$
$$s_k \left(\prod_{\substack{\{i,j\} \in \{1,\ldots,|E|\}, \\ i<j}} x_i(k) - x_j(k) \right) = 1. \tag{3.1}$$

For $k = 1, \ldots, p$, and every ordered pair of comparable elements $e_i > e_j$ in P,

$$x_i(k) - x_j(k) - \Delta_{ij}(k) = 0. \tag{3.2}$$

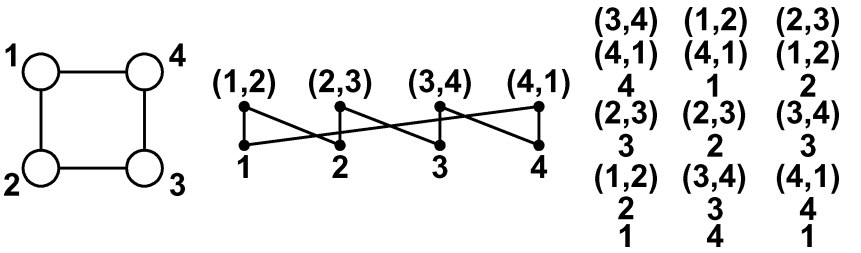

Figure 6. Via Schnyder's theorem, the square is planar because P(square) has dimension at most three.

For every ordered pair of incomparable elements of P (i.e., $e_i \not\succ e_j$ and $e_j \not\succ e_i$),

$$\prod_{k=1}^{p}\big(x_i(k) - x_j(k) - \Delta_{ij}(k)\big) = 0, \quad \prod_{k=1}^{p}\big(x_j(k) - x_i(k) - \Delta_{ji}(k)\big) = 0, \tag{3.3}$$

For $k = 1, \ldots, p$, and for every pair $\{i, j\} \in \{1, \ldots, |E|\}$,

$$\prod_{d=1}^{|E|-1}(\Delta_{ij}(k) - d) = 0, \quad \prod_{d=1}^{|E|-1}(\Delta_{ji}(k) - d) = 0.$$

Proof. With (3.1) and (3.2), we assign distinct numbers 1 to $|E|$ to the poset elements, such that the properties of a linear extension are satisfied. Equations (3.1) and (3.2) are repeated p times, so p linear extensions are created. If the intersection of these extensions is indeed equal to the original poset P, then for every incomparable pair of elements in P at least one of the p linear extensions must detect the incomparability. But this is indeed the case for (3.3), which says that for the lth linear extension the values assigned to the incomparable pair e_i, e_j do not satisfy $x_i(l) < x_j(l)$, but instead satisfy $x_j(l) > x_i(l)$. □

Proof of Theorem 1.2(ii). We simply apply the above lemma to the particular pairs of order relations of the incidence poset of the graph. Note that in the formulation we added variables $z_{\{ij\}}$ that have the effect of turning on or off an edge of the input graph. □

Example 3 (posets and planar graphs). In Figure 6 we give a demonstration of how Schnyder's theorem can be used to show planarity of graphs.

Proof of Theorem 1.2(iii). Using Lemma 2.1, we can finish the proof of part (iii). For a k-colourable subgraph H of size R, we set $y_{ij} = 1$ if edge $\{i, j\} \in E(H)$ or $y_{ij} = 0$ otherwise. By Lemma 2.1, the resulting subsystem of equations has a solution. Conversely, from a solution, the subgraph H in question is read off from those $y_{ij} \neq 0$. Solvability implies that H is k-colourable. □

Before we prove Theorem 1.2(iv), we recall that the *edge-chromatic number* of a graph is the minimum number of colours necessary to colour every edge of a graph such that no two edges of the same colour are incident on the same vertex.

