Journal of Symbolic Computation 107 (2021) 67–105

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Towards a computational proof of Vizing's conjecture using semidefinite programming and sums-of-squares ☆, ☆☆

Elisabeth Gaar [a], Daniel Krenn [b], Susan Margulies [c], Angelika Wiegele [a]

[a] Alpen-Adria-Universität Klagenfurt, Universitätsstraße 65-67, 9020 Klagenfurt, Austria
[b] Paris Lodron University of Salzburg, Hellbrunnerstraße 34, 5020 Salzburg, Austria
[c] United States Naval Academy, Annapolis, MD, USA

ARTICLE INFO

Article history:
Received 17 December 2019
Accepted 15 January 2021
Available online 1 February 2021

Keywords:
Vizing's conjecture
Algebraic model
Gröbner basis
Sum-of-squares problems
Semidefinite programming

ABSTRACT

Vizing's conjecture (open since 1968) relates the product of the domination numbers of two graphs to the domination number of their Cartesian product graph. In this paper, we formulate Vizing's conjecture as a Positivstellensatz existence question. In particular, we select classes of graphs according to their number of vertices and their domination number and encode the conjecture as an ideal/polynomial pair such that the polynomial is non-negative on the variety associated with the ideal if and only if the conjecture is true for this graph class. Using semidefinite programming we obtain numeric sum-of-squares certificates, which we then manage to transform into symbolic certificates confirming non-negativity of our polynomials. Specifically, we obtain exact low-degree sparse sum-of-squares certificates for particular classes of graphs.
The obtained certificates allow generalizations for larger graph classes. Besides computational verification of these more general

☆ An extended abstract containing the ideas of this optimization-based approach for tackling Vizing's conjecture appeared as Gaar et al. (2019). This article now also contains the full and complete proofs, new certificates only conjectured in the extended abstract, and further theoretical and computational results for particular cases. This also lead to a restructuring of the whole article, and more examples and many more remarks explaining the implications of the results are provided.

☆☆ The authors gratefully acknowledge the support of Fulbright Austria (via a Visiting Professorship at Alpen-Adria-Universität Klagenfurt). This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 764759, the Austrian Science Fund (FWF): I3199-N31 and the Austrian Science Fund (FWF): P28466-N35.

E-mail addresses: elisabeth.gaar@aau.at (E. Gaar), math@danielkrenn.at (D. Krenn), margulie@usna.edu (S. Margulies), angelika.wiegele@aau.at (A. Wiegele).

https://doi.org/10.1016/j.jsc.2021.01.003

certificates, we also present theoretical proofs as well as conjectures and questions for further investigations.

1. Introduction

Sum-of-squares and its relationship to semidefinite programming is a cutting-edge tool at the forefront of polynomial optimization (Blekherman et al., 2013). Activity in this area has exploded over the past two decades to span areas as diverse as real and convex algebraic geometry (Laurent, 2008), control theory (Jarvis-Wloszek et al., 2005), proof complexity (Grigoriev and Vorobjov, 2001), theoretical computer science (Barak et al., 2016) and even quantum computation (Barak et al., 2017). Systems of polynomial equations and other non-linear models are similarly widely known for their compact and elegant representations of combinatorial problems. Prior work on polynomial encodings includes colorings (Alon and Tarsi, 1992; Hillar and Windfeldt, 2008), stable sets (De Loera et al., 2009; Lovász, 1994), matchings (Fischer, 1988), and flows (Onn, 2004). In this project, we combine the modeling strength of systems of polynomial equations with the computational power of semidefinite programming and devise an optimization-based framework for a computational proof of an old, open problem in graph theory, namely Vizing's conjecture.

Vizing's conjecture was first proposed in 1968, and relates the sizes of minimum dominating sets in graphs G and H to the size of a minimum dominating set in the Cartesian product graph $G\Box H$; a precise formulation follows as Conjecture 2.1. Prior algebraic work on this conjecture (Margulies and Hicks, 2012) expressed the problem as the union of a certain set of varieties and thus the intersection of a certain set of ideals. However, algebraic computational results have remained largely untouched. In this project, we present an algebraic model of Vizing's conjecture that equates the validity of the conjecture to the existence of a Positivstellensatz, or a sum-of-squares certificate of non-negativity modulo a carefully constructed ideal.

By exploiting the relationship between the Positivstellensatz and semidefinite programming, we are able to produce sum-of-squares certificates for certain classes of graphs where Vizing's conjecture holds. Thus, not only are we demonstrating an optimization-based approach towards a computational proof of Vizing's conjecture, but we are presenting actual minimum degree non-negativity certificates that are algebraic proofs of instances of this combinatorial problem. Although the underlying graphs do not further what is known about Vizing's conjecture at this time (indeed the combinatorics of the underlying graphs is fairly easy), such a construction of "combinatorial" Positivstellensätze is successfully executed for the first time here. The construction process is an elegant combination of computation, guesswork, computer algebra and proofs relying on clever definitions of certain polynomials as well as tricky manipulations.

Our paper is structured as follows. In Section 2, we present the necessary background and definitions from graph theory and commutative algebra. In Section 3, we begin the heart of the paper: we describe the ideal/polynomial pair that models Vizing's conjecture as a sum-of-squares problem. This pair is parametrized by the sizes $n_{\mathcal{G}}$ and $n_{\mathcal{H}}$ of the graphs G and H respectively, and on the sizes $k_{\mathcal{G}}$ and $k_{\mathcal{H}}$ of a minimum dominating set in these graphs. In Section 4, we describe our precise process for finding the sum-of-squares certificates along with an example. In Sections 5 and 6, we present our computational results and the Positivstellensätze, i.e., the theorems that arise for various generalizations. In particular, in Section 5, we introduce certain symmetric polynomials that not only allow for a compact notation, but also are vital in proving correctness of the certificates. With the help of the developed calculus, we investigate the graph classes where $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d$ and present certificates for $d \in \{0, \ldots, 4\}$ (all other parameters arbitrary). We provide formal proofs for $d \leq 2$ and computational proofs using SageMath The SageMath Developers (2019) for $d \leq 4$. Moreover, for fixed integer d, we explain an algorithm for computing a certificate or proving that there is none of the conjectured form. Then, in Section 6, the case $k_{\mathcal{G}} = n_{\mathcal{G}} - 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1$ is considered. For this class, we obtain certificates for $n_{\mathcal{H}} \in \{2, 3\}$ ($n_{\mathcal{G}}$ arbitrary) and prove their correctness. Finally, in

Section 7, we summarize our project, state some concluding remarks and present our ideas for future work. For the sake of completeness, an appendix provides certificates (along with proofs) that arose during the application of our method but were dismissed after we obtained certificates with simpler forms.

The code accompanying this article can be found at https://gitlab.com/dakrenn/vizing-sdp-sos.[1]

2. Backgrounds and definitions

In this section, we recall all necessary definitions from graph theory, polynomial ideals and commutative algebra.

2.1. Definitions from graph theory

Given a graph G with vertex set $V(G)$, a set $D \subseteq V(G)$ is a *dominating set in* G if for each $v \in V(G) \setminus D$, there is a $u \in D$ such that v is adjacent to u (i.e., there is an edge between u and v) in G. A dominating set is called *minimum* if there is no dominating set of smaller size (i.e., cardinality). The *domination number of* G, denoted by $\gamma(G)$, is the size of a minimum dominating set in G. The decision problem of determining whether a given graph has a dominating set of size k is NP-complete (Garey and Johnson, 1979).

Given graphs G and H with edge sets $E(G)$ and $E(H)$ respectively, the Cartesian product graph $G \square H$ has vertex set[2] $V(G) \times V(H)$ and edge set

$$E(G \square H) = \big\{ \{gh, g'h'\} : g = g' \text{ and } \{h, h'\} \in E(H), \text{ or } h = h' \text{ and } \{g, g'\} \in E(G) \big\}.$$

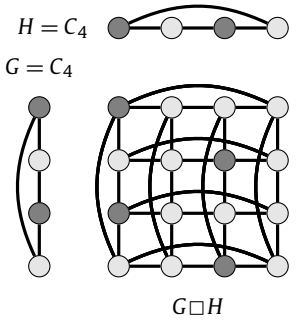
In 1968, Vadim G. Vizing conjectured the following beautiful relationship between domination numbers and Cartesian product graphs:

Conjecture 2.1 *(Vizing (1968)). Given graphs G and H, then the inequality*

$$\gamma(G)\,\gamma(H) \leq \gamma(G \square H)$$

holds.

Example 2.2. In this example, we demonstrate the Cartesian product graph of two C_4 cycle graphs:



[1] The code at https://gitlab.com/dakrenn/vizing-sdp-sos is meant to be used with the open source mathematics software Sagemath The SageMath Developers (2019) and the solver MOSEK MOSEK ApS (2017) within MATLAB.

[2] It will be convenient to use the short notation $gh = (g, h)$ for an element of the vertex set $V(G) \times V(H)$ of the Cartesian product graph $G \square H$.

In these graphs, ● represents a vertex in a minimum dominating set, and Vizing's conjecture holds with equality: $\gamma(G)\gamma(H) = 2 \cdot 2 = 4 = \gamma(G \square H)$. However, observe that some copies of G in $G \square H$ do not contain any vertices of the dominating set, i.e., they are dominated entirely by vertices in other "layers" of the graph. This example highlights the difficulty of Vizing's conjecture. ○

2.2. Historical notes

Vizing's conjecture is an active area of research spanning over fifty years. Early results have focused on proving the conjecture for certain classes of graphs. For example, in 1979, Barcalkin and German (1979) proved that Vizing's conjecture holds for graphs satisfying a certain "partitioning condition" on the vertex set. The idea of a "partitioning condition" inspired work for the next several decades, as Vizing's conjecture was shown to hold on paths, trees, cycles, chordal graphs, graphs satisfying certain coloring properties, and graphs with $\gamma(G) \leq 2$. These results are clearly outlined in the 1998 survey paper by Hartnell and Rall (1998). In 2004, Sun (2004) showed that Vizing's conjecture holds on graphs with $\gamma(G) \leq 3$. There are also results proving a weaker version of the conjecture, for example, the recent result of Zerbib (2019) showing that $\gamma(G)\gamma(H) + \max\{\gamma(G), \gamma(H)\} \leq 2\gamma(G \square H)$. The 2009 survey paper (Brešar et al., 2012) summarizes the work from 1968 to 2008, contains new results, new proofs of existing results, and comments about minimal counter-examples.

2.3. Definitions around polynomial ideals and sum-of-squares

Our goal is to model Vizing's conjecture as a semidefinite program. In particular, we will create an ideal/polynomial pair such that the polynomial is non-negative on the variety associated with the ideal if and only if Vizing's conjecture is true.

In this subsection, we present a brief introduction to polynomial ideals, and the relationship between non-negativity and sum-of-squares. This material is necessary for understanding our polynomial ideal model of Vizing's conjecture. For a more thorough introduction to this material see Blekherman et al. (2013) and Cox et al. (2007).

Throughout this section, let I be an ideal in a polynomial ring $P = \mathbb{K}[z_1, \ldots, z_n]$ over a field $\mathbb{K} \subseteq \mathbb{R}$. The *variety of the ideal* I is defined as the set

$$\mathcal{V}(I) = \{z^* \in \overline{\mathbb{K}}^n : \ f(z^*) = 0 \text{ for all } f \in I\}$$

with $\overline{\mathbb{K}}$ being the algebraic closure of $\mathbb{K}$. The variety $\mathcal{V}(I)$ is called *real* if $\mathcal{V}(I) \subseteq \mathbb{R}^n$.

We say that the ideal I is *radical* if whenever $f^m \in I$ for some polynomial $f \in P$ and integer $m \geq 1$, then $f \in I$. It should be mentioned that radical ideals and varieties are closely connected.[3]

The concrete ideals that we are using later on are all radical. This is a consequence of the following lemma.

Lemma 2.3. *(Kreuzer and Robbiano, 2000, Section 3.7.B, pg. 246) Let I be an ideal with finite variety $\mathcal{V}(I)$. If the ideal I contains a univariate square-free polynomial in each variable, then I is radical.*

The notion *square-free* implies that when a polynomial is decomposed into its unique factorization, there are no repeated factors. For example, $(z_1^2 + z_2)(z_1^4 + 2z_3 + 3)$ is square-free, but $(z_1^2 + z_2)(z_1^4 + 2z_3 + 3)^3$ is not. In particular, Lemma 2.3 implies that ideals containing $z_i^2 - z_i = z_i(z_i - 1)$ in each variable (i.e., boolean ideals) are radical.

In this work, we will make heavy use of one of the most prominent theorems of algebra, namely Hilbert's Nullstellensatz.

[3] If the ideal I is radical, then $I = I(\mathcal{V}(I))$ where $I(\mathcal{V}(I))$ is the ideal vanishing on $\mathcal{V}(I)$. We do not need this statement in our paper explicitly—the spirit of the very same, however, is present.

Theorem 2.4 *(Hilbert's Nullstellensatz). Let $\mathbb{K}$ be a field (not necessarily real, as assumed everywhere else), $P = \mathbb{K}[z_1, \ldots, z_n]$ a polynomial ring, $I \subseteq P$ an ideal and $f \in P$. If $f(z^*) = 0$ for all $z^* \in \mathcal{V}(I)$, then there is a non-negative integer r with $f^r \in I$.*

Remark 2.5. Our set-up implies the following:

- If the ideal I is radical, then $f(z^*) = 0$ for all $z^* \in \mathcal{V}(I)$ implies $f \in I$.
- If $I = \langle f_1, \ldots, f_q \rangle$ for some $f_1, \ldots, f_q \in P$, then it suffices to check all z^* that are common zeros of $f_1, \ldots, f_q$ (over the algebraic closure $\overline{\mathbb{K}}$) instead of all $z^* \in \mathcal{V}(I)$.

Therefore, if both assumptions are satisfied, then $f(z^*) = 0$ for all z^* that are common zeros of $f_1, \ldots, f_q$ (over the algebraic closure $\overline{\mathbb{K}}$) implies $f \in I$. $\triangle$

We continue with our background by recalling the necessary notation for sum-of-squares for the ideal I of the polynomial ring P. As usual, we write $f \equiv h \mod I$ whenever $f = h + g$ for some $g \in I$.

Definition 2.6. Let ℓ be a non-negative integer. A polynomial $f \in P$ is called *ℓ-sum-of-squares modulo I* (or *ℓ-sos modulo I*), if there exist polynomials $s_1, \ldots, s_t \in P$ with degrees $\deg s_i \leq \ell$ for all $i \in \{1, \ldots, t\}$ and

$$f \equiv \sum_{i=1}^{t} s_i^2 \mod I.$$

In the context of real-valued polynomials as we have it, algebraic identities like $f = \sum_{i=1}^{t} s_i^2 + g$ for some $g \in I$, are often referred to as *Positivstellensatz certificates of non-negativity*, and these identities can be found via semidefinite programming, which is at the heart of this project. We present a first example now and will describe precisely how these certificates are obtained in Section 4.

Example 2.7. Let $I = \langle z_1^2 - z_1, z_2^2 - z_2, z_1 z_2 - 1 \rangle$. In this case,

$$\begin{aligned} z_1 + z_2 - 2 &= (z_1 - z_2)^2 - (z_1^2 - z_1) - (z_2^2 - z_2) + 2(z_1 z_2 - 1) \\ &\equiv (z_1 - z_2)^2 \mod I \end{aligned}$$

and the polynomial $z_1 + z_2 - 2$ is said to be 1-sos modulo I. The certificate consists of the single polynomial $s_1 = z_1 - z_2$. $\bigcirc$

It is well-known that not all non-negative polynomials can be expressed as a sum-of-squares. However, in the particular case when the ideal is radical and the variety is finite, we can state the following.

Lemma 2.8. *Given a radical ideal I with a finite real variety and a polynomial f with $f(\mathcal{V}(I)) \subseteq \mathbb{R}$. Then f is non-negative on the variety, i.e., $\forall z^* \in \mathcal{V}(I)\colon\ f(z^*) \geq 0$, if and only if there exists a non-negative integer ℓ such that f is ℓ-sos modulo I.*

Proof. Let f be a polynomial that can be expressed as a sum-of-squares modulo I, say $f \equiv \sum_{i=1}^{t} s_i^2 \mod I$. Since all polynomials in the ideal I vanish on the variety by definition and since the real-valued $\sum_{i=1}^{t} s_i^2$ is clearly non-negative, f is non-negative on the variety $\mathcal{V}(I)$.

To prove the other direction, we recall a well-known argument. Suppose we have a polynomial f with $f(z^*) \geq 0$ for all $z^* \in \mathcal{V}(I)$. Suppose further that the finite variety $\mathcal{V}(I)$ equals $\{z_1^*, \ldots, z_t^*\}$ for a suitable t. We now construct t interpolation polynomials f_i for $i \in \{1, \ldots, t\}$ (see Gasca and Sauer, 2012) such that

$$f_i(z^*) = \begin{cases} 1 & z^* = z_i^*, \\ 0 & z^* \neq z_i^* \end{cases}$$

for all $z^* \in \mathcal{V}(I)$. Observe that the square of an interpolating polynomial is again an interpolating polynomial. Therefore, the difference polynomial

$$f(z) - \sum_{i=1}^{t} f_i^2(z) f(z_i^*) \tag{2.1}$$

vanishes on every point $\{z_1^*, \ldots, z_t^*\}$ in the variety. We now use Hilbert's Nullstellensatz (Theorem 2.4): Since the ideal I is radical, we apply Remark 2.5 on the difference polynomial (2.1) and get that it is in I. Therefore, if we let

$$s_i = f_i(z)\sqrt{f(z_i^*)},$$

we then see that

$$f \equiv \sum_{i=1}^{t} s_i^2 \mod I. \quad \square$$

We observe that the ℓ in this case is quite large, since it is the degree of the interpolating polynomial f_i, which depends on the number of points in the variety. However, we will rely on the fact that the sum-of-squares representation is not unique, and there may exist Positivstellensatz certificates of much lower degree, within reach of computation. As we will see in Section 5 and 6, this does indeed turn out to be the case.

3. Vizing's conjecture as a sum-of-squares problem

In this section, we describe Vizing's conjecture as a sum-of-squares problem. Towards that end, we will first define ideals associated with graphs G, H and $G\square H$, and then finally describe an ideal/polynomial pair where the polynomial is non-negative on the variety of the ideal if and only if Vizing's conjecture is true. We begin by creating an ideal where the variety of solutions corresponds to graphs with a given number of vertices and size of a minimum dominating set.

The notation underlying all of the definitions in this section—we will use it also through the whole article—is as follows. Let $n_{\mathcal{G}}$ and $k_{\mathcal{G}} \leq n_{\mathcal{G}}$ be fixed positive integers, and let $\mathcal{G}$ be the class of graphs on $n_{\mathcal{G}}$ vertices with a fixed[4] minimum dominating set $D_{\mathcal{G}}$ of size $k_{\mathcal{G}}$. We then turn the various edges "on" or "off" (by controlling a boolean variable $e_{gg'}$ for each possible edge $\{g, g'\}$) such that each point in the variety corresponds to a *specific* graph $G \in \mathcal{G}$.

Definition 3.1. Set $e_{\mathcal{G}} = \{e_{gg'} : \{g, g'\} \subseteq V(\mathcal{G})\}$. The ideal $I_{\mathcal{G}} \subseteq P_{\mathcal{G}} = \mathbb{K}[e_{\mathcal{G}}]$ is defined by the system of polynomial equations[5]

[4] We fix the vertices of the dominating set without loss of generality as this corresponds to a simple renaming of the vertices. Doing this avoids the introduction of additional boolean variables for the vertices and reduces the size of the corresponding isomorphism group of the variety. It is therefore algorithmically favorable.

[5] Being precise, the ideal $I_{\mathcal{G}}$ is defined by the polynomials on the left-hand side of the equations (3.1a), (3.1b) and (3.1c). However, we think that the current phrasing provides the better insight and is closer to the intended way of thinking for this work.

If one would like to write equations in a formally correct way, one first needs to evaluate the polynomial on the left-hand side at some suitable point, meaning to substitute the variables of the polynomial ring by real values. For example, the variable $e_{gg'} \in P_{\mathcal{G}}$ is substituted by some (possibly a priori unknown) $e_{gg'}^* \in \mathbb{R}$, therefore the polynomial on the left-hand side of (3.1a) becomes the equation $(e_{gg'}^*)^2 - e_{gg'}^* = 0$. Notation 3.2 is also related to this issue and brings the connection to the points in the associated variety.

We will, however, always be precise when the distinction between variable and evaluated (starred) form matters.

$$e_{gg'}^2 - e_{gg'} = 0 \qquad \text{for } \{g, g'\} \subseteq V(\mathcal{G}), \tag{3.1a}$$

$$\prod_{g' \in D_\mathcal{G}} (1 - e_{gg'}) = 0 \qquad \text{for } g \in V(\mathcal{G}) \setminus D_\mathcal{G}, \tag{3.1b}$$

$$\prod_{g' \in V(\mathcal{G}) \setminus S} \left(\sum_{g \in S} e_{gg'} \right) = 0 \qquad \text{for } S \subseteq V(\mathcal{G}) \text{ where } |S| = k_\mathcal{G} - 1. \tag{3.1c}$$

Notation 3.2. Throughout this paper, we will use the following notations: We will use z for the tuple of variables of the polynomial ring P, so $P = \mathbb{K}[z]$. When considering the variety $\mathcal{V}(I)$ associated to an ideal $I \subseteq P$, we use the notation $z^* \in \mathcal{V}(I)$ for the elements in this variety.

