# $P_4$-free Partition and Cover Numbers and Application

Alexander R. Block    Simina Brânzei    Hemanta K. Maji    Himanshi Mehta
Tamalika Mukherjee    Hai H. Nguyen

**Abstract**

$P_4$-free graphs– also known as cographs, complement-reducible graphs, or hereditary Dacey graphs–have been well studied in graph theory. Motivated by computer science and information theory applications, our work encodes (flat) joint probability distributions and Boolean functions as bipartite graphs and studies bipartite $P_4$-free graphs. For these applications, the graph properties of edge partitioning and covering a bipartite graph using the minimum number of these graphs are particularly relevant. Previously, such graph properties have appeared in leakage-resilient cryptography and (variants of) coloring problems.

Interestingly, our covering problem is closely related to the well-studied problem of product/Prague dimension of loopless undirected graphs, which allows us to employ algebraic lower-bounding techniques for the product/Prague dimension. We prove that computing these numbers is NP-complete, even for bipartite graphs. We establish a connection to the (unsolved) Zarankiewicz problem to show that there are bipartite graphs with size-$N$ partite sets such that these numbers are at least $\varepsilon \cdot N^{1-2\varepsilon}$, for $\varepsilon \in \{1/3, 1/4, 1/5, \dots\}$. Finally, we accurately estimate these numbers for bipartite graphs encoding well-studied Boolean functions from circuit complexity, such as set intersection, set disjointness, and inequality.

For applications in information theory and communication & cryptographic complexity, we consider a system where a setup samples from a (flat) joint distribution and gives the participants, Alice and Bob, their portion from this joint sample. Alice and Bob's objective is to non-interactively establish a shared key and extract the left-over entropy from their portion of the samples as independent private randomness. A genie, who observes the joint sample, provides appropriate assistance to help Alice and Bob with their objective. Lower bounds to the minimum size of the genie's assistance translate into communication and cryptographic lower bounds. We show that (the $\log_2$ of) the $P_4$-free partition number of a graph encoding the joint distribution that the setup uses is equivalent to the size of the genie's assistance. Consequently, the joint distributions corresponding to the bipartite graphs constructed above with high $P_4$-free partition numbers correspond to joint distributions requiring more assistance from the genie.

As a representative application in non-deterministic communication complexity, we study the communication complexity of nondeterministic protocols augmented by access to the equality oracle at the output. We show that (the $\log_2$ of) the $P_4$-free cover number of the bipartite graph encoding a Boolean function $f$ is equivalent to the minimum size of the nondeterministic input required by the parties (referred to as the communication complexity of $f$ in this model). Consequently, the functions corresponding to the bipartite graphs with high $P_4$-free cover numbers have high communication complexity. Furthermore, there are functions with communication complexity close to the naïve protocol where the nondeterministic input reveals a party's input. Finally, the access to the equality oracle reduces the communication complexity of computing set disjointness by a constant factor in contrast to the model where parties do not have access to the equality oracle. To compute the inequality function, we show an exponential reduction in the communication complexity, and this bound is optimal. On the other hand, access to the equality oracle is (nearly) useless for computing set intersection.

# Contents

# 1 Introduction

A graph is $P_4$*-free* if no four vertices induce a path of length three. Since the 1970s, $P_4$-free graphs—also known as cographs, complement-reducible graphs, or hereditary Dacey graphs from empirical logic [Fou69]—have been widely studied in graph theory [Ler71, Ler72, Jun78, Sei74, Sum74]. Motivated by computer science and information theory applications, our work encodes joint probability distributions and Boolean functions as bipartite graphs and studies *bipartite* $P_4$-free graphs.[1] For these applications, the graph properties of edge *partitioning* and *covering* a bipartite graph using the minimum number of these graphs are particularly relevant.[2]

The $P_4$*-free partition number* of a bipartite graph $G$ is the minimum number of $P_4$-free subgraphs partitioning $G$'s edges, denoted by $\mathsf{P_4\text{-}fp}(G)$. Similarly, the $P_4$*-free cover number* of a bipartite graph $G$ is the minimum number of $P_4$-free subgraphs covering $G$'s edges, denoted by $\mathsf{P_4\text{-}fc}(G)$. The definition extends to general graphs; however, our study focuses on bipartite graphs. We are given a bipartite graph as input, and the objective is to partition or cover its edges using bipartite graphs. $P_4$-free partition and cover numbers are natural extensions of fundamental graph properties, such as product/Prague dimension, equivalence cover number, biclique partition, and cover numbers, arboricity, and star arboricity (refer to [W$^+$96] for definitions). In turn, these graph properties have applications to theoretical computer science, information theory, and combinatorial optimization; for a discussion of these connections, see Appendix E.

In addition to being motivated by intellectual curiosity, our work illustrates that the $P_4$-free partition and cover numbers appear in diverse computer science and information theory problems (refer to problems A and B in Section 1.1). Section 1.2 presents the equivalence between the $P_4$-free partition number and Problem A, and the consequences of the graph theory results for problem A. Next, Section 1.3 demonstrates the equivalence of Problem B and the $P_4$-free cover number, and the implications of the graph results for problem B. Interestingly, we prove that the $P_4$-free cover number of a bipartite graph is either identical to or one less than the well-studied product/Prague dimension [NP77, NR78] of the complement graph (interpreted as a loopless undirected graph). Our work proves the following graph theory results (refer to Section 2 for formal statements).

1. Determining the $P_4$-free partition & cover numbers of general graphs, even bipartite ones, is $\mathsf{NP}$-complete.

2. There are bipartite graphs with size-$N$ partite sets whose $P_4$-free partition and cover numbers are at least $\varepsilon \cdot N^{1-2\varepsilon}$, for constant $\varepsilon \in \{1/3, 1/4, 1/5, \dots\}$. Furthermore, Erdős-Rényi graphs (with constant parameter) have $P_4$-free partition and cover numbers $\geqslant N/\log N$ asymptotically almost surely.

3. Finally, we encode the Boolean set intersection and disjointness functions, and the inequality function as bipartite graphs. We present tight estimates of the $P_4$-free partition and cover numbers of these graphs.

Section 3 provides a technical overview of our proof-techniques. The appendices contain all the formal definitions, the omitted proofs, and additional discussions.

[1] A bipartite $P_4$-free graph is a disjoint union of *bicliques*. Figure 4 presents a pictorial representation capturing their intuition.

[2] In contrast, [HL01] introduced the *vertex* partitioning a graph into different color-classes so that the vertices of any color-class induces a $P_4$-free graph.


(a) Problem A: Assistance for Correlation Distillation

(b) Communication and Cryptographic lower bounds

Figure 1: Part (a). A pictorial summary of the system in our motivating problem A.
Part (b). The setup samples $(x, y)$ according to the distribution $p_{XY}$ and sends $x$ to Alice and $y$ to Bob. Alice and Bob use $F$ adaptively multiple times to communicate with each other; $F$ delivers its output to both Alice and Bob. The functionality $F$ may be a communication protocol (i.e., a message forwarding functionality), or help Alice and Bob evaluate any (possibly, a stateful) functionality of their inputs. The objective of Alice and Bob is to generate a shared secret key $s$ at the end of the protocol and extract the left-over entropy in their shares as independent local randomness.

## 1.1 Motivating Problems

We encode joint probability distributions and Boolean functions as equivalent bipartite graphs and study the $P_4$-free partition and cover numbers of these graphs. Leveraging this connection, we present representative applications of these graph properties and their estimates to information theory and circuit complexity (refer to Appendix A for relevant background and terminology). In particular, consider the following illustrative representative problems from information theory and communication & cryptographic complexity motivating this study.

**Problem A. Assistance for Correlation Distillation.** Extracting randomness [ILL89, NZ93], establishing secret keys [Mau91, Mau92, Mau93, AC93, AC98], and performing general secure computation [CK88, CK90, Kil88, Kil91, DKS99, Kil00, CMW05, Wul07, Wul09, KMS16, CDLR16] with maximum efficiency and resilience from noise sources is fundamental to theoretical computer science and information theory. Towards that objective, we study the communication and cryptographic complexity of parties to agree on a shared secret and extract private local randomness from a source.

A setup (see part (a) of Figure 1.1), the only source of randomness in the system, samples $(x, y)$ according to the joint probability distribution $p_{XY}$, and (privately) sends $x$ to Alice and $y$ to Bob. Alice and Bob's objective is to agree on a shared secret key and private (independent) randomness without any additional public communication. A genie, who observes the sample $(x, y)$, provides a public $k$-bit assistance $z$ to Alice and Bob to facilitate their efforts. We emphasize that all agents Alice, Bob, and the genie are deterministic. After that, Alice and Bob locally compute the shared key $s$ from their respective local views $(x, z)$ and $(y, z)$. Finally, Alice extracts the left-over entropy from $x$ (conditioned on $(s, z)$) as her local private randomness $r_A$. Similarly, Bob extracts his local private randomness $r_B$ from the left-over entropy of $y$.

For the security of Bob's local randomness, an honest but curious Alice cannot obtain any additional information on $r_B$ beyond what is already revealed by $z$ and $s$. Analogously, Bob's view should contain no additional information on Alice's view conditioned on $z$ and $s$. Intuitively, conditioned on the genie's assistance $Z$, Alice-Bob samples' joint distribution splits into shared randomness and local independent randomness.

What is the *minimum* length $k$ of the genie's assistance sufficient for Alice and Bob to agree on a shared key and obtain secure private randomness? In particular, which distributions $p_{XY}$ need no assistance at all?

Mutual information and other common information variants (refer to Appendix D for discussion) cannot accurately measure this information-theoretic measure; thus, motivating our study. This problem is equivalent to computing the $P_4$-free partition number of a bipartite graph encoding the (flat) joint probability distribution $p_{XY}$. In particular, lower bounds to $k$ translates into lower bounds on (interactive) communication and cryptographic complexity (see part (b) of Figure 1.1).

**Problem B. Nondeterministic Communication Complexity relative to the Equality Oracle.** The nondeterministic communication complexity of the equality function is high [KN97]. However, what is the additional utility of an oracle call to the equality function in computing other functions?

Suppose Alice has input $x \in X$, Bob has input $y \in Y$, and are interested in computing the Boolean function $f\colon X \times Y \to \{0,1\}$ of their private inputs. They have access to an *equality oracle* $\mathsf{EQ}\colon \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ defined by $\mathsf{EQ}(a,b) = 1$ if and only if $a = b$. They are interested in computing $f(x,y)$ using this equality oracle and a $k$-bit nondeterministic input *without any additional communication.*

The functions $A\colon X \times \{0,1\}^k \to \{0,1\}^*$ and $B\colon Y \times \{0,1\}^k \to \{0,1\}^*$ satisfying the following constraints define a *nondeterministic protocol* for $f$ relative to the equality oracle.

1. For every input-pair $(x,y) \in X \times Y$ such that the output $f(x,y) = 1$, there exists a nondeterministic input $z \in \{0,1\}^k$ ensuring $\mathsf{EQ}(\ A(x,z)\ ,\ B(y,z)\ ) = 1$.
2. For every input-pair $(x,y) \in X \times Y$ such that the output $f(x,y) = 0$, for all nondeterministic inputs $z \in \{0,1\}^k$, we have $\mathsf{EQ}(\ A(x,z)\ ,\ B(y,z)\ ) = 0$.

The *communication complexity* of this protocol is $k$, i.e., the length of the nondeterministic input. What is the *minimum* communication complexity $k$ of the function $f$?

Intuitively, we are augmenting the nondeterministic communication protocols with an equality oracle at the output. If the $\mathsf{EQ}$ oracle is useful to compute a function $f$, then its communication complexity in our model shall be significantly lower than where the parties cannot access the $\mathsf{EQ}$ oracle. We show that this problem is identical to the $P_4$-free cover number of a bipartite graph encoding the Boolean function $f$. Our results show that the access to the equality oracle reduces the communication complexity of computing set disjointness by a constant factor compared to the model where parties do not have access to the equality oracle. To compute the inequality function, perhaps surprisingly, we show an *exponential* reduction in the communication complexity. On the other hand, access to the equality oracle is virtually useless to computing the set intersection. Section 1.3 provides the details.

**Additional Applications.** In Appendix F, we present a representative scheduling problem that naturally reduces to computing $P_4$-free partition/cover numbers. Beyond the applications above, this example highlights the innate ability of $P_4$-free graphs to encode scheduling problems that are amenable to *parallelization.*

**History.** Edge-partitioning graphs using the minimum number of $P_4$-free graphs have found applications in *leakage-resilient cryptography* [BMN17]. In particular, if $k$-bits of genie's assistance suffices for the setup in problem A, then $k$-bits of leakage also suffices for the adversary to destroy the possibility of performing general secure computation. Identifying a large $P_4$-free subgraph of a given graph is studied in clustering. For example, an *exclusive row and column bicluster* [MO04, Kai11] is identical to a $P_4$-free graph, with applications in analyzing biological data. [CFG$^+$12] used $P_4$-free partition and cover numbers to approach a coloring conjecture (a variant of Ryser's conjecture) for bipartite graphs.

#### 1.1.1 Related graph properties: Equivalence Cover Number and Product/Prague Dimension

The following discussion is specific to *loopless undirected graphs*. An *equivalence graph* is a (disjoint) union of cliques. The *equivalence cover number* of a graph $G$ is the minimum number $d$ of equivalence sub-graphs that cover the edges of $G$ [NP77, NR78]. Note that the $P_4$-free cover number is an extension of this concept to bipartite graphs. Furthermore, the equivalence cover number of $G$ is identical to the *product/Prague dimension* of the complement of the graph $G$ [W$^+$96, HIK11], the minimum $d \in \mathbb{N}$ such that the complement of the graph $G$ is an induced subgraph of $K_{\mathbb{N}}^d$ (the $d$-fold product of the infinite complete graph $K_{\mathbb{N}}$). Computing the equivalence cover number or the product dimension of a graph is $\mathsf{NP}$-complete [NP77].

The $P_4$-free cover number (for bipartite graphs) has a close connection to the product/Prague dimension.

**Proposition 1.** *If a redundancy-free*[3] *bipartite graph $G = (L, R, E)$ has a size-$d$ $P_4$-free edge-covering, then the complement bipartite graph $\overline{G} \coloneqq (L, R, L \times R \setminus E)$ is an induced subgraph of $K_2 \times K_{\mathbb{N}}^d$.*

The converse of the proposition does not hold exactly (refer to Section 3.4). However, if $\overline{G}$ is an induced subgraph of $K_2 \times K_{\mathbb{N}}^d$, then $G$ has a size-$(d+1)$ $P_4$-free cover. We prove that $\mathsf{P_4\text{-}fc}\,(G) \in \{\mathsf{pdim}\,(H)\,, \mathsf{pdim}\,(H) - 1\}$, where $G = (L, R, E \subseteq L \times R)$ is a bipartite graph, $H = (L \cup R, L \times R \setminus E)$ is the loopless undirected graph representing the complement of the bipartite graph $G$, and $\mathsf{pdim}\,(H)$ is the product/Prague dimension of $H$ (refer to Corollary 5 in Appendix K). Figure 13 presents a graph showing the necessity of this slack in the characterization. However, for most applications, an additive slack of one should be acceptable. This proposition facilitates lower-bounding the $\mathsf{P_4\text{-}fc}\,(G)$ using the algebraic lower-bounding techniques for the product/Prague dimension [LNP80, Alo86, W$^+$96, AA20].

Despite this similarity, extremal properties of the equivalence cover number and product/Prague dimension need not translate into extremal properties of the $P_4$-free cover number. For example, an $N$-vertex star has an equivalence cover number $(N-1)$ [W$^+$96]. On the other hand, the $P_4$-free cover number of any bipartite graph with size-$N$ partite sets is at most its star arboricity (because star forests are $P_4$-free), which is at most (roughly) $N/2$ [AA89]. The bottleneck here is that the $\mathsf{P_4\text{-}fc}\,(G)$ is close to $\mathsf{pdim}\,(H)$, where $H$ represents a bipartite graph, i.e., the graph $H$ is structured (triangle-free in this particular case). The graphs realizing the extremal properties for equivalence cover number and product/Prague need not have this structure. In particular, the construction of bipartite graphs with high $P_4$-free cover and partition numbers turns out to be non-trivial, and our work establishes a connection to the well-known (unsolved) Zarankiewicz problem [Bol04] and relies on probabilistic techniques to demonstrate their existence.

Appendix K also presents a variant of the product/Prague dimension to estimate the $P_4$-free partition number (see Corollary 6). Call a lower bound for the $P_4$-free partition number non-trivial if it is not already a lower bound to the $P_4$-free cover number. Unfortunately, no non-trivial lower-bounding techniques for general graphs are known for this new graph embedding property. When

[3] A graph is redundancy-free if no two vertices have an identical neighborhood.

| | 00 | 11 | 01 | 10 |
|---|---|---|---|---|
| 00 | 1 | 1 | 0 | 0 |
| 11 | 1 | 1 | 0 | 0 |
| 01 | 0 | 0 | 1 | 1 |
| 10 | 0 | 0 | 1 | 1 |

(a) Forward or flip.

| | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| 00 | 1 | 1 | 0 | 0 |
| 01 | 0 | 1 | 1 | 0 |
| 10 | 0 | 0 | 1 | 1 |
| 11 | 1 | 0 | 0 | 1 |

(b) Noisy typewriter.

Figure 2: Pictorial representation of the probability distributions (a) forward or flip, and (b) noisy typewriter distributions, for $n = 2$. Rows correspond to Alice samples, and columns correspond to Bob samples. The $(i, j)$-th entry of a matrix being 1 represents that $(i, j)$ is in the support of the distribution. The distribution is a uniform distribution over all the elements in the support. Let $G_a$ be the bipartite graph whose adjacency matrix is defined by the matrix representation of the forward and flip distribution. The graph $G_a$ is a disjoint union of $2^{n-1}$ copies of the $K_{2,2}$ biclique. Note that $G_a$ is $P_4$-free, and, hence, $\mathsf{P_4\text{-}fp}(G_a) = 1$. Let $G_b$ be the bipartite graph whose adjacency matrix is defined by the matrix representation of the noisy typewriter distribution. The graph $G_b$ is a cycle of length $2^{n+1}$. Note that $G_b$ is *not* $P_4$-free, and $\mathsf{P_4\text{-}fp}(G_b) = 2$ (the graph decomposes into two matchings).

non-trivial lower bounds for this variant of the product/Prague dimension is proven, they shall transfer to the $P_4$-free partition number.

Among several notions of product dimension for graphs [HIK11], most of which are unrelated to the property we wish to capture,[4] the graph property mentioned above is the closest and most relevant.

## 1.2 $P_4$-free Partition Number

We reduce problem A to computing the $P_4$-free partition number in Appendix B. We present the reduction's highlight. A bipartite graph $G$ naturally represents a (flat) joint distribution $p_{XY}$, where the edge-set is the support of $p_{XY}$ (see Figure 2 for examples). If $G$ is already $P_4$-free, then Alice and Bob need no assistance from the genie; the connected component's identity is their shared key $s$, and (conditioned on the identity of the shared key) their samples $r_A = (x|s)$ and $r_B = (y|s)$ are independent private randomness. If $G$ is not $P_4$-free, the genie decomposes $G$ into $G_1, \ldots, G_d$ such that each $G_i$ is $P_4$-free and the edge sets $E(G_1), \ldots .E(G_d)$ partition the edge set $E(G)$. For a joint sample $(u, v) \in E(G)$, the genie reveals the (unique) $z = i$ such that $(u, v) \in E(G_i)$. Conditioning on the genie's assistance $z = i$, Alice-Bob's samples come from the joint distribution $G_i$, which is $P_4$-free, so they agree on their shared key and secure private randomness as above. To minimize the genie's assistance, one needs to minimize $d \in \mathbb{N}$, identical to $\mathsf{P_4\text{-}fp}(G)$.

### 1.2.1 Discussion of Problem A

We begin by expanding how lower-bounding the information-theoretic measure in problem A translates into communication and cryptographic lower bounds (as in [BIKK14]). Suppose, in our model, one proves that the genie's assistance must be $k \geqslant k^*$ bits. Now consider the setting in part (b) of Figure 1.1 where there is no genie; however, the parties have access to a functionality $F$. The functionality $F$ may be an arbitrary *communication protocol* or multiple calls to arbitrary *interactive stateful functionalities* that receive adaptive inputs from Alice and Bob. In particular, $F$ may be multiple copies of the NAND-functionality, which is sufficient for general secure computation [Yao82, GMW87, Kil00]. Observe that the genie can simulate the functionality $F$'s entire

[4]Even ones that are deceptively similar sounding, for example, the "product dimension of bipartite graphs" introduced by [PRP83].

output with access to $(x, y)$. Consequently, we have the following result.

**Proposition 2.** *If $p_{XY}$ needs $k \geqslant k^*$ bits of assistance from the genie in our model, then Alice and Bob need to receive at least $k^*$ bits from $F$ in the Figure 1.1 part (b) model to establish a shared key $s$ and extract the left-over entropy in their sample as independent private randomness.*

In information theory, Gray-Wyner systems/networks are well-studied [Wyn75]. However, existing measures like mutual information and various notions of common information are inadequate to capture the information-theoretic property in Problem A accurately. For example, there are two joint distributions with identical (Shannon's) mutual information [Sha48]; however, one needs no assistance while the other needs one-bit assistance.[5] Refer to Figure 2 for the following discussion. Consider the first distribution (namely, the *forward or flip distribution*), where Alice gets i.i.d. uniformly random bits $x = (x_1, x_2, \ldots, x_n)$, and Bob either (with probability half) gets $y = x$ or $y = (\overline{x_1}, \ldots, \overline{x_n})$, i.e., every bit of $x$ is flipped. In the second distribution (the *noisy typewriter distribution*), Alice gets a uniformly random sample $x \in \{0, 1, \ldots, 2^n - 1\}$, and Bob either gets $y = x$ or $y = (x + 1) \mod 2^n$ with probability half. The bipartite graph corresponding to the forward or flip distribution is, indeed, $P_4$-free, and the bipartite graph corresponding to the noisy typewriter distribution has $P_4$-free partition number 2 (i.e., one-bit assistance is necessary and sufficient). Both distributions have $(n - 1)$ bits of mutual information; however, the first distribution needs no assistance, but the second distribution needs one-bit assistance[6] to agree on a secret key.