Proof of Theorem 1.2(iv). If the system of equations has a solution, then (1.8) ensures that all variables x_{ij} are assigned Δ roots of unity. Equation (1.9) ensures that no node is incident on two edges of the same colour. Because the graph contains a vertex of degree Δ, the graph cannot have an edge-chromatic number less than Δ, and because the graph is edge-Δ-colourable, this implies that the graph has edge-chromatic number exactly Δ. Conversely, if the graph has an edge-Δ-colouring, simply map the colouring to the Δ roots of unity and all equations are satisfied. Because Vizing's classic result shows that any graph with maximum vertex degree Δ can be edge-coloured with at most $\Delta + 1$ colours, if there is no solution, then the graph must have an edge-chromatic number of $\Delta + 1$. □

3.2. Normal forms and dual colourings

In [2] Alon and Tarsi show another polynomial encoding of k-colourability. Here we consider one curious consequence of the polynomial method for graph colourings when we use an algebraic encoding similar to that of [2]. By taking a closer look at the *normal form* of the polynomials involved, we can derive a notion of *dual colouring*, which has the nice property that a graph is dually d-colourable if and only if it is d-colourable. This gives rise to an appealing new graph invariant: the *simultaneous chromatic number* $\sigma(G)$, defined to be the smallest d such that G has a d-labelling that is simultaneously a colouring and a dual colouring.

Fix a graph $G = (V, E)$ with $V := \{1, \ldots, n\}$ and $E \subseteq \binom{V}{2}$, fix a positive integer d, and let $D := \{0, 1 \ldots, d-1\}$. Let $\alpha := \exp(\frac{2\pi i}{d}) \in \mathbb{C}$ be the primitive complex dth root of unity, so that $\alpha^0, \ldots, \alpha^{d-1}$ are distinct and $\alpha^d = 1$. For a d-labelling $c : V \longrightarrow D$ of the vertices of G, let

$$\epsilon(c) := \prod\{(\alpha^{c(i)} - \alpha^{c(j)}) : i < j,\ \{i, j\} \in E\}.$$

Clearly, c is a proper d-colouring of G if and only if $\epsilon(c) \neq 0$.

With every orientation $O = (V, A)$ of G (where A denotes the set of 'arrows' or directed edges) associate a sign, $\text{sign}^O = \pm 1$, defined by the parity of the number $|\{(i, j) \in A : i > j\}|$ of flips of O from the standard orientation (where every directed edge (i, j) has $i < j$), and an out-degree vector $\delta^O := (\delta_1^O, \ldots, \delta_n^O)$ with δ_i^O the out-degree of vertex i in O. For a non-negative integer k let $[k] \in D$ be the representative of k modulo d, and for a vector $\delta = (\delta_1, \ldots, \delta_n) \in V^n$ let $[\delta] = ([\delta_1], \ldots, [\delta_n]) \in D^V$. For a labelling $c^* : V \longrightarrow D$ of the vertices of G, let

$$\epsilon^*(c^*) := \sum\{\text{sign}^O : O \text{ orientation of } G \text{ with } [\delta^O] = c^*\}.$$

Call c^* a *dual d-colouring* of G if $\epsilon^*(c^*) \neq 0$.

Theorem 3.4. *A graph has a d-colouring, namely $c \in D^V$ with $\epsilon(c) \neq 0$ (so it is d-colourable) if and only if it has a dual d-colouring, namely $c^* \in D^V$ with $\epsilon^*(c^*) \neq 0$ (so it is dually d-colourable).*

Proof. Let G be a graph on n vertices. Consider the following radical zero-dimensional ideal I in $\mathbb{C}[x_1, \ldots, x_n]$ and its variety variety(I) in $\mathbb{C}^n$:

$$I := \langle x_1^d - 1, \ldots, x_n^d - 1 \rangle, \quad \text{variety}(I) := \{\alpha^c := (\alpha^{c(1)}, \ldots, \alpha^{c(n)}) \in \mathbb{C}^n : c \in D^V\}.$$

It is easy to see that the set $\{x_1^d - 1, \ldots, x_n^d - 1\}$ is a universal Gröbner basis (see [3] and references therein). Thus, the (congruence classes of) monomials x^{c^*}, $c^* \in D^V$ (where