Note that the polynomial ring variables (which are the components of z) correspond bijectively to the components of z^*. In particular we will use $e^*_{gg'}$ for the component of $z^* = e^*_\mathcal{G} \in \mathcal{V}(I_\mathcal{G})$ corresponding to the polynomial ring variable $e_{gg'} \in P_\mathcal{G}$.

Remark 3.3. Definition 3.1 is meaningful even in the case that $n_\mathcal{G} = 1$. The only vertex must be in the dominating set, so $k_\mathcal{G} = 1$. Pairs $\{g, g'\}$ cannot be chosen from the one-element set $V(\mathcal{G})$, thus the set of variables $e_\mathcal{G}$ is empty. This implies $P_\mathcal{G} = \mathbb{K}[e_\mathcal{G}]$ is the polynomial ring over $\mathbb{K}$ in no variables (i.e., isomorphic to $\mathbb{K}$).

The polynomials defining the ideal $I_\mathcal{G}$ disappear: There are no polynomials coming from (3.1a) again because of non-existing pairs $\{g, g'\}$. Also, there are no polynomials coming from (3.1b) as $V(\mathcal{G}) \setminus D_\mathcal{G}$ is empty because both $V(\mathcal{G})$ and $D_\mathcal{G}$ consist exactly of the same vertex. There is a contribution from (3.1c) for S being the empty set, however this is the equation $0 = 0$, so again no true contribution. Thus, the ideal $I_\mathcal{G} \subseteq P_\mathcal{G}$ only consists of 0.

This, in turn, means that the variety $\mathcal{V}(I_\mathcal{G})$ is "full" meaning in our particular situation being the set containing the empty tuple only. △

Theorem 3.4. *The points in the variety $\mathcal{V}(I_\mathcal{G})$ are in bijection to the graphs in $\mathcal{G}$.*

Proof. For $n_\mathcal{G} = k_\mathcal{G} = 1$ this is clearly true, as there is exactly one element in both $\mathcal{V}(I_\mathcal{G})$ and $\mathcal{G}$.

For $n_\mathcal{G} \geqslant 2$ consider any point $z^* \in \mathcal{V}(I_\mathcal{G})$. We use Notation 3.2. Since equations (3.1a) turn the edges "on" ($e^*_{gg'} = 1$) or "off" ($e^*_{gg'} = 0$), the point z^* defines a graph G in $n_\mathcal{G}$ vertices. Equations (3.1b) iterate over all the vertices inside the set $D_\mathcal{G}$, and ensure that for each vertex outside the set at least one edge from a vertex inside the set to this vertex is "on". Therefore, $D_\mathcal{G}$ is a dominating set. Finally, equations (3.1c) iterate over all sets S of size $k_\mathcal{G} - 1$ and ensure that at least one vertex outside S is not incident to any vertex inside S for any S. Therefore, no set S of size $k_\mathcal{G} - 1$ is a dominating set. Thus, every point $z^* \in \mathcal{V}(I_\mathcal{G})$ corresponds to a graph G on $n_\mathcal{G}$ vertices with a minimum dominating set of size $k_\mathcal{G}$.

With the intuition given above it is straightforward to construct a point in $\mathcal{V}(I_\mathcal{G})$ for a graph on $n_\mathcal{G}$ vertices with a minimum dominating set of size $k_\mathcal{G}$. □

Similarly, for fixed positive integers $n_\mathcal{H}$ and $k_\mathcal{H} \leq n_\mathcal{H}$, let $\mathcal{H}$ be the class of graphs on $n_\mathcal{H}$ vertices and a minimum dominating set of size $k_\mathcal{H}$. Again, we fix the dominating set to some $D_\mathcal{H}$ to reduce isomorphisms within the variety. Furthermore let the ideal $I_\mathcal{H}$ be defined on the polynomial ring $P_\mathcal{H} = \mathbb{K}[e_\mathcal{H}]$ with $e_\mathcal{H} = \{e_{hh'} \colon \{h, h'\} \subseteq V(\mathcal{H})\}$ such that the solutions in the variety $\mathcal{V}(I_\mathcal{H})$ are in bijection to the graphs in $\mathcal{H}$.

Next, we define the graph class $\mathcal{G}\square\mathcal{H}$ and the ideal $I_{\mathcal{G}\square\mathcal{H}}$. For the above classes $\mathcal{G}$ and $\mathcal{H}$, the graph class $\mathcal{G}\square\mathcal{H}$ is the set of product graphs $G\square H$ for $G \in \mathcal{G}$ and $H \in \mathcal{H}$. The new variables needed for the ideal are the variables corresponding to the vertices in the product graph and indicate if such a vertex is in the dominating set or not. Let $x_{\mathcal{G}\square\mathcal{H}} = \{x_{gh} \colon g \in V(\mathcal{G}), h \in V(\mathcal{H})\}$ and set $P_{\mathcal{G}\square\mathcal{H}} = \mathbb{K}[e_\mathcal{G} \cup e_\mathcal{H} \cup x_{\mathcal{G}\square\mathcal{H}}]$.

Definition 3.5. The ideal $I_{\mathcal{G}\square\mathcal{H}} \subseteq P_{\mathcal{G}\square\mathcal{H}}$ is defined by the system of polynomial equations

$$x_{gh}^2 - x_{gh} = 0, \tag{3.2a}$$

$$(1 - x_{gh})\left(\prod_{\substack{g' \in V(\mathcal{G}) \\ g' \neq g}} (1 - e_{gg'}x_{g'h})\right)\left(\prod_{\substack{h' \in V(\mathcal{H}) \\ h' \neq h}} (1 - e_{hh'}x_{gh'})\right) = 0, \tag{3.2b}$$

for $g \in V(\mathcal{G})$ and $h \in V(\mathcal{H})$.

Observe that we have no restrictions on the edge variables in this definition. It is only used as a stepping stone to the final and most important ideal in our polynomial model.

Definition 3.6. For graph classes $\mathcal{G}$ and $\mathcal{H}$, we set I_{viz} to be the ideal generated by the elements of $I_{\mathcal{G}}$, $I_{\mathcal{H}}$ and $I_{\mathcal{G}\square\mathcal{H}}$.

Note that our definition of I_{viz} depends on the specific parameters $n_{\mathcal{G}}$, $n_{\mathcal{H}}$, $k_{\mathcal{G}}$ and $k_{\mathcal{H}}$.

Notation 3.7. Analogously to Notation 3.2 we will write $z^* \in \mathcal{V}(I_{\text{viz}})$ for the elements of the variety of I_{viz}. We will use $e^*_{gg'}$, $e^*_{hh'}$ and x^*_{gh} for the component of z^* corresponding to the polynomial ring variables $e_{gg'} \in P_{\mathcal{G}}$, $e_{hh'} \in P_{\mathcal{H}}$ and $x_{gh} \in P_{\mathcal{G}\square\mathcal{H}}$ respectively.

Theorem 3.8. *The points in the variety $\mathcal{V}(I_{\text{viz}})$ are in bijection to the triples (G, H, D) where G is a graph in $\mathcal{G}$, H is a graph in $\mathcal{H}$ and D is a dominating set of any size of $G\square H$.*

Proof. We have already demonstrated in Theorem 3.4 that $\mathcal{V}(I_{\mathcal{G}})$, $\mathcal{V}(I_{\mathcal{H}})$ are in bijection to the graphs in $n_{\mathcal{G}}$, $n_{\mathcal{H}}$ vertices with minimum dominating sets of size $k_{\mathcal{G}}$, $k_{\mathcal{H}}$ respectively. It remains to investigate the restrictions placed on the x_{gh} variables, which denote whether or not the vertex $gh \in V(\mathcal{G}\square\mathcal{H})$ appears in the dominating set of the product graph.

Let $z^* \in \mathcal{V}(I_{\text{viz}})$ be a point in the variety. We use Notation 3.2. With the arguments above this point induces a graph $G \in \mathcal{G}$ and a graph $H \in \mathcal{H}$. Furthermore equations (3.2a) force the vertex variables x_{gh} to evaluate to "on" ($x^*_{gh} = 1$) or "off" ($x^*_{gh} = 0$). We define D such that the vertex gh is in D if $x^*_{gh} = 1$ and is outside D otherwise. Equations (3.2b) ensure that D is a dominating set, because every vertex gh is dominated. Indeed, it is either in the set itself (i.e., $1 - x^*_{gh} = 0$), or it is adjacent to a vertex in the dominating set D via an edge from the underlying graph in $\mathcal{G}$ or the underlying graph in $\mathcal{H}$. In particular, the edge $\{g, g'\}$ is "on" and the vertex $g'h$ is in the dominating set ($e^*_{gg'} = 1$ and $x^*_{g'h} = 1$), or the edge $\{h, h'\}$ is "on" and the vertex gh' is in the dominating set ($e^*_{hh'} = 1$ and $x^*_{gh'} = 1$). In either of these cases, the vertex gh of the box graph is dominated. Therefore, the points in the variety $\mathcal{V}(I_{\text{viz}})$ are in bijection to the graphs in $n_{\mathcal{G}}$, $n_{\mathcal{H}}$ vertices with minimum dominating sets of size $k_{\mathcal{G}}$, $k_{\mathcal{H}}$ respectively, and their corresponding product graph with a dominating set D of any size.

With the intuition given above it is straightforward to construct a point in $\mathcal{V}(I_{\mathcal{G}})$ for graphs G, H and a dominating set D in $G\square H$. □

Observe that there are no polynomials in I_{viz} enforcing minimality on the dominating set in the product graph. This is essential when we tie all of the definitions together and model Vizing's conjecture as a sum-of-squares problem. In particular, we model Vizing's conjecture as an ideal/polynomial pair, where the polynomial must be non-negative on the variety associated with the ideal if and only if Vizing's conjecture is true.

Definition 3.9. Given the graph classes $\mathcal{G}$ and $\mathcal{H}$, define

$$f_{\text{viz}} = \left(\sum_{gh \in V(\mathcal{G}) \times V(\mathcal{H})} x_{gh}\right) - k_{\mathcal{G}}k_{\mathcal{H}}.$$

Theorem 3.10. *Vizing's conjecture is true if and only if for all positive integer values of $n_{\mathcal{G}}$, $k_{\mathcal{G}}$, $n_{\mathcal{H}}$ and $k_{\mathcal{H}}$ with $k_{\mathcal{G}} \leq n_{\mathcal{G}}$ and $k_{\mathcal{H}} \leq n_{\mathcal{H}}$, f_{viz} is non-negative on $\mathcal{V}(I_{\text{viz}})$, i.e.,*

$$\forall z^* \in \mathcal{V}(I_{\text{viz}}) \colon\ f_{\text{viz}}(z^*) \geq 0.$$

Proof. Assume that Vizing's conjecture is true, and fix the values of $n_{\mathcal{G}}$, $k_{\mathcal{G}}$, $n_{\mathcal{H}}$ and $k_{\mathcal{H}}$. Therefore, for all graphs $G \in \mathcal{G}$ and $H \in \mathcal{H}$, we have $\gamma(G\square H) \geq \gamma(G)\gamma(H)$ which is equivalent to $\gamma(G\square H) - k_{\mathcal{G}}k_{\mathcal{H}} \geq 0$. The sum $\sum_{gh \in V(\mathcal{G}) \times V(\mathcal{H})} x^*_{gh}$ coming from f_{viz} equals exactly the size of the dominating set in the box graph $G\square H$. Therefore, we have $f_{\text{viz}}(z^*) \geq 0$ for all $z^* \in \mathcal{V}(I_{\text{viz}})$.

Similarly, if $f_{\text{viz}}(z^*) \geq 0$ for all $z^* \in \mathcal{V}(I_{\text{viz}})$, every dominating set in $G\square H$ has size at least $k_{\mathcal{G}}k_{\mathcal{H}}$. In particular, the minimum dominating set in $G\square H$ has size at least $k_{\mathcal{G}}k_{\mathcal{H}}$ and Vizing's conjecture is true. □

Corollary 3.11. *Vizing's conjecture is true if and only if for all positive integer values of $n_{\mathcal{G}}$, $k_{\mathcal{G}}$, $n_{\mathcal{H}}$ and $k_{\mathcal{H}}$ with $k_{\mathcal{G}} \leq n_{\mathcal{G}}$ and $k_{\mathcal{H}} \leq n_{\mathcal{H}}$, there exists an integer ℓ such that f_{viz} is ℓ-sos modulo I_{viz}.*

Proof. The ideal I_{viz} contains the univariate polynomial $z^2 - z$ for each variable. Therefore, by Lemma 2.3, I_{viz} is radical. Due to Lemma 3.8, the variety $\mathcal{V}(I_{\text{viz}})$ is finite and obviously it is real. Therefore, by Lemma 2.8, we know that a polynomial is non-negative on $\mathcal{V}(I_{\text{viz}})$, if and only if there exists an integer ℓ such that the polynomial is ℓ-sos modulo I_{viz}. Hence the result follows from Theorem 3.10. □

In this section, we have drawn a parallel between Vizing's conjecture and a sum-of-squares problem. We defined the ideal/polynomial pair $(I_{\text{viz}}, f_{\text{viz}})$ such that $f_{\text{viz}}(z^*) \geq 0$ for all $z^* \in \mathcal{V}(I_{\text{viz}})$ if and only if Vizing's conjecture is true. In the next section, we describe how to find these Positivstellensatz certificates of non-negativity, or equivalently, these Positivstellensatz certificates that Vizing's conjecture is true.

4. Methodology

4.1. Overview of the methodology

In our approach to Vizing's conjecture we "partition" the graphs G, H and $G\square H$ by their sizes (number of vertices) $n_{\mathcal{G}}$ and $n_{\mathcal{H}}$ and by the sizes of their dominating sets $k_{\mathcal{G}}$ and $k_{\mathcal{H}}$. Note that we aim for certificates for all partitions as this would prove the conjecture. However in the following we present our method which works for a fixed partition (i.e., for fixed values of $n_{\mathcal{G}}$, $k_{\mathcal{G}}$, $n_{\mathcal{H}}$ and $k_{\mathcal{H}}$), and only later relax this and generalize to parametrized partitions.

The outline is as follows:

- Step 1: Model the graph classes as ideals
- Step 2: Formulate Vizing's conjecture as sum-of-squares existence question
- Step 3: Transform to a semidefinite program
- Step 4: Obtain a numeric certificate by solving the semidefinite program
- Step 5: Guess an exact certificate
- Step 6: Computationally verify the certificate
- Step 7: Generalize the certificate
- Step 8: Prove correctness of the certificate

For fixed values of $n_{\mathcal{G}}$, $k_{\mathcal{G}}$, $n_{\mathcal{H}}$ and $k_{\mathcal{H}}$ the first step is to create the ideal I_{viz} as described in Section 3, in particular Definition 3.6. To summarize, we create the ideal I_{viz} in a suitable polynomial ring in such a way that the points in the variety $\mathcal{V}(I_{\text{viz}})$ are in bijection to the triples (G, H, D) where G is a graph in $\mathcal{G}$, H is a graph in $\mathcal{H}$ and D is a dominating set of any size of $G\square H$; see Theorem 3.8. In this polynomial ring there is a variable for each possible edge of $\mathcal{G}$ and $\mathcal{H}$ (indicating whether

this edge is present or not in the particular graphs G and H) and for each vertex of $\mathcal{G}\square\mathcal{H}$ (indicating whether this vertex is in the dominating set of $G\square H$ or not).

The second step is to use the polynomial ring variables mentioned above to reformulate Vizing's conjecture: It is true for a fixed partition if the polynomial f_{viz} (Definition 3.9) is non-negative if evaluated at all points in the variety $\mathcal{V}(I_{\text{viz}})$ of the constructed ideal. For showing that the polynomial is non-negative, we aim for rewriting it as a finite sum of squares of polynomials (modulo the ideal I_{viz}). If we find such polynomials, then these polynomials form a certificate for Vizing's conjecture for the fixed partition. To be more precise and as already described in Section 3, Vizing's conjecture is true for these fixed values of $n_{\mathcal{G}}$, $k_{\mathcal{G}}$, $n_{\mathcal{H}}$ and $k_{\mathcal{H}}$ if and only if f_{viz} is ℓ-sos modulo I_{viz}.

In the subsequent Section 4.2 we describe how to perform step three and do another reformulation, namely as a semidefinite program. Note that in order to do so, we need to have specified ℓ, the degree of the certificate. Note also that in order to prepare the semidefinite program, we use basis polynomials (i.e., special generators) of the ideals. These are obtained by computing a Gröbner basis of the ideal; see Cox et al. (2007) for more information on Gröbner bases.

The fourth step (Section 4.3) is now to solve the semidefinite program. If the program is infeasible (i.e., there exists no feasible solution), we increase ℓ. On the other hand, if the program is feasible, then we can construct a numeric sum-of-squares certificate. As the underlying system of equations—therefore the future certificate—is quite large, we iterate the following tasks: Find a numeric solution to the semidefinite program, find or guess some structure in the solution, use these new relations to reduce the size of the semidefinite program, and begin again with solving the new program. This reduces the solution space and therefore potentially also the size (number t of summands) of the certificate and the number of monomials of the s_i from Definition 2.6. The procedure above goes hand-in-hand with our next step (Section 4.4), namely obtaining (one might call it guessing) an exact certificate out of the numeric certificate.

Once we have a candidate for an exact certificate, we can check its validity computationally by summing up the squares and reducing modulo the ideal; see our step six described in Section 4.5.

We want to point out, that we still consider Vizing's conjecture for a particular partition of graphs. However, having such certificates for some partitions, one can go for generalizing them by introducing parametrized partitions of graphs. Our seventh step in Section 4.6 provides more information.

The final step is to prove that the newly obtained, generalized certificate candidate is indeed a certificate; see as well Section 4.6. Further certificates and different generalizations together with their proofs can be found in Sections 5 and 6.

4.2. Transform to a semidefinite program

Semidefinite programming refers to the class of optimization problems where a linear function with a symmetric matrix variable is optimized subject to linear constraints and the constraint that the matrix variable must be positive semidefinite. A semidefinite program (SDP) can be solved to arbitrary precision in polynomial time Vandenberghe and Boyd (1996). In practice the most prominent methods for solving an SDP efficiently are interior-point algorithms. We use the solver MOSEK MOSEK ApS (2017) within MATLAB. For more details on solving SDPs and on interior-point algorithms see Wolkowicz et al. (2000).

It is possible to check whether a polynomial f is ℓ-sos modulo an ideal with semidefinite programming. We refer to (Blekherman et al., 2013, pg. 298) for detailed information and examples. We will now present how to do so for our setting only.

Let us first fix (for example, by computing) a reduced Gröbner basis B of I_{viz} and fix a non-negative integer ℓ. Denote by v the vector of all monomials in our polynomial ring P of degree at most ℓ which can not be reduced[6] modulo I_{viz} by the Gröbner basis B. Let p be the length of the vector v. Then f_{viz} (of Definition 3.9) is ℓ-sos modulo I_{viz} if and only if there is a positive semidefinite matrix $X \in \mathbb{R}^{p\times p}$ such that f_{viz} is equal to

[6] Algorithmically speaking, we say that a polynomial f is reduced modulo the ideal I if f is the representative of $f+I$ which is invariant under reduction by a reduced Gröbner basis of the ideal I.

$$v^T X v$$

when reduced over B. Hence the SDP we end up with optimizes the matrix variable $X \in \mathbb{R}^{p \times p}$ subject to linear constraints that guarantee f_{viz} being $v^T X v$ as above. The objective function can be chosen arbitrarily because any matrix satisfying the constraints is sufficient for our purpose. More will be said on this later.

If the SDP is feasible, then due to the positive semidefiniteness we can decompose the solution X into $X = S^T S$ for some $S \in \mathbb{R}^{t \times p}$ and $t \leq p$. Subsequently, we define the polynomial s_i by the ith row of Sv and obtain

$$v^T X v = (Sv)^T (Sv) = \sum_{i=1}^{t} s_i^2 \equiv f_{\text{viz}} \mod I_{\text{viz}}. \tag{4.1}$$

Note that the last congruence holds due to the constraints in the SDP. Equation (4.1) then certifies that f_{viz} can be written as a sum of squares of the s_i, and hence, f_{viz} is ℓ-sos modulo I_{viz} according to Definition 2.6.

If the SDP is infeasible, we have an indication that there is no certificate of degree ℓ. We increase ℓ to $\ell + 1$, because f_{viz} could still be $(\ell + 1)$-sos modulo I_{viz} or possess a certificate of even higher degree. However, if no new reduced monomials appear in this increment, then by Lemma 2.8 and Theorem 3.10 Vizing's conjecture does not hold.

Example 4.1. We consider the graph classes $\mathcal{G}$ and $\mathcal{H}$ with $n_{\mathcal{G}} = 3$, $k_{\mathcal{G}} = 2$, $n_{\mathcal{H}} = 3$ and $k_{\mathcal{H}} = 2$. Using SageMath The SageMath Developers (2019) we construct the ideal I_{viz}, generated by 32 polynomials in 15 variables. Again using SageMath, we find a Gröbner basis of size 95.

First, we check the existence of a 1-sos certificate. The vector v for $\ell = 1$ has length 12, i.e., we set up an SDP with a matrix variable $X \in \mathbb{R}^{12 \times 12}$. Imposing the necessary constraints to guarantee $\sum_{i=1}^{12} s_i^2 \equiv f_{\text{viz}} \mod I_{\text{viz}}$ leads to 67 linear equality constraints. Interior-point algorithms detect infeasibility of this SDP in less than half a second, this indicates that there is no 1-sos certificate.