Wyner's common information [Wyn75] estimates the minimum assistance that removes any dependence between Alice-Bob samples. This quantity is a significant overestimation (for example, in the forward or flip distribution, it needs $(n-1)$-bits of assistance $z = (x_1, \ldots, x_{n-1})$), and Wyner's assistance eliminates the possibility of Alice and Bob agreeing on a secret key, which defeats the objective of this problem. Gács-Körner common information [GK73] estimates the length of the secret key that Alice and Bob can generate without any assistance from the genie, which results in pessimistic estimates. For example, starting with samples from the noisy typewriter distribution, Alice and Bob cannot even agree on a one-bit secret; however, appropriate one-bit assistance would help them generate an $(n - 1)$-bit secret. Likewise, non-interactive correlation distillation [MOR$^+$06, MO05] enables parties to agree on a secret non-interactively *without any assistance*. However, even without the necessity to generate independent local randomness, strong hardness of computation results are known [MOR$^+$06, MO05, Yan04, BM11, CMN14].

Refer to Appendix D for additional discussion on various forms of common information.

### 1.2.2 Our results for Problem A

Observe that the naïve assistance that reveals the XOR of the parties' inputs suffices; however, the minimum assistance may be exponentially smaller. Our work relies on suitably encoding (flat) joint distributions as bipartite graphs. We prove in Theorem 1 that ascertaining the minimum assistance is, in general, difficult. Furthermore, there are joint distributions where the minimum assistance needed is close to the naïve assistance mentioned above, yielding lower bounds in communication and cryptographic complexity. In other words, we obtain the following as a corollary to Theorem 2.

**Corollary 1.** *Let $\Omega_X = \Omega_Y = \{0, 1\}^n$. Fix $t \in \mathbb{N}$. There are joint distributions over the sample space $\Omega_X \times \Omega_Y$ that require Alice and Bob to (each) receive at least $\left(1 - \frac{2}{t+2}\right) n$ bits of communication in the model in Figure 1.1 part (b).*

[5] By tensorizing the distributions, one can increase the gap in the necessary assistance arbitrarily.

[6] The genie notifies the parties whether $y = x$ or not.

Finally, we upper-bound the minimum assistance needed for a few well-studied probability distributions i.e. when $p_{XY}$ is the $\mathsf{INT}_n$[7] or the $\mathsf{DISJ}_n$[8] joint distribution, then $\lceil n/2 \rceil$-bit assistance suffices (we explicitly provide the assistance that the genie provides and it is efficient to compute, see Theorem 3). For $\mathsf{INEQ}_N$, where $N = 2^n$, the genie needs to provide $\lceil \log n \rceil$ bits of assistance. The assistance for $\mathsf{INEQ}_N$ is optimal because we prove a matching lower bound. In general, $\min\{\log_2 N, \frac{1}{2}\log_2|\mathrm{Supp}(p_{XY})|\}$ bits of assistance suffices.[9]

## 1.3 $P_4$-free Cover Number

We reduce Problem B to the $P_4$-free cover number in Appendix C. Boolean functions naturally encode a bipartite graph's adjacency matrix; an input-pair that evaluates to 1 denotes an edge in the graph. If the graph $G$ (of a function $f$) is $P_4$-free, then parties need no nondeterministic input; they can evaluate $f$ using the $\mathsf{EQ}$ oracle.[10] Otherwise, decompose $G$ into $G_1, \ldots, G_d$ such that the union of the edge-sets of $G_1, \ldots, G_d$ is the edge-set of $G$. For input $(x, y)$ such that $f(x, y) = 1$, the nondeterministic input is $i \in \{1, \ldots, d\}$, where the edge-set of $G_i$ contains the edge $(x, y)$. Next, given this nondeterministic input, parties can evaluate $f$. For input $(x, y)$ such that $f(x, y) = 0$, no nondeterministic input can make Alice and Bob output 1. One minimizes $d \in \mathbb{N}$ to minimize the nondeterministic communication complexity, which is identical to $\mathsf{P_4\text{-}fc}(G)$.

### 1.3.1 Discussion on Problem B

The equality function in the *standard* nondeterministic communication complexity model (where parties *do not* have access to the $\mathsf{EQ}$ oracle) has high nondeterministic communication complexity. Determining the minimum nondeterministic input is equivalent to covering the input-pairs where the output is 1 using a minimum number of *combinatorial rectangles*, a.k.a., the *biclique cover number* [Juk12]. The motivating problem's objective is to characterize the utility of oracle access to the $\mathsf{EQ}$ function in computing other functions. If the $\mathsf{EQ}$ oracle is useful, then the nondeterministic communication complexity relative to the $\mathsf{EQ}$ oracle shall be lower than without accessing the $\mathsf{EQ}$ oracle. The particular notion of "reduction" considered above is similar to Karp-reduction [Kar72], which permits only one call to the oracle and no post-processing of the oracle's output. Similarly, in circuit complexity, it is typical to augment a circuit class with a more expressive gate at the output that is not computable by circuits in that class. For example, one studies the effects of augmenting $\mathsf{AC}^0$ circuits with a MAJ (majority) gate or a THR (threshold) gate at the output [ABFR91, Gol97, JKS02, GS10], enabling a controlled exploration of the gap between the power of $\mathsf{AC}^0$ and $\mathsf{TC}^0$ circuits.

### 1.3.2 Our results for Problem B

Similar to the result for $P_4$-free partition number, we prove that computing the $P_4$-free cover number is difficult (see Theorem 1), and there are functions that need nondeterministic input (roughly) the size of the parties' inputs, in other words, we obtain the following as a corollary to Theorem 2.

[7] Alice receives random $X \subseteq \{1, 2, \ldots, n\}$, and Bob receives random $Y \subseteq \{1, 2, \ldots, n\}$ conditioned on $X \cap Y \neq \emptyset$.

[8] Alice receives random $X \subseteq \{1, 2, \ldots, n\}$, and Bob receives random $Y \subseteq \{1, 2, \ldots, n\}$ conditioned on $X \cap Y = \emptyset$.

[9] Because, $\mathsf{P_4\text{-}fp}(G) \leqslant \mathsf{sa}(G) \leqslant \mathcal{O}\left(\sqrt{|E(G)|}\right)$. The last bound on the star arboricity of $G$ follows from an averaging argument and the bound of [AA89].

[10] Parties compute the connected component where their private input belongs. Then, they use the $\mathsf{EQ}$ oracle to test if they belong to the same connected component.

**Corollary 2.** *Fix $t \in \mathbb{N}$. There are Boolean functions $f: \{1, 2, \ldots, N\} \times \{1, 2, \ldots, N\} \to \{0, 1\}$ requiring at least $(1 - \frac{2}{t+2}) \log_2 N$ bits of nondeterministic input in the communication complexity model where parties have access to the* $\mathsf{EQ}$ *oracle.*

These functions are analogs of the "fooling sets" in our communication model. In the standard nondeterministic communication model, the $\mathsf{EQ}$ function is hard-to-compute and needs $n$-bits of nondeterministic input. The "fooling set" lower-bounding technique draws inspiration from this result. For a general $f$, this argument demonstrates pairs of Alice and Bob's input-sets where only the diagonal elements are 1; and the rest are 0. That is, the function $f$ has an embedded $\mathsf{EQ}$ function. The size of this "embedded $\mathsf{EQ}$" (a.k.a., the fooling set) in $f$ suffices to prove lower bounds on the nondeterministic input needed to compute $f$. In our setting, these functions that require $(1 - \frac{2}{t+2})n$-bit nondeterministic input serve as "fooling sets" in the nondeterministic communication complexity model where parties can access the $\mathsf{EQ}$ oracle.

Next, we provide estimates for some well-known functions in communication complexity (see Theorem 3). We prove that the $P_4$-free cover number of $\mathsf{DISJ}_n$ is (roughly) $\leqslant \sqrt{N}$. That is, only $n/2$ bits of nondeterministic input suffices to compute this function. Recall that, in the standard model, the function $\mathsf{DISJ}_n$ requires $n$-bit nondeterministic input because $\{(X, \{1, 2, \ldots, n\} \setminus X)\}_{X \subseteq \{1,2,\ldots,n\}}$ is a fooling set. Consequently, our result demonstrates a linear gap in the number of bits needed in our model, which indicates that the $\mathsf{EQ}$ oracle is non-trivially useful to compute $\mathsf{DISJ}_n$. We prove a lower bound showing that $0.085n$-bit assistance is necessary.

Next, we prove that the $P_4$-free cover number of $\mathsf{INT}_n$ is between $n$ and $n(1 - \frac{\log_2(n)}{n})$. Observe that the nondeterministic communication complexity of $\mathsf{INT}_n$ (without access to the $\mathsf{EQ}$ oracle) is already $\lceil \log_2 n \rceil$ bits. Consequently, $\mathsf{EQ}$ oracle's access is practically useless because the difference between the ceiling of the log of the lower and the upper bounds is at most 1 (asymptotically).

Finally, we show that $\mathsf{INEQ}_N$ needs only $\log_2 \log_2 N$ bit nondeterministic input using the $\mathsf{EQ}$ oracle (see Figure 5). Intuitively, if $N = 2^{2^s}$ and all inputs are $2^s$-bit binary strings, then the nondeterministic input is the $s$-bit index where the parties' input differ. Recall that in the standard model (without access to the $\mathsf{EQ}$ oracle), $\mathsf{INEQ}_N$ requires $\log_2 N$-bit nondeterministic input, which is exponentially higher (see Figure 7). Furthermore, using the algebraic technique of [LNP80, W$^+$96], we prove a matching lower bound to the $P_4$-free cover number of $\mathsf{INEQ}_N$. Observe that we prove that $\mathsf{P_4\text{-}fp}(\mathsf{INEQ}_N)$, not just $\mathsf{P_4\text{-}fc}(\mathsf{INEQ}_N)$, matches the lower bound for the $\mathsf{P_4\text{-}fc}(\mathsf{INEQ}_N)$.

## 2 Our Contribution

We prove the $\mathsf{NP}$-completeness of determining the $P_4$-free partition and cover numbers of a bipartite graph.

**Theorem 1** (Hardness of $P_4$-free Partition and Cover)**.** *The following languages are* $\mathsf{NP}$*-complete.*

$$P_4\textsf{-}\mathit{FREE\text{-}PART} = \{ \langle G \rangle \mid G \text{ is a bipartite graph and } \mathsf{P_4\text{-}fp}(G) \leqslant 2 \},$$
$$P_4\textsf{-}\mathit{FREE\text{-}COV} = \{ \langle G \rangle \mid G \text{ is a bipartite graph and } \mathsf{P_4\text{-}fc}(G) \leqslant 2 \}.$$

Similar problems, for example, calculating the biclique partition number/cover [Orl77] and star arboricity [Jia18] (even for bipartite graphs) are $\mathsf{NP}$-complete.

Next, we prove there are graphs $G$ with large $P_4$-free partition and cover numbers. Note that for a bipartite graph $G = (L, R, E)$, we have $\mathsf{P_4\text{-}fc}(G) \leqslant \mathsf{P_4\text{-}fp}(G) \leqslant \min\{|L|, |R|\}$ by decomposing the graph into stars rooted at vertices of the smaller partite set. Towards understanding the tightness of this naïve upper-bound, we show that, for any $N \in \mathbb{N}$ and constant $\varepsilon \in \{1/3, 1/4, \ldots\}$, there are bipartite graphs with size-$N$ partite sets and $\mathsf{P_4\text{-}fp}(G) \geqslant \mathsf{P_4\text{-}fc}(G) \geqslant \Omega(\varepsilon \cdot N^{1-2\varepsilon})$ (roughly).

**Theorem 2** (High $P_4$- Free Partition and Cover Numbers)**.** *Let $C$ be an appropriate positive absolute constant and $t \in \mathbb{N}$ be a parameter. There exists $N_0 \in \mathbb{N}$ such that for all $N \in \mathbb{N}$ and $N \geqslant N_0$, there is a graph $G_{N,t} = (L, R, E)$ such that (1) $|L| = |R| = N$, and (2)* $\mathsf{P_4\text{-}fp}\left(G_{N,t}\right) \geqslant \mathsf{P_4\text{-}fc}\left(G_{N,t}\right) \geqslant C \cdot \frac{N^{1-\frac{2}{t+2}}}{t}$.

Our constructions rely on extremal bipartite graphs that avoid $K_{t+1,t+1}$-subgraphs (the unsolved Zarankiewicz problem [Bol04]), for which only probabilistic constructions are known (refer to the discussion in Section 3.2). Explicit constructions are known only for very specialized values of $t$. However, the $P_4$-free partition and cover numbers of $G_{N,t}$ cannot be too large. For any sparse bipartite graph $G$, using an averaging argument, its star-arboricity has the upper bound $\mathsf{sa}\left(G\right) \leqslant \mathcal{O}\left(\sqrt{|E(G)|}\right)$ [AA89]. Since star forests are $P_4$-free and $G_{N,t}$ has $\mathcal{O}\left(N^{2-\frac{2}{t+1}}\right)$ edges, it implies that $\mathsf{P_4\text{-}fp}\left(G_{N,t}\right) \leqslant \mathcal{O}\left(N^{1-\frac{1}{t+2}}\right)$.

In problem A, the joint distributions corresponding to these bipartite graphs require a lot of assistance from the genie. Consequently, these lower bounds translate into communication and cryptographic complexity lower bounds. The functions corresponding to these bipartite graphs are difficult to compute for parties with nondeterministic input and access to the $\mathsf{EQ}$ oracle. If these functions are embedded in another function, then that function must have high nondeterministic communication complexity as well.

As a corollary (of the proof technique presented above), we prove the following result for dense bipartite graphs drawn from the Erdős-Rényi distribution with (constant) parameter $p \in (0, 1)$. Graphs drawn from $\mathsf{ER}(N, N, p)$ avoid bicliques with size-$(2\log_a N)$ partite sets. Therefore, we have the following result.

**Corollary 3** (High $P_4$-Free Partition and Cover Number of Erdős-Rényi Graphs)**.** *Let $p \in (0, 1)$ be a constant parameter. Let $\mathsf{ER}(N, N, p)$ represent the distribution over the sample space of all bipartite graphs over size-$N$ partite sets that includes every edge into the graph independently with probability $p$. Then, for $a = 1/p$, we have*

$$\Pr\left[\mathsf{P_4\text{-}fp}\left(G\right) \geqslant \mathsf{P_4\text{-}fc}\left(G\right) \geqslant \frac{pN}{4\log_a N} \cdot (1 - o(1)) \colon G \xleftarrow{\$} \mathsf{ER}(N, N, p)\right] \geqslant 1 - o(1).$$

Upper bounds to the $P_4$-free cover and partition numbers for bipartite Erdős-Rényi graphs is potentially an extremely challenging problem. Upper-bounding the $P_4$-free partition number of Erdős-Rényi bipartite graphs remains open.

Finally, we estimate the $P_4$-free partition and cover numbers for the graphs $\mathsf{INT}_n, \mathsf{DISJ}_n$, and $\mathsf{INEQ}_N$ that are well-studied functions from communication theory and are defined below.

1. **The Intersection Graph.** For $n \in \mathbb{N}$, let $\mathsf{INT}_n = (\{0,1\}^n, \{0,1\}^n, E)$ be the bipartite graph defined as follows. For any $u, v \in \{0,1\}^n$, we have $(u, v) \in E$ if and only if the set $U \subseteq \{1, 2, \ldots, n\}$ indicated by $u$, intersects the set $V \subseteq \{1, 2, \ldots, n\}$ indicated by $v$.
2. **The Disjointness Graph.** For $n \in \mathbb{N}$, let $\mathsf{DISJ}_n = (\{0,1\}^n, \{0,1\}^n, E)$ be the bipartite graph defined as follows. For any $u, v \in \{0,1\}^n$, we have $(u, v) \in E$ if and only if the set $U \subseteq \{1, 2, \ldots, n\}$ indicated by $u$, is disjoint from the set $V \subseteq \{1, 2, \ldots, n\}$ indicated by $v$.
3. **The Inequality Graph.** For $N \in \mathbb{N}$, let $\mathsf{INEQ}_N = (\{1, 2, \ldots, N\}, \{1, 2, \ldots, N\}, E)$ be the bipartite graph defined as follows. For any $u, v \in \{1, 2, \ldots, N\}$, we have $(u, v) \in E$ if and only if $u \neq v$.

**Theorem 3** (Estimates for Particular Graphs)**.** *For all $n, N \in \mathbb{N}$, the following statements hold.*

1. $n - \frac{1}{2}\lg(n) - \mathcal{O}(1) \leqslant \mathsf{P_4\text{-}fc}(\mathsf{INT}_n) \leqslant n$, *and* $\mathsf{P_4\text{-}fp}(\mathsf{INT}_n) \leqslant \begin{cases} 2 \cdot 2^{n/2} - 2, & \textit{even } n, \textit{ and} \\ 3 \cdot 2^{(n-1)/2} - 2, & \textit{odd } n. \end{cases}$

2. $2^{0.085n} \leqslant \mathsf{P_4\text{-}fc}(\mathsf{DISJ}_n) \leqslant \mathsf{P_4\text{-}fp}(\mathsf{DISJ}_n) \leqslant 2^{\lceil n/2 \rceil}$. *In particular,* $\mathsf{P_4\text{-}fc}(\mathsf{DISJ}_1) = \mathsf{P_4\text{-}fp}(\mathsf{DISJ}_1) = 2$.

3. $\mathsf{P_4\text{-}fc}(\mathsf{INEQ}_N) = \mathsf{P_4\text{-}fp}(\mathsf{INEQ}_N) = \lceil \log_2 N \rceil$.

Recall that for any Boolean function $f$, parties can calculate it with $\lceil \log_2 \mathsf{P_4\text{-}fc}(G(f)) \rceil$-bit nondeterministic input and one call to the $\mathsf{EQ}$ oracle, where $G(f)$ is the bipartite graph representing the Boolean function $f$. Therefore, the bounds above translate into communication bounds.

Observe the exponential gap between the upper bounds on the $P_4$-free cover and partition numbers of $\mathsf{INT}_n$. We conjecture that similar to the exponential gaps in the biclique cover and partition number of some graphs [Pin13], $\mathsf{INT}_n$ is a candidate bipartite graph witnessing an exponential gap in its $P_4$-free cover and partition numbers. Currently, the authors are unaware of any general non-trivial lower bounding technique for the partition number that is not a lower bound to the cover number for this problem.

Lower-bounding the $P_4$-free cover numbers of $\mathsf{INEQ}_N$ and $\mathsf{INT}_n$ relies on Proposition 1 and the algebraic technique of [LNP80, W+96]. Furthermore, the $P_4$-free cover and partition numbers of $\mathsf{INEQ}_N$ are exact, previously unknown for the partition number. Finally, the lower bound on the $P_4$-free cover number of $\mathsf{DISJ}_n$ uses a new counting strategy.

# 3 Technical Overview

## 3.1 Proof of Theorem 1

If a bipartite graph is $K_{2,2}$-free then any $P_4$-free subgraph of this graph is a star forest. Furthermore, the minimum number of star forests to cover or partition a graph are identical. Consequently, computing the $P_4$-free partition or cover number of any $K_{2,2}$-free graph is equivalent to computing the star arboricity of that graph. Appendix G presents the full proof.

## 3.2 Proof of Theorem 2 and Corollary 3

Our objective is to consider dense bipartite graphs $G$ that have sparse $P_4$-free subgraphs. It would suffice to ensure that the number of edges in any biclique subgraph of $G$ is linear in the total number of vertices. So, consider a bipartite graph $G = (L, R, E)$ that is $K_{t+1,t+1}$-avoiding. For any combinatorial rectangle that is a subgraph of $G$, define its *width* to be the smaller of its two dimensions. Note that the width of any combinatorial rectangle that is a subgraph of $G$ has to be $\leqslant t$; otherwise, a $K_{t+1,t+1}$-subgraph of $G$ shall exist.

Let $H$ be a $P_4$-free subgraph of $G$. It is instructive to refer to Figure 3. The width of the combinatorial rectangle corresponding to any of its connected components is $\leqslant t$. The sum of the lengths (the longer dimension of a combinatorial rectangle) of the combinatorial rectangles corresponding to each connected component is $\leqslant |L| + |R|$. Because, the length can either belong to the left partite set or to the right partite set. So, the total number of edges in $H$ is $\leqslant t(|L| + |R|)$. Consequently, any partition or cover of $G$ requires at least $\frac{|E(G)|}{t(|L|+|R|)}$ $P_4$-free subgraphs.

So, an appropriate choice for $G$ is a $K_{t+1,t+1}$-avoiding graph with as many edges as possible. These extremal properties are well-studied [FS13]. The best general lower bound obtained by the probabilistic method [ES74] yields $|E(G)| \geqslant C' N^{2-\frac{2}{t+2}}$, where $C'$ is a positive absolute constant.

