NPA Hierarchy for Quantum Isomorphism and Homomorphism Indistinguishability

Prem Nigam Kar
Technical University of Denmark, Lyngby, Denmark

David E. Roberson
Technical University of Denmark, Lyngby, Denmark

Tim Seppelt
IT-Universitetet i København, Copenhagen, Denmark

Peter Zeman
Technical University of Denmark, Lyngby, Denmark
Department of Algebra, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic

Abstract

Mančinska and Roberson [FOCS'20] showed that two graphs are quantum isomorphic if and only if they are homomorphism indistinguishable over the class of planar graphs. Atserias et al. [JCTB'19] proved that quantum isomorphism is undecidable in general. The NPA hierarchy gives a sequence of semidefinite programming relaxations of quantum isomorphism. Recently, Roberson and Seppelt [ICALP'23] obtained a homomorphism indistinguishability characterization of the feasibility of each level of the Lasserre hierarchy of semidefinite programming relaxations of graph isomorphism. We prove a quantum analogue of this result by showing that each level of the NPA hierarchy of SDP relaxations for quantum isomorphism of graphs is equivalent to homomorphism indistinguishability over an appropriate class of planar graphs. By combining the convergence of the NPA hierarchy with the fact that the union of these graph classes is the set of all planar graphs, we are able to give a new proof of the result of Mančinska and Roberson [FOCS'20] that avoids the use of the theory of quantum groups. This homomorphism indistinguishability characterization also allows us to give a randomized polynomial-time algorithm deciding exact feasibility of each fixed level of the NPA hierarchy of SDP relaxations for quantum isomorphism.

2012 ACM Subject Classification Theory of computation → Quantum information theory; Mathematics of computing → Graph theory

Keywords and phrases Quantum isomorphism, NPA hierarchy, homomorphism indistinguishability

Digital Object Identifier 10.4230/LIPIcs.ICALP.2025.105

Category Track A: Algorithms, Complexity and Games

Related Version *Full Version*: `https://arxiv.org/abs/2407.10635` [11]

Funding Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.
Prem Nigam Kar: Carlsberg Semper Ardens Accelerate CF21-0682 Quantum Graph Theory.
David E. Roberson: Carlsberg Semper Ardens Accelerate CF21-0682 Quantum Graph Theory.
Tim Seppelt: German Research Foundation (DFG) within Research Training Group 2236/2 (UnRAVeL) and European Union (ERC, SymSim, 101054974, CountHom, 101077083)
Peter Zeman: Funded by Carlsberg Semper Ardens Accelerate CF21-0682 Quantum Graph Theory and by the European Union (ERC, POCOCOP, 101071674).

52nd International Colloquium on Automata, Languages, and Programming (ICALP 2025).
Editors: Keren Censor-Hillel, Fabrizio Grandoni, Joël Ouaknine, and Gabriele Puppis
Article No. 105; pp. 105:1–105:19

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Two graphs G and H are said to be *homomorphism indistinguishable* over a class of graphs $\mathcal{F}$, written $G \cong_{\mathcal{F}} H$, if for every graph $F \in \mathcal{F}$, the number of homomorphisms from F to G is the same as the number of homomorphisms from F to H. A classic result from [12] states that two graphs G and H are isomorphic if and only if they are homomorphism indistinguishable over all graphs. Since then, several relaxations of graph isomorphism from fields as diverse as finite model theory [7, 9, 8], algebraic graph theory [6], optimisation [10, 20], machine learning [25, 15, 26], and category theory [5, 1, 14] were found to be homomorphism indistinguishability relations over suitable graph classes. Recently, a coherent theory which addresses the descriptive and computational complexity of homomorphism indistinguishability relations has begun to emerge [19, 22, 17, 23].

A ground-breaking connection between quantum information and homomorphism indistinguishability was found by Mančinska and Roberson [13]: They showed that two graphs are quantum isomorphic if and only if they are homomorphism indistinguishable over all planar graphs. Quantum isomorphism, as introduced by [3], is a natural relaxation of graph isomorphism in terms of the graph isomorphism game, where two cooperating players called Alice and Bob try to convince a referee that two graphs are isomorphic. A perfect deterministic strategy exists for the (G, H)-isomorphism game if and only if the graphs G and H are isomorphic. Two graphs G and H are said to be *quantum isomorphic*, written $G \cong_q H$, if there is a perfect quantum strategy (G, H)-isomorphism game, i.e., a perfect strategy making use of local quantum measurements on a shared entangled state.

The proof of Mančinska's and Roberson's result [13] heavily relies on certain esoteric mathematical objects called quantum groups. In more detail, the main idea of the proof is to interpret homomorphism tensors of bilabelled graphs as intertwiners of the quantum automorphism groups of the respective graphs.

Another recent result from [20] also obtained a homomorphism indistinguishability characterisation for each level of the Lasserre hierarchy of semidefinite programming (SDP) relaxations of the integer program for isomorphism between two graphs. More precisely, for each $k \in \mathbb{N}$, the authors of [20] constructed a class of graphs $\mathcal{L}_k$ such that the k^{th}-level of the Lasserre hierarchy of SDP relaxations of the integer program for deciding whether G and H are isomorphic is feasible if and only if G and H are homomorphism indistinguishable over the graph class $\mathcal{L}_k$.

It was also shown in [3] that deciding quantum isomorphism of graphs is undecidable – contrary to deciding isomorphism of graphs, which is clearly decidable and currently known to be solvable in quasipolynomial time [4]. This motivates the study of relaxations of quantum isomorphism. The NPA hierarchy [16], which can be thought of as a noncommutative analogue of the Lasserre hierarchy, is a sequence of SDP relaxations of the problem of determining if a given joint conditional probability distribution arises from quantum mechanics. In particular, the NPA hierarchy can be used to formulate a hierarchy of SDP relaxations for the problem of deciding whether two graphs are quantum isomorphic.

In light of results from [13, 20], it is natural to ask if the feasibility of each level of these SDP relaxations of quantum isomorphism can be characterised as a homomorphism indistinguishability relation over some family of graphs. Such a characterisation would make the NPA hierarchy subject to the emerging theory of homomorphism indistinguishability. For example, a recent result [23] asserts that, over every minor-closed graph class of bounded treewidth, homomorphism indistinguishability can be decided in randomized polynomial time. The NPA relaxation, being a semidefinite program, can be solved using standard

techniques such as the ellipsoid method. However, such techniques can, in polynomial time, only decide the approximate feasibility of a system. A homomorphism indistinguishability characterisation of the NPA hierarchy would imply, for each of its levels, the existence of a randomized polynomial-time algorithm for deciding exact feasibility [17, 22, 23].

Main Results. Our main contribution is a homomorphism indistinguishability characterization of each level of the NPA hierarchy, as formalized by the following theorem.

▶ **Theorem 1.** *For graphs G and H and $k \in \mathbb{N}$, the following are equivalent:*

1. *there is a solution for the k^{th}-level of the NPA hierarchy for the (G, H)-isomorphism game;*
2. *there is a level-k quantum isomorphism map from G to H;*
3. *G and H are algebraically k-equivalent;*
4. *G and H are homomorphism indistinguishable over the family of graphs $\mathcal{P}_k$.*

In particular, the k^{th}-level of the NPA hierarchy is feasible for the (G, H)-isomorphism game if and only G and H are homomorphism indistinguishable over the graph class $\mathcal{P}_k$. Here, $\mathcal{P}_k$ is a bounded-treewidth minor-closed class of planar graphs, which we construct by interpreting the NPA systems of equations in light of a correspondence between combinatorics (bilabelled graphs) and algebra (homomorphism tensors) which underpins many recent results regarding homomorphism indistinguishability [13, 10, 18, 20].

As a corollary of Theorem 1, we devise a randomized polynomial-time algorithm for deciding the exact feasibility of each level of the NPA hierarchy. To that end, we first show that the graph classes $\mathcal{P}_k$ are minor-closed and of bounded *treewidth*, which is a graph parameter roughly measuring how far is a graph from a tree. Hence, a recent result from [23] implies that, for each $k \in \mathbb{N}$, there exists a randomized polynomial-time algorithm for deciding homomorphism indistinguishability over $\mathcal{P}_k$. We strengthen this result by making the dependence on the parameter k effective.

▶ **Theorem 2.** *There exists a randomized algorithm which decides, given graphs G and H and an integer $k \geq 1$, whether the k^{th}-level of the NPA hierarchy for the (G, H)-isomorphism game is feasible. The algorithm always runs in time $n^{O(k)}k^{O(1)}$ for $n := \max\{|V(G)|, |V(H)|\}$, accepts all YES-instances, and accepts NO-instances with probability less than one half.*

Proof Techniques. The main algebraic-combinatorial tools we use are bilabelled graphs and their homomorphism tensors. *Bilabelled graphs* are graphs with distinguished vertices which are said to carry labels. To a bilabelled graph $\boldsymbol{F} = (F, u, v)$ and an unlabelled graph G, one can associated the *homomorphism tensor* $\boldsymbol{F}_G \in \mathbb{N}^{V(G)\times V(G)}$ such that $\boldsymbol{F}_G(x, y)$ for $x, y \in V(G)$ is the number of homomorphisms $h\colon F \to G$ such that $h(u) = x$ and $h(v) = y$. For example, the bilabelled graph $\boldsymbol{A} = (A, u, v)$ with $V(A) = \{u, v\}$ and $E(A) = \{uv\}$ denotes the complete 2-vertex graph each of whose vertices u and v carry one label. In the case of $\boldsymbol{A}$, the matrix $\boldsymbol{A}_G$ is just the adjacency matrix of G. The fruitfulness of this construction stems from a correspondence between combinatorial operations on bilabelled graphs and algebraic operations on homomorphism tensors. For example, the *matrix product* $(\boldsymbol{F}_1)_G \cdot (\boldsymbol{F}_2)_G$ yields the homomorphism tensor of the *series composition* of $\boldsymbol{F}_1$ and $\boldsymbol{F}_2$.