Setting up the SDP for checking the existence of a 2-sos certificate results in a problem with a matrix variable of dimension 67 and 359 linear constraints. Interior-point algorithms find a solution X of this SDP in 0.72 seconds, this guarantees the existence of a numeric 2-sos certificate for these graph classes. ◯

4.3. Obtain a numeric certificate

As described in Section 4.2 above, after solving the SDP we decompose the solution X. We do so by computing the eigenvalue decomposition $X = V^T D V$ and then setting $S = D^{1/2} V$, where D is the diagonal matrix having the eigenvalues on the main diagonal. Since X is positive semidefinite, all eigenvalues are non-negative and we can compute $D^{1/2}$ by taking the square root of each of the diagonal entries. The matrices X, V and D are obtained through numeric computations, hence there might be entries in D that are rather close to zero but not considered as zero. We may try setting these almost-zero eigenvalues to zero, which reduces the number of polynomials of the sum-of-squares certificate.

Furthermore, a zero column in S means that the corresponding monomial is not needed in the certificate. Hence, we may try to compute a certificate where we remove all monomials corresponding to almost-zero columns. This can decrease the size of the SDP considerably and a smaller size of the matrix and fewer constraints is favorable for solving the SDP. Of course, if removing these monomials leads to infeasibility of the SDP, then removing these monomials was not correct.

As already mentioned we can choose the objective function arbitrarily. Our experiments show that different objective functions lead to (significantly) different solutions. Therefore, we carefully choose a suitable objective function leading to a "nice" solution for each instance.

Example 4.2. We look again at the case we considered in Example 4.1, that is $\mathcal{G}$ and $\mathcal{H}$ with $n_{\mathcal{G}} = 3$, $k_{\mathcal{G}} = 2$, $n_{\mathcal{H}} = 3$ and $k_{\mathcal{H}} = 2$, for which we already obtained an optimal solution X and a numeric 2-sos certificate.

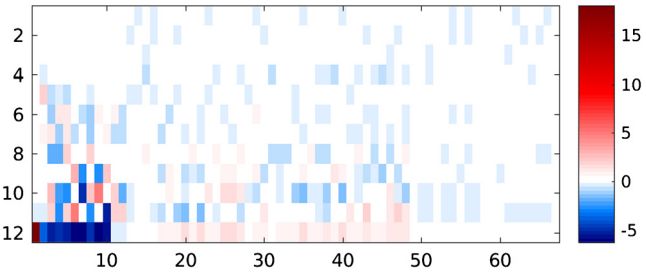


Fig. 1. Plotting the entries of the matrix S for v being the vector of all monomials in P. Every row of S corresponds to one polynomial s_i of the numeric sum-of-squares certificate and every column of S corresponds to one monomial in v. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

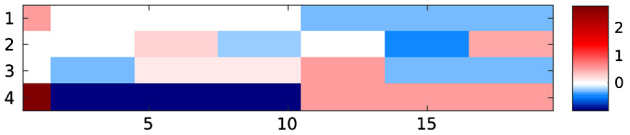


Fig. 2. Plotting the entries of matrix S as in Fig. 1, but now we only allow the coefficients of 19 monomials to be non-zero. The numeric sum-of-squares certificate consists of 4 (number of rows) polynomials in 19 (number of columns) monomials. In particular the first three rows correspond to s_1, s_2 and s_3 and the last row corresponds to s_0 as given in (4.2).

After computing (numerically) the eigenvalue decomposition $X = V^T D V$, we set all almost-zero eigenvalues to zero and compute $S = D^{1/2} V$, which results in a 12×67 matrix, i.e., 55 eigenvalues are considered as zero. In Fig. 1 a heat map of matrix S is displayed. It seems unattainable to convert this obtained solution to an exact certificate (see Section 4.4), so we take a different path.

Using different objective functions and aiming for a certificate where only certain monomials appear can lead to results with a clearer structure. If the ith monomial should not be included, we can set the ith row and column of X equal to zero and obtain another SDP, where we have fewer variables and modified constraints. We now try to use only the 19 monomials 1, x_{gh} and $x_{gh}x_{gh'}$ for all $g \in V(\mathcal{G})$ and all $h, h' \in V(\mathcal{H})$ with $h' \neq h$.

This results in an SDP with a matrix variable of dimension 19 and 99 constraints. The SDP can be solved in 0.48 seconds, and again, we obtain matrix S (after setting almost-zero eigenvalues to zero), which now is of dimension 4×19. A heat map is given in Fig. 2.

As one sees in Fig. 2, S has a certain block structure, suggesting that in each s_i the coefficients of the monomials depend only on the index $g \in V(\mathcal{G})$ and there is no dependence on the indices $h \in V(\mathcal{H})$. Therefore, we aim for a 2-sos certificate of the form $\sum_{i=0}^{n_\mathcal{G}} s_i^2 \equiv f_{\text{viz}} \mod I_{\text{viz}}$ with

$$s_i = \nu_i + \sum_{g \in V(\mathcal{G})} \lambda_{g,i} \left(\sum_{h \in V(\mathcal{H})} x_{gh} \right) + \sum_{g \in V(\mathcal{G})} \mu_{g,i} \left(\sum_{\{h,h'\} \subseteq V(\mathcal{H})} x_{gh} x_{gh'} \right) \tag{4.2a}$$

for $i \in \{1, \ldots, n_\mathcal{G}\}$ and

$$s_0 = \alpha + \beta \left(\sum_{g \in V(\mathcal{G})} \sum_{h \in V(\mathcal{H})} x_{gh} \right) + \gamma \sum_{g \in V(\mathcal{G})} \left(\sum_{\{h,h'\} \subseteq V(\mathcal{H})} x_{gh} x_{gh'} \right), \tag{4.2b}$$

where the coefficients α, β, γ, ν_i, $\lambda_{g,i}$ and $\mu_{g,i}$ are the entries of S. However, we only have the numeric values

$$S = \begin{pmatrix} 0.535 & 0.011 & 0.011 & 0.011 & -0.289 & -0.289 & -0.289 \\ 0.000 & 0.000 & 0.236 & -0.236 & -0.001 & -0.471 & 0.472 \\ -0.000 & -0.272 & 0.136 & 0.136 & 0.544 & -0.273 & -0.272 \\ 2.778 & -0.962 & -0.962 & -0.962 & 0.536 & 0.536 & 0.536 \end{pmatrix}$$

at hand and it is not obvious how to guess suitable exact numbers from it. In contrast, looking at the values

$$X = \begin{pmatrix} 8.000 & -2.667 & -2.667 & -2.667 & 1.333 & 1.333 & 1.333 \\ -2.667 & 1.000 & 0.889 & 0.889 & -0.667 & -0.444 & -0.444 \\ -2.667 & 0.889 & 1.000 & 0.889 & -0.444 & -0.667 & -0.444 \\ -2.667 & 0.889 & 0.889 & 1.000 & -0.444 & -0.444 & -0.667 \\ 1.333 & -0.667 & -0.444 & -0.445 & 0.667 & 0.222 & 0.222 \\ 1.333 & -0.444 & -0.667 & -0.445 & 0.222 & 0.667 & 0.222 \\ 1.333 & -0.444 & -0.444 & -0.667 & 0.222 & 0.222 & 0.667 \end{pmatrix},$$

it seems almost obvious which simple algebraic numbers the entries of X could be, for example 0.667 could be $2/3$. We will use that in the following section. ◯

4.4. Guess an exact certificate

We now have a guess for the structure of the certificate, but coefficients that are simple algebraic numbers are hard to determine from the numbers in S. On the other hand, the exact numbers in X seem to be rather obvious so we go back to the relation $X = S^T S$. It implies that if we fix two monomials then the inner product of the vectors of the coefficients of these monomials in all the s_i has to be equal to the corresponding number in X.

Setting up a system of equations using all possible inner products, we may obtain a solution to this system. This solution determines the coefficients in the certificate (and the certificate might be simplified even further).

Example 4.3. We continue Example 4.1, that is we consider the graph classes $\mathcal{G}$ and $\mathcal{H}$ with $n_{\mathcal{G}} = 3$, $k_{\mathcal{G}} = 2$, $n_{\mathcal{H}} = 3$ and $k_{\mathcal{H}} = 2$.

The exact numbers in X given in Example 4.2 can be guessed easily. In fact, if this guess for X is correct, every choice of S such that $S^T S = X$ gives a certificate. Using the relation $S^T S = X$ we set up a system of equations on the parameters of (4.2). To be more precise, let $\lambda_g = (\lambda_{g,i})_{i=1,\dots,n_{\mathcal{G}}}$, $\mu_g = (\mu_{g,i})_{i=1,\dots,n_{\mathcal{G}}}$ and $\nu = (\nu_i)_{i=1,\dots,n_{\mathcal{G}}}$. Then we can define the vectors $a = \binom{\nu}{\alpha}$, $b_g = \binom{\lambda_g}{\beta}$ and $c_g = \binom{\mu_g}{\gamma}$, and $S^T S = X$ (together with the guessed values for X) implies that

$$\begin{aligned} \langle a, a\rangle &= 2(n_{\mathcal{G}} - 1)^2, \\ \langle a, b_g\rangle &= -\tfrac{4}{3}(n_{\mathcal{G}} - 1), & \langle a, c_g\rangle &= \tfrac{2}{3}(n_{\mathcal{G}} - 1), \\ \langle b_g, b_g\rangle &= 1, & \langle b_g, b_{g'}\rangle &= \tfrac{8}{3}, \\ \langle c_g, c_g\rangle &= \tfrac{6}{9}, & \langle c_g, c_{g'}\rangle &= \tfrac{2}{9}, \\ \langle b_g, c_g\rangle &= -\tfrac{6}{9}, & \langle b_g, c_{g'}\rangle &= -\tfrac{4}{9} \end{aligned}$$

has to hold for each $g \in V(\mathcal{G})$, where $\langle \cdot, \cdot \rangle$ denotes the standard inner product. Under the assumption that our guess for X was correct, each solution to this system of equations leads to a valid sum-of-squares certificate (4.2).

We want a sparse certificate and the numeric solution suggests that $\nu_2 = \nu_3 = 0$ holds, so we try to obtain a solution with also $\nu_1 = 0$ (even though the numeric solution does not fit into that setting). Using these values, the equations involving the vector a determine the exact values for α, β and γ as $\alpha = \sqrt{2}(n_{\mathcal{G}} - 1)$, $\beta = -\frac{2}{3}\sqrt{2}$ and $\gamma = \frac{1}{3}\sqrt{2}$. With that, the system of equations simplifies to

$$\begin{aligned} \langle \lambda_g, \lambda_g\rangle &= \tfrac{1}{9}, & \langle \lambda_g, \lambda_{g'}\rangle &= 0, \\ \langle \mu_g, \mu_g\rangle &= \tfrac{4}{9}, & \langle \mu_g, \mu_{g'}\rangle &= 0, \\ \langle \lambda_g, \mu_g\rangle &= -\tfrac{2}{9}, & \langle \lambda_g, \mu_{g'}\rangle &= 0. \end{aligned}$$

Calculating $\sum_{i=1}^{n_\mathcal{G}} s_i^2$ we find out that, due to the system of equations, the sum-of-squares simplifies to

$$\sum_{i=1}^{n_\mathcal{G}} s_i^2 = \frac{1}{9} \sum_{g \in V(\mathcal{G})} \left(\sum_{h \in V(\mathcal{H})} x_{gh} - 2 \sum_{\{h,h'\} \subseteq V(\mathcal{H})} x_{gh} x_{gh'} \right)^2.$$

Hence, if (4.2) is a sum-of-squares certificate then also

$$s_0 = \alpha + \beta \left(\sum_{g \in V(\mathcal{G})} \sum_{h \in V(\mathcal{H})} x_{gh} \right) + \gamma \left(\sum_{g \in V(\mathcal{G})} \sum_{\{h,h'\} \subseteq V(\mathcal{H})} x_{gh} x_{gh'} \right), \tag{4.3a}$$

$$s_g = \frac{1}{3} \left(\sum_{h \in V(\mathcal{H})} x_{gh} - 2 \sum_{\{h,h'\} \subseteq V(\mathcal{H})} x_{gh} x_{gh'} \right) \quad \text{for } g \in V(\mathcal{G}), \tag{4.3b}$$

where $\alpha = \sqrt{2}(n_\mathcal{G} - 1)$, $\beta = -\frac{2}{3}\sqrt{2}$ and $\gamma = \frac{1}{3}\sqrt{2}$ is a sum-of-squares certificate. ◯

To close this section let us highlight once more that we use the SDP and its solution to find out which monomials are used in the certificate and to obtain a structure of their coefficients. In particular we do not need a solution of the SDP of high precision, so solving the SDP is not a bottleneck in this example. It will turn out that this is also true for all other examples we consider.

4.5. Computationally verify the certificate

When a certificate is conjectured, it is straightforward to verify it computationally via SageMath The SageMath Developers (2019). To do so, it is necessary to compute the Gröbner basis of I_{viz}. Observe that at this point, semidefinite programming is no longer needed.

Example 4.4. We computationally verified (using SageMath) the certificate derived in Example 4.3 for the graph classes $\mathcal{G}$ and $\mathcal{H}$ with $n_\mathcal{G} = 3$, $k_\mathcal{G} = 2$, $n_\mathcal{H} = 3$ and $k_\mathcal{H} = 2$. ◯

4.6. Generalize the certificate and prove correctness

In Sections 4.2 to 4.5, we presented a methodology for obtaining a sum-of-squares certificate for graph classes $\mathcal{G}$ and $\mathcal{H}$ with fixed parameters $n_\mathcal{G}$, $k_\mathcal{G}$, $n_\mathcal{H}$ and $k_\mathcal{H}$. Assuming that the previously found pattern generalizes, one can iterate the steps outlined above to obtain certificates for larger classes of graphs.

Example 4.5. We want to generalize the certificate for the graph classes $\mathcal{G}$ and $\mathcal{H}$ with $n_\mathcal{G} = 3$, $k_\mathcal{G} = 2$, $n_\mathcal{H} = 3$ and $k_\mathcal{H} = 2$ to the case $k_\mathcal{G} = n_\mathcal{G} - 1 \geq 1$, $n_\mathcal{H} = 3$ and $k_\mathcal{H} = 2$ for any $n_\mathcal{G} \geq 2$.

Solving the SDP for the cases $n_\mathcal{G} = 4$ and $n_\mathcal{G} = 5$ again yields nicely structured matrices and in fact, all the calculations done for the case $n_\mathcal{G} = 3$ (which we already wrote down parametrized by $n_\mathcal{G}$ above) go through.

Hence, we are able to generalize the sum-of-squares certificate (4.3) in the following way. ◯

Theorem 4.6. *For $k_\mathcal{G} = n_\mathcal{G} - 1 \geq 1$, $n_\mathcal{H} = 3$ and $k_\mathcal{H} = 2$ Vizing's conjecture is true as the polynomials*

$$s_0 = \alpha + \beta \left(\sum_{g \in V(\mathcal{G})} \sum_{h \in V(\mathcal{H})} x_{gh} \right) + \gamma \left(\sum_{g \in V(\mathcal{G})} \sum_{\{h,h'\} \subseteq V(\mathcal{H})} x_{gh} x_{gh'} \right)$$

and

$$s_g = \frac{1}{3} \left(\sum_{h \in V(\mathcal{H})} x_{gh} - 2 \sum_{\{h,h'\} \subseteq V(\mathcal{H})} x_{gh} x_{gh'} \right) \quad \text{for } g \in V(\mathcal{G}),$$

where $\alpha = \sqrt{2}(n_\mathcal{G} - 1)$, $\beta = -\frac{2}{3}\sqrt{2}$ and $\gamma = \frac{1}{3}\sqrt{2}$, are a sum-of-squares certificate with degree 2 of f_{viz}.

The proof will be given later on after introducing some more auxiliary results; see Section 6. Of course, once having the theorem above, it can be verified computationally for particular parameter values, for example for $k_{\mathcal{G}} = 4$ and $n_{\mathcal{G}} = 5$, where the computation of a Gröbner basis is feasible.

4.7. Summary

In this section we saw by an example how to use our machinery combined with clever guessing in order to obtain sum-of-squares certificates for proving that Vizing's conjecture holds for fixed values of $n_{\mathcal{G}}$, $k_{\mathcal{G}}$, $n_{\mathcal{H}}$ and $k_{\mathcal{H}}$, and how this can be used to obtain certificates for a less restricted set of parameters. We will use the next sections in order to present further certificates and generalizations that we found using our method and for which we were able to prove correctness.

5. Exact certificates for $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d$

In this section we deal with certificates for the case $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d$. Towards this end we will first prove several auxiliary results in Section 5.1. Next we present and prove certificates for $d = 0$, $d = 1$ and $d = 2$ in Sections 5.2, 5.3 and 5.4. Then in Section 5.5 we will see how this brings insight on the structure of the certificates. We are therefore able to formulate a conjecture on the structure of the certificate for general d and also present a strategy for proving it. This will be complemented by a more computational approach for checking the conjecture for a given value d; in particular we will prove the conjecture for $d = 3$ and $d = 4$ with the help of SageMath The SageMath Developers (2019).

5.1. Auxiliary results: Sigma calculus

In this section we will develop the machinery needed to prove the correctness of our (exact) certificates. It will turn out that the key is to be able to do operations with certain symmetric polynomials, which will be introduced in Definition 5.4. Another important tool will be again Theorem 2.4, Hilbert's Nullstellensatz. Its implications formulated as Remark 2.5 will be used repeatedly, for example in the proof of the following first lemma.

Lemma 5.1. *Let $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$. Then $e_{gg'} \in I_{\mathcal{G}} \subseteq I_{\text{viz}}$ holds for all $\{g, g'\} \subseteq V(\mathcal{G})$.*

Translating this lemma in terms of congruence relations, we have $e_{gg'} \equiv 0 \mod I_{\mathcal{G}}$ and $e_{gg'} \equiv 0 \mod I_{\text{viz}}$ for all $\{g, g'\} \subseteq V(\mathcal{G})$.

Let us briefly consider Lemma 5.1 from a graph theoretic point of view. Due to Theorem 3.4 the points in the variety of $I_{\mathcal{G}}$ are in bijection to the graphs in $\mathcal{G}$, which are the graphs on $n_{\mathcal{G}}$ vertices with domination number $k_{\mathcal{G}} = n_{\mathcal{G}}$. It is easy to see that such graphs can not have any edges, because otherwise the domination number would be strictly less than $n_{\mathcal{G}}$. Hence $e^*_{gg'} = 0$ holds for all points z^* in the variety of I_{viz}, when we use Notation 3.2. This intuitively justifies Lemma 5.1 by graph theoretical considerations.

Proof of Lemma 5.1. For $k_{\mathcal{G}} = n_{\mathcal{G}} = 1$ there is no $\{g, g'\} \subseteq V(\mathcal{G})$, so there is nothing to prove.

For each $\{g, g'\} \subseteq V(\mathcal{G})$, we apply Hilbert's Nullstellensatz on the polynomial $f = e_{gg'}$.

We use Notation 3.2, and let $z^* \in \mathcal{V}(I_{\mathcal{G}})$, i.e., z^* is a common zero of (3.1a), (3.1b) and (3.1c). Then clearly $e^*_{gg'} \in \{0, 1\}$ due to (3.1a). Furthermore $k_{\mathcal{G}} = n_{\mathcal{G}}$ implies that (3.1c) simplifies to the equations

$$\sum_{\substack{g \in V(\mathcal{G}) \\ g \neq g'}} e^*_{gg'} = 0 \quad \text{for } g' \in V(\mathcal{G}).$$

Therefore $e^*_{gg'} = 0$ for all $\{g, g'\} \subseteq V(\mathcal{G})$. Hence z^* is also a zero of $f = e_{gg'}$ and Hilbert's Nullstellensatz (Theorem 2.4 and Remark 2.5) implies $f = e_{gg'} \in I_{\mathcal{G}}$. □

Lemma 5.2. *Let $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d \geq 1$ for some $d \geq 0$. Moreover, let $g \in V(\mathcal{G})$ and $T \subseteq V(\mathcal{H})$ be a subset of size $|T| = d + 1$. Then*

$$\prod_{h \in T} (1 - x_{gh}) \in I_{\text{viz}}. \tag{5.1}$$

Moreover, we have

$$\prod_{h \in T} x_{gh} \equiv \sum_{r=0}^{d} (-1)^{d+r} \sum_{\substack{U \subseteq T \\ |U|=r}} \prod_{h \in U} x_{gh} \mod I_{\text{viz}}. \tag{5.2}$$

Note that also Lemma 5.2 can be justified intuitively from the graph theoretic perspective. According to Theorem 3.8, a point in the variety of I_{viz} corresponds to two graphs G and H with $n_{\mathcal{G}}$ and $n_{\mathcal{H}}$ vertices and domination numbers $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d$ respectively, and a dominating set D in $G \square H$. Due to Lemma 5.1 there is no edge in G. Hence each vertex gh in $G \square H$ either must be in the dominating set D itself, or there must be a vertex $h' \in V(H)$ such that gh' is in D and the edge $\{h, h'\}$ is in $E(H)$. In other words, for fixed $g \in V(G)$, the vertices $h \in V(H)$ with $x^*_{gh} = 1$ have to form a dominating set in H. Since every dominating set in H has at least $k_{\mathcal{H}} = n_{\mathcal{H}} - d$ vertices, at most d vertices are not in a dominating set. Therefore, whenever we choose $d + 1$ vertices from $V(H)$, at least one vertex has to be in D. Equivalently, in every set T of $d + 1$ vertices of $V(H)$ there is at least one vertex h with $x^*_{gh} = 1$, which is stated in (5.1).