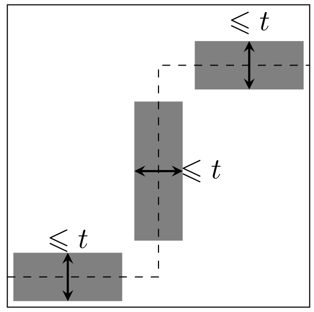



Figure 3: Let $t \in \mathbb{N}$ be a parameter. Proof intuition underlying the fact that a $K_{t+1,t+1}$-free bipartite graph cannot have a dense $P_4$-free subgraph.

An explicit construction for $K_{t+1,t+1}$-avoiding graphs for $t = 2$ is known [Bro66], which has $\frac{1}{2}N^{\frac{5}{3}} + o(N^{\frac{5}{3}})$ edges.[11] Using *norm graphs*, constructions of $K_{t,s}$-avoiding graphs for fixed $t \geqslant 2$ and $s > (t-1)!$ are known as well [KRS96, ARS99]. Note that the latter set of constructions do not apply to our setting for $t > 3$.

Similarly, to prove that $\mathsf{ER}(N, N, p)$ have high $P_4$-free partition and cover numbers (Corollary 3), we rely on the following two observations.

1. The number of edges in a bipartite graph $G \xleftarrow{\$} \mathsf{ER}(N, N, p)$ is at least $pN \cdot (1 - o(1))$, with probability $1 - o(1)$.
2. Furthermore, $G \xleftarrow{\$} \mathsf{ER}(N, N, p)$ is $K_{t+1,t+1}$-avoiding, where $t + 1 = \lceil 2\log_a N \rceil$. For completeness, following the exposition of [FK16], Appendix H proves this result using the first moment technique.

### 3.3 Upper Bounds for $\mathsf{INT}_n, \mathsf{DISJ}_n$, and $\mathsf{INEQ}_N$

**Bound for $\mathsf{INT}_n$.** The $P_4$-free cover number for $\mathsf{INT}_n$ is at most $n$. Let $G_i$ be the biclique connecting all vertices that contain the element $i \in \{1, 2, \ldots, n\}$. Then, the bicliques $G_1, \ldots, G_n$ cover $\mathsf{INT}_n$.

To upper-bound the $P_4$-free partition number of $\mathsf{INT}_n$, we prove the following general result.

**Claim 4** (Submultiplicity of $P_4$-free partition number)**.** *Suppose $G$ and $G'$ are two bipartite graphs. Then,* $\mathsf{P_4\text{-}fp}(G \times G') \leqslant \mathsf{P_4\text{-}fp}(G) \cdot \mathsf{P_4\text{-}fp}(G')$.

Using this claim, we inductively upper-bound $\mathsf{P_4\text{-}fp}(\mathsf{INT}_n)$, using base cases $\mathsf{P_4\text{-}fp}(\mathsf{INT}_1) = 1$ and $\mathsf{P_4\text{-}fp}(\mathsf{INT}_2) = 2$. Recall that $\mathsf{INT}_n$ indicates the intersection between a subset $X \subseteq \{1, 2, \ldots, n\}$ and $Y \subseteq \{1, 2, \ldots, n\}$. Consider the edges in $\mathsf{INT}_n$ where the witness of the intersection is 1, or 2. Let $A$ be the subgraph of $\mathsf{INT}_n$ formed by these edges. We argue that $\mathsf{P_4\text{-}fp}(A) \leqslant 2$. On the remainder of the edges we recurse. The remainder of the edges form a graph $B$ that is $\mathsf{INT}_{n-2} \times H$, where $H$ is a graph satisfying $\mathsf{P_4\text{-}fp}(H) = 2$. So, we get the recursion

$$\mathsf{P_4\text{-}fp}(\mathsf{INT}_n) \leqslant \mathsf{P_4\text{-}fp}(B) + 2 \leqslant \mathsf{P_4\text{-}fp}(\mathsf{INT}_{n-2}) \cdot \mathsf{P_4\text{-}fp}(H) + 2 = 2 \cdot \mathsf{P_4\text{-}fp}(\mathsf{INT}_{n-2}) + 2.$$

Consequently, we get that $\mathsf{P_4\text{-}fp}(\mathsf{INT}_n) \leqslant \begin{cases} 2 \cdot 2^{n/2} - 2, & \text{for even } n, \\ 3 \cdot 2^{(n-1)/2}, & \text{for odd } n. \end{cases}$

[11] For $t = 1$, Levi graph of a finite projective plane yields an explicit construction.

**Bound for $\mathsf{DISJ}_n$.** It is well-known that $\mathsf{DISJ}_n$ is the tensor product $\mathsf{DISJ}_1^{\times n}$. We prove that $\mathsf{P_4\text{-}fp}(\mathsf{DISJ}_2) = 2$. Consequently, we get that $\mathsf{P_4\text{-}fp}(\mathsf{DISJ}_n) \leqslant 2^{\lceil n/2 \rceil}$, by the submultiplicity of $P_4$-free partition number.

**Bound for $\mathsf{INEQ}_N$.** In fact, we prove a more general result.

**Claim 5** (Complement of a $P_4$-free graph has a small $P_4$-free partition number)**.** *Let $H$ be a $P_4$-free bipartite graph with $c \in \mathbb{N}$ connected components. Let $G$ be the complement of $H$. Then, the following bound holds.*

$$\mathsf{P_4\text{-}fc}(G) \leqslant \mathsf{P_4\text{-}fp}(G) \leqslant \begin{cases} \lceil \log_2 c \rceil, & \textit{if } H \textit{ has no isolated vertex,} \\ \lceil \log_2 c \rceil + 1, & \textit{if } H \textit{ has isolated vertices and } c > 1, \textit{ and} \\ 2, & \textit{if } H \textit{ has isolated vertices and } c = 1. \end{cases}$$

Proposition 1 (along with a suitable embedding $\varphi$) implies the upper bound $\mathsf{P_4\text{-}fc}(G) \leqslant \lceil \log_2 c \rceil$. however, we prove the stronger result that $\mathsf{P_4\text{-}fp}(G) \leqslant \lceil \log_2 c \rceil$.

Our objective is to demonstrate a $P_4$-free partition for $G$ of size $\lceil \log_2 c \rceil$. The proof starts by kernelizing the graph $G$ using the rules in [FMPS09]. Essentially, without loss of generality, one can assume that $H$ is a matching. For simplicity assume that $H$ is a matching with $c$ edges and assume that it has $c$ vertices in each partite set (i.e., there are no isolated vertices).

Next, the idea is to break the problem into half the size while including only one $P_4$-free graph in the partition of $G$. Assume, without loss of generality, that the partite sets are $L = \{1, \dots, c\}$ and $R = \{1, \dots, c\}$, and the edges in $H$ are $(i, i)$, for $1 \leqslant i \leqslant c$.

Define $L_0 \coloneqq \{1, \dots, \lfloor c/2 \rfloor\}$ and $L_1 \coloneqq L \setminus L_0$. Similarly, define $R_0 \coloneqq \{1, \dots, \lfloor c/2 \rfloor\}$ and $R_1 \coloneqq R \setminus R_0$. Observe the following.

1. The edges induced by $(L_0, R_1)$ and $(L_1, R_0)$ in $G$ are disjoint bicliques. Together, they shall form one $P_4$-free subgraph of $G$.
2. Next, the edges induced by $(L_0, R_0)$ and $(L_1, R_1)$ in $G$ are disjoint and complements of matchings as well; albeit the matchings are of size $\lfloor c/2 \rfloor$ and $\lceil c/2 \rceil$, respectively. We recursively partition the disjoint union of these graphs.

Hence, we get our result. Appendix I presents the full proofs of all the upper bound results.

### 3.4 Lower Bounds for $\mathsf{INT}_n$, $\mathsf{DISJ}_n$, and $\mathsf{INEQ}_N$

Appendix J presents the proofs for the lower bounds below.

**Bound for $\mathsf{INEQ}_N$.** We begin with a lower bound on $\mathsf{P_4\text{-}fc}(\mathsf{INEQ}_N)$ by outlining the proof of Proposition 1 below. Given a size-$d$ $P_4$-free cover $\{G_1, \dots, G_d\}$ of a bipartite graph $G = (L, R, E)$ consider the following function $\varphi \colon L \cup R \to \{1, 2\} \times \mathbb{N}^d$. For $i \in \{0, 1, \dots, d\}$, $\varphi(u)_i$ refers to the $i$-th coordinate of the mapping $\varphi(u)$. Define $\varphi(u)_0 \coloneqq 1$ if $u \in L$; otherwise, if $u \in R$, define $\varphi(u)_0 \coloneqq 2$. If the edge $(u, v) \in E$ is covered in the $G_i$ by the $k$-th connected component, then define $\varphi(u)_i = \varphi(v)_i \coloneqq k$. Since each connected component of $G_i$ is a biclique, there are no inconsistencies introduced in defining the mapping $\varphi$. All remaining undefined coordinates of the mapping $\varphi$ are completed with unique entries.

Observe that the mapping $\varphi$ has the following property. For any $u \in L$ and $v \in R$, we have $(u, v) \in E$ if and only if $\varphi(u)_0 \neq \varphi(v)_0$, and there exists $i \in \{1, \dots, d\}$ such that $\varphi(u)_i = \varphi(v)_i$. Equivalently, by taking the negation, one concludes that $(u, v) \in L \times R \setminus E$ if and only if, for all $i \in \{0, 1, \ldots, d\}$, we have $\varphi(u)_i \neq \varphi(v)_i$. Therefore, the complement of the bipartite graph $G$ is a subgraph of $K_2 \times K_{\mathbb{N}}^d$, if $\varphi$ is injective. Note that a redundancy-free graph cannot have $\varphi(u) = \varphi(v)$, for distinct vertices $u$ and $v$. Consequently, we have Proposition 1. The other direction of the proposition does not hold because the first coordinate of the mapping $\varphi$ need not be constant restricted over the vertices in $L$ or $R$. However, given $\varphi$ one can prepend a coordinate that is 1 for the vertices in $L$ and 2 for the vertices in $R$. Therefore, if $\overline{G}$ is an induced subgraph of $K_2 \times K_{\mathbb{N}}^d$, then $G$ has a size-$(d+1)$ $P_4$-free cover.

For deriving the lower bound, consider $G = \mathsf{INEQ}_N$, i.e., $\overline{G} = \mathsf{EQ}_N$. Using the algebraic lower-bounding technique of [LNP80, Alo86, W+96], one concludes $d \geqslant \lceil \log_2 N \rceil$. Therefore, $\mathsf{P_4\text{-}fc}\,(\mathsf{INEQ}_N) \geqslant \lceil \log_2 N \rceil$.

**Bound for $\mathsf{INT}_n$.** Consider $L' \subseteq L$ and $R' \subseteq R$ as the set of all possible subsets of size $\lceil n/2 \rceil$ and $\lfloor n/2 \rfloor$, respectively. The subgraph of $\mathsf{INT}_n$ induced by $L'$ and $R'$ is isomorphic to $\mathsf{INEQ}_M$, where $M = \binom{n}{\lceil n/2 \rceil}$. A lower bound for the $P_4$-free cover number for the induced subgraph $\mathsf{INT}_n[L', R']$ translates into a lower bound for $\mathsf{P_4\text{-}fc}\,(\mathsf{INT}_n)$. The result follows from the lower bound on $\mathsf{P_4\text{-}fc}\,(\mathsf{INEQ}_M)$.

**Bound for $\mathsf{DISJ}_n$.** We rely on a counting technique to obtain this lower bound. Intuitively, existing algebraic technique are useful to obtain logarithmic lower bounds. However, in this problem, we seek to prove a polynomial lower bound.

Observe that $\mathsf{DISJ}_n$ has a total of $3^n = N^{\log_2 3}$ edges, where $N = 2^n$. We prove that any $P_4$-free subgraph of $\mathsf{DISJ}_n$ has at most $N^{3/2}$ edges. Consequently, the $\mathsf{P_4\text{-}fc}\,(\mathsf{DISJ}_n)$ is at least $N^{\log_2 3 - 3/2} \approx N^{0.085}$.

## References


[AA89] I. Algor and Noga Alon. The star arboricity of graphs. *Discret. Math.*, 75(1-3):11–22, 1989. doi:10.1016/0012-365X(89)90073-3. 4, 7, 9, 30

[AA20] Noga Alon and Ryan Alweiss. On the product dimension of clique factors. *European Journal of Combinatorics*, 86:103097, 2020. 4, 32

[ABFR91] James Aspnes, Richard Beigel, Merrick L. Furst, and Steven Rudich. The expressive power of voting polynomials. In *23rd Annual ACM Symposium on Theory of Computing*, pages 402–409, New Orleans, LA, USA, May 6–8, 1991. ACM Press. doi:10.1145/103418.103461. 7

[AC93] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography - I: secret sharing. *IEEE Trans. Inf. Theory*, 39(4):1121–1132, 1993. doi:10.1109/18.243431. 2

[AC98] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography - part II: CR capacity. *IEEE Trans. Inf. Theory*, 44(1):225–240, 1998. doi:10.1109/18.651026. 2

[AG76] Rudolf Ahlswede and Peter Gács. Spreading of sets in product spaces and hypercontraction of the markov operator. *The annals of probability*, pages 925–939, 1976. 29

[AGKN13] Venkat Anantharam, Amin Gohari, Sudeep Kamath, and Chandra Nair. On maximal correlation, hypercontractivity, and the data processing inequality studied by erkip and cover. *arXiv preprint arXiv:1304.6133*, 2013. 29

[Alo86] Noga Alon. Covering graphs by the minimum number of equivalence relations. *Combinatorica*, 6(3):201–206, 1986. 4, 13

[ARS99] Noga Alon, Lajos Rónyai, and Tibor Szabó. Norm-graphs: Variations and applications. *J. Comb. Theory, Ser. B*, 76(2):280–290, 1999. doi:10.1006/jctb.1999.1906. 11

[BF88] László Babai and Péter Frankl. *Linear algebra methods in combinatorics*. University of Chicago, 1988. 30

[BG15] Salman Beigi and Amin Gohari. On the duality of additivity and tensorization. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 2381–2385. IEEE, 2015. doi:10.1109/ISIT.2015.7282882. 29

[BIKK14] Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 317–342, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-54242-8_14. 5

[BM11] Andrej Bogdanov and Elchanan Mossel. On extracting common random bits from correlated sources. *IEEE Trans. Inf. Theory*, 57(10):6351–6355, 2011. doi:10.1109/TIT.2011.2134067. 6, 29

[BMN17] Alexander R. Block, Hemanta K. Maji, and Hai H. Nguyen. Secure computation based on leaky correlations: High resilience setting. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 3–32, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-63715-0_1. 3, 29

[Bol04] Béla Bollobás. *Extremal graph theory*. Courier Corporation, 2004. 4, 9

[Bor82] Christer Borell. Positivity improving operators and hypercontractivity. *Mathematische Zeitschrift*, 180(3):225–234, 1982. doi:10.1007/BF01318906. 29

[Bro66] W. G. Brown. On graphs that do not contain a thomsen graph. *Canadian Mathematical Bulletin*, 9(3):281–285, 1966. doi:10.4153/CMB-1966-036-2. 11

[CDLR16] Ignacio Cascudo, Ivan Damgård, Felipe Lacerda, and Samuel Ranellucci. Oblivious transfer from any non-trivial elastic noisy channel via secret key agreement. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B: 14th Theory of Cryptography Conference, Part I*, volume 9985 of *Lecture Notes in Computer Science*, pages 204–234, Beijing, China, October 31 – November 3, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-53641-4_9. 2

[CFG+12] G. Chen, S. Fujita, A. Gyarfas, J. Lehel, and A. Toth. Around a biclique cover conjecture, 2012. arXiv:1212.6861. 4

[CHHK14] Parinya Chalermsook, Sandy Heydrich, Eugenia Holm, and Andreas Karrenbauer. Nearly tight approximability results for minimum biclique cover and partition. In Andreas S. Schulz and Dorothea Wagner, editors, *Algorithms - ESA 2014 - 22th Annual European Symposium, Wroclaw, Poland, September 8-10, 2014. Proceedings*, volume 8737 of *Lecture Notes in Computer Science*, pages 235–246. Springer, 2014. doi:10.1007/978-3-662-44777-2_20. 30, 31, 32

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *29th Annual Symposium on Foundations of Computer Science*, pages 42–52, White Plains, NY, USA, October 24–26, 1988. IEEE Computer Society Press. doi:10.1109/SFCS.1988.21920. 2

[CK90] Claude Crépeau and Joe Kilian. Weakening security assumptions and oblivious transfer (abstract). In Shafi Goldwasser, editor, *Advances in Cryptology – CRYPTO'88*, volume 403 of *Lecture Notes in Computer Science*, pages 2–7, Santa Barbara, CA, USA, August 21–25, 1990. Springer, Heidelberg, Germany. doi:10.1007/0-387-34799-2_1. 2

[CMN14] Siu On Chan, Elchanan Mossel, and Joe Neeman. On extracting common random bits from correlated sources on large alphabets. *IEEE Trans. Inf. Theory*, 60(3):1630–1637, 2014. doi:10.1109/TIT.2014.2301155. 6, 29

[CMW05] Claude Crépeau, Kirill Morozov, and Stefan Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In Carlo Blundo and Stelvio Cimato, editors, *SCN 04: 4th International Conference on Security in Communication Networks*, volume 3352 of *Lecture Notes in Computer Science*, pages 47–59, Amalfi, Italy, September 8–10, 2005. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-30598-9_4. 2

[DKS99] Ivan Damgård, Joe Kilian, and Louis Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In Jacques Stern, editor, *Advances in Cryptology – EUROCRYPT'99*, volume 1592 of *Lecture Notes in Computer Science*, pages 56–73, Prague, Czech Republic, May 2–6, 1999. Springer, Heidelberg, Germany. doi:10.1007/3-540-48910-X_5. 2

[DMN18] Anindya De, Elchanan Mossel, and Joe Neeman. Non interactive simulation of correlated distributions is decidable. In Artur Czumaj, editor, *29th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2728–2746, New Orleans, LA, USA, January 7–10, 2018. ACM-SIAM. doi:10.1137/1.9781611975031.174. 29

[EHM+08] Alina Ene, William G. Horne, Nikola Milosavljevic, Prasad Rao, Robert Schreiber, and Robert Endre Tarjan. Fast exact and heuristic methods for role minimization problems. In Indrakshi Ray and Ninghui Li, editors, *13th ACM Symposium on Access Control Models and Technologies, SACMAT 2008, Estes Park, CO, USA, June 11-13, 2008, Proceedings*, pages 1–10. ACM, 2008. doi:10.1145/1377836.1377838. 32, 33

[ES74] Paul Erdös and Joel Spencer. *Probabilistic methods in combinatorics*, volume 17. Academic Press New York, 1974. 10, 34

[EU18] Alessandro Epasto and Eli Upfal. Efficient approximation for restricted biclique cover problems. *Algorithms*, 11(6):84, 2018. doi:10.3390/a11060084. 31, 32

[FK16] Alan Frieze and Michał Karoński. *Introduction to random graphs*. Cambridge University Press, 2016. 11, 35

[FMPS07] Herbert Fleischner, Egbert Mujuni, Daniël Paulusma, and Stefan Szeider. Covering graphs with few complete bipartite subgraphs. In Vikraman Arvind and Sanjiva Prasad, editors, *FSTTCS 2007: Foundations of Software Technology and Theoretical Computer Science, 27th International Conference, New Delhi, India, December 12-14, 2007, Proceedings*, volume 4855 of *Lecture Notes in Computer Science*, pages 340–351. Springer, 2007. doi:10.1007/978-3-540-77050-3_28. 31, 32

[FMPS09] Herbert Fleischner, Egbert Mujuni, Daniël Paulusma, and Stefan Szeider. Covering graphs with few complete bipartite subgraphs. *Theoretical Computer Science*, 410(21):2045 – 2053, 2009. URL: http://www.sciencedirect.com/science/article/pii/S0304397508009407, doi:https://doi.org/10.1016/j.tcs.2008.12.059. 12, 38

[Fou69] DJ Foulis. Empirical logic, xeroxed course notes. *University of Massachusetts, Amherst, Massachusetts (1969-1970)*, 1969. 1

[FS13] Zoltán Füredi and Miklós Simonovits. The history of degenerate (bipartite) extremal graph problems. In *Erdős Centennial*, pages 169–264. Springer, 2013. 10

[GH07] Hermann Gruber and Markus Holzer. Inapproximability of nondeterministic state and transition complexity assuming p=!np. In Tero Harju, Juhani Karhumäki, and Arto Lepistö, editors, *Developments in Language Theory, 11th International Conference, DLT 2007, Turku, Finland, July 3-6, 2007, Proceedings*, volume 4588 of *Lecture Notes in Computer Science*, pages 205–216. Springer, 2007. doi:10.1007/978-3-540-73208-2_21. 31, 32

[GK73] Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973. 6, 28, 29

[GKS16] Badih Ghazi, Pritish Kamath, and Madhu Sudan. Decidability of non-interactive simulation of joint distributions. In Irit Dinur, editor, *57th Annual Symposium on Foundations of Computer Science*, pages 545–554, New Brunswick, NJ, USA, October 9–11, 2016. IEEE Computer Society Press. doi:10.1109/FOCS.2016.65. 29

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th Annual ACM Symposium on Theory of Computing*, pages 218–229, New York City, NY, USA, May 25–27, 1987. ACM Press. doi:10.1145/28395.28420. 5