We prove Theorem 1 by interpreting the NPA relaxations as a system of equations whose constraints involve homomorphism tensors and algebraic operations. Applying the aforementioned algebro-combinatorial correspondence, the graph class $\mathcal{P}_k$ is then obtained by reading the constraints as a description of a graph class via bilabelled graphs and

combinatorial operations. To that end, we first give various reformulations of the NPA systems of equations as listed in Items 2 and 3 of Theorem 1. The proofs follow the outline below:

- In Theorem 17, we first show that a principal submatrix of a certificate for the k^{th}-level of the NPA hierarchy for the (G, H)-isomorphism game can be interpreted as the Choi matrix of a completely positive map from $M_{V(G)^k}(\mathbb{C})$ to $M_{V(H)^k}(\mathbb{C})$ with certain properties. Such a completely positive map is known as a level-k quantum isomorphism map. We also show that the Choi matrix of such a level-k quantum isomorphism map (uniquely) extends to a certificate for the k^{th}-level of the NPA hierarchy, thus showing that the existence of such a map is equivalent to the feasibility of the k^{th}-level of the NPA hierarchy.
- In Theorem 20, restrictions of the aforementioned completely positive maps are then shown to be algebra homomorphisms mapping homomorphism tensors of $\mathcal{Q}_k$ for G to homomorphism tensors of $\mathcal{Q}_k$ for H, where $\mathcal{Q}_k$ is the set of *atomic graphs* which form the building blocks for the graph class $\mathcal{P}_k$. Such an algebra homomorphism is called an *algebraic k-equivalence.*
- Lastly, in Theorem 1, we use the correspondence between combinatorial operations on graphs and algebraic operations on their homomorphism tensors to show that the existence of an algebraic k-equivalence is equivalent to homomorphism indistinguishability over $\mathcal{P}_k$.

The overall structure of the proof of Theorem 1 is inspired by the proof of the main result of [20]. However, due to the "noncommutativity" of the NPA hierarchy, additional difficulties arise. For example, the proof of inner-product compatibility of the graph classes $\mathcal{L}_k$ from [20] is trivial, while proving the same for our graph classes $\mathcal{P}_k$ requires a creative construction.

We take a more thorough look at the graph classes $\mathcal{P}_k$ in Section 4. We show that the set of underlying graphs of the union of the bilabelled graph classes $\mathcal{P}_k$ is the set of all planar graphs. By combining this result with the convergence of the NPA hierarchy, we derive a substantially simpler proof of the homomorphism indistinguishability characterization of quantum isomorphism given in [13]. In particular, we are able to avoid the use of heavy machinery for dealing with quantum groups, which formed one of the main ingredients of the proof in [13].

▶ **Corollary 3.** *For graphs G and H, the following are equivalent:*

1. *for every k, there is a solution for the k^{th}-level of the NPA hierarchy for the (G, H)-isomorphism game,*
2. *G and H are homomorphism indistinguishable over $\bigcup_{k\in\mathbb{N}} \mathcal{P}_k$, the class of all planar graphs,*
3. *G and H are quantum isomorphic.*

The proof of Theorem 2 relies on the characterisation of the NPA hierarchy as homomorphism indistinguishability relations from Theorem 1. That is, instead of attempting to solve the NPA systems of equations, the algorithm decides whether the input graphs are homomorphism indistinguishable over the graph class $\mathcal{P}_k$. This is done by computing a basis for the finite-dimensional vector space spanned by the homomorphism tensors of the bilabelled graphs in $\mathcal{P}_k$. To that end, the algorithm utilises the inductive definition of the graph class $\mathcal{P}_k$ in terms of generators and combinatorial operations. Being linear or bilinear, their algebraic counterparts can be used to efficiently compute this basis via a fixed-point procedure, which terminates after polynomially many steps. Randomization is only necessary to deal with integers which would otherwise grow to exponential size in the course of the computation.

Outline. We introduce bilabelled graphs and homomorphism tensors in Section 2, which are our main tools to relate the algebraic question of feasibility of the NPA hierarchy to a combinatorial problem of homomorphism indistinguishability. We then introduce the graph isomorphism game and a suitable version of the NPA hierarchy for the graph isomorphism game. The proof of Theorem 1 will be broken down into a series of simpler theorems, namely Theorems 17, 20, and 24. This is done in Section 3 and the beginning of Section 4. In Section 4 we study the graph classes $\mathcal{P}_k$ in more detail and finish the proof of Corollary 3, thus providing the promised alternative proof of the result of [13]. In Section 5, we show that there is a polynomial-time randomized algorithm for each fixed level of the NPA hierarchy for quantum isomorphism.

2 Preliminaries

All graphs in this article are undirected, finite, and without multiple edges, unless stated otherwise. A graph is said to be *simple* if it does not contain any loops. A *homomorphism* $h\colon F \to G$ from a graph F to a graph G is a map $V(F) \to V(G)$ such that for all $uv \in E(F)$ it holds that $h(u)h(v) \in E(G)$. Note that this implies that any vertex in F carrying a loop must be mapped to a vertex carrying a loop in G.

Write $\hom(F, G)$ for the number of homomorphisms from F to G. For a family of graphs $\mathcal{F}$ and simple graphs G and H we write $G \cong_{\mathcal{F}} H$ if G and H are *homomorphism indistinguishable over* $\mathcal{F}$, i.e. $\hom(F, G) = \hom(F, H)$ for all $F \in \mathcal{F}$. Since the graphs G and H into which homomorphisms are counted are throughout assumed to be simple, looped graphs in $\mathcal{F}$ can generally be disregarded as they do not admit any homomorphisms into simple graphs. For background on homomorphism indistinguishability, the reader is referred to the monograph [24].

Bilabelled Graphs and Homomorphism Tensors. We recall the following definitions from [13, 10]: For $k, l \geq 1$, a (k,l)-*bilabelled graph* is a tuple $\boldsymbol{F} = (F, \boldsymbol{u}, \boldsymbol{v})$ where F is a graph and $\boldsymbol{u} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_k) \in V(F)^k$, $\boldsymbol{v} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_l) \in V(F)^l$. The $\boldsymbol{u}$ are the *in-labelled vertices* of $\boldsymbol{F}$ while the $\boldsymbol{v}$ are the *out-labelled vertices* of $\boldsymbol{F}$. Given a graph G, the *homomorphism tensor* of $\boldsymbol{F}$ for G is $\boldsymbol{F}_G \in \mathbb{C}^{V(G)^k \times V(G)^l}$ whose $(\boldsymbol{x}, \boldsymbol{y})$-entry is the number of homomorphisms $h\colon F \to G$ such that $h(\boldsymbol{u}_i) = \boldsymbol{x}_i$ and $h(\boldsymbol{v}_j) = \boldsymbol{y}_j$ for all $i \in [k]$ and $j \in [l]$.

For a (k,l)-bilabelled graph $\boldsymbol{F} = (F, \boldsymbol{u}, \boldsymbol{v})$, write $\operatorname{soe}(\boldsymbol{F}) \coloneqq F$ for the underlying unlabelled graph of $\boldsymbol{F}$. If $k = l$, write $\operatorname{Tr}(\boldsymbol{F})$ for the unlabelled graph underlying the graph obtained from $\boldsymbol{F}$ by identifying $\boldsymbol{u}_i$ with $\boldsymbol{v}_i$ for all $i \in [l]$. For $\sigma \in \mathfrak{S}_{k+l}$, write $\boldsymbol{F}^\sigma \coloneqq (F, \boldsymbol{x}, \boldsymbol{y})$ where $\boldsymbol{x}_i \coloneqq (\boldsymbol{uv})_{\sigma(i)}$ and $\boldsymbol{y}_{j-k} \coloneqq (\boldsymbol{uv})_{\sigma(j)}$ for all $1 \leq i \leq k < j \leq k+l$, i.e., $\boldsymbol{F}^\sigma$ is obtained from $\boldsymbol{F}$ by permuting the labels according to σ. We also define $\boldsymbol{F}^* \coloneqq (F, \boldsymbol{v}, \boldsymbol{u})$ the graph obtained by swapping in- and out-labels.

Let $\boldsymbol{F} = (F, \boldsymbol{u}, \boldsymbol{v})$ and $\boldsymbol{F}' = (F', \boldsymbol{u}', \boldsymbol{v}')$ be (k,l)-bilabelled and (m,n)-bilabelled, respectively. If $l = m$, write $\boldsymbol{F} \cdot \boldsymbol{F}'$ for the (k,n)-bilabelled graph obtained from them by *series composition*, whose underlying unlabelled graph obtained from the disjoint union of F and F' by identifying $\boldsymbol{v}_i$ and $\boldsymbol{u}'_i$ for all $i \in [l]$. Multiple edges arising in this process are removed. The in-labels of $\boldsymbol{F} \cdot \boldsymbol{F}'$ lie on $\boldsymbol{u}$, the out-labels on $\boldsymbol{v}'$.

If $k = m$ and $l = n$ write $\boldsymbol{F} \odot \boldsymbol{F}'$ for the *parallel composition* of $\boldsymbol{F}$ and $\boldsymbol{F}'$. That is, the underlying unlabelled graph of the (k,l)-bilabelled graph $\boldsymbol{F} \odot \boldsymbol{F}'$ is the graph obtained from the disjoint union of F and F' by identifying $\boldsymbol{u}_i$ with $\boldsymbol{u}'_i$ and $\boldsymbol{v}_j$ with $\boldsymbol{v}'_j$ for all $i \in [k]$ and $j \in [l]$. Again, multiple edges are dropped. The in-labels of $\boldsymbol{F} \odot \boldsymbol{F}'$ lie on $\boldsymbol{u}$, the out-labels on $\boldsymbol{v}$.

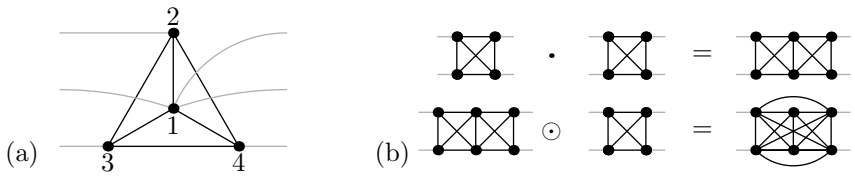

Figure 1 (a) $\boldsymbol{F} = (K_4, (2,1,3), (1,1,4))$. (b) And example of series and parallel composition.

As observed in [13, 10], the benefit of these combinatorial operations is that they have algebraic counterparts. Formally, for all graphs G and all (l,l)-bilabelled graphs $\boldsymbol{F}, \boldsymbol{F}'$, it holds that $\mathrm{soe}(\boldsymbol{F}_G) = \hom(\mathrm{soe}\,\boldsymbol{F}, G)$, $\mathrm{Tr}(\boldsymbol{F}_G) = \hom(\mathrm{Tr}\,\boldsymbol{F}, G)$, $(\boldsymbol{F}_G)^\sigma = (\boldsymbol{F}^\sigma)_G$, $(\boldsymbol{F}\cdot\boldsymbol{F}')_G = \boldsymbol{F}_G \cdot \boldsymbol{F}'_G$, and $(\boldsymbol{F} \odot \boldsymbol{F}')_G = \boldsymbol{F}_G \odot \boldsymbol{F}'_G$, where $\mathrm{soe}(X)$ denotes the sum of elements, Tr denotes the trace, $\cdot$ denotes matrix multiplication and $\odot$ denotes Schur product.