Proof of Lemma 5.2. We use Hilbert's Nullstellensatz for $f = \prod_{h \in T} (1 - x_{gh})$.

Let $z^* \in \mathcal{V}(I_{\text{viz}})$, i.e., z^* is a common zero of (3.1a), (3.1b) and (3.1c) for both $\mathcal{G}$ and $\mathcal{H}$, and of (3.2a) and (3.2b). Note that we use Notation 3.7.

Let us consider the second factor of (3.2b). If $n_{\mathcal{G}} = 1$, then there is no $g' \neq g \in V(\mathcal{G})$, so this product is empty and equals 1. If $n_{\mathcal{G}} \geq 2$, then $e^*_{gg'} = 0$ (the component of z^* corresponding to $e_{gg'}$) for all $g' \in V(\mathcal{G})$ because of Lemma 5.1, and the product equals 1 again. Hence (3.2b) implies

$$(1 - x^*_{gh}) \left(\prod_{\substack{h' \in V(\mathcal{H}) \\ h' \neq h}} \left(1 - e^*_{hh'} x^*_{gh'} \right) \right) = 0 \quad \text{for } h \in V(\mathcal{H}). \tag{5.3}$$

Furthermore $e^*_{hh'} \in \{0, 1\}$ for all $\{h, h'\} \subseteq V(\mathcal{H})$ because of (3.1a), and $x^*_{gh} \in \{0, 1\}$ for all $h \in V(\mathcal{H})$ due to (3.2a).

Assume that z^* is not a zero of f. Then clearly $x^*_{gh} = 0$ for all $h \in T$. In particular, (5.3) simplifies to

$$\prod_{\substack{h' \in V(\mathcal{H}) \\ h' \neq h}} \left(1 - e^*_{hh'} x^*_{gh'} \right) = 0 \quad \text{for } h \in T.$$

Therefore, for each $h \in T$, there is a $h' \in V(\mathcal{H})$ such that $e^*_{hh'} = 1$ and $x^*_{gh'} = 1$. As $x^*_{gh} = 0$ for all $h \in T$, we have $h' \notin T$.

If $n_{\mathcal{H}} = 1$, then $d = 0$ and $|T| = 1$. But then $V(\mathcal{H}) \setminus T$ is empty, so no choice for h' is left, a contradiction. If $n_{\mathcal{H}} \geq 2$, then with $S = V(\mathcal{H}) \setminus T$ the equation (3.1c) for $\mathcal{H}$ simplifies to

$$\prod_{h \in T} \left(\sum_{h'' \in S} e^*_{h''h} \right) = 0.$$

For each $h \in T$, the h' (defined above) is in S, so the summand $e^*_{h''h} = e^*_{hh'} = 1$ for $h'' = h'$. All other summands are either 0 or 1, hence each sum $\sum_{h'' \in S} e^*_{h''h}$ is at least one, so in particular non-zero. This is again a contradiction.

Hence for all $n_{\mathcal{G}} \geq 1$ our assumption was wrong, so z^* is a zero of f. Now, Hilbert's Nullstellensatz (Theorem 2.4 and Remark 2.5) implies $f \in I_{\text{viz}}$, so (5.1) is satisfied.

Furthermore, (5.1) above can be rewritten as

$$\prod_{h \in T} (1 - x_{gh}) \equiv 0 \mod I_{\text{viz}}.$$

Therefore, the congruence (5.2) follows from the fact that

$$\prod_{h \in T} (1 - x_{gh}) = \sum_{r=0}^{d+1} (-1)^r \sum_{\substack{U \subseteq T \\ |U|=r}} \prod_{h \in U} x_{gh}$$

holds. □

Remark 5.3. In particular for $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} \geq 1$, Lemma 5.2 implies

$$x_{gh} \equiv 1 \mod I_{\text{viz}}$$

for all $g \in V(\mathcal{G})$ and all $h \in V(\mathcal{H})$. For $k_{\mathcal{H}} = n_{\mathcal{H}} - 1$, Lemma 5.2 implies

$$x_{gh} x_{gh'} \equiv x_{gh} + x_{gh'} - 1 \mod I_{\text{viz}}$$

for all $g \in V(\mathcal{G})$ and all $\{h, h'\} \subseteq V(\mathcal{H})$. For $k_{\mathcal{H}} = n_{\mathcal{H}} - 2$, Lemma 5.2 implies

$$x_{gh} x_{gh'} x_{gh''} \equiv x_{gh} x_{gh'} + x_{gh'} x_{gh''} + x_{gh} x_{gh''} - x_{gh} - x_{gh'} - x_{gh''} + 1 \mod I_{\text{viz}}$$

for all $g \in V(\mathcal{G})$ and all $\{h, h', h''\} \subseteq V(\mathcal{H})$. △

Note that from a high-level point of view, if $k_{\mathcal{H}} = n_{\mathcal{H}} - d$, then Lemma 5.2 allows us to rewrite particular products of $d + 1$ terms as a sum of products of at most d terms and therefore to reduce the degree of polynomials.

To continue and in order to apply the above findings, we introduce the following polynomials.

Definition 5.4. Let $g \in V(\mathcal{G})$ and i be a non-negative integer. We define

$$\sigma_{g,i} = \sum_{\substack{S \subseteq V(\mathcal{H}) \\ |S|=i}} \prod_{h \in S} x_{gh}.$$

In a classical setting the polynomial $\sigma_{g,i}$ is the elementary symmetric polynomial of degree i in $n_{\mathcal{H}}$ variables. In the following we will investigate the arithmetic of the $\sigma_{g,i}$ over the ideal I_{viz} and aim for getting nice expressions for products of $\sigma_{g,i}$.

Lemma 5.5. *Let $k_{\mathcal{G}}, n_{\mathcal{G}}, k_{\mathcal{H}}, n_{\mathcal{H}} \geq 1$ and let $i \geq j$. Then*

$$\sigma_{g,i}\, \sigma_{g,j} \equiv \sum_{r=0}^{\min\{j, n_{\mathcal{H}} - i\}} \binom{j}{r} \binom{i+r}{j} \sigma_{g,i+r} \mod I_{\text{viz}}$$

holds.

Note that we can extend the summation range to $0 \leq r \leq j$ as $\sigma_{g,i} = 0$ for all $i > n_{\mathcal{H}}$. This makes the formulation of the lemma completely independent of the parameters $k_{\mathcal{G}}$, $n_{\mathcal{G}}$, $k_{\mathcal{H}}$ and $n_{\mathcal{H}}$. Moreover, we will see in the proof that we actually only need generators $x^2 - x$ in the ideal, making the lemma valid in a more general setting.

Remark 5.6. As needed later, we state Lemma 5.5 for some particular values of i and j. We have

$$\begin{aligned}\sigma_{g,1}^2 &\equiv \sigma_{g,1} + 2\sigma_{g,2} && \mod I_{\mathrm{viz}},\\ \sigma_{g,2}\sigma_{g,1} &\equiv 2\sigma_{g,2} + 3\sigma_{g,3} && \mod I_{\mathrm{viz}},\\ \sigma_{g,2}^2 &\equiv \sigma_{g,2} + 6\sigma_{g,3} + 6\sigma_{g,4} && \mod I_{\mathrm{viz}}. \quad \triangle\end{aligned}$$

Now we come back to the proof of Lemma 5.5. In the following, we use the phrase *power products* to refer to products of powers of variables with non-negative exponent, or in other words, to the summands of a polynomial without their coefficient.

Proof of Lemma 5.5. We start with a couple of remarks. All summands of $\sigma_{g,i}$ and $\sigma_{g,j}$ have degree i and j respectively. Hence all summands in the product $\sigma_{g,i}\sigma_{g,j}$ are summands of degree $i+j$. Furthermore, whenever two summands in $\sigma_{g,i}$ and $\sigma_{g,j}$ contain the same factor x_{gh}, a resulting factor x_{gh}^2 can be reduced to x_{gh} over I_{viz} because of (3.2a). Therefore, all summands in $\sigma_{g,i}\sigma_{g,j}$ are square-free and will have degree at least i and at most $i+j$. Clearly the degree is also bounded by $n_{\mathcal{H}}$. Moreover $\sigma_{g,i}$ and $\sigma_{g,j}$ are symmetric in $h \in V(\mathcal{H})$. By all these considerations, it is therefore possible to write

$$\sigma_{g,i}\,\sigma_{g,j} \equiv \sum_{r=0}^{\min\{j,n_{\mathcal{H}}-i\}} \delta_r \sigma_{g,i+r} \mod I_{\mathrm{viz}} \tag{5.4}$$

for some coefficients $\delta_r \in \mathbb{Z}$. In fact, these coefficients are non-negative.

For the following considerations, we always reduce modulo I_{viz}, therefore reducing exponents of monomials larger than one to exponents exactly one. So let us fix a power product x_i of $\sigma_{g,i}$ of degree i (i.e., $x_i = \prod_{h\in S} x_{gh}$ for some S with $|S| = i$) and count power products x_j of $\sigma_{g,j}$ so that the product $x_i x_j$ is of degree $i+r$ (as said, after reducing the power product over I_{viz}). Apparently, there have to be r factors in x_j which are not factors of x_i; there are $\binom{n_{\mathcal{H}}-i}{r}$ possible such choices. The remaining $j-r$ factors of x_j have to be among the factors of x_i, hence there are $\binom{i}{j-r}$ possible choices. Finally, we note that there are $\binom{n_{\mathcal{H}}}{i}$ choices for the fixed power product x_i above.

In total, expanding the product $\sigma_{g,i}\sigma_{g,j}$ results in a sum of $\binom{n_{\mathcal{H}}-i}{r}\binom{i}{j-r}\binom{n_{\mathcal{H}}}{i}$ power-products of degree $i+r$ for each r. We now collect these power products to determine the coefficients δ_r of the corresponding summand. Each sum $\sigma_{g,i+r}$ consists of $\binom{n_{\mathcal{H}}}{i+r}$ power products of degree $i+r$. Hence and due to the representation (5.4), we have

$$\delta_r = \binom{n_{\mathcal{H}}-i}{r}\binom{i}{j-r}\binom{n_{\mathcal{H}}}{i}\Big/\binom{n_{\mathcal{H}}}{i+r} = \frac{(i+r)!}{r!\,(j-r)!\,(i-j+r)!} = \binom{j}{r}\binom{i+r}{j},$$

which completes the proof. □

Lemma 5.5 allows us to replace products of our symmetric polynomials $\sigma_{g,i}$ by sums. This will become very handy in proving certificates.

We now go back to our particular set-up with $k_{\mathcal{H}} = n_{\mathcal{H}} - d$. The next important ingredient is the following lemma, which allows us to reduce some $\sigma_{g,d+j+1}$ of "high" degree.

Lemma 5.7. *Let $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d \geq 1$ for some $d \geq 1$. Let j be a non-negative integer. Then*

$$\sigma_{g,d+j+1} \equiv \binom{n_{\mathcal{H}}}{d+j+1} \sum_{r=0}^{d} \frac{\binom{d+1}{r}}{\binom{n_{\mathcal{H}}}{j+r}} (-1)^{d+r} \sigma_{g,j+r} \mod I_{\mathrm{viz}}$$

holds.

Proof. For each $\prod_{h\in S} x_{gh}$ in the definition of $\sigma_{g,d+j+1}$, we fix an arbitrary partition $S = T \cup W$ with T and W disjoint in a way that $|T| = d+1$ and $|W| = j$. Therefore, we obtain

$$\sigma_{g,d+j+1} = \sum_{\substack{S\subseteq V(\mathcal{H})\\ |S|=d+j+1}} \prod_{h\in S} x_{gh} = \sum_{\substack{T\cup W\subseteq V(\mathcal{H})\\ T,\,W \text{ disjoint}\\ |T|=d+1\\ |W|=j}} \Big(\prod_{h\in T} x_{gh}\Big)\Big(\prod_{h'\in W} x_{gh'}\Big).$$

With Lemma 5.2, we can reformulate this to

$$\sigma_{g,d+j+1} \equiv \sum_{\substack{T\cup W\subseteq V(\mathcal{H})\\ T,\,W \text{ disjoint}\\ |T|=d+1\\ |W|=j}} \sum_{r=0}^{d} (-1)^{d+r} \sum_{\substack{U\subseteq T\\ |U|=r}} \Big(\prod_{h\in T} x_{gh}\Big)\Big(\prod_{h'\in W} x_{gh'}\Big) \mod I_{\text{viz}}. \tag{5.5}$$

Due to symmetry in $h \in V(\mathcal{H})$, minimum degree j and maximum degree $d+j$ of the right-hand side, we can rewrite (5.5) to a representation

$$\sigma_{g,d+j+1} \equiv \sum_{r=0}^{d} (-1)^{d+r} \beta_r \sigma_{g,j+r} \mod I_{\text{viz}}$$

for some coefficients $\beta_r \in \mathbb{Z}$.

In order to determine these β_r, we count the number of power products of degree $j+r$ on the right-hand side of (5.5). There are $\binom{n_{\mathcal{H}}}{d+j+1}$ possible choices for S, only the one particular fixed partition $S = T \cup W$ and $\binom{d+1}{r}$ possible choices for U out of T. Hence there are $\binom{n_{\mathcal{H}}}{d+j+1}\binom{d+1}{r}$ power products of degree $j+r$ appearing in (5.5), all of which have the same sign. Due to the fact that $\sigma_{g,j+r}$ contains $\binom{n_{\mathcal{H}}}{j+r}$ monomials, this implies that

$$\beta_r = \binom{n_{\mathcal{H}}}{d+j+1}\binom{d+1}{r}\Big/\binom{n_{\mathcal{H}}}{j+r}. \quad \square$$

As mentioned, the lemmata above provide "reduction rules" for some quantities $\sigma_{g,i}$ or products of such quantities. We now derive explicit formulas for particular instances.

Remark 5.8. Suppose we have $d = 1$, i.e., our full set-up is $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1 \geq 1$. Then, because of Lemma 5.7 (with $d = 1$ and $j = 0$) and Lemma 5.5 (with $i = j = 1$, see also Remark 5.6), and because $\sigma_{g,0} = 1$, we have

$$\begin{aligned}\sigma_{g,2} &\equiv -\frac{1}{2} n_{\mathcal{H}}(n_{\mathcal{H}}-1)\sigma_{g,0} + (n_{\mathcal{H}}-1)\sigma_{g,1} = -\frac{1}{2} n_{\mathcal{H}}(n_{\mathcal{H}}-1) + (n_{\mathcal{H}}-1)\sigma_{g,1} \mod I_{\text{viz}}\\ \sigma_{g,1}^2 &\equiv \sigma_{g,1} + 2\sigma_{g,2} \equiv (2n_{\mathcal{H}}-1)\sigma_{g,1} - n_{\mathcal{H}}(n_{\mathcal{H}}-1) \mod I_{\text{viz}}. \qquad \triangle\end{aligned}$$

Remark 5.9. Suppose we have $d = 2$, i.e., our full set-up is $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 2 \geq 1$. Then, because of Lemma 5.7 and Lemma 5.5 (see also Remark 5.6) we have

$$\begin{aligned}\sigma_{g,3} &\equiv \frac{1}{3!\,(n_{\mathcal{H}}-3)!}\big(n_{\mathcal{H}}!\,\sigma_{g,0} - 3(n_{\mathcal{H}}-1)!\sigma_{g,1} + 6(n_{\mathcal{H}}-2)!\,\sigma_{g,2}\big)\\ &\equiv \tfrac{1}{6} n_{\mathcal{H}}(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2)\sigma_{g,0} - \tfrac{1}{2}(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2)\sigma_{g,1} + (n_{\mathcal{H}}-2)\sigma_{g,2} \mod I_{\text{viz}}\end{aligned}$$

and

$$\begin{aligned}\sigma_{g,4} &\equiv \frac{1}{4!\,(n_{\mathcal{H}}-4)!}\big((n_{\mathcal{H}}-1)!\,\sigma_{g,1} - 6(n_{\mathcal{H}}-2)!\,\sigma_{g,2} + 18(n_{\mathcal{H}}-3)!\,\sigma_{g,3}\big)\\ &\equiv \frac{1}{4!\,(n_{\mathcal{H}}-4)!}\big(3n_{\mathcal{H}}!\,\sigma_{g,0} - 8(n_{\mathcal{H}}-1)!\,\sigma_{g,1} + 12(n_{\mathcal{H}}-2)!\,\sigma_{g,2}\big)\\ &\equiv \tfrac{1}{8}n_{\mathcal{H}}(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2)(n_{\mathcal{H}}-3)\sigma_{g,0} - \tfrac{1}{3}(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2)(n_{\mathcal{H}}-3)\sigma_{g,1} +\\ &\qquad \tfrac{1}{2}(n_{\mathcal{H}}-2)(n_{\mathcal{H}}-3)\sigma_{g,2} \mod I_{\text{viz}}\end{aligned}$$

as well as

$$\begin{aligned}\sigma_{g,1}^2 &\equiv \sigma_{g,1} + 2\sigma_{g,2} \mod I_{\text{viz}}\\ \sigma_{g,2}\sigma_{g,1} &\equiv 2\sigma_{g,2} + 3\sigma_{g,3}\\ &\equiv \tfrac{1}{2}n_{\mathcal{H}}(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2)\sigma_{g,0} - \tfrac{3}{2}(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2)\sigma_{g,1} +\\ &\qquad (3n_{\mathcal{H}}-4)\sigma_{g,2} \mod I_{\text{viz}}\\ \sigma_{g,2}^2 &\equiv \sigma_{g,2} + 6\sigma_{g,3} + 6\sigma_{g,4}\\ &\equiv \tfrac{1}{4}(3n_{\mathcal{H}}-5)n_{\mathcal{H}}(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2)\sigma_{g,0} - (2n_{\mathcal{H}}-3)(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2)\sigma_{g,1} +\\ &\qquad (1+3(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2))\sigma_{g,2} \mod I_{\text{viz}}.\end{aligned}$$

As usual, we have $\sigma_{g,0} = 1$ everywhere. △

Remark 5.10. Let us fix d, i.e., our full set-up is $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d \geq 1$, and let us fix $g \in V(\mathcal{G})$.

Then, more systematically speaking, whenever f is a finite $\mathbb{K}$-linear combination of terms of the form $\sigma_{g,i}$ and $\sigma_{g,i}\sigma_{g,j}$ for non-negative integers i and j, we can reduce f to a form

$$f \equiv \sum_{i=0}^{d} \phi_i \sigma_{g,i} \mod I_{\text{viz}}$$

for efficiently computable $\phi_i \in \mathbb{K}$.

The idea is to use Lemma 5.5 for $\sigma_{g,i}\sigma_{g,j}$ in order to get rid of these products and replace them by terms of the form $\sigma_{g,i}$. After this step, one can repeatedly use Lemma 5.2 in order to replace all $\sigma_{g,i}$ for $i > d$ by linear combinations of $\sigma_{g,i}$ with $i \leq d$. All these operations are efficient; the coefficients of the individual steps are given directly in Lemmata 5.5 and 5.2. △

Finally let us mention that an implementation of the arithmetic described in the previous remark, for example with SageMath The SageMath Developers (2019), is handy: It makes it easily possible to verify the results of Remarks 5.8 and 5.9.

This completes the section on our auxiliary results which we need in the following to prove our certificates.

5.2. Certificates for $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}}$

The easiest and almost trivial case is the one with $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}}$, so $d = 0$. We get the following certificate and therefore have proven with our method that Vizing's conjecture holds in this case.

Theorem 5.11. *For $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} \geq 1$, Vizing's conjecture is true as the polynomials*

$$s_g = 0 \quad \text{for } g \in V(\mathcal{G})$$

are a 0-sos certificate of f_{viz}.

Note that we can simplify this 0-sos certificate of Theorem 5.11 to an empty sum using no polynomial, but we give the formulation of Theorem 5.11 to highlight the similarity to the other certificates we will present in this section.

Proof of Theorem 5.11. We have $x_{gh} \equiv 1 \mod I_{\text{viz}}$ for all $g \in V(\mathcal{G})$ and $h \in V(\mathcal{H})$ as already mentioned in Remark 5.3 due to Lemma 5.2. Hence we obtain

$$f_{\text{viz}} = -k_{\mathcal{G}} k_{\mathcal{H}} + \sum_{g \in V(\mathcal{G})} \sum_{h \in V(\mathcal{H})} x_{gh} \equiv -k_{\mathcal{G}} k_{\mathcal{H}} + n_{\mathcal{G}} n_{\mathcal{H}} = 0 = \sum_{g \in V(\mathcal{G})} s_g^2 \mod I_{\text{viz}},$$

so the s_g form indeed a 0-sos certificate for f_{viz}. □

Note that the certificate of Theorem 5.11 has the lowest degree possible.

5.3. Certificates for $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1$

The easiest non-trivial case is the one with $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1$, so $d = 1$. Using the above machinery (explained in the methodology Section 4) we first found a complicated sum-of-squares certificate, which is presented in Appendix A.1. We were eventually able to transform this complicated certificate to the following much easier certificate and therefore have proven with our method that Vizing's conjecture holds in this case.