[GO09] Daniel Gonçalves and Pascal Ochem. On star and caterpillar arboricity. *Discret. Math.*, 309(11):3694–3702, 2009. doi:10.1016/j.disc.2008.01.041. 33

[Gol97] Mikael Goldmann. On the power of a threshold gate at the top. *Inf. Process. Lett.*, 63(6):287–293, 1997. doi:10.1016/S0020-0190(97)00141-5. 7

[GP71] Ronald L Graham and Henry O Pollak. On the addressing problem for loop switching. *Bell System Technical Journal*, 50(8):2495–2519, 1971. 30

[GP72] Ronald L Graham and Henry O Pollak. On embedding graphs in squashed cubes. In *Graph theory and applications*, pages 99–110. Springer, 1972. 30, 31

[GS10] Parikshit Gopalan and Rocco A. Servedio. Learning and lower bounds for $ac^0$ with threshold gates. In Maria J. Serna, Ronen Shaltiel, Klaus Jansen, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 13th International Workshop, APPROX 2010, and 14th International Workshop, RANDOM 2010, Barcelona, Spain, September 1-3, 2010. Proceedings*, volume 6302 of *Lecture Notes in Computer Science*, pages 588–601. Springer, 2010. doi:10.1007/978-3-642-15369-3_44. 7

[GW88] Harold N. Gabow and Herbert H. Westermann. Forests, frames and games: Algorithms for matroid sums and applications. In *20th Annual ACM Symposium on Theory of Computing*, pages 407–421, Chicago, IL, USA, May 2–4, 1988. ACM Press. doi:10.1145/62212.62252. 30

[GW92] Harold N. Gabow and Herbert H. Westermann. Forests, frames, and games: Algorithms for matroid sums and applications. *Algorithmica*, 7(5&6):465–497, 1992. doi:10.1007/BF01758774. 30

[HIK11] Richard Hammack, Wilfried Imrich, and Sandi Klavžar. *Handbook of product graphs*. CRC press, 2011. 4, 5

[Hir35] Hermann O Hirschfeld. A connection between correlation and contingency. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 520–524. Cambridge University Press, 1935. doi:10.1017/S0305004100013517. 29

[HL01] Chinh T. Hoàng and Van Bang Le. P_4-Colorings and P_4-Bipartite Graphs. *Discrete Mathematics and Theoretical Computer Science*, 4(2):109–122, 2001. URL: https://hal.inria.fr/hal-00958951. 1

[HMR06] Michael Hirsch, Henk Meijer, and David Rappaport. Biclique edge cover graphs and confluent drawings. In Michael Kaufmann and Dorothea Wagner, editors, *Graph Drawing, 14th International Symposium, GD 2006, Karlsruhe, Germany, September 18-20, 2006. Revised Papers*, volume 4372 of *Lecture Notes in Computer Science*, pages 405–416. Springer, 2006. doi:10.1007/978-3-540-70904-6_39. 31, 32

[Hof72] AJ Hoffman. Eigenvalues and partitionings of the edges of a graph. *Linear Algebra and Its Applications*, 5(2):137–146, 1972. 30

[ILL89] Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Pseudo-random generation from one-way functions (extended abstracts). In *21st Annual ACM Symposium on Theory of Computing*, pages 12–24, Seattle, WA, USA, May 15–17, 1989. ACM Press. doi:10.1145/73007.73009. 2

[Jia18] Minghui Jiang. Trees, paths, stars, caterpillars and spiders. *Algorithmica*, 80(6):1964–1982, 2018. 8

[JK09] Stasys Jukna and Alexander S Kulikov. On covering graphs by complete bipartite subgraphs. *Discrete Mathematics*, 309(10):3399–3403, 2009. 31, 32

[JKS02] Jeffrey C. Jackson, Adam Klivans, and Rocco A. Servedio. Learnability beyond AC0. In *34th Annual ACM Symposium on Theory of Computing*, pages 776–784, Montréal, Québec, Canada, May 19–21, 2002. ACM Press. doi:10.1145/509907.510018. 7

[Juk12] Stasys Jukna. *Boolean Function Complexity: Advances and Frontiers*. Springer Publishing Company, Incorporated, 2012. 7, 26

[Jun78] Heinz A Jung. On a class of posets and the corresponding comparability graphs. *Journal of Combinatorial Theory, Series B*, 24(2):125–133, 1978. 1

[KA16] Sudeep Kamath and Venkat Anantharam. On non-interactive simulation of joint distributions. *IEEE Transactions on Information Theory*, 62(6):3419–3435, 2016. 29

[Kai11] Sebastian Kaiser. *Biclustering: methods, software and application*. PhD thesis, lmu, 2011. 4

[Kar72] Richard M. Karp. Reducibility among combinatorial problems. In Raymond E. Miller and James W. Thatcher, editors, *Proceedings of a symposium on the Complexity of Computer Computations, held March 20-22, 1972, at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York, USA*, The IBM Research Symposia Series, pages 85–103. Plenum Press, New York, 1972. doi:10.1007/978-1-4684-2001-2_9. 7

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing*, pages 20–31, Chicago, IL, USA, May 2–4, 1988. ACM Press. doi:10.1145/62212.62215. 2

[Kil91] Joe Kilian. A general completeness theorem for two-party games. In *23rd Annual ACM Symposium on Theory of Computing*, pages 553–560, New Orleans, LA, USA, May 6–8, 1991. ACM Press. doi:10.1145/103418.103475. 2

[Kil00] Joe Kilian. More general completeness theorems for secure two-party computation. In *32nd Annual ACM Symposium on Theory of Computing*, pages 316–324, Portland, OR, USA, May 21–23, 2000. ACM Press. doi:10.1145/335305.335342. 2, 5, 29

[KM01] János Körner and Katalin Marton. Relative capacity and dimension of graphs. *Discrete Mathematics*, 235(1-3):307–315, 2001. 32

[KMN20] Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Secure non-interactive simulation: Hardness & feasibility. *IACR Cryptol. ePrint Arch.*, 2020:252, 2020. URL: https://eprint.iacr.org/2020/252. 29

[KMS16] Dakshita Khurana, Hemanta K. Maji, and Amit Sahai. Secure computation from elastic noisy channels. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 184–212, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-49896-5_7. 2

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity.* Cambridge University Press, 1997. 3

[KO98] Janos Korner and Alon Orlitsky. Zero-error information theory. *IEEE Transactions on Information Theory*, 44(6):2207–2229, 1998. 32

[KPRW19] Ravi Kumar, Rina Panigrahy, Ali Rahimi, and David P. Woodruff. Faster algorithms for binary matrix factorization. In Kamalika Chaudhuri and Ruslan Salakhutdinov, editors, *Proceedings of the 36th International Conference on Machine Learning, ICML 2019, 9-15 June 2019, Long Beach, California, USA*, volume 97 of *Proceedings of Machine Learning Research*, pages 3551–3559. PMLR, 2019. URL: http://proceedings.mlr.press/v97/kumar19a.html. 31

[KRS96] János Kollár, Lajos Rónyai, and Tibor Szabó. Norm-graphs and bipartite turán numbers. *Combinatorica*, 16(3):399–406, 1996. doi:10.1007/bf01261323. 11

[KRW88] Thomas Kratzke, Bruce Reznick, and Douglas West. Eigensharp graphs: Decomposition into complete bipartite subgraphs. *Transactions of the American Mathematical Society*, 308(2):637–653, 1988. 30

[Ler71] H Lerchs. On cliques and kernels. *Department of Computer Science, University of Toronto*, 1971. 1

[Ler72] H Lerchs. On the clique-kernel structure of graphs. *Dept. of Computer Science, University of Toronto*, 1972. 1

[LNP80] László Lovász, J Nešetšil, and Ales Pultr. On a product dimension of graphs. *Journal of Combinatorial Theory, Series B*, 29(1):47–67, 1980. 4, 8, 10, 13, 41

[Mau91] Ueli M. Maurer. Perfect cryptographic security from partially independent channels. In *23rd Annual ACM Symposium on Theory of Computing*, pages 561–571, New Orleans, LA, USA, May 6–8, 1991. ACM Press. doi:10.1145/103418.103476. 2

[Mau92] Ueli M. Maurer. A universal statistical test for random bit generators. *Journal of Cryptology*, 5(2):89–105, January 1992. doi:10.1007/BF00193563. 2

[Mau93] Ueli M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, 39(3):733–742, 1993. doi:10.1109/18.256484. 2

[MMG+08] Pauli Miettinen, Taneli Mielikäinen, Aristides Gionis, Gautam Das, and Heikki Mannila. The discrete basis problem. *IEEE transactions on knowledge and data engineering*, 20(10):1348–1362, 2008. 31, 32

[MO04] Sara C Madeira and Arlindo L Oliveira. Biclustering algorithms for biological data analysis: a survey. *IEEE/ACM transactions on computational biology and bioinformatics*, 1(1):24–45, 2004. 4

[MO05] Elchanan Mossel and Ryan O'Donnell. Coin flipping from a cosmic source: On error correction of truly random bits. *Random Structures & Algorithms*, 26(4):418–436, 2005. doi:10.1002/rsa.20062. 6, 29

[MOR+06] Elchanan Mossel, Ryan O'Donnell, Oded Regev, Jeffrey E Steif, and Benny Sudakov. Non-interactive correlation distillation, inhomogeneous markov chains, and the reverse bonami-beckner inequality. *Israel Journal of Mathematics*, 154(1):299–336, 2006. 6, 29

[MOS13] Elchanan Mossel, Krzysztof Oleszkiewicz, and Arnab Sen. On reverse hypercontractivity. *Geometric and Functional Analysis*, 23(3):1062–1097, 2013. 29

[Mül96] Haiko Müller. On edge perfectness and classes of bipartite graphs. *Discrete Mathematics*, 149(1-3):159–187, 1996. 31

[NED+13] Igor Nor, Jan Engelstädter, Olivier Duron, Max Reuter, Marie-France Sagot, and Sylvain Charlat. On the genetic architecture of cytoplasmic incompatibility: inference from phenotypic data. *The American Naturalist*, 182(1):E15–E24, 2013. 31, 32, 33

[NHC+12] Igor Nor, Danny Hermelin, Sylvain Charlat, Jan Engelstadter, Max Reuter, Olivier Duron, and Marie-France Sagot. Mod/resc parsimony inference: Theory and application. *Information and Computation*, 213:23 – 32, 2012. Special Issue: Combinatorial Pattern Matching (CPM 2010). URL: http://www.sciencedirect.com/science/article/pii/S0890540112000247, doi:https://doi.org/10.1016/j.ic.2011.03.008. 31, 32, 33

[NMWA78] Dana S Nau, George Markowsky, Max A Woodbury, and D Bernard Amos. A mathematical analysis of human leukocyte antigen serology. *Mathematical Biosciences*, 40(3-4):243–270, 1978. 31, 32, 33

[NP77] J Nešetřil and Ales Pultr. A dushnik-miller type dimension of graphs and its complexity. In *International Conference on Fundamentals of Computation Theory*, pages 482–493. Springer, 1977. 1, 4, 32

[NR78] Jaroslav Nešetřil and Vojtěch Rōdl. A simple proof of the galvin-ramsey property of the class of all finite graphs and a dimension of a graph. *Discrete Mathematics*, 23(1):49–55, 1978. 1, 4, 32

[NZ93] Noam Nisan and David Zuckerman. More deterministic simulation in logspace. In *25th Annual ACM Symposium on Theory of Computing*, pages 235–244, San Diego, CA, USA, May 16–18, 1993. ACM Press. doi:10.1145/167088.167162. 2

[Orl77] James Orlin. Contentment in graph theory: Covering graphs with cliques. *Indagationes Mathematicae (Proceedings)*, 80(5):406 – 424, 1977. URL: http://www.sciencedirect.com/science/article/pii/1385725877900555, doi:https://doi.org/10.1016/1385-7258(77)90055-5. 8, 30, 31, 32

[Pec84] GW Peck. A new proof of a theorem of graham and pollak. *Discrete mathematics*, 49(3):327–328, 1984. 30, 31

[Pin13] Trevor Pinto. Biclique covers and partitions. *arXiv preprint arXiv:1307.6363*, 2013. 10, 31

[PP10] Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2602–2606. IEEE, 2010. doi:10.1109/ISIT.2010.5513743. 29

[PP11] Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information: Further results. In Alexander Kuleshov, Vladimir M. Blinovsky, and Anthony Ephremides, editors, *2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 - August 5, 2011*, pages 2861–2865. IEEE, 2011. doi:10.1109/ISIT.2011.6034098. 29

[PP14] Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information with an application to secure two-party sampling. *IEEE Trans. Inf. Theory*, 60(6):3413–3434, 2014. doi:10.1109/TIT.2014.2316011. 29

[PRP83] Svatopluk Poljak, D Rödl, and Ales Pultr. On a product dimension of bipartite graphs. *Journal of graph theory*, 7(4):475–486, 1983. 5

[Rén59] Alfréd Rényi. On measures of dependence. *Acta mathematica hungarica*, 10(3-4):441–451, 1959. doi:10.1007/BF02024507. 29

[RP14] K. Sankeerth Rao and Vinod M. Prabhakaran. A new upperbound for the oblivious transfer capacity of discrete memoryless channels. In *2014 IEEE Information Theory Workshop, ITW 2014, Hobart, Tasmania, Australia, November 2-5, 2014*, pages 35–39. IEEE, 2014. doi:10.1109/ITW.2014.6970787. 29

[Sei74] Dieter Seinsche. On a property of the class of n-colorable graphs. *Journal of Combinatorial Theory, Series B*, 16(2):191–193, 1974. 1

[Sha48] Claude E Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948. 6

[Sim90] Hans Ulrich Simon. On approximate solutions for combinatorial optimization problems. *SIAM J. Discret. Math.*, 3(2):294–310, 1990. doi:10.1137/0403025. 31, 32

[SLY06] Guoqiang Shu, David Lee, and Mihalis Yannakakis. A note on broadcast encryption key management with applications to large scale emergency alert systems. In *20th International Parallel and Distributed Processing Symposium (IPDPS 2006), Proceedings, 25-29 April 2006, Rhodes Island, Greece*. IEEE, 2006. doi:10.1109/IPDPS.2006.1639680. 32, 33

[STW20] Madhu Sudan, Himanshu Tyagi, and Shun Watanabe. Communication for generating correlation: A unifying survey. *IEEE Trans. Inf. Theory*, 66(1):5–37, 2020. doi:10.1109/TIT.2019.2946364. 29

[Sum74] David P Sumner. Dacey graphs. *Journal of the Australian Mathematical Society*, 18(4):492–502, 1974. 1

[SW03] B Schölkopf and MK Warmuth. Learning theory and kernel machines: 16th annual conference on learning theory and 7th kernel workshop (colt/kernel 2003). In *16th Annual Conference on Learning Theory and 7th Kernel Workshop (COLT/Kernel 2003)*. Springer, 2003. 31, 32

[Tve82] Helge Tverberg. On the decomposition of kn into complete bipartite graphs. *Journal of Graph Theory*, 6(4):493–494, 1982. 30, 31

[Vis08] Sundar Vishwanathan. A polynomial space proof of the graham–pollak theorem. *Journal of Combinatorial Theory, Series A*, 115(4):674–676, 2008. 30, 31

[Vis13] Sundar Vishwanathan. A counting proof of the graham–pollak theorem. *Discrete Mathematics*, 313(6):765–766, 2013. 30, 31

[VL85] JH Van Lint. {0, 1,*} distance problems in combinatorics. 1985. 30

[vLW01] Jacobus Hendricus van Lint and Richard Michael Wilson. *A course in combinatorics*. Cambridge university press, 2001. 30

[W$^+$96] Douglas Brent West et al. *Introduction to graph theory*, volume 2. Prentice hall Upper Saddle River, NJ, 1996. 1, 4, 8, 10, 13

[Wit75] Hans S Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, 1975. doi:doi.org/10.1137/0128010. 28, 29

[Wul07] Jürg Wullschleger. Oblivious-transfer amplification. In Moni Naor, editor, *Advances in Cryptology – EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 555–572, Barcelona, Spain, May 20–24, 2007. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-72540-4_32. 2

[Wul09] Jürg Wullschleger. Oblivious transfer from weak noisy channels. In Omer Reingold, editor, *TCC 2009: 6th Theory of Cryptography Conference*, volume 5444 of *Lecture Notes in Computer Science*, pages 332–349. Springer, Heidelberg, Germany, March 15–17, 2009. doi:10.1007/978-3-642-00457-5_20. 2

[WW05] Stefan Wolf and Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 467–477, Santa Barbara, CA, USA, August 14–18, 2005. Springer, Heidelberg, Germany. doi:10.1007/11535218_28. 29

[Wyn75] Aaron Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975. doi:10.1109/TIT.1975.1055346. 6, 28, 29, 30

[Yan91] Mihalis Yannakakis. Expressing combinatorial optimization problems by linear programs. *J. Comput. Syst. Sci.*, 43(3):441–466, 1991. doi:10.1016/0022-0000(91)90024-Y. 31

[Yan04] Ke Yang. On the (im)possibility of non-interactive correlation distillation. In Martin Farach-Colton, editor, *LATIN 2004: Theoretical Informatics, 6th Latin American Symposium*, volume 2976 of *Lecture Notes in Computer Science*, pages 222–231, Buenos Aires, Argentina, April 5–8, 2004. Springer, Heidelberg, Germany. 6, 29

[Yao82] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science*, pages 160–164, Chicago, Illinois, November 3–5, 1982. IEEE Computer Society Press. doi:10.1109/SFCS.1982.38. 5

[YY06] Weigen Yan and Yeong-Nan Yeh. A simple proof of graham and pollak's theorem. *Journal of Combinatorial Theory, Series A*, 113(5):892–893, 2006. 30

## A Relevant Background and Terminology

In this section, we formally introduce relevant concepts from graph theory, information theory, and communication complexity.

**Introductory Graph-theory.** Let $G = (L, R, E)$ represent an undirected bipartite graph with partite sets $L$ and $R$, and edge set $E \subseteq L \times R$. The *complement* of $G$ is the bipartite graph $G^c := (L, R, (L \times R) \setminus E)$. A *biclique* is a bipartite graph $G = (L, R, E)$ such that there exist subsets $L' \subseteq L$, $R' \subseteq R$, and $E = L' \times R'$, that is, all vertices in $L'$ are connected to all vertices in $R'$.

**Proposition 3.** *A $P_4$-free bipartite graph $G$ is a graph where each of its connected components is a biclique.*

That is, there exists $c \in \mathbb{N}$ (the number of components of the bipartite graph), disjoint subsets $L_1, L_2, \ldots, L_c \subseteq L$, and disjoint subsets $R_1, R_2, \ldots, R_c \subseteq R$, such that the edge-set satisfies $E = \bigcup_{i=1}^{c} L_i \times R_i$. Alternatively, $P_4$-free bipartite graphs are a (disjoint) *union of bicliques*. Figure 4 provides a pictorial representation of bicliques and $P_4$-free graphs.

**Remark 1.** *Cluster graphs are a similar notion in graph theory. However, they are* not *bipartite and are a union of* cliques*; (non-bipartite) graphs where every vertex connects to every other vertex. In contrast, $P_4$-free bipartite graphs are a union of bicliques, a.k.a.,* biclusters*.*

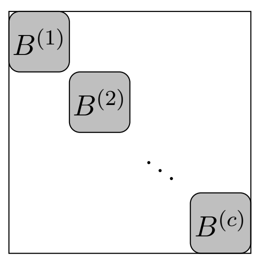



Figure 4: Pictorial representation of a $P_4$-free bipartite graph with $c$ connected components after rearranging the rows and columns appropriately. Each block $B^{(i)}$ represents a connected component in the graph, which is a biclique. It is possible that the graph has isolated vertices.

The *$P_4$-free partition number* of a bipartite graph $G = (L, R, E)$, represented by $\mathsf{P_4\text{-}fp}(G)$, is the minimum number $m$ such that there exist $P_4$-free graphs $G_i = (L, R, E_i)$, for $1 \leqslant i \leqslant m$, and the edge sets $E_1, E_2, \ldots, E_m$ partition $E$, the edge set of $G$. Similarly, the *$P_4$-free cover number* of a bipartite graph $G = (L, R, E)$, represented by $\mathsf{P_4\text{-}fc}(G)$, is the minimum number $m$ such that there exist $P_4$-free graphs $G_i = (L, R, E_i)$, for $1 \leqslant i \leqslant m$, and the edge set $E$ is the union of $E_1, E_2, \ldots, E_m$. Note that $\mathsf{P_4\text{-}fc}(G) \leqslant \mathsf{P_4\text{-}fp}(G)$, because every partition is also a cover.

Figure 5 illustrates the $P_4$-free partition of the graph corresponding to the function $\mathsf{INEQ}_N$, where $N = 4$.

**Random variables, entropy, and mutual information.** A random variable $X$ on sample space $\mathcal{X}$ is a real-valued function on $X : \mathcal{X} \to \mathbb{R}$. A discrete random variable is a random variable that takes only a finite or countably infinite number of values.

Let $X$ be a discrete random variable on a sample space $\mathcal{X}$ and probability mass function $p(x) = \Pr[X = x]$, for all $x \in \mathcal{X}$. The entropy is a measure of uncertainty of a random variable and is defined formally below.

$$\begin{array}{cccc} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{array} = \begin{array}{cccc} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{array} + \begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}$$

Figure 5: Illustration for $\mathsf{P}_4\text{-}\mathsf{fp}\,(\mathsf{INEQ}_4) = \lceil \log_2 N \rceil$, for $N = 4$.