$x^{c^*} := \prod_{i=1}^{n} x_i^{c^*(i)}$), which are those monomials not divisible by any x_i^d, form a vector space basis for the quotient $\mathbb{C}[x_1, \ldots, x_n]/I$. Therefore, every polynomial $f = \sum a_\delta \cdot x^\delta$ has a unique *normal form* $[f]$ with respect to this basis, namely the polynomial that lies in the vector space spanned by the monomials x^{c^*}, $c^* \in D^V$, and satisfies $f - [f] \in I$. It is not very hard to show that this normal form is given by $[f] = \sum a_\delta \cdot x^{[\delta]}$.

Now consider the *graph polynomial* of G,

$$f_G := \prod \{(x_i - x_j) : i < j,\ \{i, j\} \in E\}.$$

The labelling $c \in D^V$ is a d-colouring of G if and only if $\epsilon(c) = f_G(\alpha^c) \neq 0$. Thus, G is not d-colourable if and only if f_G vanishes on every $\alpha^c \in \text{variety}(I)$, which holds if and only if $f \in I$, because I is radical. It follows that G is d-colourable if and only if the representative of f_G is not zero. Because $f_G = \sum \text{sign}^O \cdot x^{\delta^O}$, with the sum extending over the $2^{|E|}$ orientations O of G, we obtain

$$[f_G] = \sum \text{sign}^O \cdot x^{[\delta^O]} = \sum_{c^* \in D^V} \epsilon^*(c^*) \cdot x^{c^*}.$$

Therefore $[f_G] \neq 0$ and G is d-colourable if and only if there is a $c^* \in D^V$ with $\epsilon^*(c^*) \neq 0$. □

Example 4. Consider the graph $G = (V, E)$, $V = \{1, 2, 3, 4\}$ and $E = \{12, 13, 23, 24, 34\}$, and let $d = 3$. The normal form of the graph polynomial can be shown to be

$$\begin{aligned}[f_G] = {} & x_1^2x_2^2x_3 - x_1^2x_2^2x_4 + x_1^2x_2x_4^2 - x_1^2x_2x_3^2 + x_1^2x_3^2x_4 - x_1^2x_3x_4^2 \\ & + x_1x_2 - x_1x_2x_3^2x_4 + x_1x_3^2x_4^2 - x_1x_3 + x_1x_2^2x_3x_4 \\ & - x_1x_2^2x_4^2 + x_3^2 - x_3x_4 + x_2^2x_3x_4^2 - x_2^2 + x_2x_4 - x_2x_3^2x_4^2.\end{aligned}$$

Note that, in general, the number of monomials appearing in the expansion of f_G can be as much as the number of orientations $2^{|E|}$; but usually it will be smaller due to cancellations that occur. Moreover, there will usually be further cancellations when moving to the normal form, so typically $[f_G]$ will have fewer monomials. In our example, out of the $2^{|E|} = 2^5 = 32$ monomials corresponding to the orientations, in the expansion of f_G only 20 appear, and in the normal form $[f_G]$ only 18 appear due to the additional cancellation,

$$-[x_1x_3^3x_4] + [x_1x_2^3x_4] = -x_1x_4 + x_1x_4 = 0.$$

Note that the graph G in this example has only six 3-colourings (which are in fact the same up to relabelling of the colours), but as many as 18 dual 3-colourings c^* corresponding to monomials x^{c^*} appearing in $[f_G]$. For instance, consider the labelling $c^*(1) = c^*(2) = c^*(4) = 0$, $c^*(3) = 2$: the only orientation O that satisfies $[\delta_j^O] = c^*(j)$ for all j is one with edges oriented as $21, 23, 24, 31, 34$, having $\text{sign}^O = 1$ and out-degrees $\delta_1^O = \delta_4^O = 0$, $\delta_3^O = 2$ and $\delta_2^O = 3$, contributing to $[f_G]$ the non-zero term $\epsilon^*(c^*) \cdot \prod_{j=1}^{4} x_j^{c^*(j)} = 1 \cdot x_1^0x_2^0x_3^2x_4^0 = x_3^2$. Thus, c^* is a dual 3-colouring (but, because $c^*(1) = c^*(2)$, it is neither a usual 3-colouring nor a *simultaneous* 3-*colouring*; see below).