Theorem 5.12. *For $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1 \geq 1$, Vizing's conjecture is true as the polynomials*

$$s_g = \left(\sum_{h \in V(\mathcal{H})} x_{gh} \right) - (n_{\mathcal{H}} - 1) \quad \text{for } g \in V(\mathcal{G})$$

are a 1-sos certificate of f_{viz}.

Proof. The polynomials s_g can alternatively be written as $s_g = \sigma_{g,1} - (n_{\mathcal{H}} - 1)$. Using Remark 5.8 yields

$$\begin{aligned} s_g^2 &= (\sigma_{g,1} - (n_{\mathcal{H}} - 1))^2 = \sigma_{g,1}^2 - 2(n_{\mathcal{H}} - 1)\sigma_{g,1} + (n_{\mathcal{H}} - 1)^2 \\ &\equiv (2n_{\mathcal{H}} - 1)\sigma_{g,1} - n_{\mathcal{H}}(n_{\mathcal{H}} - 1) - 2(n_{\mathcal{H}} - 1)\sigma_{g,1} + (n_{\mathcal{H}} - 1)^2 \\ &= \sigma_{g,1} - (n_{\mathcal{H}} - 1) \mod I_{\text{viz}}. \end{aligned}$$

Consequently, this evaluates to

$$\sum_{g \in V(\mathcal{G})} s_g^2 = \sum_{g \in V(\mathcal{G})} \big(\sigma_{g,1} - (n_{\mathcal{H}} - 1)\big) = -n_{\mathcal{G}}(n_{\mathcal{H}} - 1) + \sum_{g \in V(\mathcal{G})} \sigma_{g,1} = f_{\text{viz}} \mod I_{\text{viz}},$$

so the s_g form indeed a 1-sos certificate for f_{viz}. □

Note that the certificate of Theorem 5.12 has the lowest positive degree possible and furthermore only uses very particular monomials of degree at most 1.

5.4. Certificates for $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 2$

The next slightly more difficult case is the one for $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 2$, so $d = 2$. Also in this case we first found a more complicated certificate (see Appendix A.2) which we were able to transform to the following simple certificate.

Theorem 5.13. *For $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 2 \geq 1$, Vizing's conjecture is true as the polynomials*

$$s_g = \alpha + \beta\Big(\sum_{h \in V(\mathcal{H})} x_{gh}\Big) + \gamma\Big(\sum_{\{h,h'\} \subseteq V(\mathcal{H})} x_{gh} x_{gh'}\Big) \quad \text{for } g \in V(\mathcal{G}),$$

where

$$\begin{aligned}
\alpha &= (n_{\mathcal{H}} - 2)\big(n_{\mathcal{H}} + \tfrac{1}{2}(n_{\mathcal{H}} - 1)\sqrt{2}\big),\\
\beta &= -\big((2n_{\mathcal{H}} - 3) + (n_{\mathcal{H}} - 2)\sqrt{2}\big),\\
\gamma &= 2 + \sqrt{2},
\end{aligned}$$

are a 2-sos certificate of f_{viz}.

Remark 5.14. We want to point out that Theorem 5.13 is true whenever α, β, γ are solutions to the system of equations

$$\begin{aligned}
-(n_{\mathcal{H}} - 2) &= \alpha^2 + \frac{1}{4} n_{\mathcal{H}}(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)(3n_{\mathcal{H}} - 5)\gamma^2 \\
&\quad + n_{\mathcal{H}}(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\beta\gamma, && \text{(5.6a)}\\
1 &= \beta^2 + 2\alpha\beta - (n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)(2n_{\mathcal{H}} - 3)\gamma^2 \\
&\quad - 3(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\beta\gamma, && \text{(5.6b)}\\
0 &= 2\beta^2 + 2\alpha\gamma + (1 + 3(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2))\gamma^2 \\
&\quad + 2(3n_{\mathcal{H}} - 4)\beta\gamma, && \text{(5.6c)}
\end{aligned}$$

and that in Theorem 5.13 one particular easy solution is stated. △

Proof of Theorem 5.13. The polynomials s_g can alternatively be written as $s_g = \alpha\sigma_{g,0} + \beta\sigma_{g,1} + \gamma\sigma_{g,2}$. (Note that $\sigma_{g,0} = 1$.) Using Remark 5.8 yields

$$\begin{aligned}
s_g^2 &= (\alpha + \beta\sigma_{g,1} + \gamma\sigma_{g,2})^2\\
&= \alpha^2 + \beta^2\sigma_{g,1}^2 + \gamma^2\sigma_{g,2}^2 + 2\alpha\beta\sigma_{g,1} + 2\alpha\gamma\sigma_{g,2} + 2\beta\gamma\sigma_{g,1}\sigma_{g,2}\\
&\equiv \alpha^2 + \beta^2(\sigma_{g,1} + 2\sigma_{g,2}) + 2\alpha\beta\sigma_{g,1} + 2\alpha\gamma\sigma_{g,2}\\
&\quad + \gamma^2\big(\tfrac{1}{4}(3n_{\mathcal{H}} - 5)n_{\mathcal{H}}(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\sigma_{g,0} - (2n_{\mathcal{H}} - 3)(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\sigma_{g,1}\\
&\qquad + (1 + 3(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2))\sigma_{g,2}\big)\\
&\quad + 2\beta\gamma\big(\tfrac{1}{2}n_{\mathcal{H}}(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\sigma_{g,0} - \tfrac{3}{2}(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\sigma_{g,1}\\
&\qquad + (3n_{\mathcal{H}} - 4)\sigma_{g,2}\big) \mod I_{\text{viz}}
\end{aligned}$$

and consequently, we evaluate to

$$\begin{aligned}
\sum_{g \in V(\mathcal{G})} s_g^2 \equiv\ & \big(\alpha^2 + \gamma^2 \tfrac{1}{4}(3n_{\mathcal{H}} - 5)n_{\mathcal{H}}(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\\
&\quad + \beta\gamma n_{\mathcal{H}}(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\big)\sum_{g \in V(\mathcal{G})} \sigma_{g,0}\\
&+ \big(\beta^2 + 2\alpha\beta - \gamma^2(2n_{\mathcal{H}} - 3)(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\\
&\quad - 3\beta\gamma(n_{\mathcal{H}} - 1)(n_{\mathcal{H}} - 2)\big)\sum_{g \in V(\mathcal{G})} \sigma_{g,1}
\end{aligned}$$

$$+\big(2\beta^2+2\alpha\gamma+\gamma^2(1+3(n_{\mathcal{H}}-1)(n_{\mathcal{H}}-2))$$
$$+2\beta\gamma(3n_{\mathcal{H}}-4)\big)\sum_{g\in V(\mathcal{G})}\sigma_{g,2}\mod I_{\text{viz}}.$$

Due to the particular values of α, β and γ this simplifies to

$$\sum_{g\in V(\mathcal{G})}s_g^2\equiv-(n_{\mathcal{H}}-2)\sum_{g\in V(\mathcal{G})}\sigma_{g,0}+\sum_{g\in V(\mathcal{G})}\sigma_{g,1}$$
$$=-n_{\mathcal{G}}k_{\mathcal{H}}+\sum_{g\in V(\mathcal{G})}\sigma_{g,1}=f_{\text{viz}}\mod I_{\text{viz}}.\quad\square$$

Note that for all computationally considered instances of the form $k_{\mathcal{G}}=n_{\mathcal{G}}$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-2$, the SDP for $\ell=1$ was infeasible, so for all of those instances there seems to be no 1-sos certificate and one really needs monomials of degree 2 in the s_i in order to obtain a certificate. Nevertheless, degree 2 is still very low. Furthermore also in this sum-of-squares certificate only very particular monomials are used; it can be considered sparse therefore. This is confirmed by the following example.

Example 5.15. If we consider the case $k_{\mathcal{G}}=n_{\mathcal{G}}=4$, $n_{\mathcal{H}}=5$ and $k_{\mathcal{H}}=3$, there are 432 monomials of degree at most 2 but the certificate of Theorem 5.13 uses only 61 of them. ◯

5.5. Computational certificates for $k_{\mathcal{G}}=n_{\mathcal{G}}$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-d$

When taking a closer look at the certificates in Theorem 5.11, Theorem 5.12 and Theorem 5.13, one can guess a structure from the certificates found so far. In particular there seems to be a d-sos certificate for the case $k_{\mathcal{G}}=n_{\mathcal{G}}$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-d$. Hence, at this point, we can formulate a conjecture which intuitively seems to be the "correct" generalization.

Conjecture 5.16. *For $k_{\mathcal{G}}=n_{\mathcal{G}}\geq 1$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-d\geq 1$ with $d\geq 0$, Vizing's conjecture is true as the polynomials*

$$s_g=\sum_{i=0}^{d}\alpha_i\Bigg(\sum_{\substack{S\subseteq V(\mathcal{H})\\|S|=i}}\prod_{h\in S}x_{gh}\Bigg)\quad\text{for } g\in V(\mathcal{G}),$$

where α_i are the solutions to a certain system of polynomial equations, are a d-sos certificate of f_{viz}.

Moreover, the proofs of Theorems 5.12 and 5.13 give rise to an algorithmic approach for finding certificates. We formulate this as the following proposition.

Proposition 5.17. *Let d be a non-negative integer. Then there is an algorithm that either finds a certificate of the form as given in Conjecture 5.16 or outputs that there is no certificate of that form.*

Proof. We first describe our algorithm by following the proofs of Theorems 5.12 and 5.13.

Suppose s_g is of the form as given in Conjecture 5.16, so

$$s_g=\sum_{i=0}^{d}\alpha_i\sigma_{g,i}\quad\text{for } g\in V(\mathcal{G}),$$

where simply the definition of $\sigma_{g,i}$ (see Definition 5.4) was used. We now use binomial expansion for s_g^2. In the result there will be terms of the form $\sigma_{g,i}\sigma_{g,j}$ for $i,j\leq d$. We can now use the arithmetic described in Remark 5.10 to end up with

$$s_g^2 \equiv \sum_{i=0}^{d} \phi_i(\alpha)\, \sigma_{g,i} \mod I_{\text{viz}} \quad \text{for } g \in V(\mathcal{G}).$$

Here, $\phi_i(\alpha)$ is a polynomial in $\alpha = (\alpha_0, \ldots, \alpha_d)$ for each $0 \leq i \leq d$. Note that all coefficients of this polynomial additionally depend on the variable $n_{\mathcal{H}}$. The formal summation over all $g \in V(\mathcal{G})$ is trivial; we obtain

$$\sum_{g \in V(\mathcal{G})} s_g^2 \equiv \sum_{i=0}^{d} \phi_i(\alpha) \sum_{g \in V(\mathcal{G})} \sigma_{g,i} \mod I_{\text{viz}}.$$

In order to obtain a d-sos certificate, this has to be equal to

$$f_{\text{viz}} = -(n_{\mathcal{H}} - d) \sum_{g \in V(\mathcal{G})} \sigma_{g,0} + \sum_{g \in V(\mathcal{G})} \sigma_{g,1}.$$

Comparing the coefficients of $n_{\mathcal{G}} = \sum_{g \in V(\mathcal{G})} \sigma_{g,0}$ and the other $\sum_{g \in V(\mathcal{G})} \sigma_{g,i}$ (for $1 \leq i \leq d$) yields the system of equations

$$\phi_0(\alpha) = -(n_{\mathcal{H}} - d), \tag{5.7a}$$

$$\phi_1(\alpha) = 1, \tag{5.7b}$$

$$\phi_i(\alpha) = 0 \quad \text{for } 2 \leq i \leq d. \tag{5.7c}$$

We want to point out that the existence of a real-valued solution $\alpha_0, \ldots, \alpha_d$ (as functions in $n_{\mathcal{H}}$) is equivalent to the fact that to the s_g being as in Conjecture 5.16 form a d-sos certificate. Therefore computing the variety associated to the system of equations (5.7), i.e., finding all solutions of this system, is the last step of an algorithm that has the properties stated in Proposition 5.17, and the proof is completed. □

Remark 5.18. The system of equations (5.7) does not depend on $n_{\mathcal{G}}$, but only on d and $n_{\mathcal{H}}$. Hence, whenever we find a solution to (5.7)—this might be for a fixed value of $n_{\mathcal{H}}$ or parametrized in $n_{\mathcal{H}}$—then this gives rise to a certificate for those values and *all* possible values of $n_{\mathcal{G}} = k_{\mathcal{G}}$. △

Before we exploit the algorithm provided by Proposition 5.17 which finds a certificate of the form as given in Conjecture 5.16, let us mention that it consists of two main steps: The first step is to construct the system of equations (5.7) and the second is to find a solution to this system of equations.

Let us reconsider the proofs of Theorems 5.12 and 5.13. There, we already have a particular certificate at hand, and we prove that it is in fact a certificate by performing essentially the first main step of the algorithm. In fact the system of equations (5.6) corresponds to (5.7) for $d = 2$ as the variables (α, β, γ) (of (5.6)) equal $(\alpha_0, \alpha_1, \alpha_2)$ (of (5.7)). Even though the computations for proving the theorems above are tedious, they are straightforward.

So, let us come back to the algorithm of Proposition 5.17. For finding a certificate for general $d \geq 3$ the situation is more difficult: The computations get very messy, so it seems infeasible to get the system of equations (5.7) in closed form depending on the parameter d. Moreover, even for the case $d = 2$ it is not obvious that the system of equations (5.6) even has a solution. Still, we want to use Proposition 5.17 for obtaining more certificates, so let us consider the cases $d = 1$ and $d = 2$ once more, but this time with the help of SageMath The SageMath Developers (2019).

Using the algorithm provided in the proof of Proposition 5.17 allows to reprove Theorems 5.12 and 5.13 computationally with SageMath. It turns out that the variety of the system of equations (5.7), whose points are the solutions $(\alpha_0, \ldots, \alpha_d)$ of (5.7), is of dimension 1 which means that the dependency on $n_{\mathcal{H}}$ is the only dependency on a free parameter. For $d = 1$, the solution is essentially unique (except for the obvious replacement of s_g by $-s_g$). For $d = 2$, in the solution presented in Theorem 5.13 we can additionally replace each occurrence of $\sqrt{2}$ in any of (α, β, γ) by $-\sqrt{2}$ and obtain

another solution. In other words we can choose the signs of $\pm\sqrt{1}$ and $\pm\sqrt{2}$. This observation will be revisited in Remark 5.22.

In the same manner and with a lot of patience, we can let the algorithm run for $d = 3$ and get the result presented as Theorem 5.20 below. However, the computation can be speeded up in the following way. This will allow to also cover the case $d = 4$.

Remark 5.19. Suppose that the coefficients $\alpha_0, \ldots, \alpha_d$ are polynomials in $n_{\mathcal{H}}$ with degrees bounded by d. (This is the case for Theorems 5.12 and 5.13, so this assumption is reasonable.) Then, by fixing a particular value for $n_{\mathcal{H}}$, the time of the computation of the $\alpha_0, \ldots, \alpha_d$ is now dramatically reduced. Doing this for $d+1$ different values $n_{\mathcal{H}}$ allows to compute the coefficients $\alpha_0, \ldots, \alpha_d$ as interpolation polynomials in $n_{\mathcal{H}}$.

It should be noted that this interpolation trick is technically/computationally not as innocent as one might think: One has to carefully choose the values $n_{\mathcal{H}}$ in order to "keep track" of the branch of one particular solution, as the solution of (5.7) is not unique. △

By using the strategy explained in the previous remark, we are able to show the following.

Theorem 5.20. *For $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 3 \geq 1$, Vizing's conjecture is true as the polynomials*

$$s_g = \sum_{i=0}^{3} \alpha_i \sigma_{g,i} \quad \text{for } g \in V(\mathcal{G}),$$

where

$$\begin{aligned}
\alpha_0 &= -\tfrac{1}{6} n_{\mathcal{H}}^3 \left(\sqrt{3} + 3\sqrt{2} + 3\right) + \tfrac{1}{2} n_{\mathcal{H}}^2 \left(2\sqrt{3} + 5\sqrt{2} + 4\right) \\
&\quad - \tfrac{1}{2} n_{\mathcal{H}} \left(\tfrac{11}{3}\sqrt{3} + 6\sqrt{2} + 3\right) + \sqrt{3}, \\
\alpha_1 &= +\tfrac{1}{2} n_{\mathcal{H}}^2 \left(\sqrt{3} + 3\sqrt{2} + 3\right) - \tfrac{1}{2} n_{\mathcal{H}} \left(5\sqrt{3} + 13\sqrt{2} + 11\right) + 3\left(\sqrt{3} + 2\sqrt{2}\right) + 4, \\
\alpha_2 &= -n_{\mathcal{H}} \left(\sqrt{3} + 3\sqrt{2} + 3\right) + 3\sqrt{3} + 8\sqrt{2} + 7, \\
\alpha_3 &= \sqrt{3} + 3\sqrt{2} + 3,
\end{aligned}$$

are a 3-sos certificate of f_{viz}.

Proof. We apply the algorithm provided by Proposition 5.17 and Remark 5.19 and the claimed result follows. In particular we use SageMath The SageMath Developers (2019) in order to construct the system of equations (5.7) and to obtain a solution of it. □

Theorem 5.21. *For $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 4 \geq 1$, Vizing's conjecture is true as the polynomials*

$$s_g = \sum_{i=0}^{4} \alpha_i \sigma_{g,i} \quad \text{for } g \in V(\mathcal{G}),$$

where

$$\begin{aligned}
\alpha_0 &= \tfrac{1}{12} n_{\mathcal{H}}^4 \left(2\sqrt{3} + 3\sqrt{2} + 1\right) - \tfrac{1}{6} n_{\mathcal{H}}^3 \left(9\sqrt{3} + 12\sqrt{2} + 2\right) \\
&\quad + \tfrac{1}{12} n_{\mathcal{H}}^2 \left(52\sqrt{3} + 57\sqrt{2} - 7\right) - \tfrac{1}{6} n_{\mathcal{H}} \left(24\sqrt{3} + 18\sqrt{2} - 17\right) - 2, \\
\alpha_1 &= -\tfrac{1}{3} n_{\mathcal{H}}^3 \left(2\sqrt{3} + 3\sqrt{2} + 1\right) + \tfrac{1}{2} n_{\mathcal{H}}^2 \left(11\sqrt{3} + 15\sqrt{2} + 3\right) \\
&\quad - \tfrac{1}{6} n_{\mathcal{H}} \left(83\sqrt{3} + 99\sqrt{2} + 1\right) + 10\sqrt{3} + 10\sqrt{2} - 3,
\end{aligned}$$

$$\alpha_2 = n_{\mathcal{H}}^2\left(2\sqrt{3}+3\sqrt{2}+1\right) - n_{\mathcal{H}}\left(13\sqrt{3}+18\sqrt{2}+4\right) + 5\left(4\sqrt{3}+5\sqrt{2}\right)+2,$$
$$\alpha_3 = -2\,n_{\mathcal{H}}\left(2\sqrt{3}+3\sqrt{2}+1\right) + 15\sqrt{3}+21\sqrt{2}+5,$$
$$\alpha_4 = 4\sqrt{3}+6\sqrt{2}+2,$$

are a 4-sos certificate of f_{viz}.

Proof. We again use SageMath The SageMath Developers (2019) and apply the algorithm provided by Proposition 5.17 and Remark 5.19 to obtain the claimed certificate. □

It should be noted once more that once having algorithmically proven Theorems 5.20 and 5.21, verifying that those results indeed form a certificate—again this can be done computationally—is much easier.

Remark 5.22. Let us consider the set-up and certificate as presented in Conjecture 5.16 again. In particular, let us have a look at the coefficient α_d for various d. By using the certificates obtained in this Section 5, we may rewrite this coefficient as

$$\begin{aligned}
d=1\colon &\quad \alpha_1 = \sqrt{1},\\
d=2\colon &\quad \alpha_2 = \sqrt{2}+(1+1)\sqrt{1},\\
d=3\colon &\quad \alpha_3 = \sqrt{3}+(1+2)\sqrt{2}+(1+1+1)\sqrt{1},\\
d=4\colon &\quad \alpha_4 = \sqrt{4}+(1+3)\sqrt{3}+(1+2+3)\sqrt{2}+(1+1+1+1)\sqrt{1}.
\end{aligned}$$

We therefore ask the following question: Is it true that

$$\begin{aligned}
d=5\colon &\quad \alpha_5 = \sqrt{5}+(1+4)\sqrt{4}+(1+3+5)\sqrt{3}\\
&\qquad +(1+2+3+4)\sqrt{2}+(1+1+1+1+1)\sqrt{1},\\
d=6\colon &\quad \alpha_6 = \sqrt{6}+(1+5)\sqrt{5}+(1+4+7)\sqrt{4}+(1+3+5+7)\sqrt{3}\\
&\qquad +(1+2+3+4+5)\sqrt{2}+(1+1+1+1+1)\sqrt{1}
\end{aligned}$$

and more generally for given d that

$$\alpha_d = \sum_{i=0}^{d-1}\Big(\sum_{j=0}^{d-i-1}(1+ij)\Big)\sqrt{i+1} \tag{5.8}$$

is a choice for α_d in a certificate for Conjecture 5.16? If so, are *all* possible certificates given by choosing a sign for each square root $\pm\sqrt{i+1}$ in (5.8) (including the signs of expressions like $\sqrt{1}=1$ and $\sqrt{4}=2$, i.e., 2^d different solutions)? The latter turned out to be true for $d\in\{0,1,2,3,4\}$ by our computations. △

To summarize, in this section we have obtained certificates for the cases with $k_{\mathcal{G}}=n_{\mathcal{G}}\geq 1$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-d$ for $d\in\{0,1,2,3,4\}$ by our method. For $d\in\{0,1,2\}$ we have proven these results by hand, for $d\in\{3,4\}$ we have proven them computationally. We will continue to prove the correctness of certain certificates in the next section.