**Definition 1** (Entropy). *The entropy $H(X)$ of a discrete random variable $X$ is defined by*

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log p(x) \ .$$

The relative entropy or Kullback-Leibler distance is a measure of the distance between two distributions.

**Definition 2** (Kullback-Leibler distance). *For probability mass functions $p(x)$ and $q(x)$, the relative entropy is defined as*

$$D(p \| q) = \sum_{x \in \mathcal{X}} p(x) \log \frac{p(x)}{q(x)} \ .$$

We can now define mutual information as the relative entropy of two random variables between their joint distribution and their product distribution.

**Definition 3** (Mutual Information). *For two random variables $X$ and $Y$ with joint probability mass function $p(x,y)$ and marginal probability mass functions $p(x)$ and $p(y)$, the mutual information is defined as*

$$I(X;Y) = D(p(x,y) \| p(x)p(y)) \ .$$

**Information-theoretic Measures as Graph Properties.** Let $p_{XY}$ define a joint distribution $(X,Y)$ over a sample space $\Omega_X \times \Omega_Y$. A distribution is *flat* if the probability of sampling any element in the sample space is either zero or an appropriate positive constant. In the sequel, we consider only flat probability distributions.

Observe that flat probability distributions over the sample space $\Omega_X \times \Omega_Y$ are equivalent to bipartite graphs over partite sets $\Omega_X$ and $\Omega_Y$ (with non-empty edge-set). For example, any bipartite graph $G(\Omega_X, \Omega_Y, E)$ (uniquely) corresponds to the joint distribution $p_{XY}$ that samples a uniformly random element from the set $E$. Consequently, given a flat distribution $p_{XY}$, one defines the unique bipartite graph corresponding to it $G(p_{XY})$, and, vice-versa.

Let $I(X;Y)$ represent the *mutual information* of the random variables $X$ and $Y$. Note that $I(X;Y) = 0$ if and only if $X$ and $Y$ are independent of each other. Interestingly, one can characterize the independence of random variables as an equivalent graph property.

**Proposition 4.** *A flat distribution $p_{XY}$ satisfying $I(X;Y) = 0$ implies that the bipartite graph $G(p_{XY})$ is a biclique.*

Suppose $G$ has $c \in \mathbb{N}$ connected components, and, w.l.o.g., assume that the components are named $\{1, 2, \ldots, c\}$. Let $C$ be the function $E \to \{1, 2, \ldots, c\}$ that outputs the component's name containing an edge. One can equivalently interpret $C$ as a random variable over the sample space $\{1, 2, \ldots, c\}$ such that $C = k$ with probability $e_k/e$, where $e_k$ is the number of edges in the $k$-th component of $G$, and $e = |E|$. The Markov chain $X \leftrightarrow C \leftrightarrow Y$, an essential concept in information theory, communication complexity, and cryptography, has an equivalent characterization in graph properties.

**Proposition 5.** *For a flat $p_{XY}$, the Markov chain $X \leftrightarrow C \leftrightarrow Y$ is equivalent to the graph $G(p_{XY})$ being $P_4$-free.*

Suppose Alice gets $x$ and Bob gets $y$ sampled from a $P_4$-free flat $p_{XY}$, Section 1.2 argues that they always agree on their shared key $s$, if and only if the secret key is a function of $C(x, y)$. Furthermore, the fact that Alice and Bob's samples are independent of each other conditioned on the secret key $s$, implies that $X \leftrightarrow S \leftrightarrow Y$, and the shared key is identical to $C$.

**Communication complexity as Graph properties.** Let $f : X \times Y \to \{0, 1\}$ be a Boolean function. The bipartite graph $G(f) \coloneqq (X, Y, E)$, where $E$ is the set of all input-pairs $(x, y)$ satisfying $f(x, y) = 1$, is a unique encoding of the function $f$. Observe that the complement of the graph $G(f)$, represented by $G(f)^c$, is identical to $G(1 - f)$, where $1 - f$ is the complement of the function $f$. Figure 6 presents the graph corresponding to the functions $\mathsf{INT}_n$ and $\mathsf{DISJ}_n$, for $n = 2$, which are defined below.

In deterministic communication complexity, the set of input-pairs of the parties consistent with a particular transcript is a *combinatorial rectangle.* That is, there exist $X' \subseteq X$ and $Y' \subseteq Y$ such that any $x \in X'$ and $y \in Y'$ results in that particular transcript. Suppose the output of the function corresponding to this transcript is 1. Then, one concludes that $X'$ and $Y'$ induce a biclique in the bipartite graph $G(f)$. Otherwise, if the output of the function corresponding to the transcript is 0, the vertex sets $X'$ and $Y'$ induce a biclique in $G(1 - f)$.

We shall study the following graphs encoding well-studied functions from communication theory.

1. For $n \in \mathbb{N}$, let $\mathsf{INT}_n = (\{0, 1\}^n, \{0, 1\}^n, E)$ be the bipartite graph defined as follows. For any $u, v \in \{0, 1\}^n$, we have $(u, v) \in E$ if and only if the set $U \subseteq \{1, 2, \ldots, n\}$ indicated by $u$ intersects the set $V \subseteq \{1, 2, \ldots, n\}$ indicated by $v$.

2. For $n \in \mathbb{N}$, let $\mathsf{DISJ}_n = (\{0, 1\}^n, \{0, 1\}^n, E)$ be the bipartite graph defined as follows. For any $u, v \in \{0, 1\}^n$, we have $(u, v) \in E$ if and only if the set $U \subseteq \{1, 2, \ldots, n\}$ indicated by $u$ is disjoint from the set $V \subseteq \{1, 2, \ldots, n\}$ indicated by $v$.

3. For $N \in \mathbb{N}$, let $\mathsf{EQ}_N = (\{1, 2, \ldots, N\}, \{1, 2, \ldots, N\}, E)$ be the bipartite graph defined as follows. For any $u, v \in \{1, 2, \ldots, N\}$, we have $(u, v) \in E$ if and only if $u = v$.

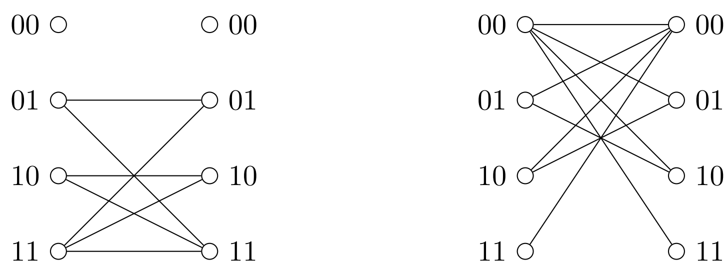
4. For $N \in \mathbb{N}$, let $\mathsf{INEQ}_N = (\{1, 2, \ldots, N\}, \{1, 2, \ldots, N\}, E)$ be the bipartite graph defined as follows. For any $u, v \in \{1, 2, \ldots, N\}$, we have $(u, v) \in E$ if and only if $u \neq v$.

Note that $\mathsf{INT}_n$ and $\mathsf{DISJ}_n$ are complements of each other, and $\mathsf{EQ}_N$ and $\mathsf{INEQ}_N$ are complements of each other. Figure 6 illustrates the graph corresponding to $\mathsf{INT}_n$ and $\mathsf{DISJ}_n$ for $n = 2$.

**Remark 2.** *It is well-known that the nondeterministic communication complexity of computing a function $f$ is equivalent to the problem of* covering *the bipartite graph $G(f)$ using the minimum number of bicliques (a.k.a., the* biclique cover number *of $G$) [Juk12].*

# B Modeling the Motivating Problem A as $P_4$-free Partition Number

Let $\Omega_X$ and $\Omega_Y$ be the sample space of Alice and Bob's samples, respectively. Let $p_{XY}$ be a uniform distribution over an arbitrary subset of $\Omega_X \times \Omega_Y$. For this probability distribution, consider a bipartite graph $G$ with partite set $\Omega_X$ and $\Omega_Y$. The edge set of $G$ contains $(x, y)$ such that the probability of sampling $(x, y)$ according to $p_{XY}$ is positive.




(a) Graph of $\mathsf{INT}_n$, for $n = 2$. (b) Graph of $\mathsf{DISJ}_n$, for $n = 2$.

Figure 6: Bipartite graphs corresponding to the distributions $\mathsf{INT}_n$ and $\mathsf{DISJ}_n$, for $n = 2$.

Recall that the genie observes the sample $(x, y)$ (that is, an edge in the graph $G$) and computes the assistance $z \in \{0,1\}^k$. Conditioned on the assistance $z$ that the genie provides, let $G_z := (\Omega_X, \Omega_Y, E_z)$, where $E_z \subseteq E$ is the set of all samples $(x, y)$ where the (deterministic) genie provides $z$ as assistance. Observe that the edge-sets in $\{E_z\}_{z\in\{0,1\}^k}$ partition the edge-set $E$.

Fix $z$, the assistance that the genie provides. Conditioned on $z$, the samples $(x, y)$ of Alice and Bob are distributed according to the flat joint distribution $p_{XY|Z=z}$, where $Z$ denotes the random variable for genie's assistance. This distribution is identical to the distribution corresponding to the graph $G_z$. Henceforth, the flat distribution $p_{XY|Z=z}$ is equivalent to the graph $G_z$.

Next, consider Alice receiving her sample $x$ and Bob receiving his sample $y$ from the joint distribution $p_{XY|Z=z} \equiv G_z$. Alice partitions her sample space $\Omega_X$ (the partition possibly depends on $z$) to obtain the secret key $s_A$. Similarly, Bob partitions his sample space $\Omega_Y$ to determine the secret key $s_B$. The fact that Alice and Bob *always* agree on the key $s = s_A = s_B$, implies that both Alice's and Bob's partitions of $\Omega_X$ and $\Omega_Y$ respect the connected components of $G_z$.[12] Consequently, the secret key $s$ is a function of $C(x, y)$, (the identifier of) the connected component where their respective samples belong.

Now, the parties use the left-over entropy in their respective samples (after agreeing on the shared key $s$). That is, Alice and Bob, respectively, use the conditional distributions $(X|Z = z, S = s)$ and $(Y|Z = z, S = s)$ as their left-over sources of independent randomness. However, unless $X \leftrightarrow (S, Z) \leftrightarrow Y$, their randomness is not independent; that is, the shared secret key and genie's assistance annihilate the correlation between Alice and Bob's samples. This constraint implies that $I(X; Y|S = s, Z = z) = 0$, which is equivalent to the graph corresponding to the flat $(X, Y|S = s, Z = z)$ being a biclique. That is, the random variables $S$ and $C$ are identical, and the graph $G_z$ is $P_4$-free (and contains at least two connected components so that $s$ has non-trivial entropy).

Consequently, our objective is to find the minimum $k \in \mathbb{N}$ such that there exists a partition of $G$ into $\{G_z\}_{z\in\{0,1\}^k}$, where each $G_z$ is $P_4$-free; that is, determine $k = \log_2(\mathsf{P_4\text{-}fp}(G))$.

[12] Suppose not. Then, assume that Alice outputs secret key $s_A$ for some vertex $x \in \Omega_X$ in a connected component, and outputs a different secret key $s'_A$ for some other vertex $x' \in \Omega_X$ in the same connected component. Consider a path in $G_z$ connecting the vertices $x$ and $x'$. There will exist $x_1$ on this path where Alice outputs secret key $x_{A,1}$, and $x_2$ $(\neq x_1)$ on this path where Alice outputs secret key $s_{A,2}$ such that $s_{A,1} \neq s_{A,1}$ and the distance between $x_1$ and $x_2$ is two. Let $y \in \Omega_Y$ be a sample of Bob that is at distance one from both $x_1$ and $x_2$ in the graph $G_z$. Obviously, the secret key output by Bob for sample $y$ disagrees with $s_{A,1}$ or $s_{A,2}$. A similar argument also holds for Bob.

# C Modeling the Motivating Problem B as $P_4$-free Cover Number

Given a Boolean function $f\colon X \times Y \to \{0,1\}$, we encode it as the bipartite graph $G(f)$ with partite sets $X$ and $Y$ such that the edge set of $G(f)$ contains all $(x,y) \in X \times Y$ such that $f(x,y) = 1$.

First, let us begin by observing that a function $f$ that may be evaluated by making one call to the $\mathsf{EQ}$ oracle without any non-deterministic input $z$ if and only if the bipartite graph $G(f)$ is $P_4$-free.[13]

Next, consider any $f$ that has a non-deterministic communication protocol using $\mathsf{EQ}$ oracle once. For every $(x,y)$ such that $f(x,y) = 1$, then the edge $(x,y) \in E(G(f))$ is covered in some graph $G_z$, where $z$ is the non-deterministic input. Following the discussion above $G_z$ is $P_4$-free. Furthermore, if $(x,y)$ is such that $f(x,y) = 0$, then the edges $(x,y) \in E(G(f))$ is not covered in any edge-set of $G_z$. Consequently, the set of all possible $G_z$ covers $G(f)$.

So, the motivating problem is to find a covering of $G(f)$ with the minimum number of $P_4$-free bipartite graphs, the $P_4$-free cover number.

# D Common Information: Discussion

**Wyner's Common Information.** Wyner's common information [Wyn75] is one of the several measures (for example, Shannon's mutual information, Gács-Körner [GK73] common information being some other prominent notions) of information that is common to $X$ and $Y$. Formally, the quantity is defined as follows.

$$J(X;Y) := \min_{Z\colon X \leftrightarrow Z \leftrightarrow Y} H(Z),$$

where $H(Z)$ is the entropy of the random variable $Z$. Intuitively, it is the smallest entropy random variable that annihilates the correlation between $X$ and $Y$. As an approximation, one can consider $Z$ with the smallest support and $p_{XY}$ being a flat. In this case, it is easy to see that $p_{XY|Z=z}$ is a biclique. Consequently, this Wyner's common information, intuitively, corresponds to partitioning the graph $G(p_{XY})$ the smallest number of bicliques, a.k.a. biclique partition number. Observe that Wyner's common information specifically kills the possibility of establishing a shared secret key; consequently, it is an inappropriate measure for our motivating problem. Furthermore, Wyner's common information can be non-zero while our genie needs to provide no assistance (refer to forward or flip distribution in Figure 2). The length of our genie's assistance may be exponentially smaller than Wyner's common information as well (refer to the noisy typewriter distribution in Figure 2).

**Non-interactive Joint Simulation of Distributions.** Information theory studies the possibility of simulating a sample from a joint distribution $(U,V)$ given multiples samples from the joint distribution $(X,Y)$, namely, *non-interactive simulation of joint distributions*. This line of research starts with the seminal works of Gács and Körner [GK73], Witsenhausen [Wit75], and Wyner [Wyn75]. In this setting, $Z = \emptyset$ (that is, the genie does not provide any assistance). The objective of the parties is to generate samples $u$ and $v$ from their local views such that the joint distribution of the samples $(u,v)$ emulates a fixed joint distribution $(U,V)$. Note that in

[13] Note that if $f$ is $P_4$-free then Alice computes the connected component $C_x$ of the bipartite graph $G(f)$ her input is. Similarly, Bob also computes the connected component $C_y$ where his input $y$ belongs. Finally, they output $\mathsf{EQ}(C_x, C_y)$.

For the other direction, suppose Alice feeds $A(x)$ to the $\mathsf{EQ}$ oracle, and Bob feeds $B(y)$ to the $\mathsf{EQ}$ oracle. Conditioned on $A(x) = B(y) = \lambda$, the set of all $(x,y)$ forms a combinatorial rectangle $R_\lambda$. Note that $R_\lambda$ are disjoint, because $A$ and $B$ are deterministic functions. So, $G(f)$ is a disjoint union of combinatorial rectangles, a.k.a., it is $P_4$-free.

our problem statement, we distilling out the shared secret key and the independent randomness. This problem is more general and $(U, V)$ can be any arbitrary distribution. Even the decision version of the problem where one has to determine whether samples from one joint distribution may be non-interactively simulated from the samples of another joint distribution, in its full generality, is a difficult problem [GKS16, DMN18]. Technically, reverse hypercontractivity [AG76, Bor82, MOR⁺06, MOS13, KA16, DMN18, BG15, MO05], and maximal correlation [Hir35, Wit75, AG76, Rén59, AGKN13] are few of the most prominent techniques employed to prove the impossibility of non-interactive simulations. We refer the interested reader to an exceptional survey by Sudan, Tyagi, and Watanabe [STW20] for a thorough introduction to this field.

**Non-interactive Correlation Distillation.** This problem is a special case of non-interactive joint simulation of distributions where the target samples of Alice and Bob are identical, that is, $U = V$. The end objective is to emulate a shared secret key that the parties agree on [MOR⁺06, MO05, Yan04, BM11, CMN14].

**Secure Non-interactive Joint Simulation.** The recent work [KMN20] initiates the study of secure non-interactive joint simulations with the stronger objective of being cryptographically secure. For example, a difference of setting from non-interactive joint simulation is that information cannot be erased. This study is motivated by defining the achievable rate of the efficiency for secure computation protocols, and characterizing the rate-achieving secure protocol constructions.

**Assisted Common Information (and Variants).** A sequence of works develops "monotone properties" for interactive protocols, which refine and generalize the notions of common information [Wyn75, GK73] discussed above. For example, [WW05] proposes *monotones* for cryptographic protocols. Recently, generalizations of common information were explored in [PP10, PP11, PP14, RP14]. These works, in general, study how well the dependence between a pair of random variables can be resolved by a piece of common information. These notions of dependence satisfy the invariant that an interactive protocol cannot reduce this quantity. Consequently, they find applications in proving rate lower bounds in interactive protocols.

**Leakage attacks in Cryptography.** The work of [BMN17] studied $P_4$-free partition number of some interesting graphs. They studied this property in the context of upper-bounding the leakage resilience of setups in the cryptographic setting. They considered using the joint samples from probability distributions $p_{XY}$ to perform two-party general secure computation in the presence of leakage. That is, the adversarial party obtains the leakage $L(X, Y)$ in addition to its local sample, where $L(\cdot, \cdot)$ is an arbitrary leakage function. Despite this leakage, the objective of the parties is to perform general secure computation using an interactive protocol. They showed that $\lceil \log_2 (G(p_{XY})) \rceil$ bits of leakage suffices to make the setup entirely useless for secure computation. They also demonstrated that the bound obtained by this technique is significantly tighter than the bound Wyner's common information entails, which is relevant to ruling out shared key agreement only, a significantly simpler task than two-party general secure computation [Kil00].

# E Relation to Other Graph Properties

In this section, we explore the connection of $P_4$-free partition and cover numbers to graph properties such as star arboricity, biclique partition, and biclique cover number.

**Star Arboricity.** A *tree* is a graph where any two vertices are connected by a unique path. A *forest* is a disjoint union of trees. The *arboricity* of a graph, represented by $\mathsf{a}(G)$, is the minimum number of forests into which its edges can be partitioned. Observe that if there exists a covering of a graph with $m$ forests then there also exists a partitioning of that graph with (at most) $m$ forests. Consequently, partitioning into and covering with the minimal number of forests are identical graph properties. One can efficiently compute the star arboricity of a graph using a greedy strategy because it is expressible as a matroid partitioning problem [GW88, GW92]. The arboricity of a graph measures how dense the graph is. A graph with many edges has high arboricity, and graphs with high arboricity contain a dense subgraph.

A *star* is a tree with one internal node, or, equivalently, is $K_{1,r}$ a biclique with where one vertex connects to $r$ vertices in the other partite set. A *star forest* is a forest whose connected components are stars. The *star arboricity* of a graph, represented by $\mathsf{sa}(G)$, is the minimum number of star forests that a graph can be partitioned into. Similar to the previous case, partitioning and covering a graph into the minimum number of star forests are equivalent. By separating the odd and the even level edges of a forest one can form two star forest partitioning its edges. Consequently, we have

$$\mathsf{a}(G) \leqslant \mathsf{sa}(G) \leqslant 2\mathsf{a}(G).$$

Note that a star forest is a $P_4$-free graph. Therefore, we conclude the following result.

**Proposition 6.** *For any bipartite graph $G$, the following bound holds.*

$$\mathsf{P_4\text{-}fc}(G) \leqslant \mathsf{P_4\text{-}fp}(G) \leqslant \mathsf{sa}(G).$$

However, this bound is poor for dense graphs, for example, the biclique $K_{N,N}$.

The following result by Algor and Alon [AA89] upper bounds the star arboricity of degree-bounded graphs.

**Imported Theorem 6** (Consequence of [AA89])**.** *For any graph $G$ with maximum degree $\Delta$, the following bound holds.*

$$\mathsf{sa}(G) \leqslant \frac{1}{2} \cdot \Delta \cdot (1 + o(1)).$$

This result already yields non-trivial upper-bounds for $\mathsf{P_4\text{-}fc}(G)$ and $\mathsf{P_4\text{-}fp}(G)$ by upper-bounding its star-arboricity for several interesting functions (for example $\mathsf{INT}_n$). Note, however, Theorem 3 provides an upper bound of $\mathsf{P_4\text{-}fc}(\mathsf{DISJ}_n)$ that is exponentially better than the upper bound entailed by [AA89].

**Biclique Partition Number.** Recall that a *biclique* is a complete bipartite graph. The *biclique partition number* of a graph, represented by $\mathsf{bp}(G)$, is the minimum number of bicliques needed to partition its edges. Graham and Pollak introduced this problem motivated by the network addressing problem and graph storage problem [GP71, GP72] (see also [BF88, VL85, YY06, vLW01]). The celebrated Graham-Pollak Theorem states that $\mathsf{bp}(K_N) = (N-1)$ [GP72, Tve82, Pec84, Vis08, Vis13]. However, all proofs are algebraic, and no purely combinatorial proof is known. In general, $\mathsf{bp}(G) \geqslant \max\{n_+(G), n_-(G)\}$ [GP72, Hof72, Tve82, Pec84], where $n_+(\cdot)$ and $n_-(\cdot)$, respectively, represent the number of positive and negative eigenvalues of the adjacency matrix of the graph.