Slightly abusing notation, we say that two graphs G and H are homomorphism indistinguishable over a family of bilabelled graphs $\mathcal{S}$, in symbols $G \cong_{\mathcal{S}} H$ if G and H are homomorphism indistinguishable over the family $\{\mathrm{soe}\,\boldsymbol{S} \mid \boldsymbol{S} \in \mathcal{S}\}$ of the underlying unlabelled graphs of $\boldsymbol{S} \in \mathcal{S}$.

We conclude this subsection by defining the notion of a minor of bilabelled graphs.

▶ **Definition 4** ([20]). *Let $\boldsymbol{M}$ and $\boldsymbol{F}$ be (k,l)-bilabelled graph. Then, M is said to be a* bilabelled minor *of $\boldsymbol{F}$, written $\boldsymbol{M} \leq \boldsymbol{F}$, if it can be obtained from $\boldsymbol{F}$ by applying a sequence of the following bilabelled minor operations:*

1. *edge contraction*
2. *edge deletion*
3. *deletion of unlabelled vertices.*

We note that the if a bilabelled graph $\boldsymbol{M}$ is a bilabelled minor of $\boldsymbol{F}$, then M is a minor of F [20, Lemma 4.12].

▶ Note 5 (drawing bilabelled graphs). Throughout the paper we will depict bilabelled graphs as follows. To draw a bilabelled graph $\boldsymbol{F} = (F, \boldsymbol{u}, \boldsymbol{v})$, we draw the graph F and attach i^{th} input "wire", depicted in grey, to u_i and j^{th} output wire to v_i. Vertices can have multiple input/output wires attached to them. The input and output wires extend to the far right and far left of the picture respectively. Finally, in order to indicate which input/output wire is which, we draw them so that they occur in numerical order (first at the top) at the edges of the picture. See Fig. 1(a) for an example of a bilabelled graph and Fig. 1(b) for an illustration of series and parallel composition, defined above.

The Graph Isomorphism Game. We begin this section by defining the graph isomorphism game. We refer the reader to [3] for more details.

▶ **Definition 6.** *Let G, H be two graphs with $|V(G)| = |V(H)|$. The (G,H)-isomorphism game is a cooperative game, involving two players Alice and Bob, and the verifier, played as follows:*

- *In each round of the game, the verifier chooses two vertices $g, g' \in V(G)$ (sampled uniformly and independently) and sends them to Alice and Bob, respectively.*
- *Alice and Bob are not allowed to communicate during a round of the game, i.e. after receiving their question from the verifier. However, they are free to strategize before the game starts.*
- *Alice and Bob respond with vertices $h, h' \in V(H)$, respectively.*

- *The verifier decides whether Alice and Bob win or lose this round of the game based on the rule function or predicate* $V(h, h' \mid g, g')$ *which is given by*

$$V(h, h' \mid g, g') = \begin{cases} 1 & \text{if } \mathrm{rel}_G(g, g') = \mathrm{rel}_H(h, h') \\ 0 & \text{otherwise} \end{cases}$$

Here $\mathrm{rel}_G(g, g') = \mathrm{rel}_H(h, h')$ *if both pairs of vertices are adjacent, non-adjacent, or identical.*

Alice and Bob can employ a wide array of strategies to play this game. A *deterministic strategy* is one that involves two functions $f_A, f_B \colon V(G) \to V(H)$, where Alice and Bob respond with $f_A(g), f_B(g')$ when presented with the questions g, g' respectively. A *perfect strategy* is one that always wins the game for Alice and Bob.

The predicate necessitates that $f_A = f_B$ for any perfect deterministic strategy (f_A, f_B). Indeed, if $g = g'$, one sees that $f_A(g) = f_B(g)$ for all $g \in V(G)$. Similarly, it is not too difficult to show that $f_A = f_B = f$ is a graph isomorphism, if it is a perfect deterministic strategy. It is also clear that if Alice and Bob answer according to some isomorphism $f \colon V(G) \to V(H)$, then this is a perfect strategy. Hence, the perfect deterministic strategies of the (G, H)-isomorphism game are in bijective correspondence with the isomorphisms of G and H.

Alice and Bob can also make use of *probabilistic strategies*. A probabilistic strategy is given by joint conditional probability distributions $(p(h, h' \mid g, g'))_{g,g' \in V(G), h,h' \in V(H)}$. Probabilistic strategies are often called *correlations* in the literature. We shall denote the set of correlations indexed by the input sets X, Y and the output sets A, B by $P(X, Y, A, B)$. In the case where $X = Y$ and $A = B$, we shall use the notation $P(X, A)$ instead.

It is easy to see that a probabilistic strategy is a perfect strategy for the (G, H)-isomorphism game if and only if $V(h, h' \mid g, g') = 0$ implies that $p(h, h' \mid g, g') = 0$ for all $g, g' \in V(G)$ and $h, h' \in V(H)$. We also note that any perfect probabilistic strategy for the (G, H)-isomorphism game satisfies that $p(h, h' \mid g, g) = 0$ for all $h \neq h' \in V(H)$ and $g \in V(H)$. Such correlations are known as *synchronous correlations*.

Quantum Isomorphism of Graphs. Throughout this paper, we shall be working with what is known as the commuting operator model of quantum mechanics. As discussed earlier, strategies making use of a shared state are known as *quantum strategies*.

▶ **Definition 7.** *A* quantum strategy *for the* (G, H)*-isomorphism game consists of a shared* state*, i.e. a unit vector* $\psi \in \mathcal{H}$ *in some Hilbert space* $\mathcal{H}$ *and self-adjoint projections* $\{E_{g,h}\}_{g \in V(G), h \in V(H)} \subseteq \mathcal{B}(\mathcal{H})$ *and* $\{F_{g',h'}\}_{g' \in V(G), h' \in V(H)} \subseteq \mathcal{B}(\mathcal{H})$ *such that:*

- $\sum_h E_{gh} = I_{\mathcal{H}}$ *and* $\sum_h F_{g,h} = I_{\mathcal{H}}$
- $E_{g,h} F_{g',h'} = F_{g',h'} E_{g,h}$ *for all* $g, g' \in V(G)$ *and* $h, h' \in V(H)$*.*

When Alice and Bob receive the questions g, g' *from the verifier, they use the PVMs* $\{E_{g,h}\}_{h \in V(H)}$ *and* $\{F_{g',h'}\}_{h' \in V(H)}$ *to perform a measurement on their part of the shared state* ψ*. In this case, the conditional probability of outputting* h, h' *when Alice and Bob receive the questions* g, g' *is given by* $p(h, h' \mid g, g') = \langle \psi, E_{g,h} F_{g',h'} \psi \rangle$*.*

Two graphs G, H are said to be *quantum isomorphic*, written $G \cong_q H$ if there is a perfect quantum strategy for the (G, H)-isomorphism game. Two graphs that are isomorphic are also quantum isomorphic as all deterministic strategies can be realized as quantum strategies. However, the converse is not true, i.e. there exist non-isomorphic graphs that are quantum isomorphic. Once again, we refer the reader to [3] for further details.

The existence of a perfect quantum strategy for the (G, H)-isomorphism game is characterized by the following proposition:

▶ **Proposition 8** ([3]). *Let G, H be two graphs with $|V(G)| = |V(H)|$. Then, the $G \cong_q H$ if and only if there exist a Hilbert space $\mathcal{H}$ and self-adjoint projections $\{E_{g,h}\}_{g\in V(G),h\in V(H)}$ such that:*

1. $\sum_{h\in V(H)} E_{g,h} = I_{\mathcal{H}}$ *for all* $g \in V(G)$,
2. $\sum_{g\in V(G)} E_{g,h} = I_{\mathcal{H}}$ *for all* $h \in V(H)$,
3. $E_{g,h}E_{g',h'} = 0$ *if* $V_{G,H}(h, h' \mid g, g') = 0$.

Given the first two conditions, the last condition is equivalent to:

$$(A(G) \otimes I_{\mathcal{H}})[E_{g,h}]_{g\in V(G),h\in V(H)} = [E_{g,h}]_{g\in V(G),h\in V(H)}(A(H) \otimes I_{\mathcal{H}}).$$

Furthermore, G and H are isomorphic if and only if there exist mutually commuting self-adjoint projections $\{E_{g,h}\}_{g\in V(G),h\in V(H)}$ satisfying the above conditions.

A Synchronous NPA Hierarchy for Quantum Isomorphism of Graphs. We shall focus on the NPA hierarchy for the graph isomorphism game in this subsection. We first define what a certificate for the k^{th}-level of the NPA hierarchy for the (G, H)-isomorphism game is. Let $\Sigma = V(G) \times V(H)$.

▶ **Definition 9.** *For two graphs G, H with $|V(G)| = |V(H)|$, a* certificate *for the k^{th} level of the NPA hierarchy of the (G, H)-isomorphism game is a positive semidefinite matrix $\mathcal{R} \in M_{\Sigma^{\leq k}}(\mathbb{C})$ such that:*

1. $\mathcal{R}_{\varepsilon,\varepsilon} = 1$
2. $\mathcal{R}_{s,t} = \mathcal{R}_{s',t'}$ *for all $r, s, r', s' \in \Sigma^{\leq k}$, such that $s^R t \sim (s')^R(t')$, where we define $\sim$ to be the coarsest equivalence relation satisfying the following two properties:*
   - *For each $x, a \in X \times A$, $s(x, a)(x, a)t \sim s(x, a)t$ for all $s, t \in \Sigma^*$.*
   - *$st \sim ts$ for all words $s, t \in \Sigma^*$.*
3. *For all words $s, s' \in \Sigma^{\leq k}$, $g \in V(G)$, $h \in V(H)$ such that $s(g, h)s' \in \Sigma^{\leq k}$, one has*

$$\sum_{h'\in V(H)} \mathcal{R}_{s(g,h')s',t} = \mathcal{R}_{ss',t} \text{ for all } t \in \Sigma^{\leq k} \tag{1}$$

$$\sum_{g'\in V(G)} \mathcal{R}_{s(g',h)s',t} = \mathcal{R}_{ss',t} \text{ for all } t \in \Sigma^{\leq k} \tag{2}$$

4. *For all $s, t \in \Sigma^{\leq k}$, if there exist consecutive $gh, g'h' \in \Sigma$ in $s^R t$ such that $\mathrm{rel}(g, g') \neq \mathrm{rel}(h, h')$ then $\mathcal{R}_{s,t} = 0$.*

We shall say that the k^{th}-level of the NPA hierarchy for the (G, H)-isomorphism game is *feasible* if there exists a certificate for the k^{th}-level of the NPA hierarchy for the same.