6. Exact certificates for $k_{\mathcal{G}}=n_{\mathcal{G}}-1$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-1$ with $n_{\mathcal{H}}\in\{2,3\}$

In this section we will finally prove Theorem 4.6 and therefore obtain a certificate for the case $k_{\mathcal{G}}=n_{\mathcal{G}}-1\geq 1$, $n_{\mathcal{H}}=3$ and $k_{\mathcal{H}}=2$. As a byproduct we will also obtain a certificate for the case $k_{\mathcal{G}}=n_{\mathcal{G}}-1\geq 1$, $n_{\mathcal{H}}=2$ and $k_{\mathcal{H}}=1$. Towards that end we will use some of the results of Section 5.1 and derive further results of a similar nature.

6.1. Auxiliary results

We start with the following lemma.

Lemma 6.1. *Let $k_{\mathcal{G}} = n_{\mathcal{G}} - 1 \geq 1$. Then $e_{gg'} \in I_{\mathcal{G}} \subseteq I_{\text{viz}}$ holds for all $\{g, g'\} \subseteq D_{\mathcal{G}}$.*

This lemma is equivalent to $e_{gg'} \equiv 0 \mod I_{\mathcal{G}}$ and $e_{gg'} \equiv 0 \mod I_{\text{viz}}$ for all $\{g, g'\} \subseteq D_{\mathcal{G}}$.

Lemma 6.1 is plausible from a graph theoretical point of view. Indeed, due to Theorem 3.4 the points in the variety of $I_{\mathcal{G}}$ are in bijection to the graphs in $\mathcal{G}$, which are the graphs on $n_{\mathcal{G}}$ vertices with domination number $k_{\mathcal{G}} = n_{\mathcal{G}} - 1$ and a minimum dominating set $D_{\mathcal{G}}$. Clearly in such graphs there are no edges between any two vertices of $D_{\mathcal{G}}$, because if there would be such an edge, the domination number would decrease. Hence, for each point in the variety of I_{viz}, we have that the component $e^*_{gg'}$ is zero for every $\{g, g'\} \subseteq D_{\mathcal{G}}$.

Proof of Lemma 6.1. For $k_{\mathcal{G}} = n_{\mathcal{G}} - 1 = 1$ there is no $\{g, g'\} \subseteq D_{\mathcal{G}}$, so there is nothing to prove.

Let $\{g, g'\} \subseteq D_{\mathcal{G}}$. We apply Hilbert's Nullstellensatz on the polynomial $f = e_{gg'}$. We have $k_{\mathcal{G}} = n_{\mathcal{G}} - 1$, therefore $|V(\mathcal{G}) \setminus D_{\mathcal{G}}| = 1$, and so let $\{\hat{g}\} = V(\mathcal{G}) \setminus D_{\mathcal{G}}$. Then clearly $g \neq \hat{g}$ and $g' \neq \hat{g}$.

We use Notation 3.2. Let $z^* \in \mathcal{V}(I_{\mathcal{G}})$, so z^* is a common zero of (3.1a), (3.1b) and (3.1c). We assume that z^* is not a zero of $f = e_{gg'}$.

Let us set $S = S_g = \{\tilde{g} \in D_{\mathcal{G}} : \tilde{g} \neq g\}$. Then, due to (3.1c) we have

$$\left(\sum_{\tilde{g} \in S_g} e^*_{\tilde{g}g}\right)\left(\sum_{\tilde{g} \in S_g} e^*_{\tilde{g}\hat{g}}\right) = 0 \tag{6.1}$$

and conclude that one of the two factors has to be zero.

Due to (3.1a), all $e^*_{\tilde{g}g}$ and $e^*_{\tilde{g}\hat{g}}$ appearing in (6.1) are in $\{0, 1\}$, and moreover $e^*_{gg'} \in \{0, 1\}$. Then $e^*_{gg'} = 1$ (as it is assumed to be non-zero), and, because $g' \in S_g$, the first factor of (6.1) is non-zero. Therefore the second factor of (6.1) must be zero and hence $e^*_{\tilde{g}\hat{g}} = 0$ for all $\tilde{g} \in S_g$.

By symmetry (switching the roles of g and g'), we obtain $e^*_{\tilde{g}\hat{g}} = 0$ for all $\tilde{g} \in S_{g'}$ and therefore get $e^*_{\tilde{g}\hat{g}} = 0$ for all $\tilde{g} \in S_g \cup S_{g'} = D_{\mathcal{G}}$. Thus,

$$\prod_{\tilde{g} \in D_{\mathcal{G}}} (1 - e^*_{\tilde{g}\hat{g}}) = 1,$$

but due to (3.1b) this product should be zero; a contradiction. Hence z^* is also a zero of $f = e_{gg'}$, and Hilbert's Nullstellensatz (Theorem 2.4 and Remark 2.5) implies that $f = e_{gg'} \in I_{\mathcal{G}}$. □

In particular we will need the following consequence of Lemma 6.1.

Corollary 6.2. *Let $k_{\mathcal{G}} = n_{\mathcal{G}} - 1 \geq 1$. Then $e_{g_1g_2}e_{g_3g_4} \in I_{\mathcal{G}} \subseteq I_{\text{viz}}$ holds for all $\{g_1, g_2\}, \{g_3, g_4\} \subseteq V(\mathcal{G})$ with $\{g_1, g_2\} \neq \{g_3, g_4\}$.*

Note that also Corollary 6.2 can be explained from a graph theoretic point of view. To be precise there can be only one edge in a graph on $n_{\mathcal{G}}$ vertices with domination number $n_{\mathcal{G}} - 1$, because an additional edge would decrease the domination number. Therefore, for each point in the variety of $I_{\mathcal{G}}$, the product of components corresponding to two different edge variables has always to be equal to 0 due to Theorem 3.4.

Proof of Corollary 6.2. If $\{g_1, g_2\} \subseteq D_{\mathcal{G}}$ or $\{g_3, g_4\} \subseteq D_{\mathcal{G}}$ the result follows from Lemma 6.1 because then $e_{g_1g_2} \in I_{\mathcal{G}}$ or $e_{g_3g_4} \in I_{\mathcal{G}}$. Hence we only have to consider the case $\{g_1, g_2\} \nsubseteq D_{\mathcal{G}}$ and $\{g_3, g_4\} \nsubseteq$

$D_{\mathcal{G}}$. Let $\{\hat{g}\} = V(\mathcal{G}) \setminus D_{\mathcal{G}}$, then without loss of generality this case is equivalent to $g_1 = g_3 = \hat{g}$ and $g_2 \neq g_4$.

We use Hilbert's Nullstellensatz like in Lemma 6.1 to prove the statement. Let $z^* \in \mathcal{V}(I_{\mathcal{G}})$ be a common zero of (3.1a), (3.1b) and (3.1c). If we can prove that z^* is also a zero of $f = e_{\hat{g}g_2} e_{\hat{g}g_4}$ we are done.

For $S = V(\mathcal{G}) \setminus \{g_2, g_4\}$, (3.1c) implies

$$\left(\sum_{g \in S} e^*_{gg_2}\right)\left(\sum_{g \in S} e^*_{gg_4}\right) = 0,$$

so one of these two factors has to be zero; without loss of generality (due to symmetry in g_2 and g_4), let us assume the first factor. As $e^*_{\tilde{g}g_2} \in \{0, 1\}$ for all $\tilde{g} \in V(\mathcal{G})$ by (3.1a), we then have in fact $e^*_{\tilde{g}g_2} = 0$ for all $\tilde{g} \in V(\mathcal{G})$. In particular we have $e^*_{\hat{g}g_2} = 0$ because $\hat{g} \in S$. This is what we wanted to show. □

We need Corollary 6.2 in order to prove the next result.

Lemma 6.3. *Let $k_{\mathcal{G}} = n_{\mathcal{G}} - 1 \geq 1$, $n_{\mathcal{H}} \in \{2, 3\}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1$. Then*

$$(1 - x_{gh_1})(1 - x_{gh_2})(1 - x_{g'h_3})(1 - x_{g'h_4}) \in I_{\text{viz}}$$

for $\{g, g'\} \subseteq V(\mathcal{G})$ and for $\{h_1, h_2\}, \{h_3, h_4\} \subseteq V(\mathcal{H})$.

Note that it would again be possible to justify Lemma 6.3 in terms of graph theory using Theorem 3.8. It would need a case distinction for $n_{\mathcal{H}} = 2$ and $n_{\mathcal{H}} = 3$ and several more case distinctions on whether g, $g' \in D_{\mathcal{G}}$, whether h_1, h_2, h_3, $h_4 \in D_{\mathcal{H}}$ and on the cardinality of $\{h_1, h_2, h_3, h_4\}$. We refrain from presenting the details here.

Proof of Lemma 6.3. First observe that without loss of generality we can assume that $g \in D_{\mathcal{G}}$, as $|D_{\mathcal{G}}| = n_{\mathcal{G}} - 1$ and therefore not both of g and g' can be in $V(\mathcal{G}) \setminus D_{\mathcal{G}}$. For notational convenience let $\{\hat{g}\} = V(\mathcal{G}) \setminus D_{\mathcal{G}}$, and note that g' might or might not be equal to $\hat{g}$.

Next observe that without loss of generality $h_4 = h_1$, because $n_{\mathcal{H}} \in \{2, 3\}$, and $h_1 \neq h_2$ and $h_3 \neq h_4$ by assumption. We obtain that the sets $\{h_1, h_2\}$ and $\{h_3, h_4\}$ are both of cardinality 2 and not disjoint.

In order to prove Lemma 6.3 we will use Hilbert's Nullstellensatz for $f = (1 - x_{gh_1})(1 - x_{gh_2})(1 - x_{g'h_1})(1 - x_{g'h_3})$ analogously as it has been done in the proofs of Lemma 6.1 and Corollary 6.2. Note that we use Notation 3.7. Towards that end let $z^* \in \mathcal{V}(I_{\text{viz}})$, i.e., z^* is a common zero of (3.1a), (3.1b) and (3.1c) for both $\mathcal{G}$ and $\mathcal{H}$ and of (3.2a) and (3.2b). Due to (3.1a) and (3.2a) all of $e^*_{gg'}$, $e^*_{hh'}$ and x^*_{gh} are either 0 or 1.

Assume that z^* is not a zero of f, then $x^*_{gh_1} = x^*_{gh_2} = x^*_{g'h_1} = x^*_{g'h_3} = 0$. Furthermore, as $g \in D_{\mathcal{G}}$ we have $e^*_{g\tilde{g}} = 0$ for all $\tilde{g} \in D_{\mathcal{G}}$ by Lemma 6.1.

Now we distinguish the two cases $n_{\mathcal{H}} = 2$ and $n_{\mathcal{H}} = 3$. For $n_{\mathcal{H}} = 2$ the above condition $e^*_{g\tilde{g}} = 0$ for all $\tilde{g} \in D_{\mathcal{G}}$ together with (3.2b) for the vertices gh_1 and gh_2 of the box graph class imply

$$1 - e^*_{g\hat{g}} x^*_{\hat{g}h_1} = 0 \quad \text{and} \quad 1 - e^*_{g\hat{g}} x^*_{\hat{g}h_2} = 0,$$

so $e^*_{g\hat{g}} = x^*_{\hat{g}h_1} = x^*_{\hat{g}h_2} = 1$ holds. Note that for $n_{\mathcal{H}} = 2$ we have $\{h_1, h_2\} = \{h_3, h_4\}$, so $\hat{g} \neq g'$ and hence $g' \in D_{\mathcal{G}}$ because $x^*_{g'h_1} = 0$. Then (3.2b) for $g'h_1$ and $g'h_3$ yields

$$1 - e^*_{g'\hat{g}} x^*_{\hat{g}h_1} = 0 \quad \text{and} \quad 1 - e^*_{g'\hat{g}} x^*_{\hat{g}h_3} = 0$$

and hence $e^*_{g'\hat{g}} = x^*_{\hat{g}h_1} = x^*_{\hat{g}h_3} = 1$. But due to Corollary 6.2 and $e^*_{g\hat{g}} = 1$ we have $e^*_{g'\hat{g}} = 0$, a contradiction. Hence the lemma holds for $n_{\mathcal{H}} = 2$.

Next we consider the case $n_{\mathcal{H}} = 3$. Here we let $\{h\} = V(\mathcal{H}) \setminus \{h_1, h_2\}$ and let $\{h'\} = V(\mathcal{H}) \setminus \{h_1, h_3\}$. Together with (3.2b) for the box graph class vertices gh_1 and gh_2, the above derived fact $e^*_{g\tilde{g}} = 0$ for all $\tilde{g} \in D_{\mathcal{G}}$ yields

$$(1 - e^*_{g\hat{g}} x^*_{\hat{g}h_1})(1 - e^*_{h_1h} x^*_{gh}) = 0 \quad \text{and} \tag{6.2a}$$

$$(1 - e^*_{g\hat{g}} x^*_{\hat{g}h_2})(1 - e^*_{h_2h} x^*_{gh}) = 0. \tag{6.2b}$$

If $e^*_{g\hat{g}} = 0$, then (6.2a) and (6.2b) imply $x^*_{gh} = 1$ and $e^*_{h_1h} = e^*_{h_2h} = 1$, which is a contradiction to Corollary 6.2. So $e^*_{g\hat{g}} = 1$ holds. Now we will distinguish the two cases $g' \neq \hat{g}$ and $g' = \hat{g}$.

Case $g' \neq \hat{g}$. We have $g' \in D_{\mathcal{G}}$ and can deduce from (3.2b) for $g'h_1$ and $g'h_3$ analogously as for g that

$$(1 - e^*_{g'\hat{g}} x^*_{\hat{g}h_1})(1 - e^*_{h_1h'} x^*_{g'h'}) = 0 \quad \text{and} \tag{6.3a}$$

$$(1 - e^*_{g'\hat{g}} x^*_{\hat{g}h_3})(1 - e^*_{h_3h'} x^*_{g'h'}) = 0. \tag{6.3b}$$

Due to Corollary 6.2 and $e^*_{g\hat{g}} = 1$ we have $e^*_{g'\hat{g}} = 0$. Therefore (6.3a) and (6.3b) imply that $e^*_{h_1h'} = e^*_{h_3h'} = 1$, which is a contradiction to Corollary 6.2. So in this case z^* is also a zero of f and hence $f \in I_{\text{viz}}$ holds because of Hilbert's Nullstellensatz.

Case $g' = \hat{g}$. Due to Corollary 6.2 and $e^*_{g\hat{g}} = 1$ we can deduce that $e^*_{g'\tilde{g}} = 0$ for all $\tilde{g} \in V(\mathcal{G}) \setminus \{g\}$. Therefore (3.2b) for the vertices $g'h_1$ and $g'h_3$ of the box graph class become

$$(1 - e^*_{g\hat{g}} x^*_{gh_1})(1 - e^*_{h_1h'} x^*_{\hat{g}h'}) = 0 \quad \text{and} \tag{6.4a}$$

$$(1 - e^*_{g\hat{g}} x^*_{gh_3})(1 - e^*_{h_3h'} x^*_{\hat{g}h'}) = 0. \tag{6.4b}$$

We have $x^*_{\hat{g}h_1} = x^*_{gh_1} = 0$, so from (6.2a) and (6.4a) it follows that $x^*_{gh} = x^*_{\hat{g}h'} = 1$ and $e^*_{h_1h} = e^*_{h_1h'} = 1$. Corollary 6.2 applied on the graph class $\mathcal{H}$ implies $h = h'$ and therefore also $h_2 = h_3$ holds. Furthermore, this corollary also implies that $e^*_{h_2h} = 0$, and hence $x^*_{\hat{g}h_2} = 1$ because of (6.2b). But this is a contradiction because $x^*_{\hat{g}h_2} = x^*_{g'h_3} = 0$. So also in this case z^* is a zero of f and therefore $f \in I_{\text{viz}}$ holds. □

Remark 6.4. In particular for $k_{\mathcal{G}} = n_{\mathcal{G}} - 1$, $n_{\mathcal{H}} \in \{2, 3\}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1$, Lemma 6.3 implies

$$\begin{aligned} x_{gh_1}x_{gh_2}x_{g'h_3}x_{g'h_4} \equiv\ & x_{gh_1}x_{gh_2}x_{g'h_3} + x_{gh_1}x_{gh_2}x_{g'h_4} + x_{gh_1}x_{g'h_3}x_{g'h_4} + x_{gh_2}x_{g'h_3}x_{g'h_4} \\ & - x_{gh_1}x_{gh_2} - x_{gh_1}x_{g'h_3} - x_{gh_2}x_{g'h_3} \\ & - x_{gh_1}x_{g'h_4} - x_{gh_2}x_{g'h_4} - x_{g'h_3}x_{g'h_4} \\ & + x_{gh_1} + x_{gh_2} + x_{g'h_3} + x_{g'h_4} - 1 \mod I_{\text{viz}} \end{aligned}$$

for all $\{g, g'\} \subseteq V(\mathcal{G})$ and all $\{h_1, h_2\}, \{h_3, h_4\} \subseteq V(\mathcal{H})$. △

Next we will need some more polynomials in order to be able to cope with $\sigma_{g,i}$ in a better way.

Definition 6.5. Let i and j be two non-negative integers. We define

$$\tau_{i,j} = \sum_{g \in V(\mathcal{G})} \sum_{\substack{g' \in V(\mathcal{G}) \\ g' \neq g}} \sigma_{g,i}\sigma_{g',j}.$$

Observe that $\tau_{i,j} = \tau_{j,i}$ holds. As a next step we will use Lemma 6.3 in order to determine $\tau_{2,2}$.

Lemma 6.6. *Let $k_{\mathcal{G}} = n_{\mathcal{G}} - 1 \geq 1$, $n_{\mathcal{H}} \in \{2, 3\}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1$. Then*

$$\tau_{2,2} \equiv 2(n_{\mathcal{H}}-1)\tau_{2,1} - (n_{\mathcal{H}}-1)^2\tau_{1,1} - n_{\mathcal{H}}(n_{\mathcal{H}}-1)(n_{\mathcal{G}}-1)\sum_{g\in V(\mathcal{G})}\sigma_{g,2}$$
$$+ n_{\mathcal{H}}(n_{\mathcal{H}}-1)^2(n_{\mathcal{G}}-1)\sum_{g\in V(\mathcal{G})}\sigma_{g,1} - \frac{1}{4}n_{\mathcal{G}}(n_{\mathcal{G}}-1)n_{\mathcal{H}}^2(n_{\mathcal{H}}-1)^2 \mod I_{\text{viz}}.$$

Proof. By definition

$$\tau_{2,2} = \sum_{g\in V(\mathcal{G})}\sum_{\substack{g'\in V(\mathcal{G})\\ g'\neq g}}\sigma_{g,2}\sigma_{g',2}$$
$$= \sum_{g\in V(\mathcal{G})}\sum_{\substack{g'\in V(\mathcal{G})\\ g'\neq g}}\left(\sum_{\{h_1,h_2\}\subseteq V(\mathcal{H})} x_{gh_1}x_{gh_2}\right)\left(\sum_{\{h_3,h_4\}\subseteq V(\mathcal{H})} x_{g'h_3}x_{g'h_4}\right)$$

holds. By using Lemma 6.3 as stated in Remark 6.4 we obtain

$$\begin{aligned}\tau_{2,2} \equiv \sum_{g\in V(\mathcal{G})}\sum_{\substack{g'\in V(\mathcal{G})\\ g'\neq g}}\sum_{\substack{\{h_1,h_2\}\subseteq V(\mathcal{H})\\ \{h_3,h_4\}\subseteq V(\mathcal{H})}}\Big(&x_{gh_1}x_{gh_2}x_{g'h_3} + x_{gh_1}x_{gh_2}x_{g'h_4}\\ &+ x_{gh_1}x_{g'h_3}x_{g'h_4} + x_{gh_2}x_{g'h_3}x_{g'h_4}\\ &- x_{gh_1}x_{gh_2} - x_{gh_1}x_{g'h_3} - x_{gh_2}x_{g'h_3}\\ &- x_{gh_1}x_{g'h_4} - x_{gh_2}x_{g'h_4} - x_{g'h_3}x_{g'h_4}\\ &+ x_{gh_1} + x_{gh_2} + x_{g'h_3} + x_{g'h_4}\\ &- 1\Big) \mod I_{\text{viz}}.\end{aligned} \tag{6.5}$$