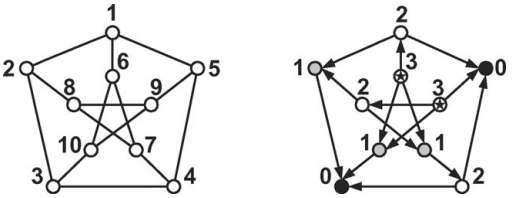

Figure 7. Left: a vertex labelling. Right: an acyclic orientation labelled with out-degrees.

Note that in this example, and seemingly often, there are many more dual colourings than colourings; this suggests a randomized heuristic to find a dual d-colouring for verifying d-colourability.

A particularly appealing notion that arises is the following: call a vertex labelling $s : V \longrightarrow D$ a *simultaneous d-colouring* of a graph G if it is simultaneously a d-colouring and a dual d-colouring of G. The *simultaneous chromatic number* $\sigma(G)$ is then the minimum d such that G has a simultaneous d-colouring. This is a strong notion that may prove useful for inductive arguments, perhaps in the study of the 4-colour problem of planar graphs, and which provides an upper bound on the usual chromatic number $\chi(G)$. First note that, like the usual chromatic number, it can be bounded in terms of the maximum degree $\Delta(G)$ as follows.

Theorem 3.5. *The simultaneous chromatic number of any graph G satisfies $\sigma(G) \leqslant \Delta(G) + 1$. Moreover, for any G and $d \geqslant \Delta(G) + 1$, there is an acyclic orientation O whose out-degree vector $\delta^O = (\delta_1^O, \ldots, \delta_n^O)$ provides a simultaneous d-colouring s defined by $s(i) := \delta_i^O$ for every vertex i.*

Proof. We prove the second (stronger) claim, by induction on the number n of vertices. For $n = 1$, this is trivially true. Suppose $n > 1$, and let $d := \Delta(G) + 1$. Pick any vertex i of maximum degree $\Delta(G)$, and let G' be the graph obtained from G by removing vertex i and all edges incident on i. Let O' be an acyclic orientation of G' and s' the corresponding simultaneous d-colouring of G' guaranteed to exist by induction. Extend O' to an orientation O of G by orienting all edges incident on i away from i, and extend s to the corresponding vertex labelling of G by setting $s(i) := \delta_i^O = d - 1$. Then O is acyclic, and therefore O is the unique orientation of G with out-degree vector δ^O. Thus,

$$\epsilon^*(s) = \sum \{\text{sign}^\theta : \theta \text{ orientation of } G \text{ with } [\delta^\theta] = s = \delta^O\} = \pm 1 \neq 0,$$

and therefore s is a dual d-colouring of G. Moreover, if j is any neighbour of i in G, then the degree of j in G' is at most $d - 2$, and therefore its label $s'(j) = \delta^{O'}(j) \leqslant d - 2$, and hence $s(j) = s'(j) \neq d - 1 = s(i)$. Therefore, s is also a d-colouring of G, completing the induction. □

Example 5 (simultaneous 4-colouring of the Petersen graph). According to Figure 7, $\delta^O = (2, 1, 0, 2, 0, 3, 1, 2, 3, 1)$. By inspection of Figure 7, $s(i) := \delta_i^O$ does indeed describe a valid 4-colouring of the Petersen graph.