Observe that the biclique partition number admits a trivial upper bound, $\mathsf{bp}(G) \leqslant$ the size of the smallest vertex cover of $G$. Determining the $\mathsf{bp}(G)$ of a general graph is a hard problem [KRW88] (even for bipartite graphs [Orl77]) and is also hard to approximate [CHHK14].

Section 1.2 establishes the connection between Wyner's common information of $p_{XY}$ [Wyn75] with the biclique partition number of the bipartite graph $G(p_{XY})$.

Since a biclique is $P_4$-free, we naturally have the following bound.

$$\begin{bmatrix} 0&1&1&1\\ 1&0&1&1\\ 1&1&0&1\\ 1&1&1&0 \end{bmatrix} = \begin{bmatrix} 0&1&1&1\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0 \end{bmatrix} + \begin{bmatrix} 0&0&0&0\\ 1&0&1&1\\ 0&0&0&0\\ 0&0&0&0 \end{bmatrix} + \begin{bmatrix} 0&0&0&0\\ 0&0&0&0\\ 1&1&0&1\\ 0&0&0&0 \end{bmatrix} + \begin{bmatrix} 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 1&1&1&0 \end{bmatrix}$$

Figure 7: Illustration for $\mathsf{bp}(\mathsf{INEQ}_N) = N$, for $N = 4$.

**Proposition 7.** *For any graph $G$, the following bound holds:*

$$\mathsf{P_4\text{-}fc}(G) \leqslant \mathsf{P_4\text{-}fp}(G) \leqslant \mathsf{bp}(G).$$

Biclique partition number entirely ignores the potential of compressing multiple bicliques into one graph. Consequently, for most graphs, the upper-bound above is loose. For example, a matching has high biclique partition number; however, its $P_4$-free partition number is one.

Let $M_G$ represent the adjacency matrix of the bipartite graph $G$. Algebraically, the notion of binary matrix factorization of $M_G$ is identical to $\mathsf{bp}(G)$ [KPRW19]. The outer product of two binary vectors represents the adjacency matrix of a biclique. That is, *Boolean rank-one matrices* are bicliques. So, the minimum $r$ such that $M_G$ is the sum of $r$ Boolean rank-one matrices represents the Boolean rank of $M_G$. Note that $\mathsf{bp}(G) = r$.

**Biclique Cover Number.** Covering a graph with the minimum number of bicliques has received significant attention in theoretical computer science [Orl77, Sim90, FMPS07, GH07, JK09, CHHK14] due to widespread application. Representative applications, for example, as [EU18] indicates, span computational biology [NMWA78, NHC+12, NED+13], data mining [MMG+08], machine learning [SW03], automata theory [GH07], communication complexity [JK09], and graph drawing [HMR06]. Let alone computing the biclique cover number exactly (which is hard even for bipartite graphs [Orl77] and chordal bipartite graphs [Mül96]), approximating it is hard as well [Sim90, GH07, CHHK14].

The biclique cover number is at most the biclique partition number; however, it can be exponentially smaller. For example, $\mathsf{bc}(K_N) = \lceil \log_2 N \rceil$ [Pin13]; but, the Graham-Pollak Theorem states that $\mathsf{bp}(K_N) = (N-1)$ [GP72, Tve82, Pec84, Vis08, Vis13]. In general, Pinto [Pin13] proved that $\mathsf{bp}(G) \leqslant (3^{\mathsf{bc}(G)} - 1)/2$, and presented a graph family achieving equality in this bound.

Observe that $\mathsf{bc}(\mathsf{EQ}_N) \geqslant N$, where $\mathsf{EQ}_N$ is a equality function with size-$N$ domain for the input of both parties. Intuitively, the graph corresponding to $\mathsf{EQ}_N$ is a matching, and no combinatorial rectangle can cover two edges of this matching. The "fooling set argument" relies on this observation to show lower bounds on $\mathsf{bc}(G)$, for a general $G$. It identifies a subset of vertices that induce a matching in the graph $G$. Therefore, the size of this matching lower-bounds $\mathsf{bc}(G)$.

Let $M_G$ be the adjacency graph of the bipartite graph $G$. Then, there are *algebraic* matrix properties of $M_G$ that help estimate the biclique cover number of $G$. For example, the non-negative rank of $M_G$[14] upper-bounds $\mathsf{bc}(G)$ [Yan91].[15]

**Equivalence Cover Number.** This discussion is specific to loopless undirected graphs. A *clique* is a complete graph. An *equivalence* graph is a graph such that each of its connected components is

[14] A non-negative rank-one matrix can be written as the outer product of two vectors whose entries are non-negative. A matrix $M$ has non-negative rank $r$, if there exist $r$ non-negative rank-one matrices that add to $M$.

[15] Consider the decomposition of $M_G$ into minimum number of non-negative rank-one matrices. Consider a biclique cover that indicates whether the entries of these non-negative rank-one matrices are positive or not. This reduction provides a biclique cover of $G$.

a clique. A size-$d$ equivalence cover of a graph $G = (V, E)$ is a set of graphs $G_1 = (V, E_1), \ldots, G_d = (V, E_d)$ such that $E_1 \cup \cdots \cup E_d = E$. The *equivalence cover number* of $G$ is the minimum $d \in \mathbb{N}$ such that a size-$d$ covering of $G$ exists. Note that the star $G = K_{1,N-1}$ has equivalence cover number $(N-1)$. We remark that the definition of equivalence cover number has an addition condition that no edge of $G$ should be covered in every equivalence subgraph. This restriction is a technicality to ensure that no two vertices receive an identical $\varphi$ mapping. Refer to [AA20] for a discussion on why this technicality may be ignore for all applications.

Given a size $d$ equivalence cover of $G$, we construct a vertex mapping $\varphi\colon V \to \mathbb{N}^d$ as follows. If the edge $(u, v) \in E$ is covered in the $j$-the connected component of the graph $G_i$, then define $\varphi(u)_i = \varphi(v)_i = j$. Since every connected component of $G_i$ is a clique, there are no conflicts in the assignment above. Finally, all remaining unfilled entries of the mapping $\varphi$ are completed with unique elements from $\mathbb{N}$. This mapping establishes the following guarantee: $(u, v)$ is an edge in $G$ if and only if there exists $i \in \{1, \ldots, d\}$ such that $\varphi(u)_i = \varphi(v)_i$. This vertex mapping (or, $d$-fold coloring) shall be useful below.

**Product/Prague Dimension.** Let $K_{\mathbb{N}}$ represent the complete graph with infinite vertices. The $K_{\mathbb{N}}^d$ be the $d$-fold graph product of the graph $K_{\mathbb{N}}$. Note that the vertices of this graph are elements in $\mathbb{N}^d$. Furthermore, two vertices $u, v \in \mathbb{N}^d$ are neighbors in this graph if and only if $u$ and $v$ differ from each other in every coordinate. The *product/Prague dimension* of a graph $H$ [NP77, NR78], represented by $\mathsf{pdim}\,(H)$, is the minimum $d \in \mathbb{N}$ such that $H$ is an induced subgraph of $K_{\mathbb{N}}^d$.

Consider the vertex mapping $\varphi\colon V \to \mathbb{N}^d$ constructed above from the size-$d$ equivalence covering of a graph $G$. This vertex mapping has the property that $(u, v)$ is *not* an edge in $G$ if and only if, for all $i \in \{1, \ldots, d\}$, we have $\varphi(u)_i \neq \varphi(v)_i$. That is, the vertex mapping $\varphi$ demonstrates that the complement graph of the graph $G$ is an induced subgraph of $K_{\mathbb{N}}^d$. That is, $\overline{G}$ is a induced subgraph of $K_{\mathbb{N}}^d$. This interpretation of the vertex mapping $\varphi$ proves that the equivalence cover number is identical to the product/Prague dimension of the complement graph.

[NP77] reduced the hardness of computing the product dimension of graphs to computing the edge chromatic number. This problem has also been studied in information theory [KO98, KM01].

# F Representative Scheduling Problem

Covering a graph with the minimum number of bicliques has received significant attention in theoretical computer science [Orl77, Sim90, FMPS07, GH07, JK09, CHHK14] due to widespread applications. Representative applications, for example, as [EU18] indicates, span computational biology [NMWA78, NHC+12, NED+13], data mining [MMG+08], machine learning [SW03], automata theory [GH07], communication complexity [JK09], security and access control [SLY06, EHM+08], and graph drawing [HMR06]. This graph property is referred to as the *biclique cover number* (also known as, bipartite dimension, and rectangle cover number).

**A representative template.** Let $U$ be the set of users and $D$ be the set of sensitive data. A Boolean matrix $G$ defines which user has access to which data. That is, $G_{u,d} = 1$ implies that the user $u \in U$ should have access to the data $d \in D$; otherwise, if $G_{u,d} = 0$, then the user $u \in U$ should not have access to the data $d \in D$. It is possible to *many-to-many multicast* a subset of data $D' \subseteq D$ to a subset of users $U' \subseteq U$. Consequently, all the users in $U'$ simultaneously receive all the data in $D'$. What is the *minimum number* of multicast necessary to help each user to receive all the data of its choice?

Note that each multicast above induces a biclique/combinatorial rectangle. Consequently, this combinatorial problem is equivalent to the biclique/rectangle cover number of the graph $G$, the minimum number of bicliques/rectangles to cover the bipartite graph/matrix $G$. Several applications mentioned above, for example, [NMWA78, SLY06, EHM+08, NHC+12, NED+13], fall into this template. If the users insist on receiving every data only once then this problem is equivalent to the biclique partition number of the graph $G$.

**Leveraging parallelism.** Observe that it may be possible to schedule multiple of these multicast instances simultaneously (refer to Figure 4). For example, two multicast instances above are non-conflicting if their sets of users and the set of data are disjoint. Clearly, non-conflicting multicast instances can be scheduled in parallel. In general, let $U_1, U_2, \dots, U_c$ be disjoint subsets of users, for arbitrary $c \in \mathbb{N}$, and $D_1, D_2, \dots, D_c$ be disjoint subsets of data. We shall enable the many-to-many multicast of the data in $D_i$ to all users in $U_i$, for $1 \leqslant i \leqslant c$. Intuitively, we have parallelized multiple non-conflicting multicast instances. What is the *minimum number* of such parallelized multicast instances necessary to help each user to receive all the data of its choice?

This problem is equivalent to the $P_4$-free cover number of the graph $G$. If each user insists on receiving each data only once, then the problem is equivalent to the $P_4$-free partition number of the graph $G$.

## G Proof of Theorem 1

Our proof of hardness for both partition and cover number is based on a result from [GO09], which shows that computing the edge partition of a bipartite planar graph into two star forests is NP-complete. For a definition of star forests and star arboricity, see Appendix E.

**Theorem 7** (Gonçalves and Ochem [GO09])**.** *For any $g > 3$, deciding whether a bipartite planar graph $G$ with girth* [16] *at least $g$ and maximum degree 3 satisfies $\mathsf{sa}(G) \leqslant 2$ is NP-complete.*

*Proof of Theorem 1 .* First we show the decision problem is in NP, that is, given a partition of the edge set of $G$ into $\leqslant 2$ components we can verify in polynomial time whether it is a $P_4$-free partition of size $\leqslant 2$ of $G$ or not. This can be done in polynomial time by checking if any set of four vertices (two in the left set and two in the right set) in each component is $P_4$-free.

Next we show that the decision problem from Theorem 7 is polynomial-time reducible to the $P_4$-free partition and cover number on bipartite graphs. The decision problem in Theorem 7 is NP-complete for any bipartite planar graph of girth at least $g > 3$; in particular, it holds for $g \geqslant 6$. Suppose we have a bipartite planar graph $G$ with girth $g \geqslant 6$ and maximum degree 3. Since $G$ has girth at least 6, there are no cycles of length less than 6 in $G$. It implies that $K_{2,2}$ is not a subgraph of $G$. Therefore, any disjoint union of bicliques in $G$ is a star forest. This implies that $\mathsf{sa}(G) = \mathsf{P_4\text{-}fp}(G) = \mathsf{P_4\text{-}fc}(G)$, since $K_{2,2}$-free graphs have the property that the $P_4$-free partition and cover numbers are both identical to the star arboricity. Thus, the star arboricity of $G$ is less than or equal to 2 if and only if so does the biclique partition number of $G$. □

## H Proof of Theorem 2

Let $H$ be a fixed graph, a classical problem in graph theory is finding the maximum number of edges in a graph on $N$ vertices which does not contain a copy of $H$.

[16] The girth of an undirected graph is the length of a shortest cycle contained in the graph.

**Definition 4** (Turan number)**.** *Turan number denoted by $ex(N,H)$ is the maximum number of edges in a graph on $N$ vertices which does not contain a copy of $H$.*

A sub-problem of special interest is when $H$ is a complete bipartite graph, this problem is commonly referred to as the Zarankiewicz problem.

**Definition 5** (Zarankiewicz function)**.** *Zarankiewicz function denoted by $z(M,N;s,t)$ is the maximum number of edges in a bipartite graph $G=(L,R,E)$ where $|L|=M$, $|R|=N$ which does not contain a sub-graph of the form $K_{s,t}$.*

**Imported Theorem 8.** *[ES74] $ex(N,K_{a,b}) \geqslant C'N^{2-\frac{a+b-2}{ab-1}}$, where $C'$ is a positive absolute constant.*

Considering the adjacency matrix of a $K_{a,b}$-free graph on $n$ vertices, we get $z(N,N,a,b) \geqslant 2ex(N,K_{a,b})$.

Let $G=(L,R,E)$ be a bipartite graph. A *combinatorial rectangle* is a set of the form $A\times B$, where $A\subseteq L$ and $B\subseteq R$. Observe that a combinatorial rectangle corresponds to a biclique if we restrict ourselves to rectangles of the form $\{A\times B : (u,v)\in A\times B \iff (u,v)\in E\}$. We shall use this fact in the sequel, to show that the $P_4$-free partition number of a $K_{t+1,t+1}$-free bipartite graph is high.

**Lemma 1.** *For a bipartite graph $G=(L,R,E)$ such that $|L|=|R|=N$, if $G$ is $K_{t+1,t+1}$-free for some $t>0$, then $\mathsf{P_4\text{-}fp}(G) \geqslant \frac{e(G)}{2Nt}$.*

*Proof.* Consider the adjacency matrix of the bipartite graph $G$. A biclique in $G$ can be represented as a combinatorial rectangle in the adjacency matrix of $G$ (as explained above). The *width* of this combinatorial rectangle is the smaller of its two dimensions, and the *length* of this combinatorial rectangle is the larger of the two dimensions. Observe that any $P_4$-free bipartite graph is the union of non-intersecting combinatorial rectangles.

Let $G'$ be a $P_4$-free bipartite sub-graph of $G$. For any combinatorial rectangle in $G'$, *length* $\leqslant 2N$ and *width* $\leqslant t$, since if *width* $= t+1 \leqslant$ *length*, then there exists a $K_{t+1,t+1}$-subgraph in $G$. This implies that $e(G') < 2Nt$, and consequently $\mathsf{P_4\text{-}fp}(G) \geqslant \frac{e(G)}{2Nt}$. □

The proof of Theorem 2 follows from the fact about Zarankiewicz function of $K_{t+1,t+1}$-free bipartite graphs and Lemma 1.

*Proof of Theorem 2 .* We construct a bipartite graph $G=(L,R,E)$ such that $|L|=|R|=N$ and it is $K_{t+1,t+1}$-free. By Imported Lemma 8,

$$e(G) = z(N,N;t+1,t+1) \geqslant 2ex(N,K_{t+1,t+1}) \geqslant 2CN^{2-\frac{2}{t+2}},$$

where $C$ is a positive absolute constant. By Lemma 1, we get that

$$\mathsf{P_4\text{-}fp}(G) \geqslant \frac{e(G)}{2Nt} = \frac{2CN^{2-\frac{2}{t+2}}}{2Nt} = C\cdot\frac{1}{t}\cdot N^{1-\frac{2}{t+2}}.$$

□

### H.1 Erdős-Rényi graphs do not have Large Bicliques

In this section, we will show that Erdős-Rényi graphs do not have *large* bicliques with *high* probability. We follow the standard outline for first moment techniques, see, for example, [FK16] Chapter 7.2. Let $G \leftarrow \mathsf{ER}(N, N, p)$, where $p \in (0,1)$ is a constant. Let $t+1 = \lceil 2\log_a N \rceil$. Let $\mathbb{N}_{t+1}$ be the random variable counting the number of $K_{t+1,t+1}$ bicliques in $G$.

Therefore, we have

$$\mathrm{E}[\mathbb{N}_{t+1}] = \binom{N}{t+1}^2 p^{(t+1)^2} \leqslant \left(\frac{\mathrm{e}N}{t+1}\right)^{2(t+1)} p^{(t+1)^2} = \left(\frac{\mathrm{e}Np^{\frac{t+1}{2}}}{t+1}\right)^{2(t+1)} \leqslant \left(\frac{\mathrm{e}N \cdot \frac{1}{N}}{t+1}\right)^{2(t+1)} = o(1).$$

Therefore, with probability $1 - o(1)$, there are no $K_{t+1,t+1}$ bicliques in $G$.

## I Estimates for $\mathsf{INT}_n$, $\mathsf{DISJ}_n$, and $\mathsf{INEQ}_N$

In this section, we establish upper bounds for $\mathsf{DISJ}_n$ and $\mathsf{INT}_n$ in terms of $P_4$-free partition/cover number (see Theorem 11 and Theorem 12). We also exhibit a non-trivial gap between the star arboricity, and the $P_4$-free partition number of $\mathsf{DISJ}_n$ (see Eq. 2 of Theorem 11).

### I.1 $P_4$-free Partition/Cover Number and Graph Products

In this section, we introduce the notion of a graph product, and we prove some properties regarding the behavior of $P_4$-free partition/cover number on graph products. These concepts are used to solve recurrence relations for $\mathsf{DISJ}_n$ and $\mathsf{INT}_n$ in the sequel.

**Definition 6** (Graph Product)**.** *Let $G_1 : (L_1, R_1, E_1)$ and $G_2 : (L_2, R_2, E_2)$ be two bipartite graphs. Let $G$ denote the* tensor product *of the two bipartite graphs $G_1$, and $G_2$, represented by $G_1 \times G_2$. The partite sets of $G$ are $L_1 \times L_2$ and $R_1 \times R_2$, and the edge set is $E(G) := \{(\ (u,a),(v,b)\ ) : (u,v) \in E_1, (a,b) \in E_2\}$.*

**Claim 9** (Product of $P_4$-free bipartite graphs is $P_4$-free)**.** *Let $G$ and $H$ be two $P_4$-free bipartite graphs, then $G \times H$ is also $P_4$-free.*

*Proof.* Let $(u_1,a_1),(u_2,a_2)$ be two distinct vertices in the left partite set of $G \times H$. Let $(v_1,b_1),(v_2,b_2)$ be two distinct vertices in the right partite set of $G \times H$. We emphasize that the vertices, for example, $u_1, u_2$ need not be distinct.

Consider the subgraph $S$ induced by these four vertices. If $e(S) \leqslant 2$, then $S$ is $P_4$-free. In the sequel, we shall prove that if $e(S) \geqslant 3$ implies that $e(S) = 4$, which proves that the graph $S$ is $P_4$-free.

Suppose, without loss of generality, we have $(u_1,a_1) \sim (v_1,b_1) \sim (u_2,a_2) \sim (v_2,b_2)$, where $x \sim y$ denotes an edge between the two vertices $x$ and $y$. We will call this assumption as the (*)-assumption in the sequel. Our objective is to prove that $(u_1,a_1) \sim (v_2,b_2)$.

**The first case.** Suppose, we have $u_1 \neq u_2$, $v_1 \neq v_2$, $a_1 \neq a_2$, and $b_1 \neq b_2$. Now, the (*)-assumption implies that $u_1 \sim v_1 \sim u_2 \sim v_2$ and $a_1 \sim b_1 \sim a_2 \sim b_2$. Since, the graphs $G$ and $H$ are themselves $P_4$-free, we have $u_1 \sim v_2$ and $a_1 \sim b_2$. Therefore, we also have $(u_1,a_1) \sim (v_2,b_2)$ in the product graph $G \times H$.

**The remaining case.** Without loss of generality, assume that $u_1 = u_2$. Similar to the above case, the (*)-assumption implies that $u_1 \sim v_1 \sim u_2 \sim v_2$ and $a_1 \sim b_1 \sim a_2 \sim b_2$. Then, the fact that $u_2 \sim v_2$ is equivalent to $u_1 \sim v_2$. Similarly, irrespective of whether $a_1 = a_2$ or not, or $b_1 = b_2$ or not, we have the fact that $a_1 \sim b_1 \sim a_2 \sim b_2$ implies $a_1 \sim b_2$. Therefore, we also have $(u_1,a_1) \sim (v_2,b_2)$.