We can further reformulate (6.5) by using the following argument. The monomials $x_{gh_1}x_{gh_2}x_{g'h_3}$ and $x_{gh_1}x_{gh_2}x_{g'h_4}$ in (6.5) are both of the form $x_{gh_1}x_{gh_2}x_{g'h}$ for some $\{h_1, h_2\} \subseteq V(\mathcal{H})$ and some $h \in V(\mathcal{H})$. Hence due to symmetry

$$\sum_{\substack{\{h_1,h_2\}\subseteq V(\mathcal{H})\\ \{h_3,h_4\}\subseteq V(\mathcal{H})}} x_{gh_1}x_{gh_2}x_{g'h_3} + x_{gh_1}x_{gh_2}x_{g'h_4} \tag{6.6}$$

can be written as

$$\delta \sum_{\substack{\{h_1,h_2\}\subseteq V(\mathcal{H})\\ h\in V(\mathcal{H})}} x_{gh_1}x_{gh_2}x_{g'h} \tag{6.7}$$

for some $\delta \in \mathbb{Z}$. In order to compute δ observe that there are $2\binom{n_{\mathcal{H}}}{2}^2$ monomials of the considered form in (6.6) and that there are $n_{\mathcal{H}}\binom{n_{\mathcal{H}}}{2}$ monomials of the considered form in (6.7). Hence $\delta = 2\binom{n_{\mathcal{H}}}{2}^2/(n_{\mathcal{H}}\binom{n_{\mathcal{H}}}{2})$. Similar arguments for the other monomials of (6.5) yield

$$\tau_{2,2} \equiv \sum_{g\in V(\mathcal{G})}\sum_{\substack{g'\in V(\mathcal{G})\\ g'\neq g}}\left(\frac{2\binom{n_{\mathcal{H}}}{2}^2}{n_{\mathcal{H}}\binom{n_{\mathcal{H}}}{2}}\sum_{\substack{\{h_1,h_2\}\subseteq V(\mathcal{H})\\ h\in V(\mathcal{H})}} x_{gh_1}x_{gh_2}x_{g'h}\right.$$

$$+\frac{2\binom{n_{\mathcal{H}}}{2}^2}{n_{\mathcal{H}}\binom{n_{\mathcal{H}}}{2}}\sum_{\substack{\{h_3,h_4\}\subseteq V(\mathcal{H})\\ h\in V(\mathcal{H})}} x_{gh}x_{g'h_3}x_{g'h_4}$$
$$-\frac{\binom{n_{\mathcal{H}}}{2}^2}{\binom{n_{\mathcal{H}}}{2}}\sigma_{g,2}-\frac{4\binom{n_{\mathcal{H}}}{2}^2}{n_{\mathcal{H}}^2}\sum_{\substack{h\in V(\mathcal{H})\\ h'\in V(\mathcal{H})}} x_{gh}x_{g'h'}-\frac{\binom{n_{\mathcal{H}}}{2}^2}{\binom{n_{\mathcal{H}}}{2}}\sigma_{g',2}$$
$$+\frac{2\binom{n_{\mathcal{H}}}{2}^2}{n_{\mathcal{H}}}\sigma_{g,1}+\frac{2\binom{n_{\mathcal{H}}}{2}^2}{n_{\mathcal{H}}}\sigma_{g',1}-\binom{n_{\mathcal{H}}}{2}^2\Bigg) \mod I_{\text{viz}},$$

which, using the definition of $\tau_{i,j}$ and $\tau_{1,2}=\tau_{2,1}$, can be simplified to

$$\tau_{2,2}\equiv 2(n_{\mathcal{H}}-1)\tau_{2,1}-(n_{\mathcal{H}}-1)^2\tau_{1,1}-n_{\mathcal{H}}(n_{\mathcal{H}}-1)(n_{\mathcal{G}}-1)\sum_{g\in V(\mathcal{G})}\sigma_{g,2}$$
$$+n_{\mathcal{H}}(n_{\mathcal{H}}-1)^2(n_{\mathcal{G}}-1)\sum_{g\in V(\mathcal{G})}\sigma_{g,1}-\frac{1}{4}n_{\mathcal{G}}(n_{\mathcal{G}}-1)n_{\mathcal{H}}^2(n_{\mathcal{H}}-1)^2 \mod I_{\text{viz}}. \quad \square$$

This completes the collection of result that we need in this section.

6.2. Certificates for $k_{\mathcal{G}}=n_{\mathcal{G}}-1$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-1$ with $n_{\mathcal{H}}\in\{2,3\}$

Now we are finally able to prove Theorem 4.6, which provides a sum-of-squares certificate of degree 2 for $k_{\mathcal{G}}=n_{\mathcal{G}}-1\geq 1$, $n_{\mathcal{H}}=3$ and $k_{\mathcal{H}}=2$. In fact we will prove the existence of sum-of-squares certificates not only in this case, but also for the case $k_{\mathcal{G}}=n_{\mathcal{G}}-1\geq 1$, $n_{\mathcal{H}}=2$ and $k_{\mathcal{H}}=1$ in the following theorem.

Theorem 6.7. *For $k_{\mathcal{G}}=n_{\mathcal{G}}-1\geq 1$, $n_{\mathcal{H}}\in\{2,3\}$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-1$ Vizing's conjecture is true as the polynomials*

$$s_0=\alpha+\beta\Bigg(\sum_{g\in V(\mathcal{G})}\sum_{h\in V(\mathcal{H})}x_{gh}\Bigg)+\gamma\Bigg(\sum_{g\in V(\mathcal{G})}\sum_{\{h,h'\}\subseteq V(\mathcal{H})}x_{gh}x_{gh'}\Bigg)$$

and

$$s_g=\kappa\Bigg(\sum_{h\in V(\mathcal{H})}x_{gh}\Bigg)-\lambda\Bigg(\sum_{\{h,h'\}\subseteq V(\mathcal{H})}x_{gh}x_{gh'}\Bigg) \quad \text{for } g\in V(\mathcal{G}),$$

where $\alpha=\sqrt{n_{\mathcal{H}}-1}(n_{\mathcal{G}}-1)$, $\beta=-\sqrt{n_{\mathcal{H}}-1}/n_{\mathcal{H}}$ and $\gamma=2/(n_{\mathcal{H}}\sqrt{n_{\mathcal{H}}-1})$, are a sum-of-squares certificate with degree 2 of f_{viz}.

In particular for $n_{\mathcal{H}}=2$ we have $\alpha=n_{\mathcal{G}}-1$, $\beta=-1$, $\gamma=1$, $\kappa=0$ and $\lambda=1$ and for $n_{\mathcal{H}}=3$ we have $\alpha=\sqrt{2}(n_{\mathcal{G}}-1)$, $\beta=-\frac{2}{3}\sqrt{2}$ $\gamma=\frac{1}{3}\sqrt{2}$, $\kappa=\frac{1}{3}$ and $\lambda=-\frac{2}{3}$.

Proof of Theorems 4.6 and 6.7. In order to prove that the polynomials s_0 and s_g for $g\in V(\mathcal{G})$ are a sum-of-squares certificate we have to show that $s_0^2+\sum_{g\in V(\mathcal{G})}s_g^2\equiv f_{\text{viz}} \mod I_{\text{viz}}$. Towards that end we can rewrite the polynomials as $s_0=\alpha+\beta\sum_{g\in V(\mathcal{G})}\sigma_{g,1}+\gamma\sum_{g\in V(\mathcal{G})}\sigma_{g,2}$ and $s_g=\kappa\sigma_{g,1}+\lambda\sigma_{g,2})$. This yields

$$s_0^2+\sum_{g\in V(\mathcal{G})}s_g^2=\Bigg(\alpha+\beta\sum_{g\in V(\mathcal{G})}\sigma_{g,1}+\gamma\sum_{g\in V(\mathcal{G})}\sigma_{g,2}\Bigg)^2+\sum_{g\in V(\mathcal{G})}(\kappa\sigma_{g,1}+\lambda\sigma_{g,2})^2$$

$$
\begin{aligned}
&= \alpha^2 + 2\alpha\beta \sum_{g\in V(\mathcal{G})} \sigma_{g,1} + 2\alpha\gamma \sum_{g\in V(\mathcal{G})} \sigma_{g,2} + \beta^2 \Big(\sum_{g\in V(\mathcal{G})} \sigma_{g,1} \Big) \Big(\sum_{g'\in V(\mathcal{G})} \sigma_{g',1} \Big) \\
&\quad + \gamma^2 \Big(\sum_{g\in V(\mathcal{G})} \sigma_{g,2} \Big) \Big(\sum_{g'\in V(\mathcal{G})} \sigma_{g',2} \Big) + 2\beta\gamma \Big(\sum_{g\in V(\mathcal{G})} \sigma_{g,1} \Big) \Big(\sum_{g'\in V(\mathcal{G})} \sigma_{g',2} \Big) \\
&\quad + \sum_{g\in V(\mathcal{G})} \Big(\kappa^2 \sigma_{g,1}^2 + 2\kappa\lambda\sigma_{g,1}\sigma_{g,2} + \lambda^2 \sigma_{g,2}^2 \Big)
\end{aligned}
$$

and therefore

$$
\begin{aligned}
s_0^2 + \sum_{g\in V(\mathcal{G})} s_g^2 =& \alpha^2 + \sum_{g\in V(\mathcal{G})} \sum_{\substack{g'\in V(\mathcal{G}) \\ g'\neq g}} \Big(\beta^2 \sigma_{g,1}\sigma_{g',1} + \gamma^2 \sigma_{g,2}\sigma_{g',2} + 2\beta\gamma\sigma_{g,1}\sigma_{g',2} \Big) \\
&+ \Big(\sum_{g\in V(\mathcal{G})} (\beta^2+\kappa^2)\sigma_{g,1}^2 + (2\beta\gamma + 2\kappa\lambda)\sigma_{g,1}\sigma_{g,2} + (\gamma^2+\lambda^2)\sigma_{g,2}^2 \\
&\qquad + 2\alpha\beta\sigma_{g,1} + 2\alpha\gamma\sigma_{g,2} \Big)
\end{aligned} \tag{6.8}
$$

holds. By using Lemma 6.6 we obtain

$$
\begin{aligned}
&\sum_{g\in V(\mathcal{G})} \sum_{\substack{g'\in V(\mathcal{G}) \\ g'\neq g}} \Big(\beta^2 \sigma_{g,1}\sigma_{g',1} + \gamma^2 \sigma_{g,2}\sigma_{g',2} + 2\beta\gamma\sigma_{g,2}\sigma_{g',1} \Big) \\
&\qquad = \beta^2\tau_{1,1} + \gamma^2\tau_{2,2} + 2\beta\gamma\tau_{1,2} \\
&\qquad \equiv \Big(2\beta\gamma + 2(n_{\mathcal{H}}-1)\gamma^2 \Big) \tau_{2,1} + \Big(\beta^2 - (n_{\mathcal{H}}-1)^2\gamma^2 \Big) \tau_{1,1} \\
&\qquad\quad - n_{\mathcal{H}}(n_{\mathcal{H}}-1)(n_{\mathcal{G}}-1)\gamma^2 \sum_{g\in V(\mathcal{G})} \sigma_{g,2} \\
&\qquad\quad + n_{\mathcal{H}}(n_{\mathcal{H}}-1)^2(n_{\mathcal{G}}-1)\gamma^2 \sum_{g\in V(\mathcal{G})} \sigma_{g,1} \\
&\qquad\quad - \tfrac{1}{4} n_{\mathcal{G}}(n_{\mathcal{G}}-1) n_{\mathcal{H}}^2 (n_{\mathcal{H}}-1)^2\gamma^2 \mod I_{\mathrm{viz}}.
\end{aligned}
$$

Furthermore, we rewrite $\sigma_{g,1}^2$, $\sigma_{g,2}\sigma_{g,1}$ and $\sigma_{g,2}^2$ as in Remark 5.6, so

$$
\begin{aligned}
&(\beta^2+\kappa^2)\sigma_{g,1}^2 + (2\beta\gamma + 2\kappa\lambda)\sigma_{g,1}\sigma_{g,2} + (\gamma^2+\lambda^2)\sigma_{g,2}^2 + 2\alpha\beta\sigma_{g,1} + 2\alpha\gamma\sigma_{g,2} \\
&\qquad \equiv (\beta^2+\kappa^2)(\sigma_{g,1} + 2\sigma_{g,2}) + (2\beta\gamma + 2\kappa\lambda)(2\sigma_{g,2} + 3\sigma_{g,3}) \\
&\qquad\quad + (\gamma^2+\lambda^2)(\sigma_{g,2} + 6\sigma_{g,3} + 6\sigma_{g,4}) + 2\alpha\beta\sigma_{g,1} + 2\alpha\gamma\sigma_{g,2} \\
&\qquad \equiv (\beta^2 + \kappa^2 + 2\alpha\beta)\sigma_{g,1} + (2\beta^2 + 2\kappa^2 + 4\beta\gamma + 4\kappa\lambda + \gamma^2 + \lambda^2 + 2\alpha\gamma)\sigma_{g,2} \\
&\qquad\quad + (6\beta\gamma + 6\kappa\lambda + 6\gamma^2 + 6\lambda^2)\sigma_{g,3} + (6\gamma^2 + 6\lambda^2)\sigma_{g,4} \mod I_{\mathrm{viz}}.
\end{aligned}
$$

The previous two identities together with (6.8) and the fact that $\sigma_{g,4} = 0$ trivially holds because $n_{\mathcal{H}} \in \{2, 3\}$ yield

$$
\begin{aligned}
s_0^2 + \sum_{g\in V(\mathcal{G})} s_g^2 \equiv& \big(\alpha^2 - \tfrac{1}{4} n_{\mathcal{G}}(n_{\mathcal{G}}-1) n_{\mathcal{H}}^2 (n_{\mathcal{H}}-1)^2\gamma^2 \big) + 2\big(\beta\gamma + (n_{\mathcal{H}}-1)\gamma^2 \big)\tau_{2,1} \\
&+ \big(\beta^2 - (n_{\mathcal{H}}-1)^2\gamma^2 \big)\tau_{1,1} \\
&+ \big(\beta^2 + \kappa^2 + 2\alpha\beta + n_{\mathcal{H}}(n_{\mathcal{H}}-1)^2(n_{\mathcal{G}}-1)\gamma^2 \big) \sum_{g\in V(\mathcal{G})} \sigma_{g,1}
\end{aligned}
$$

$$+\big(2\beta^2+2\kappa^2+4\beta\gamma+4\kappa\lambda+\gamma^2+\lambda^2 \\ +2\alpha\gamma-n_{\mathcal{H}}(n_{\mathcal{H}}-1)(n_{\mathcal{G}}-1)\gamma^2\big)\sum_{g\in V(\mathcal{G})}\sigma_{g,2} \\ +6(\beta\gamma+\kappa\lambda+\gamma^2+\lambda^2)\sum_{g\in V(\mathcal{G})}\sigma_{g,3} \mod I_{\text{viz}}.$$

In order to obtain a certificate $s_0^2+\sum_{g\in V(\mathcal{G})}s_g^2\equiv f_{\text{viz}}=-k_{\mathcal{G}}k_{\mathcal{H}}+\sum_{g\in V(\mathcal{G})}\sigma_{g,1} \mod I_{\text{viz}}$ has to hold. For $n_{\mathcal{H}}=2$ we have $\sigma_{g,3}=0$, so in this case every solution to the system of equations

$$\begin{aligned}\alpha^2-\frac{1}{4}n_{\mathcal{G}}(n_{\mathcal{G}}-1)n_{\mathcal{H}}^2(n_{\mathcal{H}}-1)^2\gamma^2&=-(n_{\mathcal{H}}-1)(n_{\mathcal{G}}-1),\\ \beta\gamma+(n_{\mathcal{H}}-1)\gamma^2&=0,\\ \beta^2-(n_{\mathcal{H}}-1)^2\gamma^2&=0,\\ \beta^2+\kappa^2+2\alpha\beta+n_{\mathcal{H}}(n_{\mathcal{H}}-1)^2(n_{\mathcal{G}}-1)\gamma^2&=1,\\ 2\beta^2+2\kappa^2+4\beta\gamma+4\kappa\lambda+\gamma^2+\lambda^2+2\alpha\gamma-n_{\mathcal{H}}(n_{\mathcal{H}}-1)(n_{\mathcal{G}}-1)\gamma^2&=0\end{aligned}$$

yields a valid certificate. It is easy to check that $\alpha=n_{\mathcal{G}}-1$, $\beta=-1$, $\gamma=1$, $\kappa=0$ and $\lambda=1$ is a solution.

For $n_{\mathcal{H}}=3$ the above equations and also

$$\beta\gamma+\kappa\lambda+\gamma^2+\lambda^2=0$$

has to be fulfilled in order to obtain a certificate. Also in this case it can be verified easily that $\alpha=\sqrt{2}(n_{\mathcal{G}}-1)$, $\beta=-\frac{2}{3}\sqrt{2}$, $\gamma=\frac{1}{3}\sqrt{2}$, $\kappa=\frac{1}{3}$ and $\lambda=-\frac{2}{3}$ is a solution to the system of equations. Therefore the polynomials s_0 and s_g for $g\in V(\mathcal{G})$ form indeed a certificate. □

6.3. *Missing certificates for $k_{\mathcal{G}}=n_{\mathcal{G}}-1$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-1$ with $n_{\mathcal{H}}\geq 4$*

Previously we have seen that in many cases it is possible to obtain a certificate not only for particular values of $n_{\mathcal{H}}$ and $k_{\mathcal{H}}$, but for general values, like it was done in Section 5. Therefore it is a natural question, whether we can generalize the certificate from Theorem 4.6 for the case $k_{\mathcal{G}}=n_{\mathcal{G}}-1\geq 1$, $n_{\mathcal{H}}=3$ and $k_{\mathcal{H}}=2$ to a certificate for the case $k_{\mathcal{G}}=n_{\mathcal{G}}-1\geq 1$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-1\geq 1$. We have successfully generalized the certificate for $n_{\mathcal{H}}=2$ with Theorem 6.7. Unfortunately it turns out that this is not possible for $n_{\mathcal{H}}\geq 4$.

Example 6.8. There seems to be no 2-sum-of-squares certificate for the case $n_{\mathcal{G}}=4$, $k_{\mathcal{G}}=3$, $n_{\mathcal{H}}=4$, $k_{\mathcal{H}}=3$ that uses only the monomials of the form 1, x_{gh} and $x_{gh}x_{gh'}$ for all $g\in V(\mathcal{G})$ and all $\{h,h'\}\subseteq V(\mathcal{H})$, as the corresponding SDP is infeasible.

The SDP for the case $n_{\mathcal{G}}=4$, $k_{\mathcal{G}}=3$, $n_{\mathcal{H}}=4$, $k_{\mathcal{H}}=3$ which takes into account all monomials of degree at most 2 is feasible. Therefore we expect that there is an exact 2-sum-of-squares certificate using all monomials also for these parameter values. ◯

When we take a closer look on the proofs of Section 6.1 and 6.2 we get some insight in why this is the case. First, Lemma 6.3 is not true anymore for $n_{\mathcal{G}}\geq 4$, so we can not use the reduction of all products of 4 variables as presented in Remark 6.4. Furthermore $\sigma_{g,4}$ is not equal to 0 anymore for $n_{\mathcal{G}}\geq 4$, so in the proof of Theorem 4.6 the coefficient of $\sigma_{g,4}$ would have to be 0, which is not possible as the coefficient is $6\gamma^2+6\lambda^2$.

As a result we would have to search for a certificate with more monomials than just 1, x_{gh} and $x_{gh}x_{gh'}$ for the case $k_{\mathcal{G}}=n_{\mathcal{G}}-1$ and $k_{\mathcal{H}}=n_{\mathcal{H}}-1$ for $n_{\mathcal{H}}\geq 4$.

7. Conclusions and future work

7.1. Conclusions

In this project, we modeled Vizing's conjecture as an ideal/polynomial pair such that the polynomial is non-negative on the variety of a particularly constructed ideal if and only if Vizing's conjecture is true. We were able to produce low-degree, sparse Positivstellensatz certificates of non-negativity for certain classes of graphs using an innovative collection of techniques ranging from semidefinite programming to clever guesswork to computer algebra.

In particular, Vizing's conjecture with parameters $k_{\mathcal{G}} = n_{\mathcal{G}} - 1 \geq 1$, $k_{\mathcal{H}} = n_{\mathcal{H}} - 1$ and $n_{\mathcal{H}} \in \{2, 3\}$ has a 2-sum-of-squares Positivstellensatz certificate. Furthermore Vizing's conjecture with parameters $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d$ has a d-sum-of-squares Positivstellensatz certificate for $d \leq 4$. We have conjectured a broader combinatorial pattern based on these certificates, but proving validity is left to future work.

However, at this time, we have indeed proved Vizing's conjecture for several classes of graphs using sum-of-squares certificates. Although we have not advanced what is currently known about Vizing's conjecture, we have introduced a completely new technique (still to be thoroughly explored) to the literature of possible approaches.

7.2. Future work

The most pressing matter that arises in this paper is the following. We have investigated the case $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d$. In the future we want to prove Conjecture 5.16 or find other certificates for the cases $d \geq 5$. In particular it would be interesting to know if there is an easy structure for the leading coefficient α_d in such a certificate as mentioned in Remark 5.22.

On a small scale, in order to obtain more insight on the structure of certificates a next step will be to investigate further specific parameter settings. In particular, finding a certificate for the case $k_{\mathcal{G}} = 1$ (and all other parameters arbitrary) is among our next candidates.

On a large scale, it is known that Vizing's conjecture holds if one of the graphs G or H has domination number at most three (Brešar et al., 2012), therefore, to find new results we need to get certificates for $k_{\mathcal{G}} \geq 4$ and $k_{\mathcal{H}} \geq 4$. Furthermore, it suffices to consider graphs that contain no isolated vertices. For such graphs the number of vertices is at least twice the domination number (Ore, 1962). Hence, parameters where we can obtain new results on Vizing's conjecture must satisfy $n_{\mathcal{G}} \geq 8$, $k_{\mathcal{G}} \geq 4$, $n_{\mathcal{H}} \geq 8$, and $k_{\mathcal{H}} \geq 4$.