There are many new combinatorial and computational problems related to this new graph invariant, which behaves quite differently from the usual chromatic number. For instance, the direct analogue of Brooks' theorem (every connected graph with maximum degree Δ that is neither complete nor an odd cycle is Δ-colourable) fails. It is not hard to verify that the simultaneous chromatic number of the cycle C_n is 2 if and only if n is a multiple of 4; thus, the hexagon satisfies $\sigma(C_6) = 3 > \Delta(C_6)$. Which are the simultaneous chromatic Brooks graphs, *i.e.*, those with $\sigma(G) = \Delta(G)$? What is the complexity of deciding if a graph is simultaneously d-colourable? Which graphs are simultaneously d-colourable for small d? For $d = 2$, the complete answer was given by L. Lovász [28] during a discussion at the Oberwolfach Mathematical Institute, as follows.

Theorem 3.6 (Lovász). *A connected bipartite graph $G = (A, B, E)$ has simultaneous chromatic number $\sigma(G) = 2$ if and only if at least one of $|A|$ and $|B|$ has the same parity as $|E|$.*

Acknowledgements

The authors are grateful to the anonymous referees, whose suggestions greatly improved the presentation of our paper. We would also like to thank Monique Laurent, Peter Malkin, Pablo Parrilo, Bernd Sturmfels, Frank Vallentin, Robert Weismantel, and Alexander Woo for their helpful comments and support.

References

[1] Alon, N. (1999) Combinatorial Nullstellensatz. *Combin. Probab. Comput.* **8** 7–29.
[2] Alon, N. and Tarsi, M. (1992) Colorings and orientations of graphs. *Combinatorica* **12** 125–134.
[3] Babson, E., Onn, S. and Thomas, R. R. (2003) The Hilbert zonotope and a polynomial time algorithm for universal Gröbner bases. *Adv. Appl. Math.* **30** 529–544.
[4] Bachoc, C. and Vallentin, F. (2008) New upper bounds for kissing numbers from semidefinite programming. *J. Amer. Math. Soc.* **21** 909–924.
[5] Bayer, D. A. (1982) The division algorithm and the Hilbert scheme. PhD thesis, Harvard University.
[6] Brownawell, W. D. (1987) Bounds for the degrees in the Nullstellensatz. *Ann. of Math.* **126** 577–591.
[7] Buss, S. and Pitassi, T. (1996) Good degree bounds on Nullstellensatz refutations of the induction principle. In *IEEE Conference on Computational Complexity*, pp. 233–242.
[8] Chao, C.-Y. and Chen, Z. (1993) On uniquely 3-colorable graphs. *Discrete Math.* **112** 374–383.
[9] Cox, D., Little, J. and O'Shea, D. (1992) *Ideals, Varieties and Algorithms*, Springer Undergraduate Texts in Mathematics.
[10] Cox, D., Little, J. and O'Shea, D. (1998) *Using Algebraic Geometry*, Springer Graduate Texts in Mathematics.
[11] De Loera, J. A. (1995) Gröbner bases and graph colorings. *Beitrage zur Algebra und Geometrie* **36** 89–96.
[12] de Klerk, E., Pasechnik, D. and Schrijver, A. (2007) Reduction of symmetric semidefinite programs using the regular $*$-representation. *Math. Programm. Ser. B* **109** 613–624.
[13] Dyer, M. and Greenhill, C. (2000) On Markov chains for independent sets. *J. Algorithms* **35** 17–49.
[14] Eliahou, S. (1992) An algebraic criterion for a graph to be four-colourable. In *Aportaciones Matemáticas*, Vol. 6 of *Soc. Matemática Mexicana, Notas de Investigacion*, pp. 3–27.
[15] Fischer, K. G. (1988) Symmetric polynomials and Hall's theorem. *Discrete Math.* **69** 225–234.
[16] Garey, M. and Johnson, D. (1979) *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman.