Given a perfect strategy for the (G, H)-isomorphism game, where $\{E_{g,h}\}_{g\in V(G),h\in V(H)}$ are Alice's measurement operators and the shared state is ψ, we can construct a certificate for any level of the NPA hierarchy in the following way: for level-k, we consider the Gram matrix of the vectors $\{E_{g_1,h_1} \cdots E_{g_l,h_l}\psi\}_{g_1h_1\cdots g_lh_l\in\Sigma^{\leq k}}$.

The following proposition shows that the NPA hierarchy for the graph isomorphism game converges, i.e there is a solution for each level of the NPA hierarchy for the (G, H)-isomorphism if an only if $G \cong_q H$; see [11, Appendix B.2] for details. Proposition 10 gives two of the implications in Corollary 3, specifically it shows that items (1) and (3) are equivalent.

▶ **Proposition 10.** *Let G, H be two graphs with $|V(G)| = |V(H)|$, and $\Sigma = V(G) \times V(H)$. Then, the (G, H)-isomorphism game has a perfect quantum strategy if and only if for each $k \in \mathbb{N}$, there exists a certificate for the k^{th}-level of the NPA hierarchy.*

3 NPA Hierarchy and Homomorphism Tensors

In this section, we shall give several algebro-combinatorial reformulations of the existence of a certificate for the k^{th} level of the NPA hierarchy of the graph isomorphism game. These reformulations allow us to interpret the existence of a certificate for the k^{th} level of the NPA hierarchy as a homomorphism indistinguishability characterization. We shall discuss the graph-theoretic implications of our results in the next section.

Quantum Isomorphism Relaxation via Completely Positive Maps. In this subsection, we show that a principal submatrix of a certificate for the k^{th}-level of the NPA hierarchy for quantum isomorphism can be interpreted as the Choi matrix of a completely positive map from $M_{V(G)^k}(\mathbb{C})$ to $M_{V(G)^k}(\mathbb{C})$ satisfying certain properties. We then show that the Choi matrix of such a completely positive map uniquely extends to a certificate for the k^{th}-level of the NPA hierarchy for quantum isomorphism. Thus feasibility of the k^{th}-level of the NPA hierarchy for the graph isomorphism game is equivalent to the existence of a completely positive map satisfying certain properties. In order to make these notions precise, we now introduce the atomic bilabelled graphs, which will be the building blocks of the graph classes that we shall construct in the next section.

▶ **Definition 11.** *Let $k \geq 1$. A (k,k)-bilabelled graph $\boldsymbol{F} = (F, \boldsymbol{u}, \boldsymbol{v})$ is atomic if all its vertices are labelled. We define two classes of atomic graphs (see Section 3):*

- *The class $\mathcal{Q}_k^P$ is the class of (k,k)-bilabelled minors of the graph $\boldsymbol{C}_k := (C_k, (1,\dots,k), (k+1,\dots,2k))$ with $V(C_k) = [2k]$ and $E(C_k) = \{\{i, i+1(\mod k)\} : i \in [2k], i \neq k, 2k\}$.*
- *The class $\mathcal{Q}_k^S$ is the class of (k,k)-bilabelled minors of the graph $\boldsymbol{M}_k := (M_k, (1,\dots,k), (k+1,\dots,2k))$ with $V(M_k) = [2k]$ and $E(M_k) = \{\{i, i+k\} : i \in [k]\}$*

Finally, we define $\mathcal{Q}_k := \mathcal{Q}_k^P \cup \mathcal{Q}_k^S$.

We also define two specific atomic graphs $\boldsymbol{J}_k, \boldsymbol{I}_k \in \mathcal{Q}_k$ for each $k \in \mathbb{N}$.

- *$\boldsymbol{J}_k := (J_k, (1,\dots,k), (k+1,\dots 2k))$ with $V(J_k) = [2k]$ and $E(J_k) = \emptyset$*
- *$\boldsymbol{I}_k := (I_k, (1,\dots k), (1,\dots k))$ with $V(I_k) = [k]$ and $E(I_k) = \emptyset$*

In other words, $\boldsymbol{J}_k$ and $\boldsymbol{I}_k$ are obtained from $\boldsymbol{M}_k$ by deleting and contracting all the edges respectively. These atomic graphs are special in the sense that one has $(\boldsymbol{J}_k)_G = J$ and $(\boldsymbol{I}_k)_G = I$ for all graphs G, where I and J are the identity and all ones matrix respectively. We also note that $\boldsymbol{J}_k \in \mathcal{Q}_k^S, \mathcal{Q}_k^P$ and $\boldsymbol{I}_k \in \mathcal{Q}_k^S$, but $\boldsymbol{I}_k \notin \mathcal{Q}_k^P$.

We can now define quantum isomorphism maps using homomorphism tensors of graphs in $\mathcal{Q}_k$:

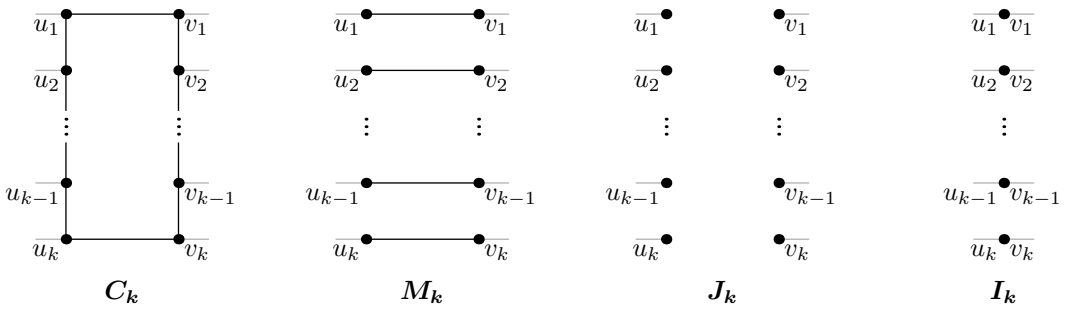

Figure 2 Atomic graphs.

▶ **Definition 12.** *Let G and H be graphs and $k \in \mathbb{N}$. A linear map $\Phi : \mathbb{C}^{V(G)^k \times V(G)^k} \to \mathbb{C}^{V(H)^k \times V(H)^k}$ is a* level k quantum isomorphism map *from G to H if the following holds:*

$$\Phi \text{ is completely positive,} \tag{3}$$

$$\Phi(\boldsymbol{F}_G \odot X) = \boldsymbol{F}_H \odot \Phi(X) \text{ for all } \boldsymbol{F} \in \mathcal{Q}_k^P \text{ and } X \in \mathbb{C}^{V(G)^k \times V(G)^k}, \tag{4}$$

$$\Phi(I) = I = \Phi^*(I), \tag{5}$$

$$\Phi(J) = J = \Phi^*(J), \tag{6}$$

$$\Phi(\boldsymbol{F}_G) = \boldsymbol{F}_H \text{ for all } F \in \mathcal{Q}_k, \tag{7}$$

$$\Phi(\boldsymbol{X}^\sigma) = \Phi(\boldsymbol{X})^\sigma \text{ for all } \sigma \in \mathcal{C}(1, \dots, k, 2k, \dots, k+1). \tag{8}$$

▶ Note 13. Note that conditions (3) and (5) state that any level k quantum isomorphism map is a completely positive, trace-preserving, unital map. Also note that condition (7) implies the part of conditions (5) and (6) on the map Φ, and thus we are being a bit redundant. However, we do need to explicitly include the conditions on the adjoint Φ^*. Lastly, we are being a bit imprecise since we should really write $\boldsymbol{I}_G, \boldsymbol{I}_H, \boldsymbol{J}_G$, and $\boldsymbol{J}_H$.

We now prove some lemmas that will be useful for our proof that existence of a level k quantum isomorphism map is equivalent to the feasibility of the k^{th} level of the NPA hierarchy.

▶ **Lemma 14.** *Let G and H be graphs, $k \in \mathbb{N}$, and suppose that Φ is a level k quantum isomorphism map from G to H. If M is the Choi matrix of Φ, then $M_{s,t} = 0$ if any cyclic permutation of $s^R t$ contains consecutive terms gh and $g'h'$ such that $\mathrm{rel}(g, g') \neq \mathrm{rel}(h, h')$.*

▶ **Lemma 15.** *Let G and H be graphs and $k \in \mathbb{N}$. If Φ is a level k quantum isomorphism map from G to H, then $\Phi(\boldsymbol{F}_G X) = \boldsymbol{F}_H \Phi(X)$ and $\Phi(X \boldsymbol{F}_G) = \Phi(X)\boldsymbol{F}_H$ for all $\boldsymbol{F} \in \mathcal{Q}_k$ and $X \in \mathbb{C}^{V(G)^k \times V(G)^k}$.*

For our last lemma we need to introduce some notation. For disjoint subsets $R_G, R_H \subseteq [k]$, and $s = g_1 h_1 \dots g_k h_k \in (V(G) \times V(H))^k$, we denote by $s(R_G, R_H)$ the set of all strings $s' = g'_1 h'_1 \dots g'_k h'_k$ such that $g'_i = g_i$ for $i \notin R_G$ and $h'_i = h_i$ for $i \notin R_H$. For example, if $k = 3$ and $s = g_1 h_1 g_2 h_2 g_3 h_3$, then

$$s(\{1\}, \{3\}) = \left\{ g'_1 h_1 g_2 h_2 g_3 h'_3 \in (V(G) \times V(H))^3 : g'_1 \in V(G),\ h'_3 \in V(H). \right\}$$

Additionally, for any subset $R \in [k]$ we denote by $s \setminus R$ the substring of s obtained by removing its i^{th} entry for each $i \in R$.

▶ **Lemma 16.** *Let G and H be graphs and suppose that Φ is a level k quantum isomorphism map from G to H. If M is the Choi matrix of Φ, then for any $s, t \in (V(G) \times V(H))^k$, disjoint subsets $S_G, S_H \subseteq [k]$, and disjoint subsets $T_G, T_H \subseteq [k]$, we have that*

$$\sum_{s' \in s(S_G, S_H),\ t' \in t(T_G, T_H)} M_{s', t'} \tag{9}$$

depends only on the equivalence class of $\sim$ that $(s \setminus (S_G \cup S_H))^R (t \setminus (T_G \cup T_H))$ lies in.