This exhaustive case analysis completes the proof. □

**Claim 10** (Sub-multiplicativity of the $P_4$-free Partition Number)**.** *Let $G$ and $H$ be two bipartite graphs, then the following holds for their graph product*

$$\mathsf{P_4\text{-}fp}\left(G \times H\right) \leqslant \mathsf{P_4\text{-}fp}\left(G\right) \cdot \mathsf{P_4\text{-}fp}\left(H\right) \ .$$

*Proof.* Suppose $\mathsf{P_4\text{-}fp}(G) = k$, and the graph $G$ partitions into graphs $G_1, \ldots, G_k$, such that the graph $G_i$, for every $1 \leqslant i \leqslant k$, is a $P_4$-free graph. Similarly, suppose $\mathsf{P_4\text{-}fp}(H) = \ell$, and the graph $H$ partitions into $H_1, \ldots, H_\ell$, such that $H_j$, for every $1 \leqslant j \leqslant \ell$, is a $P_4$-free graph. Therefore, one can partition $G \times H$ as follows.

$$(G \times H) = \left(\sum_{i=1}^{k} G_i\right) \times \left(\sum_{j=1}^{\ell} H_j\right) = \sum_{i=1}^{k}\sum_{j=1}^{\ell} G_i \times H_j.$$

By Claim 9, each $G_i \times H_j$ graph is $P_4$-free.

Furthermore, every edge in the graph $G \times H$ occurs exactly once in a unique graph $G_i \times H_j$. For example, consider an edge $e = (\ (u,a),(v,b)\ ) \in E(G \times H)$. Let $1 \leqslant i \leqslant k$ be the unique index such that $(u,v) \in E(G_i)$. Let $1 \leqslant j \leqslant \ell$ be the unique index such that $(a,b) \in E(H_j)$. Note that $e \in E(G_i \times H_j)$, and $e \notin E(G_{i'} \times H_{j'})$ for any other $i \neq i' \in [k]$ and $j \neq j' \in [\ell]$.

Therefore, $G_i \times H_j$, for $1 \leqslant i \leqslant k$, and $1 \leqslant j \leqslant \ell$, is a $P_4$-free partition of the graph $G \times H$. Consequently, we have $\mathsf{P_4\text{-}fp}(G \times H) \leqslant k\ell$. □

For any bipartite graph $G$, since $\mathsf{P_4\text{-}fc}(G) \leqslant \mathsf{P_4\text{-}fp}(G)$, the claim below follows.

**Corollary 4** (Sub-multiplicativity of the $P_4$-free Cover Number)**.** *Let $G$ and $H$ be two bipartite graphs, then the following holds for their graph product.*

$$\mathsf{P_4\text{-}fc}\left(G \times H\right) \leqslant \mathsf{P_4\text{-}fc}\left(G\right) \cdot \mathsf{P_4\text{-}fc}\left(H\right)$$

## I.2 Bound on $\mathsf{DISJ}_n$

We show an upper bound for $\mathsf{P_4\text{-}fp}(\mathsf{DISJ}_n)$ where we use the fact that $\mathsf{DISJ}_n$ is the tensor product $\mathsf{DISJ}_1^{\times n}$, and we show a lower bound for $\mathsf{sa}(\mathsf{DISJ}_n)$, thus exhibiting a gap between the two measures.

**Theorem 11.** *For any $n \in \mathbb{N}$, the following bounds hold on the disjointness graph $D_n$.*

$$\mathsf{P_4\text{-}fp}\left(\mathsf{DISJ}_n\right) = \mathsf{P_4\text{-}fp}\left(\mathsf{DISJ}_1^n\right) \leqslant 2^{\lceil n/2 \rceil}, \tag{1}$$

$$\mathsf{sa}\left(\mathsf{DISJ}_n\right) > \lceil (3/2)^n \rceil = \left\lceil 2.25^{n/2} \right\rceil. \tag{2}$$

*Proof.* For the first bound, we proceed by induction on $n$. For the base cases, observe that $\mathsf{P_4\text{-}fp}(\mathsf{DISJ}_1) = \mathsf{P_4\text{-}fp}(\mathsf{DISJ}_2) = 2$. Next, for any $2 < n \in \mathbb{N}$, we have

$$\begin{aligned}\mathsf{P_4\text{-}fp}\left(\mathsf{DISJ}_n\right) = \mathsf{P_4\text{-}fp}\left(\mathsf{DISJ}_{n-2} \times \mathsf{DISJ}_2\right) &\leqslant \mathsf{P_4\text{-}fp}\left(\mathsf{DISJ}_{n-2}\right) \cdot \mathsf{P_4\text{-}fp}\left(\mathsf{DISJ}_2\right), && \text{(using Claim 10)}\\ &\leqslant 2^{\lceil n-2/2 \rceil} \cdot 2, && \text{using the inductive hypothesis}\\ &= 2^{\lceil n/2 \rceil}.\end{aligned}$$

This observation completes the inductive proof.

For the second bound, note that a star forest over partite sets $L$ and $R$ has $< |L| + |R| = 2 \cdot 2^n$ edges in it. Note that $e(\mathsf{DISJ}_n) = 3^n$. Therefore, one needs $> \lceil (3/2)^n \rceil$ star forests to partition the edges of $\mathsf{DISJ}_n$. □

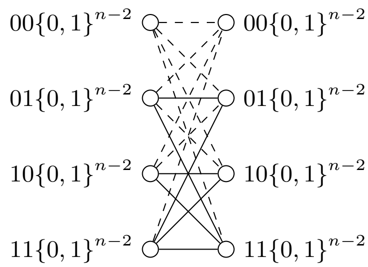



Figure 8: Partition of edges of $\mathsf{INT}_n$ into two sets.

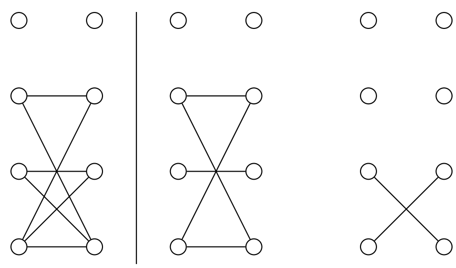


Figure 9: Partition of $G_1$ in Lemma 2 in two $P_4$-free graphs.

## I.3 Bound on $\mathsf{INT}_n$

We give an upper bound for $\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_n\right)$ in this section. Before we discuss our result, it is instructive to see that $\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_n\right) \leqslant \mathsf{P_4\text{-}fp}\left(\mathsf{INT}_{n-1}\right) + \mathsf{P_4\text{-}fp}\left(\mathsf{DISJ}_{n-1}\right)$, and by working out this recurrence relation we could have obtained a worse bound of $\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_n\right) \leqslant 3 \cdot 2^{n/2} - 3$.

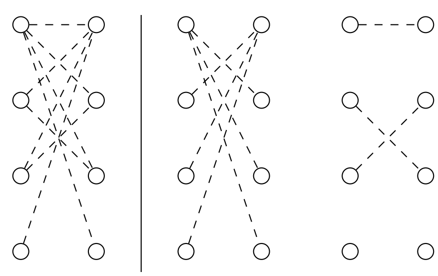


Figure 10: Partition of $H_1$ in Lemma 2 in two $P_4$-free graphs.

**Lemma 2.** *For all $n \in \mathbb{N}$ and $n \geqslant 3$,* $\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_n\right) \leqslant 2\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_{n-2}\right) + 2$

*Proof.* Consider the graph $\mathsf{INT}_n$. We partition the edges of $\mathsf{INT}_n$ into two sets. Consider an edge $(u, v)$ where $u, v \in \{0,1\}^n$. Let $u' \in \{0,1\}^2$ represent the two most significant bits in $u$, define $v'$ similarly. Let $b_{uv}$ be an indicator variable that takes value 1 when $u'$ and $v'$ intersect, and 0 otherwise.

If for the edge $(u, v)$, $b_{uv} = 1$, then we add the edge to the "bold" set. When $b_{uv} = 0$, we add the edge in the "dashed" set (refer to Figure 8). Let $G$ be the subgraph induced by the bold edges, and let $H$ be the subgraph induced by the dashed edges.

Next, we note that $G = K_{2^{n-2},2^{n-2}} \times G_1$ where $G_1$ is a graph with $P_4$-free partition number 2. See Figure 9 for an illustration. Similarly, $H = \mathsf{INT}_{n-2} \times H_1$ where $H_1$ has $P_4$-free partition number 2. See Figure 10 for an illustration. Combing the above observations, we get that

$$\begin{aligned}
\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_n\right) &\leqslant \mathsf{P_4\text{-}fp}\left(G\right) + \mathsf{P_4\text{-}fp}\left(H\right) \\
&\leqslant \mathsf{P_4\text{-}fp}\left(K_{2^{n-2},2^{n-2}} \times G_1\right) + \mathsf{P_4\text{-}fp}\left(\mathsf{INT}_{n-2} \times H_1\right) \\
&\leqslant \mathsf{P_4\text{-}fp}\left(K_{2^{n-2},2^{n-2}}\right) \cdot \mathsf{P_4\text{-}fp}\left(G_1\right) + \mathsf{P_4\text{-}fp}\left(\mathsf{INT}_{n-2}\right) \cdot \mathsf{P_4\text{-}fp}\left(H_1\right) && \text{(By Claim 10)} \\
&\leqslant 2 + 2\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_{n-2}\right)
\end{aligned}$$

□

The main theorem of this section is presented below.

**Theorem 12.** *For all even $n \in \mathbb{N}$,*

$$\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_n\right) \leqslant 2 \cdot 2^{n/2} - 2.$$

*For all odd $n \in \mathbb{N}$,*

$$\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_n\right) \leqslant 3 \cdot 2^{(n-1)/2} - 2.$$

*Proof.* The following holds for all even $n$.

$$\begin{aligned}
\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_n\right) &\leqslant 2\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_{n-2}\right) + 2 \\
&\leqslant 2^k \mathsf{P_4\text{-}fp}\left(\mathsf{INT}_{n-2k}\right) + 2 + 2^2 + \ldots + 2^k && \forall k \in [n-2, n/2-1] \\
&\leqslant 2^{n/2-1}\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_2\right) + \sum_{i=1}^{n/2-1} 2^i \\
&= 2^{n/2} + 2 \cdot (2^{n/2-1} - 1) && \because \mathsf{P_4\text{-}fp}\left(I_2\right) = 2 \\
&= 2 \cdot 2^{n/2} - 2
\end{aligned}$$

Similar to the analysis above, when $n$ is odd the result below follows

$$\mathsf{P_4\text{-}fp}\left(\mathsf{INT}_n\right) \leqslant 3 \cdot 2^{(n-1)/2} - 2\ .$$

This completes the proof. □

### I.4 $P_4$-free partition number of complement of Matching

Let $N(v)$ denote the neighbours of vertex $v$ in a graph. We use the kernalization technique used in [FMPS09] presented below.

**Definition 7.** *For any given graph $G : (V, E)$, let $K(G)$ be the graph such that when the following two rules are applied on $K(G)$, the graph does not change. The rules are as follows:*

1. *If the degree of any vertex is 0, then we remove the vertex.*
2. *If $\exists\ u, v \in V$, such that $N(u) = N(v)$, then we remove $u$ from the graph.*

[FMPS09] note that for any graph $G$ the biclique partition number of $G$ and $K(G)$ are equal. The next proposition gives a similar relationship for $P_4$-free partition number.

**Proposition 8.** *For any graph $G$,* $\mathsf{P_4\text{-}fp}\left(G\right) = \mathsf{P_4\text{-}fp}\left(K(G)\right).$

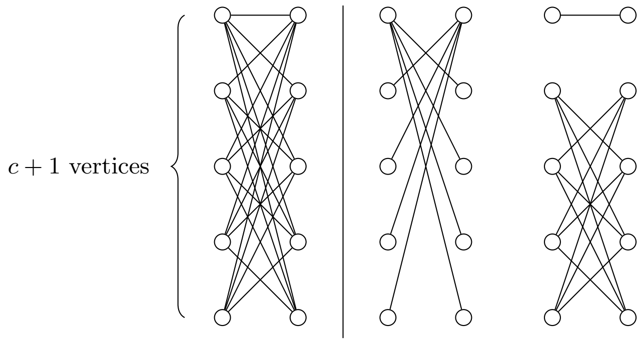



Figure 11: $G'$ and partition of edges of $G'$ in two sets, as in Claim 5, shown here for $c = 4$.

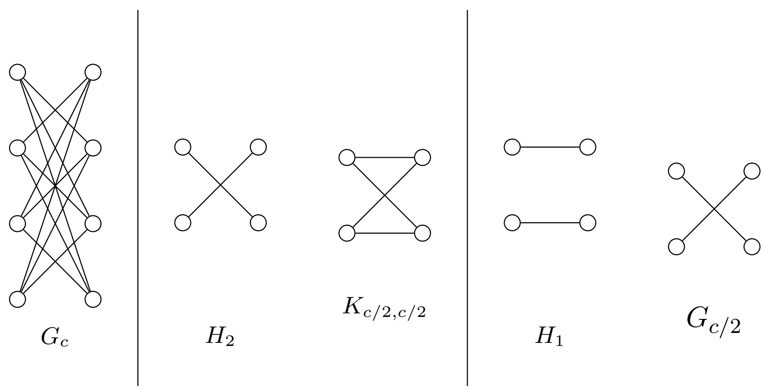



Figure 12: Representation of decomposition of $G_c$ in Claim 5, shown here for $c = 4$. Edges of $G_c$ are partitioned into the following two sets: $H_2 \times K_{c/2,c/2}$ and $H_1 \times G_{c/2}$.

In the sequel, we use this observation to show an upper bound on the $P_4$-free partition number of the complement of a $P_4$-free graph.

*Proof of Claim 5* . Consider the graph $G' = K(K_{N,N} \setminus G)$. When $G$ contains isolated vertices, observe that $G'$ is isomorphic to the first graph in Figure 11 i.e. $G'$ is isomorphic to a complete bipartite graph with $c+1$ vertices in each partite set and a matching of size $c$ removed. The edge set of $G'$ can be partitioned as follows: remove all the edges incident to the vertices with degree $c+1$ (note that there is only one vertex in each partite set of degree $c+1$) *except* the edge connecting them to each other. These removed edges form a $P_4$-free graph, call it $S$. We analyze the $P_4$-free partition number of the remaining graph separately.

Let $G_c$ denote the remaining graph. $G_c$ is a bipartite graph with $c$ vertices in each partite set and a perfect matching removed. Observe that $E(G_c)$ is the union of $H_1 \times G_{\lceil c/2 \rceil}$ and $H_2 \times K_{\lceil c/2 \rceil, \lfloor c/2 \rfloor}$ (as demonstrated in Figure 12). Therefore, we get the following

$$\begin{aligned} \mathsf{P_4\text{-}fp}\,(G_c) &\leqslant \mathsf{P_4\text{-}fp}\left(H_1 \times G_{\lceil c/2 \rceil}\right) + \mathsf{P_4\text{-}fp}\left(H_2 \times K_{\lceil c/2 \rceil, \lceil c/2 \rceil}\right) \\ &\leqslant \mathsf{P_4\text{-}fp}\left(G_{c/2}\right) + 1 \end{aligned}$$

Solving the recursion we get $\mathsf{P_4\text{-}fp}\,(G_c) \leqslant \lceil \log c \rceil$, therefore

$$\mathsf{P_4\text{-}fp}\,(G) \leqslant \mathsf{P_4\text{-}fp}\,(G_c) + \mathsf{P_4\text{-}fp}\,(S) \leqslant \lceil \log c \rceil + 1\ .$$

Furthermore, when $G$ is a perfect matching, $K_{N,N} \setminus G$ is isomorphic to $G_N$ (biclique with perfect matching removed), hence $\mathsf{P_4\text{-}fp}\,(K_{N,N} \setminus G) \leqslant \lceil \log N \rceil$. □

# J Lower Bounds

This section presents the proof of all our lower bounds.

## J.1 Lower Bound on $\mathsf{DISJ}_n$

In this section we prove a polynomial lower bound on the $P_4$-free partition/cover number of $\mathsf{DISJ}_n$.

**Lemma 3.** *For all $n \in \mathbb{N}$, the following bound holds.*

$$\mathsf{P_4\text{-}fp}\left(\mathsf{DISJ}_n\right) \geqslant \mathsf{P_4\text{-}fc}\left(\mathsf{DISJ}_n\right) \geqslant N^{\log_2 3 - 3/2} \approx N^{0.085}$$

We will use the following claim for the proof of Lemma 3.

**Claim 13.** *Any $P_4$-free subgraph of $\mathsf{DISJ}_n$ has at most $N\sqrt{N}$ edges.*

Assuming the above claim, we prove Lemma 3 as follows.

*Proof of Lemma 3 .* First, observe that there are $3^n$ edges in $\mathsf{DISJ}_n$. By Claim 13, any $P_4$-free subgraph of $\mathsf{DISJ}_n$ has at most $N\sqrt{N}$ edges. Therefore, we have

$$\mathsf{P_4\text{-}fp}\left(\mathsf{DISJ}_n\right) \geqslant \mathsf{P_4\text{-}fc}\left(\mathsf{DISJ}_n\right) \geqslant \frac{3^n}{N\sqrt{N}} = N^{\log_2 3 - 3/2} \approx N^{0.085}$$

as desired. □

### J.1.1 Proof of Claim 13

First, we state and prove all the claims that are needed for the proof of Claim 13.

**Claim 14.** *Any biclique subgraph of $\mathsf{DISJ}_n$ has at most $N$ edges.*

*Proof.* We use the set representation of $\mathsf{DISJ}_n$, that is, both partite sets are the set of all the subsets of $\{1, 2, \ldots, n\}$. Suppose a biclique $G = (L', R', E)$ is a subgraph of $\mathsf{DISJ}_n$. Let $\mathcal{L} = \cup_{S \in L'} S$ and $\mathcal{R} = \cup_{T \in R'} T$. Then it is clear that $\mathcal{L}$ is disjoint from $\mathcal{R}$. This implies that $|\mathcal{L}| + |\mathcal{R}| \leqslant n$. Observe that the number of vertices in the left partite set $L'$ is at most $2^{|\mathcal{L}|}$ and the number of vertices in the right partite set $R'$ is at most $2^{|\mathcal{R}|}$. Therefore, the number of edges in $G$ is at most $2^{|\mathcal{L}|} \cdot 2^{|\mathcal{R}|} \leqslant 2^n = N$, which completes the proof. □

**Claim 15.** *Let $\{(a_i, b_i)\}_{i \in \mathbb{N}}$ be a sequence of non-negative numbers. Then,*

$$\sum_{i \in \mathbb{N}} a_i b_i \leqslant \sqrt{\left(\max_{i \in \mathbb{N}} a_i b_i\right)\left(\sum_{i \in \mathbb{N}} a_i\right)\left(\sum_{i \in \mathbb{N}} b_i\right)}.$$

*Furthermore, equality holds if and only if (a) for all $i \in \mathbb{N}$, one has $a_i > 0$ iff $b_i > 0$. (b) all positive $a_i$s are constant, and (c) all positive $b_i$s are constant.*

*Proof.*

$$\sum_{i \in \mathbb{N}} a_i b_i \leqslant \max_{i \in \mathbb{N}} \sqrt{a_i b_i} \cdot \sum_{i \in \mathbb{N}} \sqrt{a_i b_i}$$

$$\leqslant \sqrt{\max_{i \in \mathbb{N}} a_i b_i} \cdot \left(\sum_{i \in \mathbb{N}} a_i\right)^{1/2} \left(\sum_{i \in \mathbb{N}} b_i\right)^{1/2}. \qquad \text{(Cauchy-Schwartz)}$$

□

Now, we are ready to prove Claim 13.

*Proof of Claim 13* . Suppose $G$ is a $P_4$-free subgraph of $\mathsf{DISJ}_n$. Let $K_{a_1,b_1}, K_{a_2,b_2}, \ldots, K_{a_m,b_m}$ be the (biclique) connected components of $G$, where $a_i \in \mathbb{N}, b_i \in \mathbb{N}$ for every $1 \leqslant i \leqslant m$ and $m \in \mathbb{N}$. The total number of edges in $G$ is $\sum_{i=1}^{m} a_i b_i$. We shall show that $\sum_{i=1}^{m} a_i \cdot b_i \leqslant N\sqrt{N}$. By Claim 14, it holds that $a_i \cdot b_i \leqslant N$ for every $1 \leqslant i \leqslant m$. Since all the left partite sets of $K_{a_1,b_1}, K_{a_2,b_2}, \ldots, K_{a_m,b_m}$ are disjoint, it holds that $\sum_{i=1}^{m} a_i \leqslant N$. Similarly, $\sum_{i=1}^{m} b_i \leqslant N$. Therefore, applying Claim 15, the following inequality holds.

$$\sum_{i=1}^{m} a_i b_i \leqslant \sqrt{\left(\max_i a_i b_i\right)\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{i=1}^{m} b_i\right)}$$
$$\leqslant \sqrt{N \cdot N \cdot N} = N^{3/2}$$

Thus, any $P_4$-free subgraph of $\mathsf{DISJ}_n$ has at most $N^{3/2}$ edges. □

### J.2 Bounds on $P_4$-free Cover Number of $\mathsf{INT}_n$

In this section, we prove a lower bound and a upper bound on the $P_4$-free cover number of $\mathsf{INT}_n$.

**Lemma 4.** *For all $n \in \mathbb{N}$, the following bounds hold.*

$$n - \frac{1}{2}\left(\lg \pi + \lg\left(\frac{n+1}{2} + \frac{1}{4} + \frac{1}{64(n+1)}\right)\right) \leqslant \mathsf{P_4\text{-}fc}\left(\mathsf{INT}_n\right) \leqslant n$$

First, we state all the claims needed for the proof of Lemma 4.