Therefore, in our future work we intend to continue pushing the computational aspect of this project. One way to do so is to exploit symmetries in order to simplify the computation of a Gröbner basis, as computing the Göbner basis is one of the computational bottlenecks. One alternative possibility to deal with this bottleneck is to avoid the computation of a Gröbner basis by increasing the number of variables in the SDP. Another question of interest is if one could use symmetry to reduce the complexity of the SDP.

Up to now we always used the solution of the SDP in order to obtain insight in the structure of the certificate and then algebraic manipulations yielded the actual certificate. It would be interesting to solve the SDP exactly over the algebraic reals and not only to a high precision over the rationals, in order to obtain an exact certificate as soon as the SDP is solved. However, this is a highly non-trivial task and is left for future research.

Another line of research is to change the model from a Positivstellensatz certificate to a Hilbert's Nullstellensatz certificate, and thus change from numeric semidefinite programming to exact arithmetic linear algebra. This approach must also be thoroughly investigated.

Finally, it would be very interesting to conjecture a global relationship between the values of $n_{\mathcal{G}}$, $n_{\mathcal{H}}$, $k_{\mathcal{G}}$ and $k_{\mathcal{H}}$, and the degree of the Positivstellensatz certificate, and perhaps even recast the conjecture in terms of the theta body hierarchy described in Gouveia et al. (2010).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. More complicated "intermediate" certificates

In Sections 5.2, 5.3 and 5.4 we presented simple sum-of-squares certificates for the case $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - d$ with $d \in \{0, 1, 2\}$. In fact, these easy certificates where obtained only after some computational experiments, in which more complicated certificates were found. We present these intermediate results and certificates here in this appendix.

For obtaining such a certificate, we use the machinery presented in Section 4.3 to get a numerical certificate. From this, we can guess a structure of the occurring coefficients, like it was done in Example 4.2. We will see that these more complicated certificates—they were found by an SDP solver—have a geometric aspect. By studying this aspect it was possible to simplify the more complicated certificates to the certificates presented in Sections 5.3 and 5.4. Hence retrospectively, these more complicated certificates are formally not needed for the proofs of existence of sum-of-squares certificates. Nevertheless we include them here to give a more accurate and complete picture of the process of how to obtain certificates.

A.1. $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1$

In this case the certificates found by observing a structure and guessing the coefficients of the numerical certificate have the following form.

Theorem A.1. *For $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 1 \geq 1$, Vizing's conjecture is true as the polynomials*

$$s'_i = \frac{1}{\sqrt{n_{\mathcal{G}}}} \sum_{g \in V(\mathcal{G})} \lambda_{g,i} \left(\sum_{h \in V(\mathcal{H})} x_{gh} \right)$$

for $i \in \{1, \ldots, n_{\mathcal{G}} - 1\}$ and

$$s'_{n_{\mathcal{G}}} = \frac{1}{\sqrt{n_{\mathcal{G}}}} \left(-k_{\mathcal{G}} k_{\mathcal{H}} + \sum_{(g,h) \in V(\mathcal{G}) \times V(\mathcal{H})} x_{gh} \right),$$

where $\lambda_{g,i}$ are solutions to the system of equations

$$\sum_{i=1}^{n_{\mathcal{G}}-1} \lambda_{g,i}^2 = n_{\mathcal{G}} - 1 \qquad \text{for } g \in V(\mathcal{G}), \tag{A.1a}$$

$$\sum_{i=1}^{n_{\mathcal{G}}-1} \lambda_{g,i} \lambda_{g',i} = -1 \qquad \text{for } \{g, g'\} \subseteq V(\mathcal{G}), \tag{A.1b}$$

are a 1-sos certificate of f_{viz}.

We can prove this theorem directly, but go a different way here: This result is one intermediate step and useful and necessary for conjecturing Theorem 5.12. But once Theorem 5.12 is proved, Theorem A.1 is not a dependency anymore. Therefore, we can reuse the statement made in Theorem 5.12 in the proof here without falling into a cyclic argumentation.

Proof of Theorem A.1. In Theorem 5.12 we have already determined a 1-sos certificate of f_{viz} with s_g, $g \in V(\mathcal{G})$, so we know that $\sum_{g \in V(\mathcal{G})} s_g^2 \equiv f_{\text{viz}} \mod I_{\text{viz}}$. Hence in order to prove that also the

s_i' form a certificate, it is enough to prove that $\sum_{i=1}^{n_\mathcal{G}} (s_i')^2 = \sum_{g \in V(\mathcal{G})} s_g^2$. We use the abbreviation $\sigma_{g,1} = \sum_{h \in V(\mathcal{H})} x_{gh}$ (see Definition 5.4) and do this by

$$\begin{aligned}
\sum_{i=1}^{n_\mathcal{G}} (s_i')^2 &= \frac{1}{n_\mathcal{G}} \Bigg[\sum_{i=1}^{n_\mathcal{G}-1} \Bigg(\sum_{g \in V(\mathcal{G})} \lambda_{g,i}^2 \sigma_{g,1}^2 + 2 \sum_{\{g,g'\} \subseteq V(\mathcal{G})} \lambda_{g,i} \lambda_{g',i} \sigma_{g,1} \sigma_{g',1} \Bigg) \\
&\qquad + (k_\mathcal{G} k_\mathcal{H})^2 - 2 k_\mathcal{G} k_\mathcal{H} \sum_{g \in V(\mathcal{G})} \sigma_{g,1} + \sum_{g \in V(\mathcal{G})} \sigma_{g,1}^2 + 2 \sum_{\{g,g'\} \subseteq V(\mathcal{G})} \sigma_{g,1} \sigma_{g',1} \Bigg] \\
&= \frac{1}{n_\mathcal{G}} \Bigg[\sum_{g \in V(\mathcal{G})} \Bigg(1 + \sum_{i=1}^{n_\mathcal{G}-1} \lambda_{g,i}^2 \Bigg) \sigma_{g,1}^2 + 2 \sum_{\{g,g'\} \subseteq V(\mathcal{G})} \Bigg(1 + \sum_{i=1}^{n_\mathcal{G}-1} \lambda_{g,i} \lambda_{g',i} \Bigg) \sigma_{g,1} \sigma_{g',1} \\
&\qquad + (k_\mathcal{G} k_\mathcal{H})^2 - 2 k_\mathcal{G} k_\mathcal{H} \sum_{g \in V(\mathcal{G})} \sigma_{g,1} \Bigg] \\
&\overset{(A.1)}{=} \frac{1}{n_\mathcal{G}} \Bigg[n_\mathcal{G} \sum_{g \in V(\mathcal{G})} \sigma_{g,1}^2 + (k_\mathcal{G} k_\mathcal{H})^2 - 2 k_\mathcal{G} k_\mathcal{H} \sum_{g \in V(\mathcal{G})} \sigma_{g,1} \Bigg] \\
&\overset{k_\mathcal{G} = n_\mathcal{G}}{=} \sum_{g \in V(\mathcal{G})} \sigma_{g,1}^2 + k_\mathcal{G} k_\mathcal{H}^2 - 2 k_\mathcal{H} \sum_{g \in V(\mathcal{G})} \sigma_{g,1} \\
&= \sum_{g \in V(\mathcal{G})} \left(\sigma_{g,1}^2 - 2 k_\mathcal{H} \sigma_{g,1} + k_\mathcal{H}^2 \right) = \sum_{g \in V(\mathcal{G})} \left(\sigma_{g,1} - k_\mathcal{H} \right)^2 = \sum_{g \in V(\mathcal{G})} s_g^2,
\end{aligned}$$

and so the proof is complete. □

Theorem A.1 requires the solution of a system of equations. We obtain a solution in the following explicit form.

Lemma A.2. *Suppose $n_\mathcal{G}$ is a positive integer and $V(\mathcal{G}) = \{1, \ldots, n_\mathcal{G}\}$. For $g \in V(\mathcal{G})$ and $i \in \{1, \ldots, n_\mathcal{G} - 1\}$ define*

$$\lambda_{g,i} = \begin{cases} 0 & \text{for } i < n_\mathcal{G} - g, \\ \sqrt{\dfrac{n_\mathcal{G}(n_\mathcal{G} - g)}{n_\mathcal{G} - g + 1}} & \text{for } i = n_\mathcal{G} - g, \\ -\dfrac{\lambda_{n_\mathcal{G}-i,i}}{i} & \text{for } i > n_\mathcal{G} - g. \end{cases}$$

Then these $\lambda_{g,i}$ are a solution to the system of equations (A.1).

Proof. Consider $\lambda_{g,i}$ to be defined as stated in the lemma. We will show that it satisfies the equations (A.1).

We start with an initial remark: Observe that $\lambda_{g,i} = \lambda_{g',i}$ whenever $i > n_\mathcal{G} - g$ and $i > n_\mathcal{G} - g'$ hold for all $\{g, g'\} \subseteq V(\mathcal{G})$.

First we prove by induction that

$$\sum_{i=n_\mathcal{G}-g+1}^{n_\mathcal{G}-1} \lambda_{g,i}^2 = \frac{g-1}{n_\mathcal{G} - g + 1} \tag{A.2}$$

holds for every $g \in V(\mathcal{G})$. Indeed, (A.2) is trivially satisfied for $g = 1$, as both sides are equal to zero. In the induction step we assume the (A.2) holds for g and prove that it also holds for $g+1$. Towards this end consider

$$\sum_{i=n_{\mathcal{G}}-g}^{n_{\mathcal{G}}-1} \lambda_{g+1,i}^2 = \lambda_{g+1,n_{\mathcal{G}}-g}^2 + \sum_{i=n_{\mathcal{G}}-g+1}^{n_{\mathcal{G}}-1} \lambda_{g+1,i}^2.$$

Our initial remark implies that

$$\sum_{i=n_{\mathcal{G}}-g}^{n_{\mathcal{G}}-1} \lambda_{g+1,i}^2 = \frac{\lambda_{g,n_{\mathcal{G}}-g}^2}{(n_{\mathcal{G}}-g)^2} + \sum_{i=n_{\mathcal{G}}-g+1}^{n_{\mathcal{G}}-1} \lambda_{g,i}^2.$$

By using the induction hypothesis and the definition of $\lambda_{g,n_{\mathcal{G}}-g}$, this can be further simplified to

$$\sum_{i=n_{\mathcal{G}}-g}^{n_{\mathcal{G}}-1} \lambda_{g+1,i}^2 = \frac{1}{(n_{\mathcal{G}}-g)^2} \frac{n_{\mathcal{G}}(n_{\mathcal{G}}-g)}{n_{\mathcal{G}}-g+1} + \frac{g-1}{n_{\mathcal{G}}-g+1} = \frac{g}{n_{\mathcal{G}}-g}.$$

Hence, this proves that (A.2) holds also for $g+1$ and therefore for all $g \in V(\mathcal{G})$.

Next we consider the system of equations that has to be satisfied. Observe that $\lambda_{g,i} = 0$ for $i < n_{\mathcal{G}} - g$. This and (A.2) imply

$$\sum_{i=1}^{n_{\mathcal{G}}-1} \lambda_{g,i}^2 = \lambda_{g,n_{\mathcal{G}}-g}^2 + \sum_{i=n_{\mathcal{G}}-g+1}^{n_{\mathcal{G}}-1} \lambda_{g,i}^2 = \frac{n_{\mathcal{G}}(n_{\mathcal{G}}-g)}{n_{\mathcal{G}}-g+1} + \frac{g-1}{n_{\mathcal{G}}-g+1} = n_{\mathcal{G}} - 1$$

and, again because of our initial remark, we have

$$\begin{aligned}\sum_{i=1}^{n_{\mathcal{G}}-1} \lambda_{g,i}\lambda_{g',i} &= \lambda_{g,n_{\mathcal{G}}-g}\left(-\frac{\lambda_{g,n_{\mathcal{G}}-g}}{n_{\mathcal{G}}-g}\right) + \sum_{i=n_{\mathcal{G}}-g+1}^{n_{\mathcal{G}}-1} \lambda_{g,i}^2 \\ &= -\left(\frac{1}{n_{\mathcal{G}}-g}\right)\frac{n_{\mathcal{G}}(n_{\mathcal{G}}-g)}{n_{\mathcal{G}}-g+1} + \frac{g-1}{n_{\mathcal{G}}-g+1} = -1.\end{aligned}$$

Therefore the proposed solution for $\lambda_{g,i}$ is indeed a solution to the system of equations (A.1). □

A.2. $k_{\mathcal{G}} = n_{\mathcal{G}}$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 2$

In this case, we again can find certificates by recognizing a structure in a numeric certificate and guessing the coefficients. Such a certificate is of the following form.

Theorem A.3. *For $k_{\mathcal{G}} = n_{\mathcal{G}} \geq 1$ and $k_{\mathcal{H}} = n_{\mathcal{H}} - 2 \geq 1$, Vizing's conjecture is true as the polynomials*

$$s_i' = \frac{1}{\sqrt{n_{\mathcal{G}}}}\left(\sum_{g\in V(\mathcal{G})} \lambda_{g,i}\left(\sum_{h\in V(\mathcal{H})} x_{gh}\right) + \sum_{g\in V(\mathcal{G})} \mu_{g,i}\left(\sum_{\{h,h'\}\subseteq V(\mathcal{H})} x_{gh}x_{gh'}\right)\right)$$

for all $i \in \{1, \ldots, n_{\mathcal{G}} - 1\}$ and

$$s_{n_{\mathcal{G}}}' = \frac{1}{\sqrt{n_{\mathcal{G}}}}\left(n_{\mathcal{G}}\alpha + \beta\left(\sum_{g\in V(\mathcal{G})}\sum_{h\in V(\mathcal{H})} x_{gh}\right) + \gamma \sum_{g\in V(\mathcal{G})}\left(\sum_{\{h,h'\}\subseteq V(\mathcal{H})} x_{gh}x_{gh'}\right)\right),$$

where α, β and γ are solutions of (5.6) and $\lambda_{g,i}$ and $\mu_{g,i}$ are solutions of the system of equations

$$\sum_{i=1}^{n_{\mathcal{G}}-1} \lambda_{g,i}^2 = (n_{\mathcal{G}}-1)\beta^2 \qquad \text{for } g \in V(\mathcal{G}), \tag{A.3a}$$

$$\sum_{i=1}^{n_{\mathcal{G}}-1} \mu_{g,i}^2 = (n_{\mathcal{G}}-1)\gamma^2 \qquad \text{for } g \in V(\mathcal{G}), \tag{A.3b}$$

$$\sum_{i=1}^{n_{\mathcal{G}}-1} \lambda_{g,i}\mu_{g,i} = (n_{\mathcal{G}}-1)\beta\gamma \qquad \text{for } g \in V(\mathcal{G}), \tag{A.3c}$$

$$\sum_{i=1}^{n_{\mathcal{G}}-1} \lambda_{g,i}\lambda_{g',i} = -\beta^2 \qquad \text{for } \{g, g'\} \subseteq V(\mathcal{G}), \tag{A.3d}$$

$$\sum_{i=1}^{n_{\mathcal{G}}-1} \mu_{g,i}\mu_{g',i} = -\gamma^2 \qquad \text{for } \{g, g'\} \subseteq V(\mathcal{G}), \tag{A.3e}$$

$$\sum_{i=1}^{n_{\mathcal{G}}-1} \lambda_{g,i}\mu_{g',i} = -\beta\gamma \qquad \text{for } \{g, g'\} \subseteq V(\mathcal{G}), \tag{A.3f}$$

are a 2-sos certificate of f_{viz}.

Sketch of the proof. The proof can be done analogously to the proof of Theorem A.3, hence we want to show that

$$\sum_{i=1}^{n_{\mathcal{G}}} (s_i')^2 = \sum_{g \in V(\mathcal{G})} s_g^2,$$

where the s_i are those from Theorem 5.13. Towards that end we first simplify and express s_i' in terms of $\sigma_{g,i}$. Then we use binomial expansion to express the squares. In the result we can use (A.3) in order to eliminate all expressions of the form $\sigma_{g,i}\sigma_{g',j}$ and in order to simplify all expressions of the form $\sigma_{g,i}\sigma_{g,j}$. Eventually it is easy to see that the result is in fact a reformulation of $\sum_{g \in V(\mathcal{G})} s_g^2$. Hence the s_i' form a certificate due to Theorem 5.13. □

References

Alon, Noga, Tarsi, Michael, 1992. Colorings and orientations of graphs. Combinatorica 12, 125–134.

Barak, Boaz, Hopkins, Samuel, Kelner, Jonatan, Kothari, Pravesh, Moitra, Ankur, Potechin, Aaron, 2016. A nearly tight sum-of-squares lower bound for the planted clique problem. In: FOCS 2016 IEEE 57th Annual Symposium on Foundations of Computer Science.

Barak, Boaz, Kothari, Pravesh K., Steurer, David, 2017. Quantum entanglement, sum of squares, and the log rank conjecture. In: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC '17. Montreal, QC, Canada, June 19–23, 2017, New York, NY. Association for Computing Machinery (ACM), pp. 975–988.

Barcalkin, A., German, L., 1979. The external stability number of the cartesian product of graphs. Bul. Akad. Stiinte RSS Moldoven. 1 (94), 5–8.

Blekherman, Grigoriy, Parrilo, Pablo A., Thomas, Rekha R. (Eds.), 2013. Semidefinite Optimization and Convex Algebraic Geometry. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA.

Brešar, Boštjan, Dorbec, Paul, Goddard, Wayne, Hartnell, Bert L., Henning, Michael A., Klavžar, Sandi, Rall, Douglas F., 2012. Vizing's conjecture: a survey and recent results. J. Graph Theory 69 (1–2), 46–76.

Cox, David A., Little, John, O'Shea, Donal, 2007. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics). Springer-Verlag New York, Inc., Secaucus, NJ, USA.

Fischer, Klaus G., 1988. Symmetric polynomials and Hall's theorem. Discrete Math. 69 (3), 225–234.

Gaar, Elisabeth, Krenn, Daniel, Margulies, Susan, Wiegele, Angelika, 2019. An optimization-based sum-of-squares approach to Vizing's conjecture. In: ISSAC'19—Proceedings of the 2019 ACM International Symposium on Symbolic and Algebraic Computation. ACM, New York, pp. 155–162.

Garey, Michael R., Johnson, David S., 1979. Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman and Company.
Gasca, Mariano, Sauer, Thomas, 2012. Polynomial interpolation in several variables. Adv. Comput. Math. 12 (4), 377–410.
Gouveia, João, Parrilo, Pablo A., Thomas, Rekha R., 2010. Theta bodies for polynomial ideals. SIAM J. Optim. 20 (4), 2097–2118.
Grigoriev, Dima, Vorobjov, Nicolai, 2001. Complexity of Null- and Positivstellensatz proofs. Ann. Pure Appl. Log. 113 (1–3), 153–160.
Hartnell, Bert, Rall, Douglas F., 1998. Domination in cartesian products: Vizing's conjecture. In: Domination in Graphs (New York). In: Mono. Textbooks Pure and Appl. Math. Dekker, pp. 163–189.
Hillar, Christopher J., Windfeldt, Troels, 2008. Algebraic characterization of uniquely vertex colorable graphs. J. Comb. Theory, Ser. B 98 (2), 400–414.
Jarvis-Wloszek, Zachary, Feeley, Ryan, Tan, Weehong, Sun, Kunpeng, Packard, Andrew, 2005. Control Applications of Sum of Squares Programming. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 3–22.
Kreuzer, Martin, Robbiano, Lorenzo, 2000. Computational Commutative Algebra. I. Springer, Berlin.
Laurent, Monique, 2008. Sums of squares, moment matrices and optimization over polynomials. IMA Vol. Math. Appl. 149, 157–270.
De Loera, Jesus A., Lee, Jon, Margulies, Susan, Onn, Shmuel, 2009. Expressing combinatorial optimization problems by systems of polynomial equations and the Nullstellensatz. Comb. Probab. Comput. 18 (4), 551–582.
Lovász, Laszlo, 1994. Stable sets and polynomials. Discrete Math. 124, 137–153.
Margulies, Susan, Hicks, Illya V., 2012. An algebraic exploration of dominating sets and Vizing's conjecture. Electron. J. Comb. 19 (2), p1. 30.
MOSEK ApS, 2017. The MOSEK Optimization Toolbox for MATLAB Manual. Version 8.1.
Onn, Shmuel, 2004. Nowhere-zero flow polynomials. J. Comb. Theory, Ser. A 108 (2), 205–215.
Ore, Øystein, 1962. Theory of Graphs, Vol. 38. American Mathematical Society (AMS), Providence, RI.
The SageMath Developers, 2019. SageMath Mathematics Software (Version 8.6). http://www.sagemath.org.
Sun, Liang, 2004. A result on Vizing's conjecture. Discrete Math. 275 (1), 363–366.
Vandenberghe, Lieven, Boyd, Stephen, 1996. Semidefinite programming. SIAM Rev. 38 (1), 49–95.
Vizing, Vadim G., 1968. Some unsolved problems in graph theory. Usp. Mat. Nauk 23, 117–134.
Wolkowicz, Henry, Saigal, Romesh, Vandenberghe, Lieven (Eds.), 2000. Handbook of Semidefinite Programming. Theory, Algorithms, and Applications, Vol. 27. Springer, Cham.
Zerbib, Shira, 2019. An improved bound in Vizing's conjecture. Graphs Comb. 35 (6), 1401–1404. MR 4035865.