▶ **Theorem 17.** *Let G and H be graphs and $k \in \mathbb{N}$. Then the following are equivalent:*

1. *The k^{th} level of the NPA hierarchy is feasible for the (G, H)-isomorphism game.*
2. *There exists a level k quantum isomorphism map from G to H.*
3. *There exists a level k quantum isomorphism map from H to G.*

The idea is to use a principal submatrix of a certificate $\mathcal{R}$ for the k^{th} level of the NPA hierarchy as the Choi matrix of a linear map and show that this map is a level k quantum isomorphism map. Conversely, one takes the Choi matrix of a level k quantum isomorphism map and shows that the remaining entries needed in a certificate for the NPA hierarchy can be determined by the entries from the Choi matrix alone. The equivalence of the final item follows from the fact that the first item is clearly symmetric in G and H.

We remark that it follows from Definition 9 2 that the extension of the Choi matrix M to the certificate $\mathcal{R}$ is in fact unique.

It should also be noted that not all elements of $\mathcal{Q}_k^S$ were needed to prove that item (2) implies item (1) above. This is related to the fact that it is in fact possible to generate these unused bilabelled graphs from those that were used in the proof. However, redefining the set $\mathcal{Q}_k^S$ to only contain those that were used does not make it any easier to prove that (1) implies (2), and we will need these extra graphs later.

Isomorphisms Between Matrix Algebras. In this subsection, we shall see how a quantum isomorphism map restricts to a homomorphism between algebras containing homomorphism tensors for G to homomorphism tensors for H of graphs in $\mathcal{Q}_k$. This brings us a step closer to interpreting a solution for the k^{th}-level of the NPA hierarchy as a homomorphism indistinguishability relation.

A matrix algebra $\mathcal{A} \subseteq M_{n^k}(\mathbb{C})$ is *S-partially coherent* if it is unital, self-adjoint, contains J, and is closed under Schur product with any matrix in S. Further, $\mathcal{A}$ is *cyclically-symmetric* if $A^\sigma \in \mathcal{A}$, for every $A \in \mathcal{A}$ and $\sigma \in \mathcal{C}(1, \dots, k, 2k, \dots, k+1)$.

▶ **Definition 18.** *Let S_k be the set of homomorphism tensors of (k,k)-bilabelled atomic graphs for G in $\mathcal{Q}_k^P$. For a graph G, we define the algebra $\widehat{\mathcal{Q}}_G^k$ as the minimal cyclically-symmetrical S_k-partially coherent algebra containing homomorphism tensors of all (k,k)-bilabelled graphs in $\mathcal{Q}_k$ for G.*

▶ **Definition 19.** *Two n-vertex graphs G and H are* algebraically k-equivalent *if there is* algebraic k-equivalence*, i.e., a vector space isomorphism $\varphi\colon \widehat{\mathcal{Q}}_G^k \to \widehat{\mathcal{Q}}_H^k$ such that*

1. *$\varphi(M^*) = \varphi(M)^*$ for all $M \in \widehat{\mathcal{Q}}_G^k$,*
2. *$\varphi(MN) = \varphi(M)\varphi(N)$ for all $M, N \in \widehat{\mathcal{Q}}_G^k$,*
3. *$\varphi(\boldsymbol{F}_G \odot M) = \boldsymbol{F}_H \odot \varphi(M)$ for all $\boldsymbol{F} \in \mathcal{Q}_k^P$ and any $M \in \widehat{\mathcal{Q}}_G^k$,*
4. *$\varphi(I) = I$, $\varphi(J) = J$ and $\varphi(\boldsymbol{F}_G) = \boldsymbol{F}_H$ for all $\boldsymbol{F} \in \mathcal{Q}_k$,*
5. *$\varphi(M^\sigma) = \varphi(M)^\sigma$ for all $M \in \widehat{\mathcal{Q}}_G^k$ and $\sigma \in \mathcal{C}(1, \dots, k, 2k, \dots, k+1)$,*
6. *φ is trace preserving.*

Note that every algebraic k-equivalence is sum-preserving, i.e., $\operatorname{soe}(\varphi(X)) = \operatorname{soe}(X)$ for all $X \in \hat{\mathcal{Q}}_k$. Indeed, $\operatorname{soe}(\varphi(X)) = \operatorname{Tr}(J\varphi(X)) = \operatorname{Tr}(\varphi(JX)) = \operatorname{Tr}(JX) = \operatorname{soe}(X)$.

▶ **Theorem 20.** *Let $k \geq 1$. Two graphs G and H are algebraically k-equivalent if and only if there is a level-k quantum isomorphism map from G to H.*

Proof. The proof is similar to [20, Theorem 3.14 and Theorem 3.16]. ◀

4 Homomorphism Indistinguishability

In this section, we shall finish the proof of the main theorem by constructing the graph classes $\mathcal{P}_k$ such that homomorphism indistinguishability over $\mathcal{P}_k$ is equivalent to the feasibility of the k^{th}-level of the NPA hierarchy.

▶ **Definition 21.** *Let $\mathcal{P}_k$ be the class of (k,k)-bilabelled graphs generated by the set of atomic graphs $\mathcal{Q}_k$ under parallel composition with graphs from $\mathcal{Q}_k^P$, series composition, and the action of the group $\mathcal{C}(1,\dots,k,2k,\dots,k+1)$ on the labels.*

We remark that the action of $\mathcal{C}(1,\dots,k,2k,\dots,k+1)$ on a bilabelled graph $\boldsymbol{F} \in \mathcal{P}_k$ corresponds to "rotating" the drawing of $\mathcal{F}$.

Inner-product Compatibility of $\mathcal{P}_k$. A class of (k,k)-bilabelled graphs $\mathcal{T}$ is said to be *inner-product compatible* if for all $\boldsymbol{R}, \boldsymbol{S} \in \mathcal{T}$, there is a $\boldsymbol{Q} \in \mathcal{T}$ such that $\mathrm{Tr}(\boldsymbol{R}^* \cdot \boldsymbol{S}) = \mathrm{soe}(\boldsymbol{Q})$.

▶ **Lemma 22.** *The graph classes $\mathcal{P}_k$ are inner-product compatible for each $k \in \mathbb{N}$.*

▶ **Theorem 23** ([20, Theorem 27])**.** *Let $\mathcal{S}$ be an inner-product compatible class of (k,k)-bilabelled graphs containing J. Write $\mathcal{S}_G$ for the homomorphism tensors $\{\boldsymbol{F}_G \mid \boldsymbol{F} \in \mathcal{S}\}$, and let $\mathbb{C}S_G \subseteq M_{V(G)^k}(\mathbb{C})$ denote the vector space spanned by $\mathcal{S}_G$. Then, the following are equivalent:*

1. *G and H are homomorphism indistinguishable over $\mathcal{S}$.*
2. *there exists a sum-preserving vector space isomorphism $\varphi : \mathbb{C}\mathcal{S}_G \to \mathbb{C}\mathcal{S}_H$ such that $\varphi(\boldsymbol{F}_G) = \boldsymbol{F}_H$ for all $\boldsymbol{F} \in S$.*

The next theorem completes the proof of Theorem 1.

▶ **Theorem 24.** *Let $k \geq 1$. Two graphs G and H are homomorphism indistinguishable over $\mathcal{P}_k$ if and only if they are partially k-equivalent.*

Proof. The main idea of the proof is to note that $\mathbb{C}(\mathcal{P}_k)_G = \hat{\mathcal{Q}}_k^G$ for any graph G. Now, by Theorem 23, it is clear that G and H are homomorphism indistinguishable over $\mathcal{P}_k$ if and only if there is a sum-preserving vector space isomorphism from $\hat{\mathcal{Q}}_k^G$ to $\hat{\mathcal{Q}}_k^H$. Since every algebraic k-equivalence is sum-preserving, it is clear that if G and H are algebraically k-equivalent, then $G \cong_{\mathcal{P}_k} H$.

On the contrary, if we assume that $G \cong_{\mathcal{P}_k} H$, then there is a sum preserving vector space isomorphism $\varphi\colon \hat{\mathcal{Q}}_k^G$ to $\hat{\mathcal{Q}}_k^H$ such that $\varphi(\boldsymbol{F}_G) = \boldsymbol{F}_H$ for all $\boldsymbol{F} \in \mathcal{P}_k$. Hence, if $\boldsymbol{F}_1, \boldsymbol{F}_2 \in \mathcal{P}_k$, then

$$\varphi((\boldsymbol{F}_1)_G(\boldsymbol{F}_2)_G) = \varphi((\boldsymbol{F}_1 \cdot \boldsymbol{F}_2)_G) = (\boldsymbol{F}_1 \cdot \boldsymbol{F}_2)_H = (\boldsymbol{F}_1)_H(\boldsymbol{F}_2)_H = \varphi((\boldsymbol{F}_1)_G)\varphi((\boldsymbol{F}_2)_G).$$

Similarly, if $\boldsymbol{F}_2 \in \mathcal{Q}_k^P$, then we can show that $\varphi((\boldsymbol{F}_1)_G \odot (\boldsymbol{F}_2)_G) = \varphi((\boldsymbol{F}_1)_G) \odot \varphi((\boldsymbol{F}_2)_G)$. Other than φ being trace-preserving, the remaining conditions from Definition 19 can be proven in similar manners. The fact φ is trace-preserving follows from it being sum-preserving and $\mathcal{P}_k$ being inner-product compatible. ◀

Planarity and Minor-closedness of $\mathcal{P}_k$. In this subsection, we shall look at the graph classes $\mathcal{P}_k$ in more detail. The first thing we note is that for each $k \in \mathbb{N}$, one has that $\mathcal{P}_k \subseteq \mathcal{L}_k$, which were the classes of graphs constructed in [20] to obtain a homomorphism indistinguishability charatcterization for the Lasserre hierarchy of SDP relaxations of graph isomorphism. We refer the reader to [20] for more details.