**Claim 16.** *For every $n \in \mathbb{N}$, the following bound holds.*

$$\lg \binom{n}{\lfloor n/2 \rfloor} \geqslant n - \frac{1}{2}\left(\lg \pi + \lg\left(\frac{n+1}{2} + \frac{1}{4} + \frac{1}{64(n+1)}\right)\right)$$

**Claim 17.** *Let $G$ be a bipartite graph. Then, for every induced subgraph $H$ of $G$, the following inequality holds.*

$$\mathsf{P_4\text{-}fc}\left(H\right) \leqslant \mathsf{P_4\text{-}fc}\left(G\right)$$

Assuming above claims, we prove Lemma 4 as follows.

*Proof of Lemma 4* . **Upper Bound.** Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. For each $1 \leqslant i \leqslant n$, construct a subgraph $G_i = (L_i, R_i, E_i)$ of $\mathsf{INT}_n$ that connect all sets that contain the element $i$ in $[n]$. More formally, $L_i = R_i = \{S \subseteq [n] \colon S \ni i\}$, and $E_i = \{(S,T) \colon S \in L_i, T \in R_i\}$. Note that $G_i$ is a biclique and it has $4^{n-1}$ edges. Note also that every edge in $\mathsf{INT}_n$ is covered by at least some one graph $G_i$, for some $i \in [n]$ that witnesses the intersection of the two sets. It implies that $G_1, G_2, \ldots, G_n$ is a $P_4$-free cover of $\mathsf{INT}_n$. Therefore, it holds that $\mathsf{P_4\text{-}fc}\left(\mathsf{INT}_n\right) \leqslant n = \lg N$.

**Lower Bound.** Consider the induced subgraph $G = (L', R', E')$ of $\mathsf{INT}_n$, where $L' = \{S \subseteq [n] \colon |S| = \lfloor \frac{n}{2} \rfloor\}$, $R' = \{T \subseteq [n] \colon |T| = \lceil \frac{n}{2} \rceil\}$. Observe that each vertex $S \in L'$ is connected to every $T \in R'$ except when $T = [n] \setminus S$. Thus, graph $G$ is the complement of a matching of size $M$, where $M = \binom{n}{\lfloor n/2 \rfloor}$. Using the algebraic lower-bounding technique of [LNP80] and Proposition 1, one concludes that

$$\mathsf{P_4\text{-}fc}\left(G\right) \geqslant \lceil \lg M \rceil \geqslant n - \frac{1}{2}\left(\lg \pi + \lg\left(\frac{n+1}{2} + \frac{1}{4} + \frac{1}{64(n+1)}\right)\right),$$

where the last inequality follows from Claim 16. Finally, by Claim 17, $\mathsf{P_4\text{-}fc}(G) \leqslant \mathsf{P_4\text{-}fc}(\mathsf{INT}_n)$. Therefore, we have

$$n - \frac{1}{2}\left(\lg \pi + \lg\left(\frac{n+1}{2} + \frac{1}{4} + \frac{1}{64(n+1)}\right)\right) \leqslant \mathsf{P_4\text{-}fc}(\mathsf{INT}_n),$$

as desired. □

### J.2.1 Proof of claims

*Proof of Claim 16.* Consider two cases as follows.

**Case 1:** $n$ is even. By the lower bound for central binomial coefficient Appendix J.2.2,

$$\lg\binom{n}{n/2} \geqslant \lg \frac{2^n}{\sqrt{\pi\left(\frac{n}{2}+\frac{1}{4}+\frac{1}{64n}\right)}} = n - \frac{1}{2}\left(\lg \pi + \lg\left(\frac{n}{2}+\frac{1}{4}+\frac{1}{64n}\right)\right)$$

**Case 2:** $n$ is odd. Note that $\binom{n}{(n-1)/2} = \frac{1}{2}\binom{n+1}{(n+1)/2}$.

$$\begin{aligned}\lg\binom{n}{(n-1)/2} = \lg\binom{n+1}{(n+1)/2} - 1 &\geqslant \lg \frac{2^{n+1}}{\sqrt{\pi\left(\frac{n+1}{2}+\frac{1}{4}+\frac{1}{64(n+1)}\right)}} - 1 \\ &= n - \frac{1}{2}\left(\lg \pi + \lg\left(\frac{n+1}{2}+\frac{1}{4}+\frac{1}{64(n+1)}\right)\right)\end{aligned}$$

In both cases, we have

$$\lg\binom{n}{\lfloor n/2 \rfloor} \geqslant n - \frac{1}{2}\left(\lg \pi + \lg\left(\frac{n+1}{2}+\frac{1}{4}+\frac{1}{64(n+1)}\right)\right),$$

since $\frac{n}{2}+\frac{1}{64n}$ is an increasing function in $n$. □

*Proof of Claim 17.* Observe that if a graph is $P_4$-free, then every induced subgraph of that graph is also $P_4$-free. It follows that $\mathsf{P_4\text{-}fc}(H) \leqslant \mathsf{P_4\text{-}fc}(G)$ as desired. □

### J.2.2 Tight Estimation of the Central Binomial Coefficient

In this section, we shall prove that

$$\frac{4^n}{\sqrt{\pi\left(n+\frac{1}{4}+\frac{1}{32n}\right)}} \leqslant \binom{2n}{n} \leqslant \frac{4^n}{\sqrt{\pi\left(n+\frac{1}{4}+\frac{1}{46n}\right)}}$$

holds for all $n \in \mathbb{N}$.

For brevity, let $a_k := \binom{2k}{k}$. The proof shall proceed in three high-level steps.

1. First, we need to find the limit $L := \lim_{n\to\infty}\binom{2n}{n}\cdot\sqrt{n}\cdot 4^{-n}$.

   **Claim 18.** $L = \frac{1}{\sqrt{\pi}}$.

2. Next, for the upper bound, consider the following sequence.

$$\left\{b_n := a_n \cdot \frac{\sqrt{f(n)}}{4^n}\right\}_{n\in\mathbb{N}}.$$

Suppose this sequence has the property that $\lim_{n\to\infty} f(n)/n = 1$. Then, $\lim_{n\to\infty} b_n = L$ as well.

Suppose this sequence has the additional property that it is a (weakly) increasing sequence. Then, $b_n$ must tend to $L$ from below. Consequently, we shall have the result that

$$a_n \cdot \frac{\sqrt{f(n)}}{4^n} \leqslant L = \frac{1}{\sqrt{\pi}} \iff a_n \leqslant \frac{4^n}{\sqrt{\pi f(n)}}.$$

Therefore, all that remains is to choose $f(n)$ such that $b_n$ is (weakly) increasing.

**Claim 19.** *If $f\colon \mathbb{R}\to\mathbb{R}$ be defined by $f(x) = x + \frac{1}{4} + \frac{1}{46x}$, then $\{b_n\}_{n\in\mathbb{N}}$ is weakly increasing.*

The proof proceeds by showing that, for all $k \in \mathbb{N}$, we have

$$b_{k+1} \geqslant b_k \iff a_{k+1} \cdot \frac{\sqrt{f(k+1)}}{4^{k+1}} \geqslant a_k \cdot \frac{\sqrt{f(k)}}{4^k} \iff \left(\frac{a_{k+1}}{4\cdot a_k}\right)^2 \geqslant \frac{f(k)}{f(k+1)}.$$

3. Similarly, for the lower bound, it suffices to find $g\colon \mathbb{R}\to\mathbb{R}$ such that

   (a) $\left\{c_n := a_n \cdot \frac{\sqrt{g(n)}}{4^n}\right\}_{n\in\mathbb{N}}$ is (weakly) decreasing, and

   (b) $\lim_{n\to\infty} g(n)/n = 1$.

   **Claim 20.** *If $g\colon \mathbb{R}\to\mathbb{R}$ be defined by $g(x) = x + \frac{1}{4} + \frac{1}{32x}$, then $\{c_n\}_{n\in\mathbb{N}}$ is weakly decreasing.*

### J.2.3 Proof of Claim 18

$$\begin{aligned}
\binom{2n}{n}\cdot 4^{-n} &= \frac{(2n)!}{(n!)^2}\cdot\frac{1}{4^n}\\
&= \frac{n-1/2}{n}\cdot\frac{n-3/2}{n-1}\cdots\frac{1-1/2}{1}\\
&= \prod_{i=1}^{n}\left(1-\frac{1/2}{i}\right).\\
\binom{2n}{n}\cdot 4^{-n}\cdot(n+1/2)\cdot 2 &= \frac{n+1/2}{n}\cdot\frac{n-1/2}{n-1}\cdots\frac{3/2}{1}\\
&= \prod_{i=1}^{n}\left(1+\frac{1/2}{i}\right).\\
\implies \binom{2n}{n}\cdot 4^{-n}\sqrt{2n+1} &= \sqrt{\prod_{i=1}^{n}\left(1-\frac{(1/2)^2}{i^2}\right)}.
\end{aligned}$$

Recall the following identity

$$\frac{\sin(\pi x)}{\pi x} = \prod_{i\in\mathbb{Z}^*}\left(1-\frac{x}{i}\right) = \prod_{i\in\mathbb{N}}\left(1-\frac{x^2}{i^2}\right).$$

Therefore,

$$\lim_{n\to\infty}\binom{2n}{n}\cdot 4^{-n}\sqrt{2n+1} = \sqrt{\frac{\sin(\pi/2)}{\pi/2}} = \sqrt{\frac{2}{\pi}}.$$

Consequently, $L = 1/\sqrt{\pi}$.

### J.2.4 Proof of Claim 19

We need to prove, for all $k \in \mathbb{N}$,

$$\begin{aligned}
& \left(\frac{a_{k+1}}{4a_k}\right)^2 \geqslant \frac{k+1/4+1/46k}{(k+1)+1/4+1/46(k+1)} \\
\iff\quad & \left(\frac{k+1/2}{k+1}\right)^2 = \frac{k^2+k+1/4}{k^2+2k+1} \geqslant \frac{k+1/4+1/46k}{k+5/4+1/46(k+1)} \\
\iff\quad & k^3+(9/4)k^2+(35/23)k+5/16+1/184(k+1) \geqslant k^3+(9/4)k^2+(35/23)k+(27/92)+1/46k \\
\iff\quad & 115+2/(k+1) \geqslant 108+8/k \\
\iff\quad & 7 \geqslant 8/k-2/(k+1),
\end{aligned}$$

which is true for all $k \geqslant 1$ (because the RHS above is a decreasing function).

### J.2.5 Proof of Claim 20

We need to prove, for all $k \in \mathbb{N}$,

$$\begin{aligned}
& \left(\frac{a_{k+1}}{4a_k}\right)^2 = \frac{k^2+k+1/4}{k^2+2k+1} \leqslant \frac{k+1/4+1/32k}{k+5/4+1/32(k+1)} \\
\iff\quad & k^3+(9/4)k^2+(49/32)k+(5/16)+1/128(k+1) \leqslant k^3+(9/4)k^2+(49/32)k+(5/16)+(1/32k) \\
\iff\quad & k \leqslant 4(k+1),
\end{aligned}$$

which is true for any positive $k$.

## K Connection to Graph Embedding

### K.1 $P_4$-free Cover

**Claim 21.** *If a bipartite graph $G = (L, R, E)$ has a size-$d$ $P_4$-free covering, then the complement bipartite graph $\overline{G} = (L, R, L \times R \setminus E)$ is an induced subgraph of $K_2 \times K_{\mathbb{N}}^d$.*

*Proof.* Let $G_1, \ldots, G_d$ be a size-$d$ $P_4$-free cover of $G$. Define a vertex mapping $\varphi\colon L \cup R \to K_2 \times K_{\mathbb{N}}^d$ as follows. Let $\varphi(u)_i$ denote the $i$-th coordinate of the mapping $\varphi(u)$. Define $\varphi(u)_0 = 0$, for all $u \in L$, and $\varphi(v)_0 = 1$, for all $v \in R$. For $i \in \{1, \ldots, d\}$, define $\varphi(u)_i = \varphi(v)_i = k$, for every edge $(u, v)$ in the $k$-th connected component of $G_i$. All remaining entries of $\varphi$ are filled with unique values. One can verify that $(u, v) \in L \times R \setminus E$ if and only if $\varphi(u)$ and $\varphi(v)$ differ in every coordinate, that is, $\varphi(u)_i \neq \varphi(v)_i$ for every $i \in \{0, 1, \ldots, d\}$. Therefore, the complement bipartite graph $\overline{G}$ is an induced subgraph of $K_2 \times K_{\mathbb{N}}^d$.

We emphasize that the vertex mapping $\varphi$ has the additional property that $\varphi(u)$ and $\varphi(v)$ have $t$ identical coordinates if and only if the edge $(u, v)$ is covered in $t$ $P_4$-free graphs among $G_1, \ldots, G_d$. This property shall be useful in the proof of Claim 23. □

**Claim 22.** *If a loopless undirected graph $H = (L \cup R, E)$ is an induced subgraph of $K_{\mathbb{N}}^d$ and $E \subseteq L \times R$, then the bipartite graph $H' = (L, R, L \times R \setminus E)$ has a size-$d$ $P_4$-free covering.*

*Proof.* Suppose a loopless undirected graph $H = (L \cup R, E)$ is an induced subgraph of $K_{\mathbb{N}}^d$ and $E \subseteq L \times R$. Then, there exists a vertex mapping $\varphi \colon L \cup R \to \mathbb{N}^d$ such that $(u, v) \in E$ if and only if there exists $i \in \{1, 2, \ldots, d\}$ such that $\varphi(u)_i = \varphi(v)_i$. Define a new vertex mapping $\varphi^+ \colon L \cup R \to \{1, 2\} \times \mathbb{N}^d$ as follows.

$$\varphi^+(u) = \begin{cases} (1, \varphi(u)), & \text{if } u \in L \\ (2, \varphi(u)), & \text{otherwise.} \end{cases}$$

For $i \in \{1, 2, \ldots, d\}$, define $G_i = (L, R, E_i)$ such that $E_i$ is the set of all $u \in L$ and $v \in R$ such that $\varphi^+(u)_i = \varphi^+(v)_i$. Observe that the set of vertices $u \in L$ such that $\varphi^+(u)_i = k$ and the set of vertices $v \in R$ such that $\varphi^+(u)_i = k$ for some $k \in \mathbb{N}$ form a biclique, and each $E_i$ is a disjoint union of bicliques. Furthermore, an edge $(u, v) \in E$ if and only if there exists an $i \in \{1, 2, \ldots, d\}$ such that $\varphi(u)_i = \varphi(v)_i$ which is equivalent to $\varphi^+(u)_i = \varphi^+(v)_i$. This implies that $E_i$ cover the edge $(u, v)$. Therefore, $E_1, E_2, \ldots, E_d$ is a $P_4$-free cover of $H$.

The $G_1, \ldots, G_d$ have the property that if an edges $(u, v)$ is covered $t$ times by these $P_4$-free graphs, then $\varphi^+(u)$ intersects $\varphi^+(v)$ in exactly $t$ coordinates. This property of the vertex mapping shall be useful in the proof of Claim 24. □

The following result is a consequence of Claim 21 and Claim 22.

**Corollary 5.** *Let $G = (L, R, E)$ be a bipartite graph and $H = (L \cup R, E)$ be a loopless undirected graph. Then, the following identity holds.*

$$\mathsf{pdim}\,(H) \in \{\mathsf{P_4\text{-}fc}\,(G)\,, \mathsf{P_4\text{-}fc}\,(G) + 1\}\,,$$

*or equivalently*

$$\mathsf{P_4\text{-}fc}\,(G) \in \{\mathsf{pdim}\,(H) - 1, \mathsf{pdim}\,(H)\}\,.$$

The additive slack of 1 in Corollary 5 is necessary. Figure 13 gives an example.

## K.2 $P_4$-free Partition

Suppose a graph $H$ is an induced subgraph of $K_{\mathbb{N}}^d$ via a vertex mapping $\varphi \colon V(H) \to \mathbb{N}^d$. The vertex mapping $\varphi$ is a *partition* if the following conditions are satisfied.

1. If $(u, v) \in E(H)$, then $\varphi(u)_i \neq \varphi(v)_i$, for all $i \in \{1, 2, \ldots, d\}$.
2. If $(u, v) \notin E(H)$, then there exists a *unique* $i \in \{1, 2, \ldots, d\}$ such that $\varphi(u)_i = \varphi(v)_i$.

We emphasize that in an unrestricted vertex mapping, instead of (2) above, we insist that there exists an $i \in \{1, 2, \ldots, d\}$ (not necessarily a *unique* $i$). Let $\mathsf{pdim}^*\,(H)$ represent the minimum $d \in \mathbb{N}$ such that $H$ is an induced subgraph of $K_{\mathbb{N}}^d$ via a partition vertex mapping.

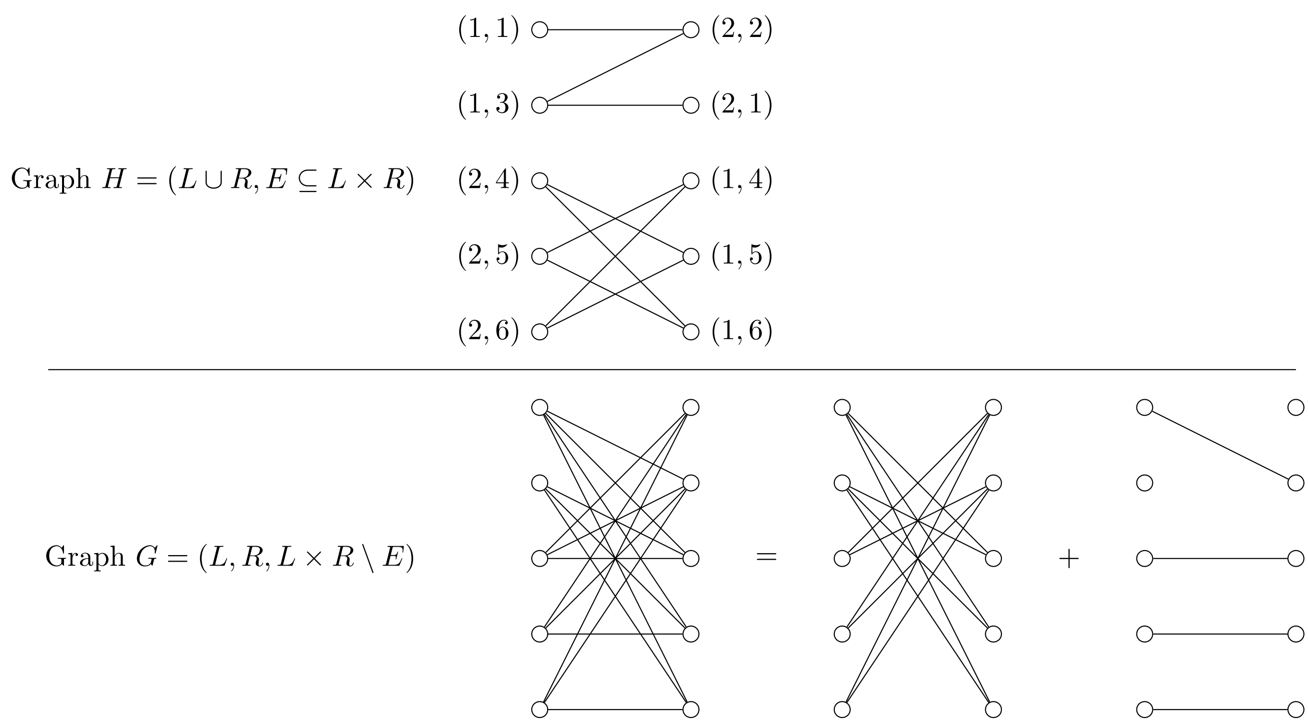



Figure 13: Example for the tightness of Corollary 5. Note that the loopless undirected graph $H = (L \cup R, E) = P_4 + C_6$, where $E \subseteq L \times R$, is an induced subgraph of $K_2 \times K_{\mathbb{N}}$. The (partition) vertex mapping of each vertex is explicitly mentioned next to it. However, the bipartite graph $G = (L, R, L \times R \setminus E)$ is not $P_4$-free and, hence, $\mathsf{P_4\text{-}fc}\,(G) \geqslant 2$; in fact, we have $\mathsf{P_4\text{-}fc}\,(G) = \mathsf{P_4\text{-}fp}\,(G) = 2$. The edges of $G$ partition into $K_{2,3} + K_{3,2}$ and $4K_{1,1}$.

**Claim 23.** *If a bipartite graph $G = (L, R, E)$ has a size-$d$ $P_4$-free partitioning, then the complement bipartite graph $\overline{G} = (L, R, L \times R \setminus E)$ is an induced subgraph of $K_2 \times K_{\mathbb{N}}^d$ via a partition vertex mapping.*

**Claim 24.** *If a loopless undirected graph $H = (L \cup R, E)$ is an induced subgraph of $K_{\mathbb{N}}^d$ via a partition vertex mapping and $E \subseteq L \times R$, then the bipartite graph $H' = (L, R, L \times R \setminus E)$ has a size-$d$ $P_4$-free partitioning.*

The proofs of Claim 23 and Claim 24 are identical to the proofs of Claim 21 and Claim 22, respectively, utilizing the fact that the vertex mapping is a partition. As a consequence of Claim 23 and Claim 24, we have the following result.

**Corollary 6.** *Let $G = (L, R, E)$ be a bipartite graph and $H = (L \cup R, E)$ be a loopless undirected graph. Then, the following identity holds.*

$$\mathsf{pdim}^*\,(H) \in \{\mathsf{P_4\text{-}fp}\,(G)\,, \mathsf{P_4\text{-}fp}\,(G) + 1\}\,,$$

*or equivalently*

$$\mathsf{P_4\text{-}fp}\,(G) \in \{\mathsf{pdim}^*\,(H) - 1, \mathsf{pdim}^*\,(H)\}\,.$$