[17] Hillar, C. J. and Windfeldt, T. (2008) An algebraic characterization of uniquely vertex colorable graphs. *J. Combin. Theory Ser. B* **98** 400–414.
[18] Impagliazzo, P., Pudlák, P. and Sgall, J. (1999) Lower bounds for polynomial calculus and the Groebner basis algorithm. *Comput. Complexity* **8** 127–144.
[19] Jin, G. (1995) Triangle-free four-chromatic graphs. *Discrete Math.* **145** 151–170.
[20] Kollár, J. (1988) Sharp effective Nullstellensatz. *J. Amer. Math. Soc.* **1** 963–975.
[21] Kreuzer, M. and Robbiano, L. (2000) *Computational Commutative Algebra I*, Springer, Heidelberg.
[22] Lasserre, J. B. (2001) Polynomials nonnegative on a grid and discrete optimization. *Trans. Amer. Math. Soc.* **354** 631–649.
[23] Laurent, M. (2007) Semidefinite representations for finite varieties. *Math. Programm.* **109** 1–26.
[24] Laurent, M. and Rendl, F. (2005) Semidefinite programming and integer programming. In *Handbook on Discrete Optimization* (K. Aardal, G. Nemhauser and R. Weismantel, eds), Elsevier, pp. 393–514.
[25] Lazard, D. (1977) Algèbre linéaire sur $\mathbb{K}[X_1, \ldots, X_n]$ et élimination. *Bull. Soc. Math. France* **105** 165–190.
[26] Li, S. R. and Li, W. W. (1981) Independence number of graphs and generators of ideals. *Combinatorica* **1** 55–61.
[27] Lovász, L. (1994) Stable sets and polynomials. *Discrete Math.* **124** 137–153.
[28] Lovász, L. (2002) *Oberwolfach Meeting on Geometric Convex Combinatorics*, Mathematisches Forschungsinstitut Oberwolfach, Germany, June 2002.
[29] Margulies, S. (2008) Computer algebra, combinatorics, and complexity: Hilbert's Nullstellensatz and NP-complete problems. PhD dissertation, UC Davis.
[30] Matiyasevich, Y. (1974) A criteria for colorability of vertices stated in terms of edge orientations (in Russian). *Discrete Analysis* (Novosibirsk) **26** 65–71.
[31] Matiyasevich, Y. (2001) Some algebraic methods for calculation of the number of colorings of a graph (in Russian). *Zapiski Nauchnykh Seminarov POMI* **293** 193–205 (available via `www.pdmi.ras.ru`).
[32] Mnuk, M. (2001) Representing graph properties by polynomial ideals. In *Computer Algebra in Scientific Computing CASC 2001: Proc. Fourth International Workshop on Computer Algebra in Scientific Computing, Konstanz 2001* (V. G. Ganzha, E. W. Mayr and E. V. Vorozhtsov, eds), Springer, pp. 431–444.
[33] Onn, S. (2004) Nowhere-zero flow polynomials. *J. Combin. Theory Ser. A* **108** 205–215.
[34] Parrilo, P. (2002) An explicit construction of distinguished representations of polynomials nonnegative over finite sets. IfA Technical Report AUT02-02.
[35] Parrilo, P. (2003) Semidefinite programming relaxations for semialgebraic problems. *Math. Programm. Ser. B* **96** 293–320.
[36] Schnyder, W. (1989) Planar graphs and poset dimension, *Order* **5** 323–343.
[37] Schrijver, A. (1986) *Theory of Linear and Integer Programming*, Wiley InterScience Series in Discrete Mathematics and Optimization, Wiley, Chichester.
[38] Shauger, S. E. (1998) Results on the Erdős–Gyárfás conjecture in $K_{1,m}$-free graphs. In *Proc. Twenty-ninth Southeastern International Conference on Combinatorics Graph Theory and Computing* (Boca Raton, FL, 1998). *Congr. Numer.* **134** 61–65.
[39] Simis, A., Vasconcelos, W. and Villarreal, R. (1994) On the ideal theory of graphs. *J. Algebra* **167** 389–416.
[40] Yannakakis, M. (1991) Expressing combinatorial optimization problems by linear programs. *J. Comput. Syst. Sci.* **43** 441–466.