Indeed, for each $k \in \mathbb{N}$ it is not too difficult to see that $\mathcal{Q}_k \subseteq \mathcal{A}_k$ (where $\mathcal{A}_k$ are the atomic graphs used to construct $\mathcal{L}_k$ in [20]). Moreover, the set of allowed operations while constructing $\mathcal{P}_k$ from $\mathcal{Q}_k$ is also a subset of the set of operations allowed while constructing $\mathcal{L}_k$ from $\mathcal{A}_k$. In fact, for $k = 1$, it is not too difficult to show that $\mathcal{P}_k = \mathcal{L}_k$ is the set of all outerplanar graphs. We note here that the class $\mathcal{P}_k$ is not the set of k-outerplanar graphs for $k \neq 1$. For any $k \in \mathbb{N}$, one can construct a k-outerplanar graph in $\mathcal{P}_2$. The following lemma is immediate from [20, Lemma 28]:

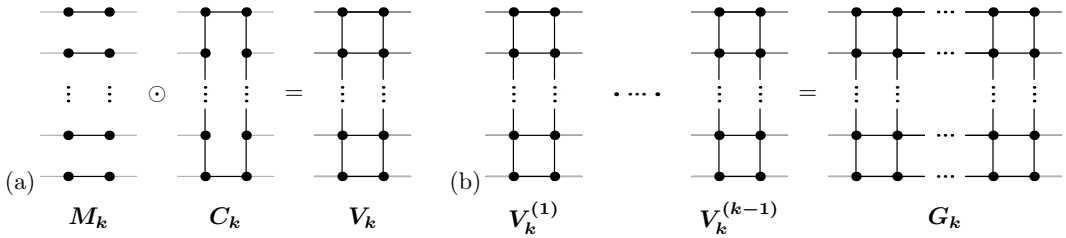

Figure 3 (a) Construction of the graphs $\boldsymbol{V}_k$. (b) Construction of the graph $\boldsymbol{G}_k$.

▶ **Lemma 25.** *Let $\boldsymbol{F} \in \mathcal{P}_k$ be a (k,k)-bilabelled graph. Then, the treewidth of the underlying graph* $\operatorname{soe}(\boldsymbol{F})$ *is at most* $3k-1$.

We now work towards giving an alternate proof of the main result of [13] that shows that two graphs are quantum isomorphic if and only if they are homomorphism indistinguishable over all planar graphs. Let $\mathcal{P} := \bigcup_{k=1}^{k} \mathcal{P}_k$. Then, it follows from the main theorem (Theorem 1) and convergence of NPA hierarchy (Proposition 10) that $G \cong_q H$ is equivalent to $G \cong_{\mathcal{P}} H$. This proves Corollary 3 with the exception of the claim in item (2) that $\mathcal{P}$ is the set of all planar graphs. We now work towards completing the proof of Corollary 3.

First, we show that for each $k \in \mathbb{N}$, the graph class $\mathcal{P}_k$ only contains planar graphs. We begin by precisely defining what it means for a bilabelled graph to be planar. We use the definition given in [13].

▶ **Definition 26.** *Given a (k,l)-bilabelled graph $\boldsymbol{G} = (G, \boldsymbol{a}, \boldsymbol{b})$ we define the graph G^0 as the graph obtained from G by adding a cycle $C = \alpha_1, \ldots, \alpha_k, \beta_l, \ldots, \beta_1$ and the edges $a_i\alpha_i$ and $b_j\beta_j$ for each $i \in [k]$ and $j \in [l]$, and say that $\boldsymbol{G}$ is planar if G^0 has a planar embedding where the cycle C is the boundary of a face. We shall refer to C as the* enveloping cycle *of G^0, and usually consider planar embeddings where C is the boundary of the outer face.*

▶ **Lemma 27.** *For each $k \in \mathbb{N}$, the class of graphs $\mathcal{P}_k$ is contained in the set of all planar bilabelled graphs.*

We will also need that the class $\mathcal{P}_k$ is closed under taking minors (recall the notion of minors of bilabelled graphs from Section 2) and that $\operatorname{soe}(\mathcal{P}_k)$ is closed under minors and disjoint unions. The proofs of these facts are almost identical to the analogous proofs for the class $\mathcal{L}_k$ used in [20].

▶ **Lemma 28.** *For each $k \in \mathbb{N}$, the class of bilabelled graphs $\mathcal{P}_k$ is minor-closed.*

▶ **Lemma 29.** *For each $k \in \mathbb{N}$, the class of graphs* $\operatorname{soe}(\mathcal{P}_k)$ *is minor-closed and union-closed.*

We now work towards showing that although each $\mathcal{P}_k$ has bounded treewidth, their union contains arbitrarily large grids.

▶ **Lemma 30.** *For each $k \in \mathbb{N}$, the class of graphs $\mathcal{P}_k$ contains the $k \times k$ grid.*

Proof. Let $\boldsymbol{V}_k \in \mathcal{P}_k$ denote the graph obtained by the parallel composition of $\boldsymbol{C}_k$ and $\boldsymbol{M}_k$, i.e $\boldsymbol{V}_k := \boldsymbol{M}_k \odot \boldsymbol{C}_k$. Note that this parallel composition is allowed as $\boldsymbol{C}_k \in \mathcal{Q}_k^P$. Clearly, $\operatorname{soe}(\boldsymbol{V}_k)$ is the vertical grid with 2 columns and k rows (see Figure 3). Define $\boldsymbol{G}_k$ to be the graph constructed by the series composition of $k-1$ copies of $\boldsymbol{V}_k$, i.e. $\boldsymbol{G}_k = \boldsymbol{V}_k^{(1)} \cdot \ldots \cdot V_k^{(k-1)}$, where each $\boldsymbol{V}_k^{(i)}$ is a copy of $\boldsymbol{V}_k$. It is clear from Figure 3 that $\operatorname{soe} \boldsymbol{G}_k$ is the $k \times k$ grid. ◀

We now need a standard result from graph minor theory that follows from [21]:

▶ **Theorem 31.** *For every planar graph G, there is a natural number n_G such that G is a minor of the $n_G \times n_G$ grid.*

The following is immediate from Lemma 27, Lemma 29, Lemma 30 and Theorem 31:

▶ **Corollary 32.** *The set $\mathcal{P} = \bigcup_{k\in\mathbb{N}} \mathrm{soe}(\mathcal{P}_k)$ is the set of all planar graphs.*

Recalling the discussion preceding Lemma 27, this completes the proof of Corollary 3, and thus gives us the promised alternative proof of the result of [13].

5 Exact Feasibility of NPA in Randomized Polynomial Time

Being a semidefinite program, the NPA relaxation can be solved using standard techniques such as the ellipsoid method. However, such techniques can, in polynomial time, only decide the approximate feasibility of a system. In this section, we use homomorphism indistinguishability to give a randomized algorithm for deciding exact feasibility of each level of the NPA hierarchy.

▶ **Theorem 2.** *There exists a randomized algorithm which decides, given graphs G and H and an integer $k \geq 1$, whether the k^{th}-level of the NPA hierarchy for the (G, H)-isomorphism game is feasible. The algorithm always runs in time $n^{O(k)}k^{O(1)}$ for $n := \max\{|V(G)|, |V(H)|\}$, accepts all YES-instances, and accepts NO-instances with probability less than one half.*

By a recent result [23, Theorem 1.1], homomorphism indistinguishability over every minor-closed graph class of bounded treewidth can be decided in randomized polynomial time. In Theorem 1, we have established that the k^{th}-level of the NPA hierarchy for the (G, H)-isomorphism game is feasible for two graphs G and H if and only if they are homomorphism indistinguishable over $\mathcal{P}_k$. By Lemmas 25 and 29, the graph class $\mathcal{P}_k$ is minor-closed and of bounded treewidth. Hence, by [23, Theorem 1.1], the feasibility of the k^{th}-level of the NPA hierarchy can be decided in randomized polynomial time for every fixed k. However, this result assumes k to be fixed and not part of the input.

Modular Homomorphism Indistinguishability. As a first step towards Theorem 2, we show that it can be decided in deterministic polynomial time whether G and H are *homomorphism indistinguishable over $\mathcal{P}_k$ modulo a prime p*, i.e. $\hom(F, G) \equiv \hom(F, H) \mod p$ for all $F \in \mathcal{P}_k$. We work over a finite field in order to avoid memory issues with too large integers.

▶ **Theorem 33.** *There exists a deterministic algorithm which decides, given graphs G and H, an integer $k \geq 1$, and a prime p, whether G and H are homomorphism indistinguishable over $\mathcal{P}_k$ modulo p. The algorithm runs in time $n^{O(k)}(k \log p)^{O(1)}$ for $n := \max\{|V(G)|, |V(H)|\}$.*

The algorithm in Theorem 33 decides whether G and H are homomorphism indistinguishable over $\mathcal{P}_k$ by computing a basis B for the $\mathbb{F}_p$-vector space S spanned by homomorphism matrices of bilabelled graphs in $\mathcal{P}_k$. More precisely,

$$S := \mathrm{span}\,\{\boldsymbol{P}_G \oplus \boldsymbol{P}_H \mid \boldsymbol{P} \in \mathcal{P}_k\} \subseteq \mathbb{F}_p^{(V(G)^k \cup V(H)^k) \times (V(G)^k \cup V(H)^k)}$$

where $\boldsymbol{P}_G \oplus \boldsymbol{P}_H := \left(\begin{smallmatrix} \boldsymbol{P}_G & 0 \\ 0 & \boldsymbol{P}_H \end{smallmatrix}\right)$. A basis $B \subseteq S$ can be computed iteratively as follows. We initialise B with the singleton set containing $\boldsymbol{J}_G \oplus \boldsymbol{J}_H$. Subsequently, we repeatedly apply the operations from Definition 21 to compute new vectors. Whenever a new vector is linearly

Algorithm 1 Modular NPA.

Input: Graphs G and H, an integer $k \geq 1$, a prime p in binary.
Output: Whether G and H are homomorphism indistinguishable over $\mathcal{P}_k$ modulo p.

for every $\boldsymbol{A} \in \mathcal{B}_k$, compute the homomorphism matrices $\boldsymbol{A}_G \in \mathbb{F}_p^{V(G)^k \times V(G)^k}$ and $\boldsymbol{A}_H \in \mathbb{F}_p^{V(H)^k \times V(H)^k}$;
initialise $B \leftarrow \{\boldsymbol{J}_G \oplus \boldsymbol{J}_H\} \subseteq \mathbb{F}_p^{(V(G)^k \cup V(H)^k) \times (V(G)^k \cup V(H)^k)}$;
foreach $\boldsymbol{A} \in \mathcal{B}_k$ **do**
  if $\boldsymbol{A}_G \oplus \boldsymbol{A}_H \notin \operatorname{span}(B)$ **then**
    add $\boldsymbol{A}_G \oplus \boldsymbol{A}_H$ to B;
repeat
  foreach $\boldsymbol{A} \in \mathcal{B}_k^P$, $v \in B$ **do**
    $w \leftarrow (\boldsymbol{A}_G \oplus \boldsymbol{A}_H) \odot v$;
    if $w \notin \operatorname{span}(B)$ **then**
      add w to B;
  foreach $v_1, v_2 \in B$ **do**
    $w \leftarrow v_1 \cdot v_2$;
    if $w \notin \operatorname{span}(B)$ **then**
      add w to B;
  foreach $\sigma \in \mathcal{C}(1, \dots, k, 2k, \dots, k+1)$, $v \in B$ **do**
    $w \leftarrow v^\sigma$;
    if $w \notin \operatorname{span}(B)$ **then**
      add w to B;
until *B is not updated*;
if $\mathbf{1}_G^T v \mathbf{1}_G = \mathbf{1}_H^T v \mathbf{1}_H$ *for all* $v \in B$ **then**
  accept;
else
  reject;

independent from the vectors already in B, we add it to B. Since the dimension of S is at most $2n^{2k}$, this process takes polynomial number of steps and is formally described in Algorithm 1.

In order to achieve a better runtime in Theorem 33, we give size-$O(k)$ sets $\mathcal{B}_k^P$ and $\mathcal{B}_k^S$ of bilabelled graphs generating $\mathcal{Q}_k^P$ and $\mathcal{Q}_k^S$. Let $\mathcal{B}_k \coloneqq \mathcal{B}_k^P \cup \mathcal{B}_k^S$.

▶ **Lemma 34.** *Let $k \geq 1$ and consider the following (k,k)-bilabelled graphs.*

- $\boldsymbol{J} \coloneqq (J, (1, \dots, k), (k+1, \dots, 2k))$ *with* $V(J) = [2k]$ *and* $E(J) = \emptyset$,
- *for $i \in [2k]$ and $j \coloneqq i+1$ if $i < 2k$ and $j \coloneqq 1$ otherwise, the graphs $\boldsymbol{C}^{=i}$ and $\boldsymbol{C}^{\sim i}$ which are obtained from $\boldsymbol{J}$ by, respectively, identifying or connecting the vertices i and j,*
- $\boldsymbol{I} \coloneqq (I, (1, \dots, k), (1, \dots, k))$ *with* $V(I) = [k]$ *and* $E(I) = \emptyset$,
- *for $i \in [k]$, the graphs $\boldsymbol{M}^{\neq i} = (M^{\neq i}, (1, \dots, k), (1, \dots, i-1, i', i+1, \dots, k))$ with $V(M^{\neq i}) = [k] \cup \{i'\}$, $E(M^{\neq i}) = \emptyset$ and $\boldsymbol{M}^{\sim i} = (M^{\sim i}, (1, \dots, k), (1, \dots, i-1, i', i+1, \dots, k))$ with $V(M^{\sim i}) = [k] \cup \{i'\}$, $E(M^{\sim i}) = \{ii'\}$.*

Then $\mathcal{Q}_k^P$ is generated by $\mathcal{B}_k^P \coloneqq \{\boldsymbol{J}\} \cup \{\boldsymbol{C}^{=i}, \boldsymbol{C}^{\sim i} \mid i \in [2k]\}$ under parallel composition and $\mathcal{Q}_k^S$ is contained by the graph class generated by $\mathcal{B}_k^S \coloneqq \{\boldsymbol{I}\} \cup \{\boldsymbol{M}^{\neq i}, \boldsymbol{M}^{\sim i} \mid i \in [k]\}$ under series composition.

▶ **Lemma 35.** *Algorithm 1 is correct.*

Proof. Let B denote the set computed when Algorithm 1 terminates. We first argue that the vectors in B span S. Clearly, $B \subseteq S$ and thus $\operatorname{span}(B) \subseteq S$. The inclusion $S \subseteq \operatorname{span}(B)$ is shown by induction on the operations used in Definition 21 to define $\mathcal{P}_k$. The simplest graph in that set is $\boldsymbol{J}$. It holds that $\boldsymbol{J}_G \oplus \boldsymbol{J}_H \in B$, by initialisation. By Lemma 34, it holds that the homomorphism matrices of all bilabelled graphs in $\mathcal{Q}_k$ are in $\operatorname{span}(B)$. For the inductive step, let $\boldsymbol{P} \in \mathcal{P}_k$ be some graph.

If $\boldsymbol{P} = \boldsymbol{R} \cdot \boldsymbol{S}$ for the graphs $\boldsymbol{R}, \boldsymbol{S} \in \mathcal{P}_k$ to which the inductive hypothesis applies then $\boldsymbol{R}_G \oplus \boldsymbol{R}_H, \boldsymbol{S}_G \oplus \boldsymbol{S}_H \in \operatorname{span}(B)$. Hence, we may write $\boldsymbol{R}_G \oplus \boldsymbol{R}_H = \sum \alpha_i b_i$ and $\boldsymbol{R}_G \oplus \boldsymbol{R}_H = \sum \beta_i b_i$ for some $\alpha_i, \beta_i \in \mathbb{F}_p$ and $b_i \in B$. Since the algorithm terminated, it holds that $b_i \cdot b_j \in \operatorname{span}(B)$ for all i, j. Thus, $\boldsymbol{P}_G \oplus \boldsymbol{P}_H = \sum \alpha_i \beta_j b_i \cdot b_j \in \operatorname{span}(B)$. The cases when $\boldsymbol{P} = \boldsymbol{R} \odot \boldsymbol{S}$ for $\boldsymbol{R} \in \mathcal{Q}_k^P$ and when $\boldsymbol{P} = \boldsymbol{R}^\sigma$ for $\sigma \in \mathcal{C}(1, \dots, k, 2k, \dots, k+1)$ follow analogously.

It remains to argue that the acceptance condition $\mathbf{1}_G^T v \mathbf{1}_G = \mathbf{1}_H^T v \mathbf{1}_H$ for all $v \in B$ is correct. To that end, first assume that G and H are homomorphism indistinguishable over $\mathcal{P}_k$. Then for every $\boldsymbol{P} \in \mathcal{P}_k$ it holds that

$$\mathbf{1}_G^T (\boldsymbol{P}_G \oplus \boldsymbol{P}_H) \mathbf{1}_G = \operatorname{soe}(\boldsymbol{P}_G) = \operatorname{soe}(\boldsymbol{P}_H) = \mathbf{1}_H^T (\boldsymbol{P}_G \oplus \boldsymbol{P}_H) \mathbf{1}_H.$$

Since S is spanned by these vectors, it follows that $\mathbf{1}_G^T v \mathbf{1}_G = \mathbf{1}_H^T v \mathbf{1}_H$ for all $v \in B$.

Conversely, suppose that $\mathbf{1}_G^T v \mathbf{1}_G = \mathbf{1}_H^T v \mathbf{1}_H$ holds for all $v \in B$. Let $\boldsymbol{P} \in \mathcal{P}_k$ be arbitrary. By the previous claim, $\boldsymbol{P}_G \oplus \boldsymbol{P}_H \in \operatorname{span}(B)$. Hence, the assumption implies that $\operatorname{soe}(\boldsymbol{P}_G) = \operatorname{soe}(\boldsymbol{P}_H)$, as desired. ◀

▶ **Lemma 36.** *Algorithm 1 terminates in time $n^{O(k)}(k \log p)^{O(1)}$, where n is the maximum of $|V(G)|$ and $|V(H)|$.*

Proof. The initialisation (above Line 6) can be completed in time $n^{O(k)} k^{O(1)} (\log p)^{O(1)}$ noting that the set $\mathcal{B}_k$ is of size $O(k)$ by Lemma 34.

Throughout the execution of the algorithm, B is a set of linearly independent vectors in a $2n^{2k}$-dimensional vector space over $\mathbb{F}_p$. This implies that the loop in Line 6 is entered at most $2n^{2k}$ many times. It further more implies that the checks for linear independence in Lines 4, 9, 13 and 17 can be carried out in $n^{O(k)}(\log p)^{O(1)}$.

In each iteration of in Line 6, the first inner loop is entered at most $n^{O(k)} k^{O(1)}$ times. The second inner loop is entered at most $n^{O(k)}$ times. The third inner loops is entered at most $n^{O(k)} k^{O(1)}$ times. This yields the overall runtime bound. ◀

Reducing NPA to Modular NPA. If $G \ncong_{\mathcal{P}_k} H$, then there exists a graph $F \in \mathcal{P}_k$ such that $\hom(F, G) \neq \hom(F, H)$. Since $\hom(F, G), \hom(F, H) \leq n^{|V(F)|}$ for $n := \max\{|V(G)|, |V(H)|\}$, it follows that G and H are also not homomorphism indistinguishable over $\mathcal{P}_k$ modulo every prime p greater than $n^{|V(F)|}$. Unfortunately, there is a priori no bound on the size of F in terms of n. In this section, we give such a bound and thereby derive Theorem 2 from Theorem 33. For $l \in \mathbb{N}$, write $(\mathcal{P}_k)_{\leq l} := \{F \in \mathcal{P}_k \mid |V(F)| \leq l\}$.

▶ **Theorem 37.** *If $k \geq 1$, G, H are graphs on at most n vertices, and $f_k(n) := 2k \cdot 4^{n^{2k}}$, then*

$$G \cong_{\mathcal{P}_k} H \iff G \cong_{(\mathcal{P}_k)_{\leq f_k(n)}} H.$$

Towards Theorem 37, we define the following complexity measure $\nu \colon \mathcal{P}_k \to \mathbb{N}$ inductively. If $\boldsymbol{Q} \in \mathcal{Q}_k$, then $\nu(\boldsymbol{Q}) := 1$. For $\boldsymbol{F} \in \mathcal{P}_k$, define $\nu(\boldsymbol{F})$ inductively as the least number $n \in \mathbb{N}$ such that there exist

1. $\boldsymbol{F}' \in \mathcal{P}_k$ and $\boldsymbol{Q} \in \mathcal{Q}_k^P$ such that $\boldsymbol{F} = \boldsymbol{Q} \odot \boldsymbol{F}'$ and $n = \nu(\boldsymbol{F}')$, or

2. $\boldsymbol{F}', \boldsymbol{F}'' \in \mathcal{P}_k$ such that $\boldsymbol{F} = \boldsymbol{F}' \cdot \boldsymbol{F}''$ and $n = \max\{\nu(\boldsymbol{F}'), \nu(\boldsymbol{F}'')\} + 1$, or
3. $\boldsymbol{F}' \in \mathcal{P}_k$ and $\sigma \in \mathcal{C}(1, \dots, k, 2k, \dots, k+1)$ such that $\boldsymbol{F} = (\boldsymbol{F}')^\sigma$ and $n = \nu(\boldsymbol{F}')$.

By Definition 21, $\nu\colon \mathcal{P}_k \to \mathbb{N}$ is well-defined.

▶ **Lemma 38.** *Let $k \geq 1$. For every $\boldsymbol{F} \in \mathcal{P}_k$, it holds that $\boldsymbol{F}$ has at most $2k \cdot 2^{\nu(\boldsymbol{F})}$ vertices.*

As in Section 5, we consider a sequence of nested spaces of homomorphism matrices. For $l \geq 1$, write

$$S_l \coloneqq \operatorname{span}\{\boldsymbol{F}_G \oplus \boldsymbol{F}_H \mid \boldsymbol{F} \in \mathcal{P}_k, \nu(\boldsymbol{F}) \leq l\} \subseteq \mathbb{R}^{(V(G)^k \cup V(H)^k) \times (V(G)^k \cup V(H)^k)}.$$

Clearly, $S_1 \subseteq S_2 \subseteq \cdots \subseteq S \coloneqq \bigcup_{l \geq 1} S_l$. The space S is of dimension at most $2n^{2k}$. The following lemma shows that $S_{2n^{2k}} = S$.

▶ **Lemma 39.** *If $l \geq 1$ is such that $S_l = S_{l+1}$, then $S_l = S$.*

Proof of Theorem 37. Only the backward implication requires a justification. Suppose that G and H are homomorphism indistinguishable over all graphs in $\mathcal{P}_k$ of size at most $2k \cdot 4^{n^{2k}}$.

Let $\boldsymbol{F} \in \mathcal{P}_k$ be of arbitrary size. By Lemma 39, there exist $\boldsymbol{F}^i \in \mathcal{P}_k$ with $\nu(\boldsymbol{F}^i) \leq 2n^{2k}$ and coefficients $\alpha_i \in \mathbb{R}$ such that $\boldsymbol{F}_G \oplus \boldsymbol{F}_H = \sum \alpha_i \boldsymbol{F}^i_G \oplus \boldsymbol{F}^i_H$. By Lemma 38, the $\boldsymbol{F}^i$ have at most $2k \cdot 4^{n^{2k}}$ many vertices. Thus, $\hom(\operatorname{soe}(\boldsymbol{F}^i), G) = \hom(\operatorname{soe}(\boldsymbol{F}^i), H)$, by assumption. Hence,

$$\begin{aligned}
\hom(\operatorname{soe}(\boldsymbol{F}), G) &= \mathbf{1}_G^T (\boldsymbol{F}_G \oplus \boldsymbol{F}_H) \mathbf{1}_G = \sum \alpha_i \mathbf{1}_G^T (\boldsymbol{F}^i_G \oplus \boldsymbol{F}^i_H) \mathbf{1}_G \\
&= \sum \alpha_i \hom(\operatorname{soe}(\boldsymbol{F}^i), G) = \sum \alpha_i \hom(\operatorname{soe}(\boldsymbol{F}^i), H) \\
&= \sum \alpha_i \mathbf{1}_H^T (\boldsymbol{F}^i_G \oplus \boldsymbol{F}^i_H) \mathbf{1}_H = \hom(\operatorname{soe}(\boldsymbol{F}), H).
\end{aligned}$$

Here, $\mathbf{1}_G, \mathbf{1}_H \in \mathbb{R}^{V(G)^k \cup V(H)^k}$ denote the indicator vectors on the coordinates which correspond to G and H, respectively. Hence, G and H are homomorphism indistinguishable over $\mathcal{P}_k$. ◀

It remains to derive Theorem 2 from Theorems 33 and 37.

Proof of Theorem 2. A randomized algorithm for the problem Theorem 2 proceeds as similar to [23, Algorithm 2]. Let $N \coloneqq 2k \cdot 4^{n^{2k}}$ be as in Theorem 37. For $\lceil 4 \log(N \log(n)) \rceil = n^{O(k)}$ times, sample an integer $N \log n < p \leq (N \log n)^2$. This integer requires $n^{O(k)}$ many bits. In time $n^{O(k)}$, deterministically check whether p is a prime [2]. If it is a prime, run Algorithm 1 for G, H, k, and p. By Lemma 36, this takes time $n^{O(k)} k^{O(1)}$. If the algorithm asserts that $G \ncong_{\mathcal{P}_k} H$, reject. Otherwise, proceed. If p is not a prime, proceed to the next iteration.

By the proof of [23, Theorem 1.1], the probability of incorrectly accepting an instance such that $G \ncong_{\mathcal{P}_k} H$ is less than $1/2$. ◀

References

1 Samson Abramsky, Tomáš Jakl, and Thomas Paine. Discrete Density Comonads and Graph Parameters. In Helle Hvid Hansen and Fabio Zanasi, editors, *Coalgebraic Methods in Computer Science*, pages 23–44, Cham, 2022. Springer International Publishing. doi:10.1007/978-3-031-10736-8_2.

2 Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, September 2004. doi:10.4007/annals.2004.160.781.

3 Albert Atserias, Laura Mančinska, David E. Roberson, Robert Šámal, Simone Severini, and Antonios Varvitsiotis. Quantum and non-signalling graph isomorphisms. *Journal of Combinatorial Theory, Series B*, 136:289–328, 2019. doi:10.1016/j.jctb.2018.11.002.

4 László Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In Daniel Wichs and Yishay Mansour, editors, *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 684–697. ACM, 2016. doi:10.1145/2897518.2897542.

5 Anuj Dawar, Tomáš Jakl, and Luca Reggio. Lovász-Type Theorems and Game Comonads. In *36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021, Rome, Italy, June 29 - July 2, 2021*, pages 1–13. IEEE, 2021. doi:10.1109/LICS52264.2021.9470609.

6 Holger Dell, Martin Grohe, and Gaurav Rattan. Lovász Meets Weisfeiler and Leman. *45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, pages 40:1–40:14, 2018. doi:10.4230/LIPICS.ICALP.2018.40.

7 Zdeněk Dvořák. On recognizing graphs by numbers of homomorphisms. *Journal of Graph Theory*, 64(4):330–342, 2010. doi:10.1002/jgt.20461.

8 Eva Fluck, Tim Seppelt, and Gian Luca Spitzer. Going Deep and Going Wide: Counting Logic and Homomorphism Indistinguishability over Graphs of Bounded Treedepth and Treewidth. In Aniello Murano and Alexandra Silva, editors, *32nd EACSL Annual Conference on Computer Science Logic (CSL 2024)*, volume 288 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 27:1–27:17, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CSL.2024.27.

9 Martin Grohe. Counting Bounded Tree Depth Homomorphisms. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 507–520, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/3373718.3394739.

10 Martin Grohe, Gaurav Rattan, and Tim Seppelt. Homomorphism Tensors and Linear Equations. In Mikołaj Bojańczyk, Emanuela Merelli, and David P. Woodruff, editors, *49th International Colloquium on Automata, Languages, and Programming (ICALP 2022)*, volume 229 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 70:1–70:20, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ICALP.2022.70.

11 Prem Nigam Kar, David E Roberson, Tim Seppelt, and Peter Zeman. NPA hierarchy for quantum isomorphism and homomorphism indistinguishability. *arXiv preprint arXiv:2407.10635*, 2024. doi:10.48550/arXiv.2407.10635.

12 László Lovász. Operations with structures. *Acta Mathematica Academiae Scientiarum Hungarica*, 18(3):321–328, September 1967. doi:10.1007/BF02280291.

13 Laura Mančinska and David E. Roberson. Quantum isomorphism is equivalent to equality of homomorphism counts from planar graphs. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 661–672, 2020. doi:10.1109/FOCS46700.2020.00067.

14 Yoàv Montacute and Nihil Shah. The Pebble-Relation Comonad in Finite Model Theory. In Christel Baier and Dana Fisman, editors, *LICS '22: 37th Annual ACM/IEEE Symposium on Logic in Computer Science, Haifa, Israel, August 2 - 5, 2022*, pages 13:1–13:11. ACM, 2022. doi:10.1145/3531130.3533335.

15 Christopher Morris, Martin Ritzert, Matthias Fey, William L. Hamilton, Jan Eric Lenssen, Gaurav Rattan, and Martin Grohe. Weisfeiler and Leman Go Neural: Higher-Order Graph Neural Networks. *Proceedings of the AAAI Conference on Artificial Intelligence*, 33:4602–4609, 2019. doi:10.1609/aaai.v33i01.33014602.

16 Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, July 2008. doi:10.1088/1367-2630/10/7/073013.

17 Daniel Neuen. Homomorphism-Distinguishing Closedness for Graphs of Bounded Tree-Width. In Olaf Beyersdorff, Mamadou Moustapha Kanté, Orna Kupferman, and Daniel Lokshtanov, editors, *41st International Symposium on Theoretical Aspects of Computer Science (STACS 2024)*, volume 289 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 53:1–53:12, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.STACS.2024.53.

18 Gaurav Rattan and Tim Seppelt. Weisfeiler–Leman and Graph Spectra. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2268–2285. Society for Industrial and Applied Mathematics, 2023. doi:10.1137/1.9781611977554.ch87.

19 David E. Roberson. Oddomorphisms and homomorphism indistinguishability over graphs of bounded degree, 2022. arXiv:2206.10321v1.

20 David E Roberson and Tim Seppelt. Lasserre hierarchy for graph isomorphism and homomorphism indistinguishability. *TheoretiCS*, 3, 2024. doi:10.46298/THEORETICS.24.20.

21 Neil Robertson and P.D Seymour. Graph minors. iii. planar tree-width. *Journal of Combinatorial Theory, Series B*, 36(1):49–64, 1984. doi:10.1016/0095-8956(84)90013-3.

22 Tim Seppelt. Logical Equivalences, Homomorphism Indistinguishability, and Forbidden Minors. In Jérôme Leroux, Sylvain Lombardy, and David Peleg, editors, *48th International Symposium on Mathematical Foundations of Computer Science (MFCS 2023)*, volume 272 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 82:1–82:15, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2023.82.

23 Tim Seppelt. An Algorithmic Meta Theorem for Homomorphism Indistinguishability. In Rastislav Královič and Antonín Kučera, editors, *49th International Symposium on Mathematical Foundations of Computer Science (MFCS 2024)*, volume 306 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 82:1–82:19, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2024.82.

24 Tim Seppelt. *Homomorphism Indistinguishability*. Dissertation, RWTH Aachen University, Aachen, 2024. doi:10.18154/RWTH-2024-11629.

25 Keyulu Xu, Weihua Hu, Jure Leskovec, and Stefanie Jegelka. How Powerful are Graph Neural Networks? In *International Conference on Learning Representations*, 2018. URL: https://openreview.net/forum?id=ryGs6iA5Km.

26 Bohang Zhang, Jingchu Gai, Yiheng Du, Qiwei Ye, Di He, and Liwei Wang. Beyond Weisfeiler–Lehman: A Quantitative Framework for GNN Expressiveness. In *The Twelfth International Conference on Learning Representations*, 2024. URL: https://openreview.net/forum?id=HSKaGOi7Ar.